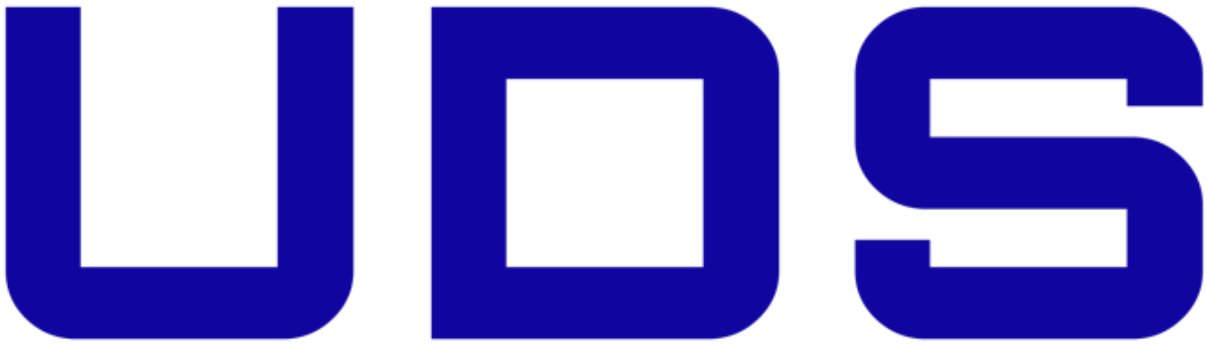


LIBRO

REDES DE COMPUTADORAS II

Ingeniería en sistemas computacionales

6to CUATRIMESTRE

Marco Estratégico de Referencia

ANTECEDENTES HISTORICOS

Nuestra Universidad tiene sus antecedentes de formación en el año de 1979 con el inicio de actividades de la normal de educadoras "Edgar Robledo Santiago", que en su momento marcó un nuevo rumbo para la educación de Comitán y del estado de Chiapas. Nuestra escuela fue fundada por el Profesor de Primaria Manuel Albores Salazar con la idea de traer Educación a Comitán, ya que esto representaba una forma de apoyar a muchas familias de la región para que siguieran estudiando.

En el año 1984 inicia actividades el CBTiS Moctezuma Ilhuicamina, que fue el primer bachillerato tecnológico particular del estado de Chiapas, manteniendo con esto la visión en grande de traer Educación a nuestro municipio, esta institución fue creada para que la gente que trabajaba por la mañana tuviera la opción de estudiar por las tarde.

La Maestra Martha Ruth Alcázar Mellanes es la madre de los tres integrantes de la familia Albores Alcázar que se fueron integrando poco a poco a la escuela formada por su padre, el Profesor Manuel Albores Salazar; Víctor Manuel Albores Alcázar en septiembre de 1996 como chofer de transporte escolar, Karla Fabiola Albores Alcázar se integró como Profesora en 1998, Martha Patricia Albores Alcázar en el departamento de finanzas en 1999.

En el año 2002, Víctor Manuel Albores Alcázar formó el Grupo Educativo Albores Alcázar S.C. para darle un nuevo rumbo y sentido empresarial al negocio familiar y en el año 2004 funda la Universidad Del Sureste.

La formación de nuestra Universidad se da principalmente porque en Comitán y en toda la región no existía una verdadera oferta Educativa, por lo que se veía urgente la creación de una institución de Educación superior, pero que estuviera a la altura de las exigencias de los jóvenes que tenían intención de seguir estudiando o de los profesionistas para seguir preparándose a través de estudios de posgrado.

Nuestra Universidad inició sus actividades el 18 de agosto del 2004 en las instalaciones de la 4ª avenida oriente sur no. 24, con la licenciatura en Puericultura, contando con dos grupos de cuarenta alumnos cada uno. En el año 2005 nos trasladamos a nuestras propias instalaciones en la carretera Comitán – Tzimol km. 57 donde actualmente se encuentra el campus Comitán y el Corporativo UDS, este último, es el encargado de estandarizar y controlar todos los procesos operativos y Educativos de los diferentes Campus, Sedes y Centros de Enlace Educativo, así como de crear los diferentes planes estratégicos de expansión de la marca a nivel nacional e internacional.

Nuestra Universidad inició sus actividades el 18 de agosto del 2004 en las instalaciones de la 4ª avenida oriente sur no. 24, con la licenciatura en Puericultura, contando con dos grupos de cuarenta alumnos cada uno. En el año 2005 nos trasladamos a nuestras propias instalaciones en la carretera Comitán – Tzimol km. 57 donde actualmente se encuentra el campus Comitán y el corporativo UDS, este último, es el encargado de estandarizar y controlar todos los procesos operativos y educativos de los diferentes campus, así como de crear los diferentes planes estratégicos de expansión de la marca.

MISIÓN

Satisfacer la necesidad de Educación que promueva el espíritu emprendedor, aplicando altos estándares de calidad Académica, que propicien el desarrollo de nuestros alumnos, Profesores, colaboradores y la sociedad, a través de la incorporación de tecnologías en el proceso de enseñanza-aprendizaje.

VISIÓN

Ser la mejor oferta académica en cada región de influencia, y a través de nuestra Plataforma Virtual tener una cobertura Global, con un crecimiento sostenible y las ofertas académicas innovadoras con pertinencia para la sociedad.

VALORES

- Disciplina
- Honestidad
- Equidad

- Libertad

ESCUDO

El escudo de la UDS, está constituido por tres líneas curvas que nacen de izquierda a derecha formando los escalones al éxito. En la parte superior está situado un cuadro motivo de la abstracción de la forma de un libro abierto.

ESLOGAN

"Mi Universidad"

ALBORES

Es nuestra mascota, un Jaguar. Su piel es negra y se distingue por ser líder, trabaja en equipo y obtiene lo que desea. El ímpetu, extremo valor y fortaleza son los rasgos que distinguen.

Redes de computadoras II

Objetivo de la materia: Al terminar el curso el estudiante deberá tener los conocimientos básicos acerca de la conmutación, así como la habilidad para administrar switches, teniendo como base de apoyo el programa packet tracer donde la finalidad es trabajar en un simulador de redes.

UNIDAD I MÁSCARA DE SUBRED DE LONGITUD VARIABLE

1.1. Packet Tracer
1.2. Instalación y configuración para practicas packet tracer
1.3. Uso de VLSM.
1.4. Operaciones con VLSM.
1.5. Resumen de rutas
1.6. Configuración de VLSM.
1.7. Ejercicios con VLSM.
1.8. Algoritmos de enrutamiento dinámico.
1.9. RIP
1.10. OSPF.
1.11. IGRP
1.12. Configuración de enrutamiento dinámico

UNIDAD II CONMUTACIÓN

2.1. Introducción.
2.2. Ethernet
2.3. Conmutación en redes LAN
2.4. Uso de los puentes
2.5. Puentes de aprendizaje
2.6. Puentes con árbol de expansión
2.7. Repetidores
2.8. Puertas de enlace
2.9. Concepto de hub
2.10. Concepto de router
2.11. Conceptos de switches.

UNIDAD III: CAPA DE RED

3.1. Conmutación de paquetes de almacenamiento y reenvío
3.2. Servicios proporcionados a la capa de transporte
3.3. Implementación del servicio sin conexión
3.4. Implementación del servicio orientado a conexión
3.5. Comparación entre las redes de circuitos virtuales y las redes de datagrama
3.6. Principio de optimización
3.7. Algoritmo de la ruta más corta
3.8. Enrutamiento por difusión
3.9. Enrutamiento multidifusión
3.10. Elementos de un switch
3.11. Proceso de arranque del switch.
3.12. Conceptos
3.13. Ingreso a la consola del switch.
3.14. Administración de la tabla de direcciones MAC.
3.15. Configuración de direcciones MAC

UNIDAD IV: VLANS

4.1. Introducción a las vlans.
4.2. Configuración de las vlan
4.3. Vlan en packet tracer
4.4. Vtp
4.5. Modos vtp
4.6. Utilizar vtp en una red
4.7. Algoritmos de control de congestión
4.8. Configuración vtp
4.9. Configuración servidor vtp
4.10. Configuración clientes vtp
4.11. Configuración vlan en vtp

ÍNDICE

UNIDAD I MÁSCARA DE SUBRED DE LONGITUD VARIABLE

Las máscaras de subred de tamaño variable o VLSM (del inglés *Variable Length Subnet Mask*) representan otra de las tantas soluciones que se implementaron para evitar el agotamiento de direcciones IP en IPv4 (1987), como la división en subredes (1985), el enrutamiento sin clases CIDR (1993), NAT y las direcciones IP privadas.

Otra de las funciones de VLSM es descentralizar las redes y de esta forma conseguir redes más seguras y jerárquicas.

Si se utiliza una máscara de subred de tamaño fijo (la misma máscara de subred en todas las subredes), todas las subredes van a tener el mismo tamaño. Por ejemplo, si la subred más grande necesita 200 hosts, todas las subredes van a tener el mismo tamaño de 256 direcciones IP (nota: se ha redondeado hacia arriba, hacia la siguiente potencia, de 2). Si una subred que necesita 10 equipos, se asigna la misma subred de 256 direcciones, aunque las restantes 246 direcciones no se utilicen. Incluso los enlaces seriales (WAN), que solo necesitan dos direcciones IP, requieren una subred de 256 direcciones. (nota: en realidad serian 254 direcciones asignables a los hosts, ya que hay que descontar la dirección de la subred (todo cero en la parte de la identificación del host) y la dirección de broadcast (todo unos en la parte de la identificación del host)).

Planificación de subredes de tamaño variable

Una subred es un conjunto de direcciones IP y con ella se pueden hacer dos cosas: asignar direcciones IP a los equipos o dividirlo nuevamente en subredes más pequeñas. En cada división, las subredes primera y última no se usan (actualmente, la mayoría del hardware ya soporta el poder trabajar con ambas, primera y última, aunque se deberá de comprobar antes de hacer uso de éstas). Este tipo tiene una aplicación parecida al direccionamiento IP donde la primera identificaba la red y la última es de broadcast - en este caso, la primera identificaba la subred y la última se aplicaba al broadcast

de subred. Cabe aclarar que no se usan para asignar direcciones IP a los equipos, pero sí se pueden usar para dividirlas en subredes más pequeñas.

El concepto básico de VLSM es muy simple: se toma una red y se divide en subredes fijas, luego se toma una de esas subredes y se vuelve a dividir, tomando bits "prestados" de la porción de hosts, ajustándose a la cantidad de hosts requeridos por cada segmento de nuestra red.

Por ejemplo, si se toma la dirección de red 192.168.1.0/24 y se subdivide usando una máscara

/26 tendremos 4 subredes (192.168.1.0/26, 192.168.1.64/26, 192.168.1.128/26 y 192.168.1.192/26). Suponga que se construye un enlace serie entre dos routers y tomamos para ello una de las subredes (la 192.168.1.0/26): con esta máscara de subred sin aplicar vlsm se desperdiciarían 60 direcciones utilizables (2^6=64 menos las 2 direcciones aplicadas a las interfaces de los routers dan

62 hosts, [64-2=62] una dirección para el nombre de la red o dirección de red y la otra para la dirección de difusión o broadcast).

Ahora, si se aplica vlsm a la subred anterior (la 192.168.1.0/26) y se toman "prestados" 4 bits de la porción de host tendríamos otras 16 subredes /30 (192.168.1.0/30, 192.168.1.4/30, 192.168.1.8/30, 192.168.1.12/30, 192.168.1.16/30 y así sucesivamente hasta la 192.168.1.60/30) cada una con un total de 4 direcciones totales pero solamente dos direcciones utilizables y no se genera desperdicio. Finalmente podemos tomar cualquiera de ellas, por ejemplo, la 192.168.1.4/30 y aplicar las direcciones 192.168.1.5/30 y 192.168.1.6/30 a las interfaces de los routers.

Protocolos de enrutamiento

Los protocolos de enrutamiento que soportan VLSM deben mantener y enviar, cuando difundan la información de su tabla de enrutamiento a través de la red, la máscara de subred asociada a cada una de las direcciones IP de cada entrada o ruta de encaminamiento.

Ejemplos de protocolos de encaminamiento que admiten VLSM son RIP versión 2, OSPF, las versiones más recientes de BGP, y EIGRP.

Alternativas

Una alternativa para ahorrar las escasas direcciones públicas, es utilizar direcciones privadas (RFC 1918), en combinación con traducción NAT, especialmente en las direcciones que no necesitan ser alcanzados desde fuera de la red interna. También es posible, en algunos casos, que un enlace serial se "preste" la dirección IP de otro enlace conectado al mismo router; sin embargo, esto implica la desventaja de que ya no se puede acceder directamente a ese enlace, por ejemplo, mediante un ping.

La alternativas de VLSM son más propias para el tipo de enrutamiento, en cuestiones de IPv6 es sumamente importante tener en cuenta las solicitudes dadas por el servidor para así poder crear el pool de direcciones dadas por el router inalámbrico.

1.1. Packet tracer

En este punto los alumnos deben realizar prácticas directamente con redes es importante saber que los alumnos puedan realizar las practicas, al no contar con switches o el cableado necesario cableado o conexiones entre varios equipos sin alterar los equipos de cómputo. Para eso se necesita la virtualización, es decir, un simulador en el que se pueda utilizar todas las herramientas de estas prácticas, existe un software el cual se puede utilizar para poder realizar estas actividades.

Cisco ofrece una herramienta con la que es posible diseñar redes y realizar simulaciones sobre su uso. Esta aplicación gratuita se llama Packet Tracer y puede descargarse desde la web oficial de Cisco.

Con esta herramienta, estudiantes, docentes y profesionales pueden testear el funcionamiento de redes, ciberseguridad y el internet de las cosas (IoT).

Packet Tracer dispone de una interfaz intuitiva que facilita su utilización a la hora de añadir los distintos elementos que componen la red, pudiendo conectarse unos con otros y realizar las configuraciones necesarias de red en apenas unos clics.

Para poder descargarlo solo hay que acceder a la página oficial, descargarlo e instalarlo.

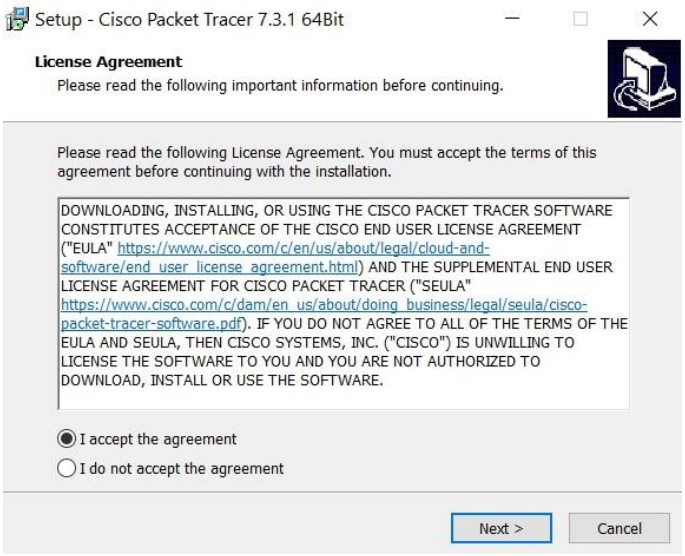
1.2. Instalación y configuración de packet tracer

Una vez iniciamos sesión en id.cisco.comA mitad de página aproximadamente podrás encontrar la link para descarga; Windows Desktop Version Clic en la versión que requieras para tu equipo y guardar el archivo.

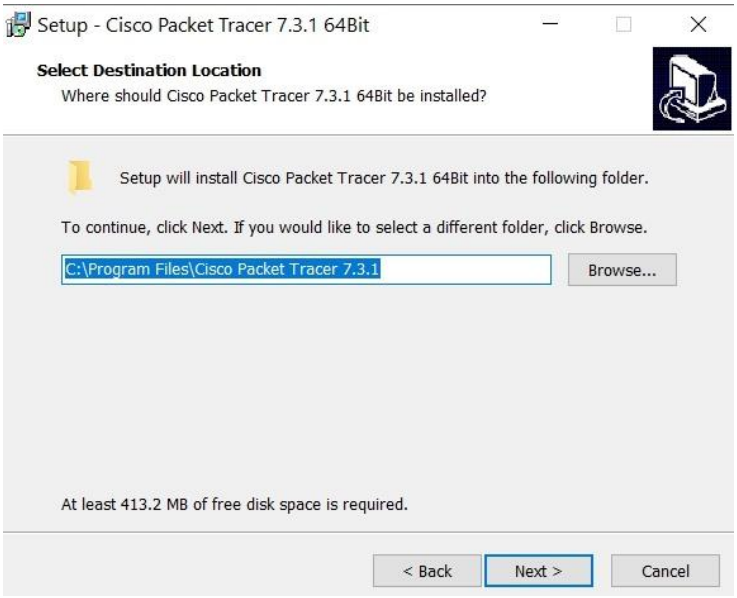
Instalar Cisco Packet Tracer

Doble clic al instalador.

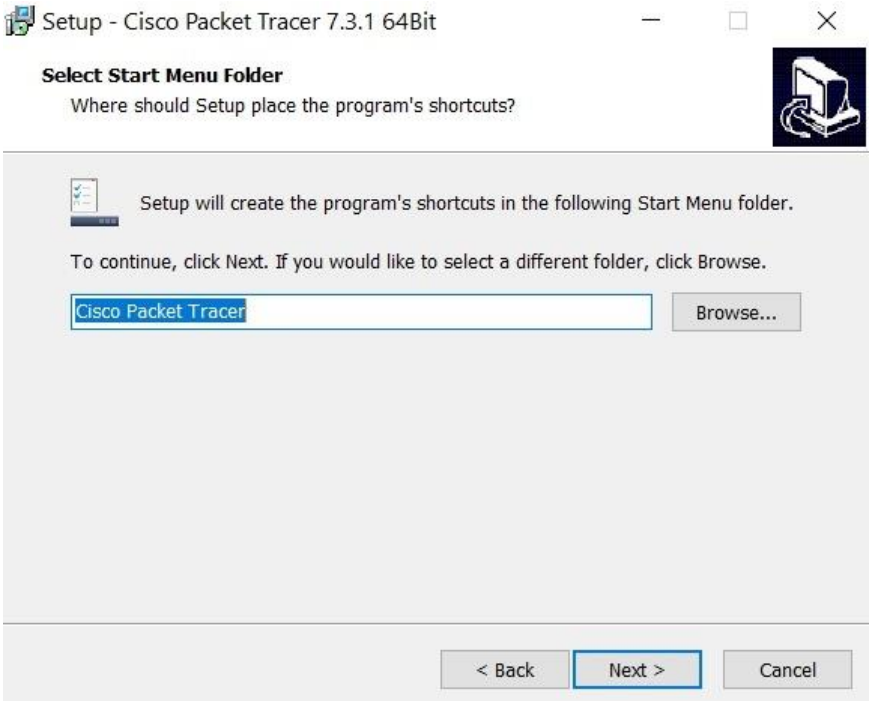
Aceptamos el contrato de licencia y clic a **Next**.



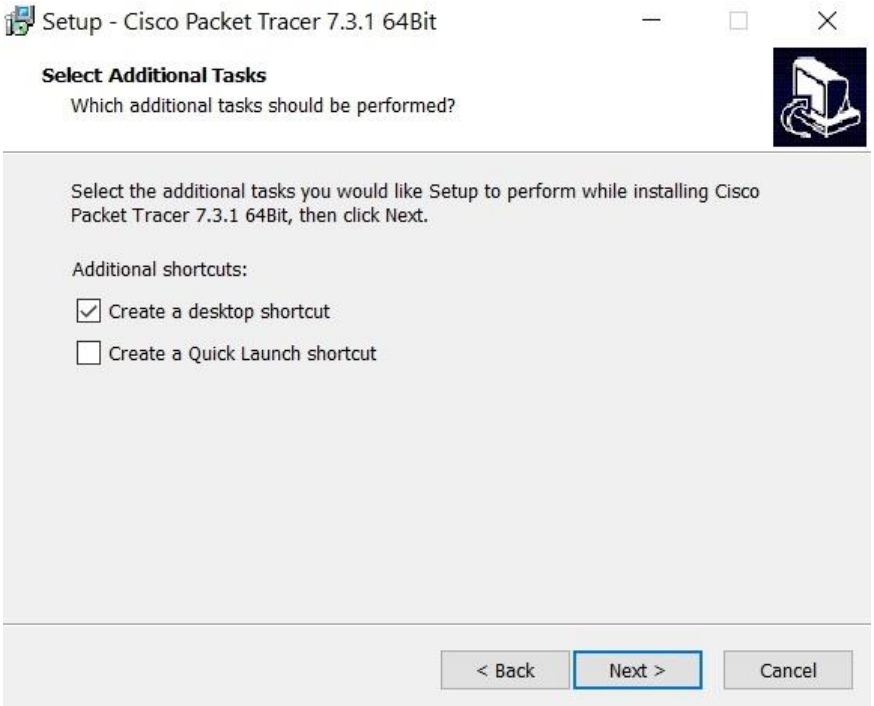
Indicamos carpeta de instalación o aceptamos la sugerida y clic a **Next**.



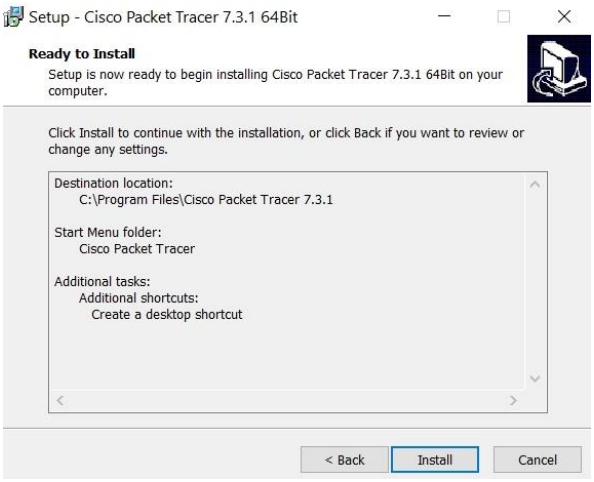
Aceptamos nombre de carpeta de menú sugerida o modificamos y clic en **Next**.



Revisamos opciones de accesos directos y clic en **Next**.



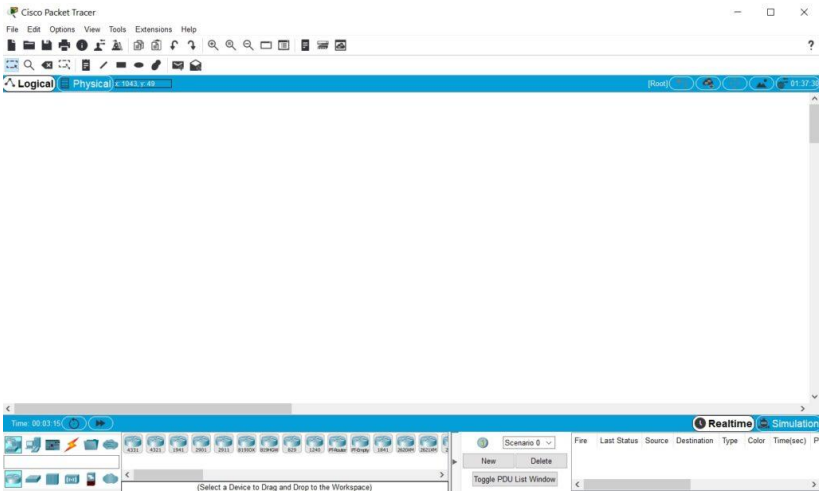
Todo listo! Clic en **Install**.



Si todo va bien un ratito después veremos la pantalla de finalización, clic en **Finish**.

En esta instancia se abre la aplicación. Es probable que nos pida nuevamente las credenciales de nuestra cuenta de Cisco Networking Academy.

Y listo, nuestra herramienta de simulación lista para utilizarse.



1.3. Uso de VLSM.

A medida que las subredes IP han crecido, los administradores han buscado formas de utilizar su espacio de direccionamiento con más eficiencia. En esta sección se presenta una técnica que se denomina VLSM.

Con VLSM, un administrador de red puede usar una máscara larga en las redes con pocos hosts, y una máscara corta en las subredes con muchos hosts.

Para poder implementar VLSM, un administrador de red debe usar un protocolo de enrutamiento que brinde soporte para él. Los routers Cisco admiten VLSM con los protocolos de enrutamiento OSPF, IS- IS integrado,EIGRP, RIP v2 y enrutamiento estático.

VLSM permite que una organización utilice más de una máscara de subred dentro del mismo espacio de direccionamiento de red. La implementación de VLSM maximiza la eficiencia del direccionamiento y con frecuencia se la conoce como división de subredes en subredes.

Los protocolos de enrutamiento con clase necesitan que una sola red utilice la misma máscara de subred. Por ejemplo, una red con la dirección de 192.168.187.0 puede usar sólo una máscara de subred, por ejemplo 255.255.255.0.

Un protocolo de enrutamiento que admite VLSM le confiere al administrador de red la libertad para usar distintas máscaras de subred para redes que se encuentran dentro de un sistema autónomo. La Figura muestra un ejemplo de cómo un administrador de red puede usar una máscara de 30 bits para las conexiones de red, una máscara de 24 bits para las redes de usuario e incluso una máscara de 22 bits para las redes con hasta 1000 usuarios.

Un desperdicio de espacio

En el pasado, se suponía que la primera y la última subred no debían utilizarse. El uso de la primera subred, conocida como la subred cero, no se recomendaba debido a la confusión que podría producirse si una red y una subred tuvieran la misma dirección. Este concepto también se aplicaba al uso de la última subred, conocida como la subred de unos. Con la evolución de las tecnologías de red y el agotamiento de las direcciones IP, el uso de la primera y la última subred se ha convertido en una práctica aceptable si se utilizan junto con VLSM.

El equipo de administración de red ha pedido prestados tres bits de la porción de host de la dirección Clase C que se ha seleccionado para este esquema de direccionamiento. Si el equipo decide usar la subred cero, habrá ocho subredes utilizables. Cada subred puede admitir 30 hosts. Si el equipo decide utilizar el comando no ip subnet-zero, habrá siete subredes utilizables con 30 hosts en cada subred. Los routers Cisco con la versión 12.0 o posterior del IOS Cisco, utilizan la subred cero por defecto.

Cada una de las oficinas remotas de Sydney, Brisbane, Perth y Melbourne puede tener 30 hosts. El equipo se da cuenta que tiene que direccionar los tres enlaces WAN punto a punto entre Sydney, Brisbane, Perth y Melbourne. Si el equipo utiliza las tres últimas subredes para los enlaces WAN, se usarán todas las direcciones disponibles y no habrá más espacio para el crecimiento. El equipo también habrá desperdiciado las 28 direcciones de host de cada subred simplemente para direccionar tres redes punto a punto. Este

esquema de direccionamiento implicaría un desperdicio de un tercio del espacio de direccionamiento potencial.

Este tipo de esquema de direccionamiento es adecuado para las LAN pequeñas. Sin embargo, representa un enorme desperdicio si se utilizan conexiones punto a punto.

1.4. Operaciones con VLSM.

Es increíble lo popular que es el tema de la división en subredes (o subneteo como algunos lo llaman muy coloquialmente o subnetting como se diría correctamente en inglés), en especial VLSM, seguramente por la dificultad que representa empezar con él. Dada esta premisa y que la maestría sólo se logra con ejercicios y práctica, decidí documentar en este Blog algunos de los ejercicios que le puse a mis estudiantes de Comunicaciones en el primer examen parcial del semestre (2° del 2008), espero que les resulte útil y que hagan los otros ejercicios propuestos. Estos son ejercicios de **dificultad baja**, aumentaré la dificultad en futuras entradas usando subredes de mayores tamaños con redes base de gran tamaño (por ejemplo una clase B o una clase A) . Por lo pronto **describiré un ejercicio y su solución,** al final de la entrada dejaré otro ejercicio y su solución para descargar en archivos independientes.

El problema

Dada la **red 192.168.0.0/24**, desarrolle un esquema de **direccionamiento que cumpla con los siguientes requerimientos**. **Use VLSM**, es decir, optimice el espacio de direccionamiento tanto como sea posible.

1. Una subred de **20 hosts** para ser asignada a la VLAN de Profesores

2. Una subred de **80 hosts** para ser asignada a la VLAN de Estudiantes
3. Una subred de **20 hosts** para ser asignada a la VLAN de Invitados
4. Tres subredes de **2 hosts** para ser asignada a los enlaces entre enrutadores.

Solución

Ordeno las subredes en orden decreciente: **80, 20,**
20, 2, 2, 2.

Para **80 hosts** necesito **7 bits** (2^7=128, menos red y broadcas 126 hosts máx.), por lo tanto, el prefijo de subred del primer bloque sería **/25** (8-7=1; 24+1=25) Tomando la subred cero, la primera dirección de subred sería 192.168.0.0/25, broadcast 192.168.0.127, por lo tanto el rango asignable sería .1 hasta .126.

Para **20 hosts** necesito **5 bits** (2^5=32, es decir 30 hosts máx.). Prefijo: **/27** (8-5=3, 24+3=27); Dir. de red: 192.168.0.128/27, broadcast 192.168.0.159. Rango asignable .129-.158.

La siguiente subred es del **mismo tamaño** y el prefijo es el mismo. Dir. de red:

192.168.0.160/27 , broadcast 192.168.0.191, rango .161-.190.

Los **enlaces** entre enrutadores **sólo necesitan 2 bits** (2^2=4, es decir 2 hosts máx) por lo tanto el prefijo debe ser **/30** (8-2=6, 24+6=30). Dir. de enlace 1: 192.168.0.192, Dir. De broadcast en enlace 1: 192.168.0.195, rango .193- Dir. Enlace 2: 192.168.0.196/30, .194.

Broadcast en enlace 2: 192.168.0.199, rango .197-.198. Dir. Enlace 3: 192.168.0.200/30, Broadcast enlace 3: 192.168.0.203, rango: .201-.202.

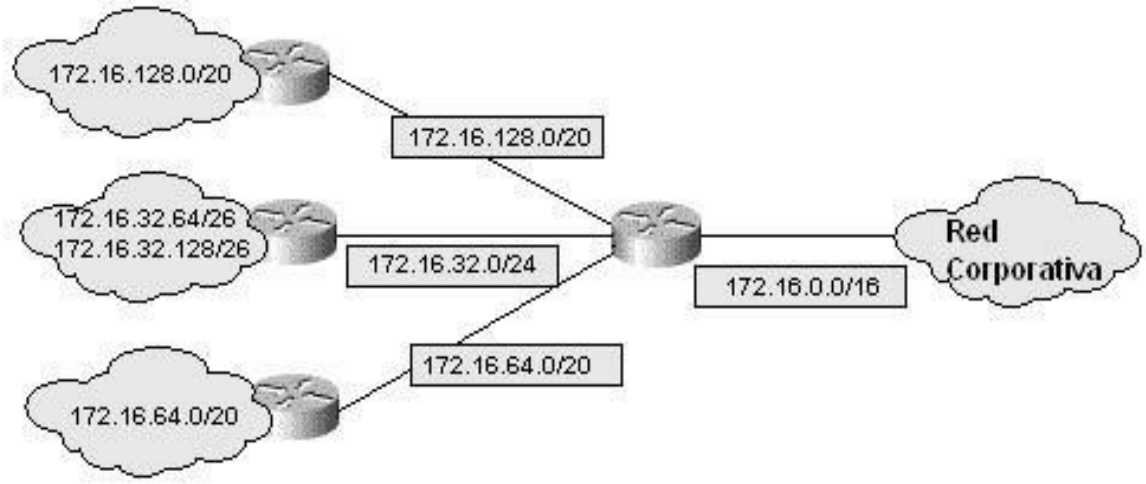
El esquema resultado es:

Red	Dir	Broadcast	Rango	Máscara
Estudiantes (80)	192.168.0.0/25	192.168.0.127	.1-.126	255.255.255.128
Profesores (20)	192.168.0.128/27	192.168.0.159	.129-158	255.255.255.224
Invitados (20)	192.168.0.160/27	192.168.0.191	.161-190	255.255.255.224
Enlace 1(2)	192.168.0.192/30	192.168.0.195	.193-194	255.255.255.252
Enlace 2(2)	192.168.0.196/30	192.168.0.199	.197-198	255.255.255.252
Enlace 3(2)	192.168.0.200/30	192.168.0.203	.201-202	255.255.255.252

Se puede observar que los rangos de direcciones asignados son continuos y que queda disponible para crecimiento futuro un rango de direcciones desde 204 en adelante.

1.5. Resumen de rutas.

El resumen de ruta **CIDR** (agregación de ruta o supernetting) reduce la cantidad de rutas que un router debe mantener en sus tablas anunciando y manteniendo una sola dirección que contengas a las demás.



El router de resumen tiene múltiples entradas de redes consecutivas, siendo este el principal factor en el resumen de ruta, pero solo anunciara al router remoto la red que contiene a todas las demás.

Explicación de funcionamiento de CIDR

Imagina que un router posee un rango de redes directamente conectadas, de la 172.16.168.0/24 a la

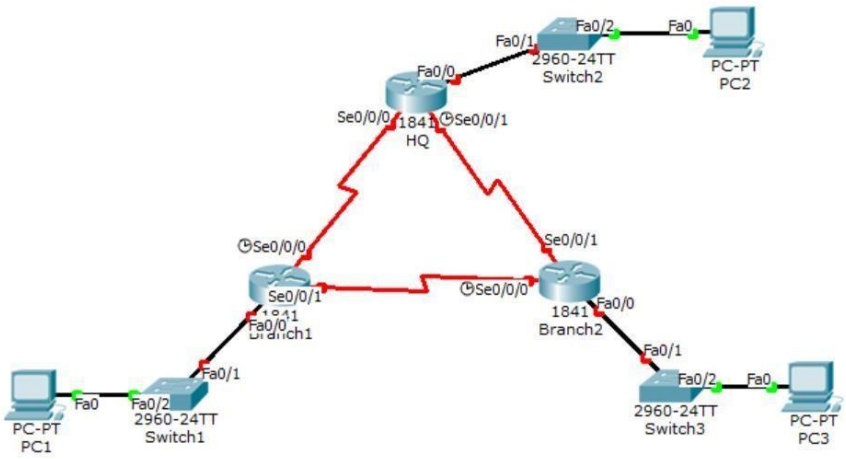
172.16.175.0/24. El router buscara el bit común más alto para determinar cuál será el resumen de ruta.Por lo tanto para el rango especificado el router utilizara la dirección

172.16.168.0/21 para el resumen de ruta solicitado.

Dirección de subred	Primer octeto	Segundo octeto	Tercer octeto		Cuarto octeto
172.16.168.0/24	10101100	00010000	10101	000	00000000
172.16.169.0/24	10101100	00010000	10101	001	00000000
172.16.170.0/24	10101100	00010000	10101	010	00000000
172.16.171.0/24	10101100	00010000	10101	011	00000000
172.16.172.0/24	10101100	00010000	10101	100	00000000
172.16.173.0/24	10101100	00010000	10101	101	00000000
172.16.174.0/24	10101100	00010000	10101	110	00000000
172.16.175.0/24	10101100	00010000	10101	111	00000000
	Bits comunes = 21			Bits no comunes o de host	
	Resumen 172.16.168.0/21				

1.6. Configuración de VLSM.

Hoy vamos a ver enrutamiento dinámico con OSPF en una red con tres Routers y tres PCs en la que vamos previamente vamos a crear un diseño VLSM de acuerdo con los requisitos que vamos a ver a continuación. El esquema de red es el que podemos ver en la siguiente imagen, y el ejercicio que podemos realizar en el simulador Packet Tracert.



A lo largo de esta práctica vamos a aprender los siguientes conceptos

- Crear un diseño de VLSM eficaz de acuerdo con determinados requisitos
- Asignar direcciones adecuadas a las interfaces y documentarlo
- Conectar una red de acuerdo con el Diagrama de topología
- Configurar routers incluyendo OSPF
- Configurar y propagar una ruta estática predeterminada
- Verificar el funcionamiento OSPF

Paso 1: Diseño de VLSM

El diseño de VLSM deberá cumplir los siguientes requisitos. La red 172.20.0.0/16 debe dividirse en subredes para proporcionar direcciones para las LAN y los enlaces seriales. Es muy recomendable realizar los cálculos de VLSM en papel.

La LAN de HQ necesitará 8000 direcciones

Red : 172.20.0.0/19 --- Broadcast : 172.20.31.255/19

La LAN de Branch1 necesitará 4000 direcciones

Red : 172.20.32.0/20 --- Broadcast : 172.20.47.255/20

La LAN de Branch2 necesitará 2000 direcciones

Red : 172.20.48.0/21 --- Broadcast :
172.20.55.255/20

Los enlaces entre los routers necesitarán dos direcciones para
cada enlace

Red : 172.20.56.0/30 --- Broadcast :
172.20.56.3/30

Red : 172.20.56.4/30 --- Broadcast :
172.20.56.7/30

Red : 172.20.56.8/30 --- Broadcast :
172.20.56.11/30

La dirección loopback que representa en vínculo entre el router HQ y el ISP utilizará la red

10.10.1
0.0/30.

Red : 10.10.10.0/30 --- Broadcast :
10.10.10.3/30

Paso 2: Asignar las direcciones a las interfaces

-Recordamos que para introducir una ip a una interfaz en un router Cisco haremos doble clic sobre él, entramos a la pestaña CLI y haremos lo siguiente...

, one per line. End with CNTL/Z.
Router(config)#interface <nombre de la interfaz>

Router(config-if)#ip address <Direccion IP interfaz>
<Máscara de red> Router(config-if)#no shutdown

-Mientras que para introducir una IP a un PC nos iremos a Desktop > IP Configuration

IP Address : 172.20.31.254

Subnet Mask : 255.255.224.0

Default Gateway : 172.20.0

-Para que el ejercicio quede de forma correcta y al 100% debemos introducir IPs que correspondan a las que vamos a ver a continuación.

Asigne la primera dirección de host válida en la red 10.10.10.0/30 para la interfaz Loopback 1 en el router

HQ. Haremos lo siguiente.

Router(config)#interface loopback0

Router(config-if)#ip address 10.10.10.1 255.255.255.252

Asigne la primera dirección IP válida de la red LAN de HQ a la interfaz LAN del router HQ. Haremos lo siguiente.

Router(config-if)#interface fa0/0

Router(config-if)#ip address 172.20.0.1 255.255.224.0

Router(config-if)#no shutdown

Asigne la última dirección IP válida de la red LAN de HQ a la PC2. IP Address : 172.20.31.254

Subnet Mask : 255.255

Default Gateway : 172.20.0.1

Asigne la primera dirección IP válida de la red LAN de Branch1 a la interfaz LAN del router Branch1. Router(config)#interface fa0/0

Router(config-if)#ip address 172.20.32.1 255.255.240.0

Router(config-if)#no shutdown

Asigne la última dirección IP válida de la red LAN de Branch1 a PC1. IP Address : 172.20.47.254

Subnet Mask : 255.255.224.0

Default Gateway : 172.20.32.1

Asigne la primera dirección IP válida de la red LAN de Branch2 a la interfaz LAN del router Branch2. Router(config)#interface fa0/0

Router(config-if)#ip address 172.20.48.1 255.255.248.0

Router(config-if)#no shutdown

Asigne la última dirección IP válida de la red LAN de Branch2
a PC3. IP Address : 172.20.48.1

Subnet Mask : 255.255.248.0

Default Gateway : 172.20.48.1

Asigne la primera dirección IP válida de la red de enlace entre HQ y Branch1 a la interfaz Serial

0/0/0 del router HQ.
Router(config)#interfac
e s0/0/0

Router(config-if)#ip address 172.20.56.1 255.255.255.252

Router(config-if)#no shutdown

Asigne la última dirección IP válida de la red de enlace entre HQ y Branch1 a la interfaz Serial 0/0/0 del router Branch.

Router(config)#interface s0/0/0

Router(config-if)#ip address 172.20.56.2 255.255.255.252

Router(config-if)#no shutdown

Asigne la primera dirección IP válida de la red de enlace entre HQ y Branch2 a la interfaz Serial

0/0/1 del router HQ.
Router(config)#interface
s0/0/1

Router(config-if)#ip address 172.20.56.5 255.255.255.252

Router(config-if)#no shutdown

Asigne la última dirección IP válida del HQ a la red de enlace Branch2 para la interfaz Serial0/0/1 del router Branch2.

Router(config)#interface s0/0/1

Router(config-if)#ip address 172.20.56.6 255.255.255.252

Router(config-if)#no shutdown

Asigne la primera dirección IP válida del HQ a la red de enlace Branch1 para la interfaz Serial 0/0/1 del router Branch1.

Router(config)#interface s0/0/1

Router(config-if)#ip address 172.20.56.9 255.255.255.252

Router(config-if)#no shutdown

Asigne la última dirección IP válida del Branch1 a la red de enlace Branch2 para la interfaz

Serial0/0/0 del router Branch2.

Router(config)#interfac e s0/0/0

Router(config-if)#ip address 172.20.56.10 255.255.255.252

Router(config-if)#no shutdown

Al acabar la configuración de las interfaces el resultado del ejercicio será del 78%

Paso 3: Preparar la red

Configure el nombre de host del router. (En cada Router) Router(config)#hostname HQ

Router(config)#hostname Branch1

Router(config)#hostname Branch2

Desactive la búsqueda de DNS. (En cada Router) Router(config)#no ip domain-lookup

Configure una contraseña de modo EXEC. (En cada Router) Router(config)#enable secret class

Configure un mensaje del día. (En cada Router) Router(config)#banner motd #Bienvenido a la consola#

Configure una contraseña para las conexiones de la consola. (En cada Router) Router(config)#line console 0

Router(config-line)#password cisco

Router(config-line)#login

Configure una contraseña para las conexiones de VTY. (En cada Router) Router(config)#line vty 0 4

Router(config-line)#password cisco

Router(config-line)#login

Configure un tiempo de espera EXEC de 15 minutos. (en cada Router) Router(config-line)#exec

Router(config-line)#exec-timeout 15

Configurar el clockrate de las interfaces DCE en 64000

HQ(config)#interface s0/0/1

HQ(config-if)#clock rate 64000

Branch1(config)#interface s0/0/0

Branch1(config-if)#clock rate 64000

Branch2(config)#interface s0/0/0

Branch2(config-if)#clock rate 64000

Paso 4: Configuración de OSPF Configuración OSPF en Router HQ

HQ(config)#router ospf 1

HQ(config-router)#network 172.20.32.0 0.0.15.255 area 0

HQ(config-router)#network 172.20.48.0 0.0.7.255 area 0

Configuración OSPF en Router Branch 1

Branch1(config)#router ospf 1

Branch1(config-router)#network 172.20.0.0 0.0.31.255 area 0

Branch1(config-router)#network 172.20.48.0 0.0.7.255 area 0

Configuración OSPF en Router Branch2

Branch2(config)#router ospf 1

Branch2(config-router)#network 172.20.0.0 0.0.31.255 area 0

Branch2(config-router)#network 172.20.32.0 0.0.15.255 area 0

Configuracion extra de OSPF

Además de estas configuraciones tendremos que tener en cuenta lo siguiente:

Tendremos que deshabilitar las actualizaciones de OSPF para las redes LAN. Para ello en cada Router usaremos el comando passive interface. Branch2(config)#router ospf 1

Router(config-router)#passive-interface fa0/0

Utilizaremos el comando default-information originate para incluir la ruta estática en las actualizaciones

OSPF que se envían desde el Router HQ. Esto lo realizaremos sólo en el Router HQ HQ(config-router)#default-information originate

Por último configuraremos la ruta estática por defecto que simula el enlace de ISP. HQ(config-if)#ip route 0.0.0.0 0.0.0.0 loopback1

1.7. Ejercicios con VLSM.

Dada la siguiente dirección de red: 172.25.0.0/16, dividala en subredes de las siguientes capacidades:

2 subredes de 1000 hosts

2000 hosts

5 hosts

60 hosts

70 hosts

15 enlaces de 2 hosts por enlace

El potencial ideal de la red base sería 2^16-2, es decir **65534 hosts si no usamos subredes,** osea que debemos esperar que esa capacidad potencial no se desperdicie mucho, en especial si usamos VLSM. Lo anterior nos permite saber que **los requerimientos aparentes (4165 hosts) caben de sobra en la red base**.

Procedimiento

Vamos a **ordenar las subredes decrecientemente** para asegurar que el direccionamiento no quede fraccionado.

Subred de **2000** Hosts Subred de **1000** Hosts Subred de **1000** Hosts Subred de **70** Hosts Subred de **60** Hosts Subred de **5** Hosts

15 subredes de
2 Hosts

Una vez ordenados los requerimientos, procedemos a operar la división en subredes como si fuéramos a **usar** subredes de **máscara fija para la subred actual y la siguiente.** Es decir, hacemos los cálculos para una subred y dejamos indicada cuál sería la siguiente subred, sólo que, como usamos máscara variable sabemos que la siguiente subred puede o no tener la misma máscara (usualmente la tendrá más larga).

Análisis del procedimiento para la primera subred

Para la primera subred necesitamos 11 bits (2^11=2048-2=2046 hosts, 10 bits no son suficientes ya que sólo alcanzaría para 1024). Como tenemos 16 bits originales para hosts, tomamos éstos 11 bits de la parte de host y dejamos el resto para subred, es decir, 5 bits para subred (adicionales a la máscara de red original).

172.25. {SSSSSHHH.HHHHHHHH}, donde S es bit de subred y H es bit de host Nuestra primera red es 172.25.0.0/21 y la siguiente sería 172.25.8.0/21 (como si aplicáramos máscara fija). La siguiente red con la misma máscara es importante, debido a que a partir de ésa es que tomamos las siguientes subredes, ésta nos marca el final de la subred asignada y el comienzo del espacio libre. De la dirección y máscara de la primera subred

se deducen los otros datos importantes: broadcast y rango asignable. Ya sabemos que la dirección de subred es aquella que tiene todos los bits de host en cero y los bits de host son aquella porción de la dirección de red que se corresponden con los ceros de la máscara de red, es decir, para nuestra 1a subred la máscara es 255.255.248.0 o /21, por lo tanto, la dirección 172.25.0.0 es una Dir. de subred ya que los bits que en la máscara son cero también son cero en la dirección de red. La dirección de broadcast es aquella en la que los bits de hosts son todos 1, es decir, para la primera subred la dirección de broadcast es172.25.7.255, ya que en ésta dirección, los bits que en la máscara son ceros, en la dirección de broadcast son unos. Y el resto de direcciones entre la dir de red y la dir de broadcast son asignables, es decir de 172.25.0.1 hasta 172.25.7.254. Tenga en cuenta que en estas direcciones hay algunas que pueden engañar como las 15 direcciones que terminan en 255 (por ejemplo

172.25.5.255), esas direcciones, aunque tengan el último octeto en 255 no son de broadcast, ya que la máscara /21 nos dice que la porción de host incluye bits del tercer octeto (.5), por lo tanto, no todos los bits de host son unos y por lo tanto no es una dirección de broadcast. Lo mismo ocurre con otras tantas direcciones que terminarán en 0 pero que no son de subred por la misma (similar) razón por la que la anterior no era de broadcast.

El procedimiento para las demás es igual, pero con menos análisis

Todo lo que hay que explicar y racionalizar en éste –difícil!! problema de subredes está dicho en la sección anterior, digamos que los principios están descritos. Lo que haremos de acá en adelante es repetir esta mecánica, ya que entendemos la justificación de la misma, por lo tanto, asegúrese de entender lo que indica el párrafo anterior y la justificación de la primera subred. La segunda subred es de **1000 hosts,** por lo tanto, necesito **10 bits** (2^10=1024 menos dir. de red y de broadcast = 1022 hosts máximo). Éstos los tomo de la parte de host, quedando así 6 bits de subred. Del cálculo **de la subred anterior sabemos que la siguiente sería la 172.25.8.0**/21, osea que a partir del cálculo de la subred anterior tomamos la siguiente subred (la actual) **pero con una máscara más**

larga (/22) dado que necesitamos menos capacidad. De ésto se desprenden los otros dos números, la dir. de **broadcast es 172.25.11.255/22** y las direcciones después de la de red y antes de la de broadcast son **asignables (172.25.8.1 hasta 172.25.11.254).** Como del cálculo de esta subred vamos a tomar la siguiente, de una vez **digamos cual sería la siguiente subred sin cambiar la máscara:**

172.25.12.0/22. La tercera subred es también de **1000 hosts,** por lo que **no cambia la máscara** y del ejercicio anterior ya tenemos la dirección de subred: **172.25.12.0/22.**

La dirección de broadcast es entonces 172.25.15.255/22 y las direcciones asignables 172.25.12.1/22 hasta 172.25.15.254/22).

La siguiente subred con la misma máscara sería 172.25.16.0/22. La cuarta subred es de **70 hosts,** para los que necesito **7 bits** (2^7=128 menos broadcast y subred 126 hosts máx), que tomo de la parte más baja de la porción de host lo que me deja 9 bits de lo que tenía originalmente en host (16 bits), por lo tanto, la máscara de subred queda en /25. **La dir. de red es 172.25.16.0/25**, la dir de broadcast es 172.25.16.127/25 y las direcciones asignables desde 172.25.16.1/25 hasta

172.25.16.126/25.

La siguiente subred sería

172.25.16.128/25 La quinta subred es de **60 hosts,** necesito **6 bits** (2^6=64-2=62 hosts máximo) y de ahí que la máscara de subred sea /26. La dir de red es **172.25.16.128/26,** la dir de broadcast es 172.25.16.191/26 y las direcciones asignables son 172.25.16.129/26 hasta 172.25.16.190/26. **La siguiente subred sería 172.25.16.192/26** La siguiente subred es de **5 hosts** por lo tanto **la máscara será /29** (haga el cálculo). La dirección de subred es **172.25.16.192/29,**

la dirección de broadcast es 172.25.16.199/29 y las direcciones asignables de 172.25.16.193/29 hasta 172.25.16.198/29 (inclusive). La **siguiente subred sería 172.25.16.200/29** Las últimas son **las subredes de enlaces WAN** que sólo admiten dos hosts, por lo tanto, necesito sólo 2 bits de host y sin hacer más cálculos tengo que **la máscara es /30 (de todos modos, para enlaces punto a punto, usualmente WAN, siempre se usa ésta máscara).** Las direcciones de subred serían **172.25.16.200/30, 172.25.16.204/30,**–.16.**208/30,** –16.**212/30,** –16.**216/30,** –16.**220/30,** –16.**224/30,** –16.**228/30,** –16.**232/30,** –16.**236/30,** –16.**240/30,** –16.**244/30,** –16.**248/30,** –16.**252/30, – 17.0/30.**

Por favor deduzcan las direcciones asignables y las direcciones de broadcast de cada una de éstas subredes de enlaces punto a punto. Note que la última dirección rompió el límite del octeto y pasó de la **.16.252** a la **.17.0**. Note que el ejercicio esta cuidadosamente planeado para romper **los límites de octeto** que tanto **malacostumbra a los estudiantes** y para incluir direcciones en los rangos de asignación que pueden engañar como aquellas direcciones de hosts que tienen 0 ó 255 en su último octeto.

17.0/30. Por favor deduzcan uds. las direcciones asignables y las direcciones de broadcast de cada una de éstas subredes de enlaces punto a punto. Note que la última dirección rompió el límite del octeto y pasó de la **.16.252** a la **.17.0**. Note que el ejercicio esta cuidadosamente planeado para romper los límites de octeto que tanto malacostumbran a los estudiantes y para incluir direcciones en los rangos de asignación que pueden engañar como aquellas direcciones de hosts que tienen 0 ó 255 en su último octeto.

Note también que, a pesar de haber usado tantas direcciones y tantas subredes, todavía queda un rango gigantesco por asignar, todas las direcciones por encima de 172.25.17.0 en adelante siguen libres. Y finalmente también note mi insistencia en siempre escribir la

máscara de subred, que es en efecto el criterio que define qué tipo de dirección es una dirección IP (de red, de broadcast o de host) y además que es la que le permite a un PC o nodo de red determinar cómo encapsular un paquete (si con la dir física del enrutador o con la dir física del par -del otro PC-).

1.8. Algoritmos de enrutamiento dinámico.

Los protocolos de enrutamiento para la capa de red son usados para resolver peticiones de servicios de envío de paquetes de datos a través de diferentes redes de datos. El objetivo de esta sección es analizar algunos de los protocolos de enrutamiento vector-distancia y Estado de Enlace.

Propósitos de los protocolos de enrutamiento y de los sistemas autónomos

El objetivo de un protocolo de enrutamiento es crear y mantener una tabla de enrutamiento. Esta tabla contiene las redes conocidas y los puertos asociados a dichas redes. Los routers utilizan protocolos de enrutamiento para administrar la información recibida de otros routers, la información que se conoce a partir de la configuración de sus propias interfaces, y las rutas configuradas manualmente. Los protocolos de enrutamiento aprenden todas las rutas disponibles, incluyen las mejores rutas en las tablas de enrutamiento y descartan las rutas que ya no son válidas. El router utiliza la información en la tabla de enrutamiento para enviar los paquetes de datos.

El algoritmo de enrutamiento es fundamental para el enrutamiento dinámico. Al haber cambios en la topología de una red, por razones de crecimiento, reconfiguración o falla, la información conocida acerca de la red también debe cambiar. La información conocida debe reflejar una visión exacta y coherente de la nueva topología.

1.9. RIP.

RIP (Routing information protocolo, protocolo de información de encaminamiento)

RIP es un protocolo de encaminamiento interno, es decir para la parte interna de la red, la que no está conectada al backbone de Internet. Es muy usado en sistemas de conexión a internet como infovia, en el que muchos usuarios se conectan a una red y pueden acceder por lugares distintos.

Cuando un usuario se conecta el servidor de terminales (equipo en el que finaliza la llamada) avisa con un mensaje RIP al router más cercano advirtiendo de la dirección IP que ahora le pertenece.

Así podemos ver que RIP es un protocolo usado por distintos routers para intercambiar información y así conocer por donde deberían enrutar un paquete para hacer que éste llegue a su destino.

Es necesario que se tengan ciertos conocimientos de manejo de dispositivos Cisco y del simulador de redes Packet Tracer.

La forma más sencilla para configurar un enrutamiento dinámico es mediante el uso del protocolo RIP (Routing Information Protocol).

Por medio de este protocolo se puede conseguir que los routers compartan información sobre las redes que conocen, de manera que un router llegue a aprender las rutas hacia redes que no se encuentran directamente conectadas a él.

Para hacer la configuración del protocolo hay que decidir con qué interfaces (tarjetas de red) se va a comunicar con otros routers, así como la versión del protocolo a utilizar, usualmente la 2. Esas interfaces deben poner en contacto ambos routers, y los dos han de utilizar la misma versión. A través de esas tarjetas se envía la información de enrutamiento (mensajes RIP, llamados actualizaciones, con la información sobre las rutas para alcanzar las redes remotas)

Comando network para RIP en Cisco

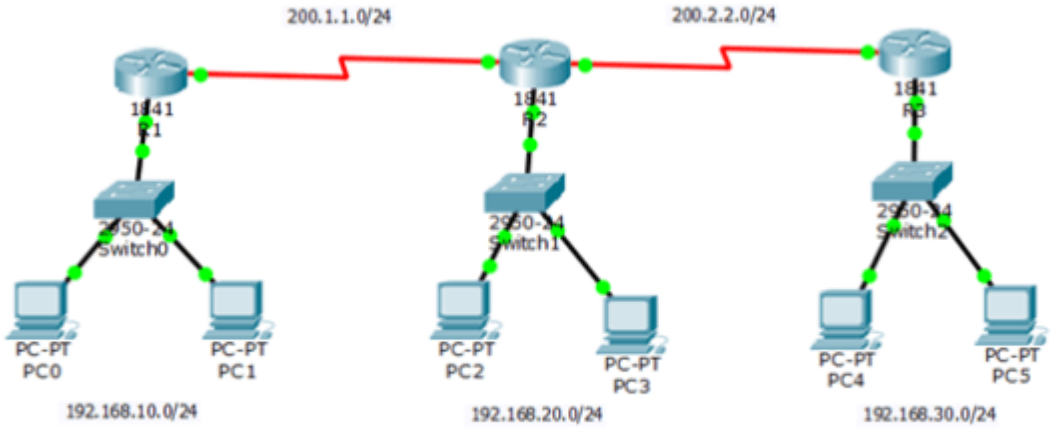
La base de la configuración del protocolo RIP en Cisco se encuentra en el comando network.

Dicho comando cumple con dos propósitos:

Informar a RIP sobre qué interfaces interviene en el envío y recepción de actualizaciones de enrutamiento.

Pedir a RIP que anuncie a los demás routers la existencia de la red.

La mejor manera de verlo es mediante un ejemplo, realizado con el Packet Tracer:



En el diagrama tenemos tres routers (R1, R2 y R3) conectados entre sí como se puede ver, a través de conexiones seriales (cables rojos) y con switches a una red privada cada uno.

La configuración de RIP en R2 será:

R2>enable

R2#configure terminal

R2(config)#router rip

R2(config-router)#version 2

R2(config-router)#network 200.1.1.0

R2(config-router)#network 200.2.2.0

R2(config-router)#network 192.168.20.0

Al establecer network 200.1.1.0 estamos indicando que las interfaces en esa red (la conexión serie) se utilicen para enviar y recibir actualizaciones de enrutamiento. Además de eso esa red será anunciada al resto de posibles routers presentes (en este caso no la notifica a R1, pues está en esa misma red y ya la conoce, en cambio sí que se lo notifica a R3). El caso de la red 200.2.2.0 es semejante.

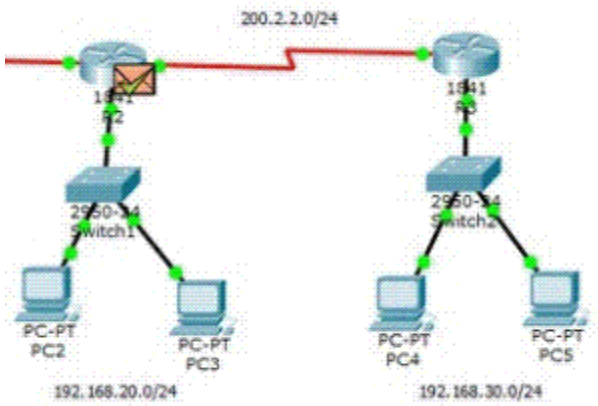
Con la sentencia network 192.168.20.0 estamos indicando que dicha red sea notificada a los otros routers (R1 y R3). Evidentemente, por la interfaz de dicha red se enviarán actualizaciones de enrutamiento que no son necesarias, pues no hay ningún router conectado allí. Se puede evitar esto estableciendo la interfaz como pasiva.

Para ello, en el archivo de configuración del ejemplo tenemos puesto:

R2(config-router)#passive-interface f0/0

De manera semejante se configuran los otros dos routers. En ellos no hemos configurado el passive-interface, para comprobar la diferencia al hacer la simulación; se podrá ver cómo los paquetes RIP se mueven por las interfaces, salvo en aquellas establecidas como pasivas.

En el archivo de ejemplo, al abrir Packet Tracer, si elegimos la opción simulación y observamos el paso de los paquetes, observaremos cómo los de RIP se desplazan como esperábamos, por las interfaces que no se establecieron como pasivas.



Aquí puedes encontrar un ejemplo: https://www.youtube.com/watch?v=Ln6Lg5jWM5o

1.10. OSPF.

OSPF (Open shortest path first, El camino más corto
primero)

OSPF se usa, como RIP, en la parte interna de las redes, su forma de funcionar es bastante sencilla. Cada router conoce los routers cercanos y las direcciones que posee cada router de los cercanos. Además de esto cada router sabe a que distancia (medida en routers) está cada router. Así cuando tiene que enviar un paquete lo envía por la ruta por la que tenga que dar menos saltos.

Así por ejemplo un router que tenga tres conexiones a red, una a una red local en la que hay puesto de trabajo, otra (A) una red rápida frame relay de 48Mbps y una línea (B) RDSI de 64Kbps. Desde la red local va un paquete a W que esta por A a tres saltos y por B a dos saltos.

El paquete iría por B sin tener en cuenta la saturación de la linea o el ancho de banda de la linea.

La O de OSPF viene de abierto, en este caso significa que los algoritmos que usa son de disposición pública.

OSPF es probablemente el protocolo IGP más utilizado en redes grandes; IS-IS, otro protocolo de encaminamiento dinámico de enlace-estado, es más común en grandes proveedores de servicios. Como sucesor natural de RIP, acepta VLSM y CIDR desde su inicio. A lo largo del tiempo, se han ido creando nuevas versiones, como OSPFv3 que soporta IPv6 o las extensiones multidifusión para OSPF (MOSPF), aunque no están demasiado extendidas. OSPF puede "etiquetar" rutas y propagar esas etiquetas por otras rutas.

Una red OSPF se puede descomponer en regiones (áreas) más pequeñas. Hay un área especial llamada área backbone que forma la parte central de la red a la que se encuentran conectadas el resto de áreas de la misma. Las rutas entre las diferentes áreas circulan siempre por el backbone, por lo tanto todas las áreas deben conectar con el backbone. Si no es posible hacer una conexión directa con el backbone, se puede hacer un enlace virtual entre redes.

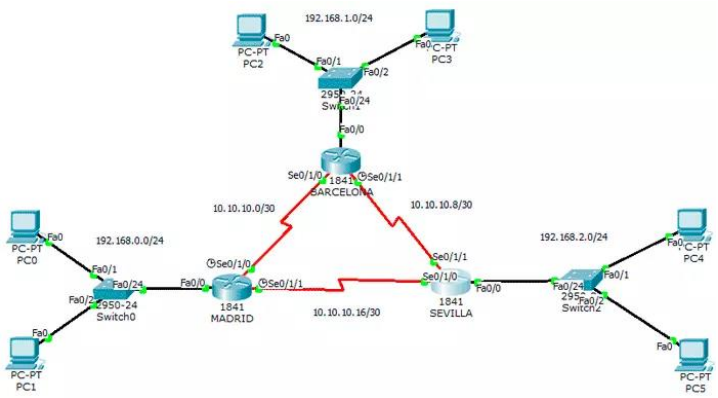
Los routers (también conocidos como encaminadores) en el mismo dominio de multidifusión o en el extremo de un enlace punto-a-punto forman enlaces cuando se descubren los unos a los otros. En un segmento de red Ethernet los routers eligen a un router designado (Designated Router, DR) y un router designado secundario o de copia (Backup Designated Router, BDR) que actúan como hubs para reducir el tráfico entre los diferentes routers. OSPF puede usar tanto multidifusiones (multicast) como unidifusiones (unicast) para enviar paquetes de bienvenida y actualizaciones de enlace-estado. Las direcciones de multidifusión usadas son 224.0.0.5 y 224.0.0.6. Al contrario que RIP o BGP, OSPF no usa ni TCP ni UDP, sino que se encapsula directamente sobre el protocolo IP poniendo "89" en el campo protocolo.

OSPF organiza un sistema autónomo (AS) en áreas. Estas áreas son grupos lógicos de routers cuya información se puede resumir para el resto de la red. Un área es una unidad

de encaminamiento, es decir, todos los routers de la misma área mantienen la misma información topológica en su base de datos de estado-enlace (Link State Database): de esta forma, los cambios en una parte de la red no tienen por qué afectar a toda ella, y buena parte del tráfico puede ser "parcelado" en su área.

ESQUEMA DE RED OSPF

El esquema de la red que queremos emular es el que se ve en la imagen siguiente. Podemos ver que tenemos 3 Routers (MADRID, BARCELONA y SEVILLA) y en cada una de las redes hay 2 equipos clientes y un switch. Cada router puede estar pro ejemplo, en ciudades diferentes. Cada una de las redes tiene un direccionamiento diferente y los routers están unidos a través de cable Serial. El resto de conexiones son ethernet. Lo que queremos conseguir es: si se cae la conexión entre MADRID y BARCELONA, que los paquetes que vayan de MADRID a SEVILLA y luego a BARCELONA. Gracias a este enrutamiento dinámico tenemos un HA (High Availability) a nivel de conexiones de red.



En al siguiente tabla se muestra el direccionamiento que he usado para cada uno de los equipos del esquema de red. Hay que prestar especial atención a las direcciones IPs asignadas en los routers, ya que llevan 3 direcciones IPs en sus interfaces de red (2 Serials y una ethernet):

ZONA	EQUIPO	IPS	MÁSCARA DE RED	GATEWAY
MADRID	PC0	192.168.0.100	255.255.255.0	192.168.0.1
	PC1	192.168.0.101	255.255.255.0	192.168.0.1
	Switch0	-----	-----	-----
	Router0	192.168.0.1	255.255.255.0	-----
		10.10.10.1	255.255.255.252	-----
		10.10.10.17	255.255.255.252	-----
BARCELONA	PC2	192.168.1.100	255.255.255.0	192.168.1.1
	PC3	192.168.1.101	255.255.255.0	192.168.1.1
	Switch1	-----	-----	-----
	Router1	192.168.1.1	255.255.255.0	-----
		10.10.10.2	255.255.255.252	-----
		10.10.10.9	255.255.255.252	
SEVILLA	PC4	192.168.2.100	255.255.255.0	192.168.2.1
	PC5	192.168.2.101	255.255.255.0	192.168.2.1
	Switch2	-----	-----	-----
	Router2	192.168.2.1	255.255.255.0	-----
		10.10.10.18	255.255.255.252	-----
		10.10.10.10	255.255.255.252	-----

EQUIPOS CLIENTES

Añadiremos los equipos clientes (6 equipos) y configuraremos su interfaz de red con la dirección IP y la máscara de red de la tabla del punto 2. Se deberá prestar atención a la puerta de enlace de cada zona, ya que es diferente. La puerta de enlace de cada zona (MADRID, BARCELONA y SEVILLA) se corresponde con la dirección ip del router de dicha zona.

SWITCHES

Los switches no necesitan configuración y solamente servirán para interconectar los equipos clientes (PCs) con su router.

ROUTERS

La configuración de los 3 routers (modelo 1841) la vamos a realizar exclusivamente en modo Terminal. Recuerda que por defecto las 2 interfaces de red Serials no vienen por defecto en el router, tienes que añadirlas desde la interfaz Web en la pestaña Physical->WIC-2T:

El concepto es sencillo, tenemos que añadir a cada router las 3 redes a las que está conectado. Deberemos usar las Wildcards en lugar de la máscara de Red. El wildcard es al

contrario que la máscara de red. Para una máscara de red 255.255.255.0 le corresponde un wildcard de 0.0.0.255.

El enrutamiento OSPF necesita un Process ID. Este ID va desde 1 hasta 65535. En este ejemplo usaré el Process ID 1 en todos los routers.

También necesitamos un ID de área entre 0 y 4294967295. Usaremos el valor 1 en todas las redes que configuremos para OSPF.

A continuación os dejo la configuración en modo consola para los tres routers:

ROUTER1 (Madrid):

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.0.0 0.0.0.255 area 1
Router(config-router)#network 10.10.10.0 0.0.0.3 area 1
Router(config-router)#network 10.10.10.16 0.0.0.3 area 1
```

ROUTER2 (Barcelona):

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 1
```

Router(config-router)#network 10.10.10.0 0.0.0.3 area 1

Router(config-router)#network 10.10.10.8 0.0.0.3 area 1

ROUTER3 (Sevilla):

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#router ospf 1

Router(config-router)#network 192.168.2.0 0.0.0.255 area 1

Router(config-router)#network 10.10.10.8 0.0.0.3 area 1

Router(config-router)#network 10.10.10.16 0.0.0.3 area 1

Si queremos comprobar las rutas dinámicas de OSPF configuradas en los routers, debemos salir del modo de configuración y ejecutar el siguiente comando:

Router#show ip route ospf

ROUTER1 (Madrid):

Router#show ip route ospf

10.0.0.0/30 is subnetted, 3 subnets

- 10.10.10.8 [110/128] via 10.10.10.18, 00:53:14, Serial0/1/1
- [110/128] via 10.10.10.2, 00:53:14, Serial0/1/0
- 192.168.1.0 [110/65] via 10.10.10.2, 00:53:14, Serial0/1/0
- 192.168.2.0 [110/65] via 10.10.10.18, 00:53:14, Serial0/1/1

ROUTER2 (Barcelona):

Router#show ip route ospf

10.0.0.0/30 is subnetted, 3 subnets

- 10.10.10.16 [110/128] via 10.10.10.10, 01:00:36, Serial0/1/1
    - [110/128] via 10.10.10.1, 01:00:36, Serial0/1/0
- 192.168.0.0 [110/65] via 10.10.10.1, 01:00:36, Serial0/1/0
- 192.168.2.0 [110/65] via 10.10.10.10, 01:00:36, Serial0/1/1

ROUTER3 (Sevilla):

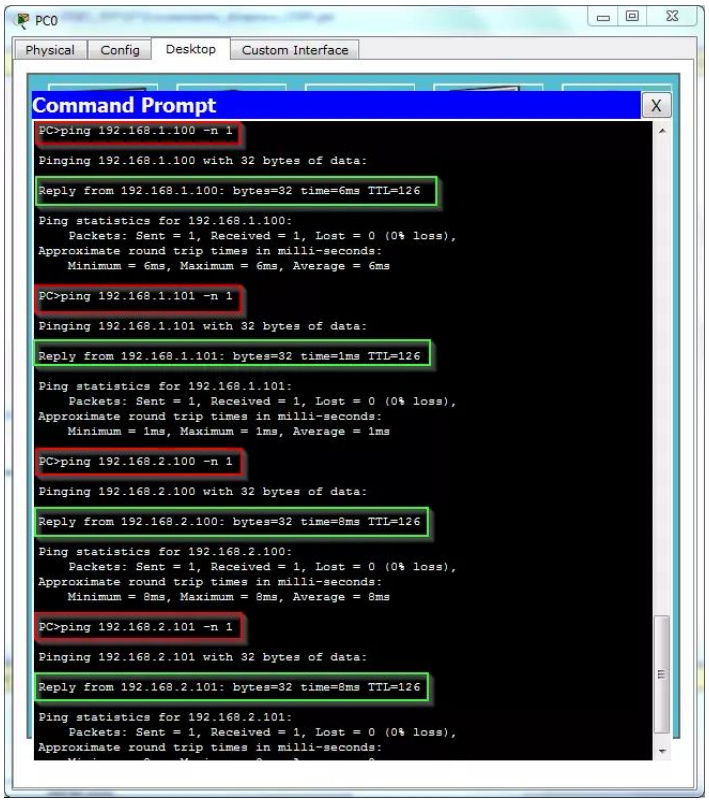
Router#show ip route ospf

10.0.0.0/30 is subnetted, 3 subnets

- 10.10.10.16 [110/128] via 10.10.10.10, 01:00:36, Serial0/1/1
    - [110/128] via 10.10.10.1, 01:00:36, Serial0/1/0
- 192.168.0.0 [110/65] via 10.10.10.1, 01:00:36, Serial0/1/0
- 192.168.2.0 [110/65] via 10.10.10.10, 01:00:36, Serial0/1/1

PROBAR EL ENRUTAMIENTO OSPF

Para comprobar que el routing está funcionando correctamente, entraremos en la Terminal de PC0 de MADRID (por ejemplo) y haremos Ping al resto de equipos clientes en BARCELONA y SEVILLA. Posiblemente el primer y segundo ping falle. Esto es debido a que los routers tienen que aprender las rutas, pero luego todo irá a la perfección.



BGP (Border gateway protocol, protocolo de la pasarela externa)

BGP es un protocolo muy complejo que se usa en la interconexión de redes conectadas por un backbone de internet. Este protocolo usa parámetros como ancho de banda, precio de la conexión, saturación de la red, denegación de paso de paquetes, etc. para enviar un paquete por una ruta o por otra. Un router BGP da a conocer sus direcciones IP a los routers BGP y esta información se difunde por los routers BGP cercanos y no tan cercanos. BGP tiene sus propios mensajes entre routers, no utiliza RIP.

BGP es usado por grandes proveedores de conectividad a internet. Por ejemplo, una empresa (A) tiene alquilada una línea a telefónica-data. La empresa A no hace BGP y posiblemente los routers más cercanos no utilizarán BGP, pero si los que interconecten Telefónica-Data con Hispanix (punto neutro de interconexión en España).

1.11 IGRP.

IGRP (***Interior Gateway Routing Protocol***, o *Protocolo de enrutamiento de gateway interior*) es un protocolo propietario patentado y desarrollado por **CISCO** que se emplea conjuntamente con el protocolo TCP/IP según el modelo (OSI) Internet. La versión original del IP fue diseñada y desplegada con éxito en 1986. Se utiliza comúnmente como Interior Gateway Protocol (IGP) para intercambiar datos dentro de un Sistema Autónomo, pero también se ha utilizado extensivamente como Exterior Gateway Protocol (EGP) para el enrutamiento inter-dominio.

IGRP es un protocolo de enrutamiento basado en la tecnología vector-distancia, aunque también tiene en cuenta el estado del enlace. Utiliza una métrica compuesta para determinar la mejor ruta basándose en el ancho de banda, el retardo, la confiabilidad y la carga del enlace. El concepto es que cada router no necesita saber todas las relaciones de ruta/enlace para la red entera. Cada router publica destinos con una distancia correspondiente. Cada router que recibe la información, ajusta la distancia y la propaga a los routers vecinos. La información de la distancia en IGRP se manifiesta de acuerdo a la métrica. Esto permite configurar adecuadamente el equipo para alcanzar las trayectorias óptimas.

IGRP es un protocolo con clase, lo que significa que no pueden manipularse las máscaras de red (utiliza las máscaras por defecto de cada Clase) IGRP es un protocolo que actualmente no se soporta en sistema operativo de **CISCO** (IOS).

4.12 configuración de enrutamiento dinámico.

El enrutamiento adaptativo, también llamado enrutamiento dinámico, es un proceso para determinar la ruta óptima que debe seguir un paquete de datos a través de una red para llegar a un destino específico. El enrutamiento adaptativo se puede comparar con un viajero tomando una ruta diferente hacia el trabajo después de saber que el tráfico en su ruta habitual está retrasado. El enrutamiento adaptativo utiliza algoritmos y protocolos de

enrutamiento que leen y responden a cambios en la topología de la red. Además de Open Shortest Path First (OSPF), otros protocolos de enrutamiento que facilitan el enrutamiento adaptativo incluyen el protocolo de Sistema Intermedio a Sistema Intermedio (IS-IS) para redes grandes como internet y el protocolo de información de enrutamiento (RIP) para transporte de corta distancia.

Al igual que el GPS, que utiliza información sobre las condiciones del camino para redirigir a los conductores, el enrutamiento adaptativo utiliza información sobre la congestión de la red y la disponibilidad del nodo para dirigir los paquetes. Cuando un paquete llega a un nodo, el nodo utiliza información compartida entre routers de red para calcular qué ruta es la más adecuada. Si la ruta predeterminada está congestionada, el paquete se envía a lo largo de una ruta de acceso diferente y la información se comparte entre routers de red.

Ventajas y retos del enrutamiento adaptativo

El propósito del enrutamiento adaptativo es ayudar a prevenir fallos en la entrega de paquetes, mejorar el rendimiento de la red y aliviar la congestión de la red. El enrutamiento adaptativo puede causar que los nodos se sobrecarguen, sin embargo, debido a las complejas decisiones de procesamiento que toman. Dado que los enrutadores comparten información sobre la topología de red, el enrutamiento adaptativo puede ser menos seguro que los procesos de enrutamiento no adaptativos, y requiere más ancho de banda.

Enrutamiento adaptativo vs. enrutamiento no adaptativo

El enrutamiento adaptativo es una alternativa al enrutamiento estático no adaptativo, que requiere que los ingenieros de red configuren manualmente rutas fijas para paquetes. Cuando un nodo no está disponible en un entorno de enrutamiento estático, el paquete debe esperar que el nodo vuelva a estar disponible o el paquete no se entregará. El enrutamiento estático se utiliza a menudo para las topologías de red cerradas

simples, mientras que el enrutamiento adaptativo se utiliza a menudo para las topologías de red compleja y abierta.

UNIDAD 2.- CONMUTACIÓN

2.1. Introducción

Antes de entrar de lleno en el significado del término conmutación, vamos a proceder a descubrir su origen etimológico. En concreto, deriva del latín, de conmutación, que es fruto de la suma de dos partes claramente diferenciadas como son:

- -El prefijo –con- que significa –junto o –unión.
- -El verbo –mutare, que puede traducirse como cambiar.

La noción de conmutación alude al acto y la consecuencia de conmutar: reemplazar o cambiar algo. El término tiene varias acepciones de acuerdo al contexto.

En el ámbito de la telefonía, la conmutación refiere a determinar el camino que vincula a dos usuarios durante el desarrollo de una comunicación. La conmutación, de este modo, posibilita que una señal arribe a su destino después de salir de su origen.

La informática emplea la idea de conmutación de paquetes para referirse a una cierta forma de envío de datos. Se llama paquete a un conjunto de datos que tiene dos partes: la información en sí misma y la información que señala qué ruta debe seguir el paquete en la red hasta llegar a su destino. La conmutación de paquetes busca la manera adecuada para que la información se transmita lo más rápido que sea posible. Para poder conocer más a fondo la conmutación de paquetes, merece la pena descubrir las ventajas y desventajas de la misma. En este caso, entre sus aspectos más positivos podemos destacar el hecho de que incrementa la rentabilidad de la

red, ofrece una comunicación interactiva, aumenta la flexibilidad de la red y que si hay un error este únicamente afecta a un paquete y no al resto.

Con respecto a sus aspectos en contra, podemos señalar que están que pueden darse casos de duplicidad de paquetes, que se requiere mayor dificultad en lo que se refiere a los equipos de conmutación intermedios y que, en ocasiones y ante determinadas circunstancias concretas, se produce una disminución de lo que es el rendimiento del canal.

Otro uso de conmutación aparece en el terreno de la química. En este caso, la conmutación es el proceso que lleva a un elemento a tener un solo estado de oxidación luego de haber tenido dos estados diferentes. De esta forma, la conmutación hace que un mismo elemento sea reducido y, a la vez, oxidado, todo en la misma reacción. En el plano judicial, se conoce como conmutación de pena a un indulto parcial que beneficia a un condenado, modificando su castigo. La conmutación supone dejar sin efecto una punición para adoptar otra más benévola. Una persona que fue condenada a permanecer dos años de prisión por un delito puede resultar beneficiada por una conmutación de pena que le permita obtener una libertad condicional mientras realiza trabajos comunitarios.

En el ámbito del Derecho Penal es donde cobra protagonismo esa conmutación de pena que podemos establecer que puede ser de varios tipos. Así, puede suponer lo que es una reducción de la duración de la citada pena o bien se puede referir a lo que es la calidad de la pena en sí. Un ejemplo de esto último sería que a una persona se le sustituyera su pena de muerte por una reclusión perpetua.

2.2 Ethernet.

Ethernet es la forma más popular para una red de área local (LAN) o red de área extensa (WAN) para conectarse a dispositivos, como computadoras, impresoras y servidores que requieren una conexión a Internet. Su perfil técnico es el **protocolo IEEE 802.3** y esto especifica cómo los dispositivos se conectan a Internet. Es una alternativa al Wi-Fi y, por lo general, proporciona una conexión mucho más confiable y

más rápida ya que **no tiene la interferencia** de otros dispositivos que usan la misma red.

Una red Ethernet puede conectar dispositivos a velocidades de hasta 100 Gbit/s actualmente, aunque esto podría aumentarse a 400 Gbit/s para fines de este año. Como comparación, este método de transferencia de datos solo tuvo velocidades máximas de 2.94 (Mbit/s) cuando se introdujo por primera vez en 1980.

Sin embargo, no solo conecta dispositivos a Internet. También se usa para conectar dispositivos entre sí, por ejemplo, computadoras a computadoras, computadoras a impresoras, a parlantes para videoconferencias y muchos más.

EQUIPAMIENTO DE ETHERNET

Para que una red Ethernet se ejecute correctamente, todos los dispositivos que se van a conectar requieren tarjetas o adaptadores instalados. Vienen como estándar en la mayoría de los dispositivos. Luego se conectan entre sí utilizando cables de categoría 5 (Cat5) o de categoría 6 (Cat6).

Este tipo particular de cable permite que los datos viajen en ambas direcciones, lo que significa que tienen la capacidad de transmitir datos en todo momento, sin ninguna latencia.

Enrutadores (routers) Ethernet, concentradores y ahora conmutadores (switches), es a lo que se conectan los cables desde una computadora para enrutar los datos de red a su destino.

COMO FUNCIONA ETHERNET

En un nivel muy simple, ethernet funciona enviando paquetes de datos a la red (enviados usando *frames*, que incluye los datos y la dirección de donde viene y se está enviando, etiquetado

VLAN, información de corrección de errores y calidad de servicio de información).

Con una red tradicional basada en concentradores (hubs), el paquete se enviará cuando la ruta a la red sea libre. Todos los demás dispositivos de la red verifican el paquete a medida que se mueve por la red para ver si es el destinatario. Si lo son, el destinatario lo recogerá. Sin embargo, si ya hay un paquete de datos usando la red, esperará hasta que la ruta sea clara antes de enviar el paquete a la red más amplia.

El método más moderno es usar un switch/conmutador (en lugar de un concentrador/hub), ya que erradica los problemas asociados con una red –en uso**ll** porque solo envía el tráfico al puerto especificado, en lugar de a la red completa.

Debido a que ethernet contiene dos canales, significa que la ruta es mucho más eficiente que los modos alternativos de envío de paquetes de datos a través de la red.

LOS BENEFICIOS DE ETHERNET

Los principales beneficios del uso de ethernet para una LAN se deben a que es simple configurar una red.

- **No requiere ningún trabajo de construcción para su instalación,** es compatible con la mayoría de los enrutadores y dispositivos, como las computadoras portátiles (aunque es posible que se necesite un adaptador), computadoras de escritorio, impresoras y otras periferias comúnmente utilizadas en el hogar o la oficina.
- A menudo, **la conexión es más confiable** que depender de WiFi, ya que la señal de un solo enrutador puede no ser tan estable en toda la oficina.
- También es posible que obtenga **mejores velocidades** por enlace ascendente y por enlace descendente en comparación con ADSL, lo que significa que puede compartir archivos grandes más rápido entre computadoras y no usará los límites de descarga de banda ancha si no tiene un plan ilimitado.

Ethernet es la tecnología de red de área local más extendida en la actualidad, la norma IEEE 802.3 define las reglas para configurar una red Ethernet. Es una red CSMA/CD de banda base a 10

Mbps., que funciona con cableado coaxial fino y grueso, par trenzado y fibra óptica; como tecnología de red maneja dos aspectos:

- *La*
  física.
- *La*
  lógica.

La capa física y la capa de enlace de datos. La capa física describe las características físicas de la red y el hardware usado. Esta capa incluye: topología, hardware de transmisión, equipo usado, etc.

Ethernet es popular porque permite un buen equilibrio entre velocidad, costo y facilidad de instalación. Estos puntos fuertes, combinados con la amplia aceptación en el mercado y la habilidad de soportar virtualmente todos los protocolos de red populares, hacen a Ethernet la tecnología ideal para la red de la mayoría los usuarios de la informática actual.

En términos generales, *Ethernet* es un sistema para el trasporte digital de datos a través de sistemas de cómputo local. Ethernet es una tecnología de transmisión de datos de alta velocidad que fue inventada en 1973. En 1980 Digital Equipment Corporation (DEC), Intel y Xerox, desarrollaron el hardware para Ethernet a 3 Mb, el cual ganó gran aceptación en el mundo de la computación.

CARACTERISTICAS

- 10 Megabits/segundo, es la velocidad básica.

- 100 Megabits/segundo, en instalaciones TX
- 1000Megabits/segundo, tecnología prevista en breve.
- Utilización de conmutadores permite tener un ancho de banda acumulado
- ·Mayor tamaño de paquete máximo de 1400 bytes. Normalmente, solo 1024 de datos

Resumen de las características físicas de Ethernet.

Características	Valor	Valores IEEE 802.3					
	Ethernet	10Base5	10Base2	10Base5	10BaseT	100BaseTX	100BaseT4
Velocidad de los datos (Mbps)	10	10	10	1	10	100	10
Método de señalización	Banda de base	Banda de base	Banda de base	Banda de base	Banda de base	Banda de base	Banda ancha
Longitud máxima del segmento (m)	500	500	185	250	100 con pares trenzados no blindados	100 UTP o STP	1800
Soporte	Coaxial de 50-ohmios (grueso)	Coaxial de 50-ohmios (grueso)	Coaxial de 50-ohmios (fino)	Pares trenzados sin blindaje	Pares trenzados sin blindaje	Categoría 5 Pares trenzados blindados o sin blindaje	Coaxial de 75-ohmios
Topología	Bus	Bus	Bus	Estrella	Estrella	Estrella	Bus

CSMA/CD: Carrier Sense Multiple Access with Collision Detection. Acceso múltiple por detección de portadora y colisión, es el medio de comunicación físico de Ethernet. Todos los dispositivos se conectan a la red y contienden igualmente para transmitir. Si un dispositivo descubre el signo de otro dispositivo que está transmitiendo, aborta la transmisión y lo reintenta después de una breve pausa.

ESTANDAR (NORMATIVIDAD)

La norma de Ethernet fue definida por el Instituto para los Ingenieros Eléctricos y Electrónicos *(IEEE)* como IEEE Standard 802.3. Adhiriéndose a la norma de IEEE, los equipo y protocolos de red pueden interoperar eficazmente.

La velocidad de transmisión de datos en Ethernet es de 10Mbits/s en las configuraciones habituales pudiendo llegar a ser de 100Mbits/s en las especificaciones Fast Ethernet, y en la actualidad se puede encontrar el gigaethernet que maneja una velocidad de 1000Mbits/s.

Provee tasas de transmisión de 10Mbps sobre par trenzado a una distancia de hasta 100 metros sin repetidores, aunque requiere de dos cables, uno para transmitir y otro para recibir. Se pueden utilizar conectores RJ-45, aunque solo se utilizan 4 de los 8 pines. Una red se puede construir con las tarjetas de red, cable trenzado y uno o más hubs. Un hub se puede conectar a otro expandiendo la red, resultando en una red con topología de estrella físicamente, pero siendo un bus lógico. Dos estaciones no pueden estar separadas por más de 4 hubs conectados a través de 5 segmentos de cables. Se le puede dar la vuelta a este problema, interconectando varias redes, es decir, utilizando un backbone de una red 10BASE-5 o incluso una 10BASE-2.

FAST ETHERNET

Esta tecnología es un estándar abierto internacional (IEEE 802.3u), no ha sido desarrollado ni es propiedad de ninguna compañía. Este tipo de estándar abierto protege la inversión de una compañía en tecnología por asegurar un nicho de mercado flexible y competitivo. Los derechos para desarrollar, fabricar y vender productos Fast Ethernet no tienen que ser comprados o licenciados. Cualquier compañía puede desarrollar productos Fast Ethernet, favoreciendo la competitividad y la bajada de precios. Estos factores hacen que esta tecnología sea dominante en muchos entornos, pues son los mismos factores que hicieron líder en su ámbito a su predecesor Ethernet en los años 80 y principios de los 90.

Para redes Ethernet que necesitan mayores velocidades, se estableció la norma Fast Ethernet (IEEE 802.3u). Esta norma elevó los límites de 10 Megabits por segundo (Mbps.) de Ethernet a 100 Mbps, con cambios mínimos a la estructura del cableado existente.

Fast Ethernet es una tecnología LAN (Local Area Network = Red de área local) y esta diseñada para conectar computadoras sobre un área pequeña, como pueden ser oficinas, edificios o pequeñas instituciones como un campus universitario de tamaño pequeño, por ejemplo. Esta tecnología no esta pensada para ser utilizada sobre áreas extensas, como campus de gran tamaño o ciudades enteras, para estos entornos se usaran tecnologías WAN (Wide Area Network = Red de área extensa), que son sistemas diseñados para conectar elementos o LAN's ha otros elementos o LAN's sobre un área extensa. Una posible definición de LAN puede ser "Un sistema de conexión directa entre varias computadoras".

CARATERISTICAS

Fast Ethernet es una red de comunicación de datos en serie, a través de pares de cobre o fibra óptica. Su velocidad es de 100 Mbits por segundo, siendo posible la comunicación Full-Dúplex. Esto permite tasas de transferencias a la hora de recibir y enviar hasta 12.1 Mbytes por segundo y modo Full-Dúplex.

TIPÓLOGIA

Fast Ethernet usa una topología lógica (es decir, su manera de funcionar es...) de BUS, y físicamente tiene forma de estrella, con los nodos conectados a un hub (o repetidor) central. Este hub actúa como el bus de la red, además de que limpian eléctricamente la señal y permiten que, si una conexión falla, las demás sigan funcionando.

Forma de comunicación

Los nodos (Computadoras, impresoras, ...) se comunican entre ellos por medio de "frames" (marcos), su unidad básica de comunicación, que es una estructura o manera de organizar los datos, sabiendo a quien debe llegar y de quién procede.

Para lograr este objetivo, a cada nodo se le asigna una dirección única, diferente de la del resto de los nodos (MAC address), sin entrar en detalles, esta dirección se aloja en la interfaz de red de cada nodo, teniendo cada tarjeta que hay en el mercado una dirección diferente. Así, un frame se estructura en tres campos de datos, uno para la dirección de destino, otro para la dirección fuente, y un tercero donde se envían los datos en sí mismo que queremos enviar (datos del mensaje o payload).direccion de destino direccion de origen Datos del mensaje *Frame simplifcado*

La manera en la que se gestionan los frames es la siguiente, en una red compuesta por 4 nodos, A, B, C y D, si A genera un frame con destino a D, este frame es "escuchado" por B, C y D, pero solo lo acepta D, ya que B y C lo descartan porque la dirección destino del frame no es la suya (lo "filtran"), y D al ver que tiene como destino a él lo coge.

Esto tiene una consecuencia muy importante: solo un nodo puede transmitir a la vez en la red, ya que si otro emite habría problemas, para ello existe un mecanismo que implemente una serie de reglas para el acceso al medio (cable), sin profundizar demasiado, decir que se CSMA/CD:

• CS - Carrier Sense ("sentir" la portadora). ¿Hay alguién hablando?

• MA - Multiple Access (Acceso múltiple). Lo que tu oyes yo también lo oigo.

• CD - Collision Detection (detección de portadora). ¡Mira, estamos hablando a la vez

Así sería su funcionamiento:

- Si el medio está desocupado, transmitir.
- Si está ocupado, esperar.
- Si ocurre una colisión, esperar un tiempo aleatorio e ir al paso 1.

También existe una dirección especial, la dirección "broadcast", los frames con esta dirección de destino son escuchados por todos los miembros y procesados por todos ellos. Un uso típico de este uso es hacer desde un nodo una petición a todos los nodos para saber qué servicios provee cada nodo a la red y que sean accesibles desde el nodo que realizó la petición.

Otro caso particular es que un nodo entre en estado "promiscuo", es decir, procesa todos los frames que encuentra, aunque no sean para él, esto tiene una función para el diagnóstico de la red.

Protocolos

El sistema de comunicación por frames proporciona un nivel básico de comunicación (correspondiente a las capas 1 y 2 OSI, esto se explica más adelante), para que el intercambio de datos entre nodos sea útil y eficiente se utilizan una serie de reglas, llamadas protocolos.

Ejemplo: Tenemos una red formada por dos nodos, A y B, A quiere obtener un pequeño fichero de texto de B, para ello, utilizan unos tipos de frames con una estructura muy concreta para saber en todo momento que se quiere hacer:

- Abrir fichero destino origen mensaje direccion de B direccion de A Abre "datos.txt" A B abre

- Respuesta a abrir destino origen mensaje abierto B A direccion de A direccion de B Abierto "datos.txt"
- Leer fichero destino origen mensaje direccion de B direccion de A A B lee Lee "datos.txt"
- Respuesta a leer fichero destino origen mensaje B A direccion de A direccion de B texto caracteres de "datos.txt"

Se trata de una manera simple de intercambiar datos, y en realidad mecanismos semejantes se usan para transferir páginas web desde sitios de Internet al navegador (TCP/IP y HTTP).

Como se puede apreciar, los protocolos están a otro nivel lógico que los frames, estos están relacionados con el medio físico, mientras que las ordenes 1-4 son independientes del medio por el que se transmitan, esta jerarquía de protocolos y/o de funcionamiento y su abstracción entre ellas es la base de las comunicaciones (ver modelo OSI).

Tipos de Ethernet - Hay tres tipos de Fast Ethernet:

- 100BASE-TX para el uso con cable UTP de categoría 5.
- 100BASE-FX para el uso con cable de fibra óptica.
- 100BASE-T4 que utiliza un par de cables más para permitir el uso con cables UTP de categoría 3.

La norma 100BASE-TX se ha convertido en la más popular debido a su íntima compatibilidad con la norma Ethernet 10BASE-T. En cada punto de la red se debe determinar el número de usuarios que realmente necesitan las prestaciones más altas, para decidir que segmentos del troncal necesitan ser específicamente reconfigurados para

100BASE-T y seleccionar el hardware necesario para conectar dichos segmentos "rápidos" con los segmentos 10BASE-T existentes.

También conocida como THICK ETHERNET (Ethernet grueso), es la Ethernet original. Fue desarrollada originalmente a finales de los 70 pero no se estandarizó oficialmente hasta 1983.

Utiliza una topología en BUS, con un cable coaxial que conecta todos los nodos entre sí. En cada extremo del cable tiene que llevar un terminador. Cada nodo se conecta al cable con un dispositivo llamado transceptor.

El cable usado es relativamente grueso (10mm) y rígido. Sin embargo es muy resistente a interferencias externas y tiene pocas pérdidas. Se le conoce con el nombre de RG8 o RG11 y tiene una impedancia de

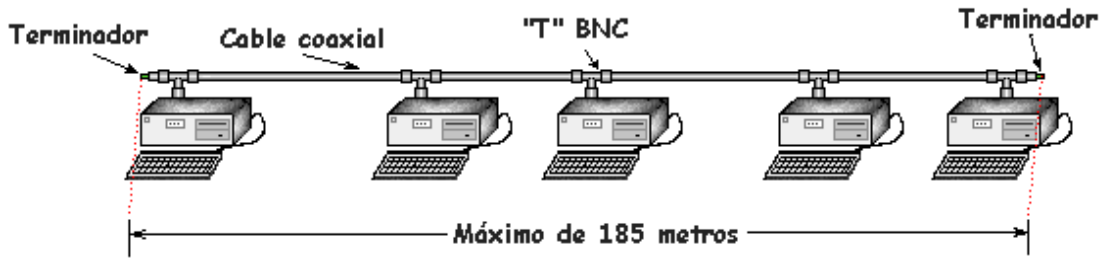
50 ohmios. Se puede usar conjuntamente con el 10 Base-2.

En la mayoría de los casos, el costo de instalación del coaxial y los transceptores de las redes

10 Base-5 las hacía prohibitivas, lo que indujo la utilización de un cable más fino y, por tanto. más barato, que además no necesitaba transceptores insertados en él. Se puede decir que 10

Base-2 es la versión barata de 10 Base-5. Por esto, también se le conoce Thin Ethernet

(Ethernet fino) o *cheaper-net(red barata)*.



}

Tipología de redes

Una topología describe la relación geográfica de los nodos de la red. Las tres topologías mas usadas son: *Estrella, Anillo y de Bus*.

Topología de Estrella

La topología de Estrella es una buena elección siempre que se tenga varias unidades dependientes de un procesador, esta es la situación de una típica mainframe, donde el personal requiere estar accesando frecuentemente esta computadora. En este caso, todos los cables están conectados hacia un solo sitio, esto es, un panel central.

Equipo como unidades de multiplexaje, concentradores y pares de cables solo reducen los requerimientos de cableado, sin eliminarlos y produce alguna economía para esta topología. Resulta económica la instalación de un nodo cuando se tiene bien planeado s u establecimiento, ya que este requiere de un cable desde el panel central, hasta el lugar donde se desea instalarlo. Con esta topología, se reduce al máximo una posible falla en la red, ya que cuando ocurre una falla un nodo, afecta mínimamente al resto de la red.

> De hecho, la tecnología de par trenzado de Ethernet usa esta topología, los concentradores, proveen múltiples puertos que están conectados con cable telefónico estándar.

Topología de anillo

La topología de anillo está diseñada como una arquitectura circular, con cada nodo conectado directamente a otros dos nodos. Toda la información de la red pasa a través de

cada nodo hasta que es tomado por el nodo apropiado. Este esquema de cableado mues tra alguna economía respecto al de estrella. El anillo es fácilmente expandido para conectar mas nodos, aunque en este proceso interrumpe la operación de la red mientras se instala el nuevo nodo.

Así también, el movimiento físico de un nodo requiere de dos pasos separados: desconectar para remover el nodo y otra vez reinstalar el nodo en su nuevo lugar.

La tecnología óptica FDDI está basada en una topología dual de nanillo.

Topología de Bus

El diseño de bus es una arquitectura abierta, flexible y robusta. Todos los nodos conectados en paralelo en una sección del cable. Una o más secciones acopladas, y los nodos, forman un solo segmento de red. El bus es la parte básica para la construcción de redes Ethernet y generalmente consiste de algunos segmentos de bus unidos ya sea por razones geográficas, administrativas u otras.

Como la topología de bus es un diseño en paralelo, nuevos nodos pueden ser instalados en alguna parte sin afectar la comunicación.

El bus principal también puede ser expandido en sus puntos finales con una mínima afección y nuevas secciones pueden ser insertadas en la parte media de algún segmento.

LOS ESTADOS DEL PROTOCOLO SPANNING TREE

Los estados del protocolo Spanning Tree son los siguientes:

- Bloquear: Ninguna trama enviada, se escuchan BPDU
- Escuchar: Ninguna trama enviada, escuchar tramas.
- Aprender: Ninguna trama se envía, aprender direcciones.

- Enviar: Tramas enviadas, aprender direcciones.
- Desactivado: Ninguna trama enviada, no se escuchan BPDU

TECNOLOGÍA DE SERVIDOR DELGADO

Dataquest ha descrito a un servidor delgado como "un dispositivo especial basado en hardware diseñado para realizar una sola o un especializado conjunto de funciones con acceso de clientes independientemente del sistema operativo o protocolo propietario". Servidores de terminales, impresoras y recientemente los servidores de terminales de un solo puerto serie (Lantronix los denomina servidores delgados universales) se incluyen en esta noción de independencia de los protocolos propietarios y la habilidad de servir para varias funciones diferentes. La aplicación del controlador de RAID discutida anteriormente, es una de las muchas aplicaciones donde estos servidores delgados universales pueden usarse para poner cualquier dispositivo o "cosa" en la red. El reciente desarrollo del servidor delgado universal de un solo puerto serie hace económicamente posible conectar a la red incluso dispositivos únicos con puertos serie - antes de este desarrollo, los usuarios tenían sólo soluciones multipuerto que a veces eran demasiado caras cuando los dispositivos serie estaban muy lejanos y separados.

Podría alguien hacer la pregunta, ¿pero no han sido usados PC's dedicados para conectar a una red algunos dispositivos serie con éxito? La respuesta a esto sería algo así como un "sí cualificado" - cualificado porque requirió al diseñador del producto con el puerto serie disponer de un software capaz de ejecutarse en el PC y entonces tener una aplicación software que permitiera al PC estar conectando a una red para acceder a la aplicación. ¡Esta tarea sería algo semejante a los problemas de poner Ethernet en el propio dispositivo serie! Para tener éxito, un servidor delgado debe ofrecer una solución simple conectando a una red un dispositivo y permitir el acceso a dicho dispositivo como si estuviera localmente disponible a través de su puerto serie. Adicionalmente, el servidor delgado debe mantener la multitud de posibilidades de conexión que un

dispositivo puede requerir en ambos lados de la red y de la conexión serie. ¿Debe conectarse el dispositivo todo el tiempo a un servidor específico o PC?

2.3 Conmutación en redes LAN

Un switch es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento de la red, problemas de congestión y embotellamientos. El switch puede agregar mayor ancho de banda, acelerar la salida de tramas, reducir tiempo de espera y actualmente el costo por puerto tiende a bajar (costo económico). Opera generalmente en la capa 2 del modelo OSI4 (también existen de capa 3 y últimamente multicapas), reenvía las tramas en base a la dirección MAC5.

La Tecnología basada en switch denominada también LAN Switching, ofrece métodos eficaces para optimizar sustancialmente el uso del ancho de banda de una red (proporciona gran cantidad de ancho de banda agregado) al asignar un ancho de banda dedicado a cada equipo terminal a diferencia de una red LAN compartida. Reduce los cuellos de botella, además de contar con una velocidad de reenvió de tramas muy elevada (baja latencia6), soporte a conexiones full dúplex, soporte de conexiones 10/100/1000 Mbps. (Megabits por segundo) y con un coste económico muy bajo por puerto del switch.

Si un equipo terminal envía un mensaje a otro de la red mediante el switch, este solo será enviado al equipo receptor y no así a toda la red (como lo hacen los Hubs), evitando colisiones en ese instante con otros equipos7.

Una red 10BaseT8 conmutada con 20 equipos, cuenta con 10Mbps. cada equipo, teniendo entonces una capacidad de tráfico total de 200Mbps. En caso de usar 100BaseT9 se tendría con 20 equipos además de contar con comunicación full dúplex (2000 * 2) una capacidad de

4000Mbps. de rendimiento total (Throughput10), en el mejor de los casos.

ALMACENAR Y ENVIAR (STORE AND FORWARD), la trama completa es recibida en los buffers del switch, se hace una comprobación de redundancia cíclica (CRC) para verificar tramas corruptas, si se encuentra un error la trama es descartada (trama corrupta). También son descartadas las tramas pequeñas (runt, menores a 64 bytes), o las tramas grandes (giant, mayores a 1518 bytes). Si la trama no contiene ningún error se obtiene la dirección MAC destino, buscándola en la tabla de filtrado de direcciones, para ser reenviada. Soporta distintas velocidades en los puertos del switch.

CORTAR Y ENVIAR (CUT-THROUGH), el switch empieza a retransmitir la trama antes de recibirla por completo. Obtiene solo la dirección MAC origen de la trama, esta es buscada en la tabla de filtrado de direcciones, para ser reenviado. No realiza la comprobación de redundancia cíclica, tampoco una verificación de tramas runt ni giant. La latencia del switch es reducida. Es más usado en redes que operan a una misma velocidad.

CORTAR Y ENVIAR MODIFICADO (FRAGMENTFREE, CUT-THROUGH MODIFICADO), en vez de tomar como el cut-through solo la dirección MAC (6 bytes), este toma los primeros

64 bytes. Evita tramas runts (resultado de colisiones), desechándolos. No controla tramasgiants. Es también conocida como `Bus´, es la que conecta todos los puertos del switch internamente (en el switch).

El switch internamente es como una red en miniatura, donde cada puerto se comunica con los demás y maneja mucho tráfico entre ellos. En el switch el ancho de banda interno determina el rendimiento individual de todos sus puertos. Existen 2 arquitecturas utilizadas para su implementación.

a. Bus, es un bus interno de muy alta velocidad (arriba de los 3 Gbps.), pero compartido.

b. Múltiples Buses (Crossbar), la matriz de conmutación es realmente un conmutador o switch.

Redes LAN compartidas

Las redes LAN son aquellas redes LAN que comparten el ancho de banda entre todos sus equipos terminales. En una LAN compartida, los usuarios comparten un único canal de comunicación, de modo que todo el ancho de banda de la red es asignada al equipo emisor de información, quedando el resto de equipos en situación de espera.

Son denominados redes LAN compartidas a aquellas que hacen uso de Hubs, con o sin salida hacia otras redes mediante enrutadores (Reuters) o switches de capa 3 con capacidad de enrutador.

Una red de 10BaseT con 20 equipos cuenta entonces con un aproximado de 0.5 Mbps. (10Mbps. / 20 Equipos) asignado a cada equipo, tomando como caso una red donde equipos terminales desean transmitir datos por la red. La disminución de ancho de banda hace que aplicaciones como por ejemplo multimedia no puedan realizarse de buena manera, además de que con el tiempo ciertas aplicaciones tenderán a hacer uso de una gran parte del ancho de banda llegando a un límite de ancho restringido y notándose claramente el retardo de la comunicación entre equipos emisor y receptor.

Conmutacion en redes Ethernet

La conmutación es el proceso por el cual un router o un switch, reciben un paquete por una interfaz y lo reenvían a otra interfaz concreta.

La función más importante que realiza la conmutación Ethernet es la de encapsular los paquetes en el tipo de trama de enlace de datos correcto para el enlace de datos de salida.

Conmutacion Ethernet nivel

Según (mailxmail, 2015)Los conmutadores poseen la capacidad de aprender y almacenar las direcciones de red de nivel 2 de los dispositivos alcanzables a través de cada uno de sus puertos. (mailxmail, 2015). Esto permite que la información dirigida a un dispositivo, vaya desde el puerto origen al puerto destino.

BRIDGE

- Un Bridge es un dispositivo que interconecta y transfiere tramas entre dos o más segmentos de una LAN.
- Guarda una tabla de direcciones MAC y sus puertos asociados. Así, el puente envía o descarta tramas basándose en las entradas de su tabla.
- Todas las decisiones que toma el puente se basan en direcciones MAC de capa 2, y no afecta al direccionamiento lógico de capa 3
- Un puente dividirá un dominio de Colisión, pero no tiene efecto sobre un dominio lógico o de Brocadas

SWITCH :

•Es un bridge rápido multipuesto, que, en vez de crear 2 dominios de colisión, en cada puerto crea su propio dominio de Colisión.

•Las tramas se envían solo a través del puerto correspondiente. Si no se conoce la dirección destino, la trama se reenvía a través de todos los puertos.Al ser Ethernet un medio compartido (solo un nodo puede transmitir datos a la vez), cuantos más equipos haya en un segmento de red, más posibilidades hay de que ocurran colisiones.

Por tanto, el hecho de segmentar la red, evita esa retransmisión de colisiones.

Podemos segmentar a nivel de capa 2 (Switch), donde encontramos dominios de Colisión y a nivel de capa 3 (Routers), donde encontramos dominios de Broadcast.

DOMINIO DE COLISIÓN

Según (eltallerdelbit, 2009) dijo que si definimos Dominio de Colisión como el segmento de red física donde pueden ocurrir colisiones entre los equipos conectados a ese segmento de red.

Los dispositivos de capa 1 no dividen los dominios de colisión. (eltallerdelbit, 2009). Los dispositivos de capa 2 y 3 sí lo hacen.

Ethernet se implementa en capa 1 y capa 2. Sobre todo en la mitad inferior de la capa de enlace de datos, que es conocida como subcapa Control de acceso al medio (Media Access Control, MAC), y la capa física.

La subcapa Control de enlace lógico (Logical Link Control, LLC) sigue siendo relativamente independiente del equipo físico que se utilizará para el proceso de comunicación. (eltallerdelbit,2009).

DOMINIO DE BROADCAST:

Para comunicarse con todos los Dominios de Colisión, los nodos en la red envían tramas con dirección MAC destino 0xFFFFFFFFFFFF

Esta es una dirección a la que debe responder una
NIC.

Esto implica, que al haber dispositivos de capa 2, estos pueden inundar la red con las retransmisiones de Broadcast, formando así una tormenta de Broadcast

Las causas de esto pueden ser equipos, el uso de NetBIOS, el uso de ARP, aplicaciones multicast. Un dominio de Broadcast es un grupo de dominios de colisión conectados por dispositivos de capa 2 y delimitados por dispositivos de capa 3.

Funcionamiento:

– Se establece una conexión física permanente entre las estaciones durante la comunicación.

– Fases:

- Establecimiento del circuito: realización de llamada, realización de conexiones en los nodos.
- Transferencia de datos: normalmente en ambos sentidos (full-dúplex)
- Desconexión: liberación de recursos

2.4 Uso de los puentes

Antes de entrar de lleno a la tecnología de los puentes, veamos algunas situaciones comunes en las cuales se utilizan los puentes. Mencionaremos tres razones por las cuales una sola organización podría terminar trabajando con varias LAN.

En primer lugar, muchas universidades y departamentos corporativos tienen sus propias redes LAN para conectar sus propias computadoras personales, servidores y dispositivos como impresoras. Dado que los objetivos de los distintos departamentos difieren, los distintos departamentos pueden establecer dife- rentes redes LAN, sin importarles lo que hagan los demás departamentos. Pero tarde o temprano surge la necesidad de interacción, y aquí es donde entran los puentes. En este ejemplo surgieron múltiples redes LAN debido a la autonomía de sus propietarios.

En segundo lugar, la organización puede estar distribuida geográficamente en varios edificios, sepa- rados por distancias considerables. Puede ser más económico tener redes LAN independientes en

cada edificio y conectarlas mediante puentes y unos cuantos enlaces de fibra óptica de larga distancia que ten- der todos los cables hacia un solo switch central. Incluso si es fácil tender los cables, existen límites en cuanto a sus longitudes (por ejemplo, 200 m para Gigabit Ethernet de par trenzado). La red no funcionaría con cables más largos debido a la excesiva atenuación de la señal, o al retardo de viaje redondo. La única solución es dividir la LAN e instalar puentes para unir las piezas y poder incrementar la distancia física total que se puede cubrir.

En tercer lugar, tal vez sea necesario dividir lo que por lógica es una sola LAN en varias redes LAN individuales (conectadas mediante puentes) para manejar la carga. Por ejemplo, en muchas universida- des grandes, hay miles de estaciones de trabajo disponibles para los estudiantes y el cuerpo docente. Las empresas también pueden tener miles de empleados. La escala de este sistema hace imposible poner todas las estaciones de trabajo en una sola LAN; hay muchas más computadoras que puertos en cualquier hub Ethernet y más estaciones de lo que se permite en una sola Ethernet clásica.

Incluso si fuera posible cablear todas las estaciones de trabajo juntas, al colocar más estaciones en un hub Ethernet o en una red Ethernet clásica no se agrega capacidad. Todas las estaciones comparten la misma cantidad fija de ancho de banda. Entre más estaciones haya, menor será el ancho de banda prome- dio por estación.

Sin embargo, dos redes LAN separadas tienen el doble de la capacidad de una sola LAN. Los puentes permiten unir redes LAN y mantener al mismo tiempo esta capacidad. La clave es no enviar tráfico a los puertos en los que no se necesita, de modo que cada LAN pueda operar a toda velocidad. Este comporta- miento también aumenta la confiabilidad, ya que en una sola LAN, un nodo defectuoso que siga transmi- tiendo un flujo continuo de basura puede llegar a obstruir toda la LAN completa. Al decidir qué reenviar o no, los puentes actúan como puertas contra incendios en un edificio, pues evitan que un solo nodo errático haga fallar todo el sistema.

Para que estos beneficios pudieran estar fácilmente disponibles, los puentes ideales tendrían que ser totalmente transparentes. Debería ser posible comprar los puentes, conectar los cables de LAN en los puentes y que todo funcionara a la perfección en un instante. No debería existir la necesidad de cambios de hardware o de software, ni de configurar switches de direcciones o descargar tablas de enrutamiento o parámetros, nada de eso. Simplemente conectar los cables y seguir con nuestras actividades cotidianas. Lo que es más, la operación de las redes LAN existentes no se debería ver afectada por los puentes para nada. En cuanto a las estaciones, no debería haber ninguna diferencia

observable en cuanto a si son parte o no de una LAN con puente. Debería ser igual de fácil mover estaciones alrededor de una LAN con puente que moverlas en una sola LAN.

2.5 Puentes de aprendizaje

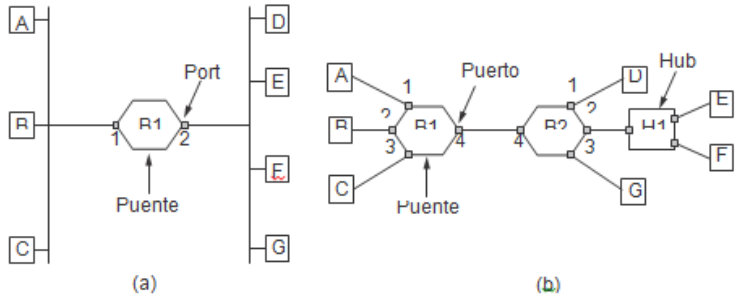
La topología de dos redes LAN conectadas por un puente se muestra en la figura 4-41 para dos casos. En el lado izquierdo, dos redes LAN multiderivación (por ejemplo, redes Ethernet clásicas) se unen me- diante una estación especial (el puente) que se sitúa entre ambas redes LAN. Del lado derecho, se unen redes LAN con cables punto a punto, incluyendo un hub. Los puentes son los dispositivos a los que se conectan las estaciones y el hub. Si la tecnología de LAN es Ethernet, los puentes son mejor conoci- dos como switches Ethernet.

Los puentes se desarrollaron cuando se usaban redes Ethernet clásicas, por lo que a menudo se mues- tran en topologías con cables multiderivación, como en la figura 4-41(a). Sin embargo, todas las topolo- gías en la actualidad están compuestas de cables punto a punto y switches. Los puentes funcionan de la misma forma en ambas configuraciones. Todas las estaciones conectadas al mismo puerto en un puente pertenecen al mismo dominio de colisión, y éste es distinto al dominio de colisión para otros puertos. Si hay más de una estación, como en una red Ethernet clásica, un hub o un enlace half-dúplex, se utiliza el protocolo CSMA/CD para enviar tramas.

Sin embargo, hay una diferencia en cuanto a la forma en que se construyen las redes LAN con puentes. Para conectar redes LAN multiderivación con puentes, se agrega un puente como una nueva estación en cada LAN multiderivación, como en la figura 4-41(a). Para conectar redes LAN punto a punto mediante puentes, los hubs se conectan a un puente o, lo que es preferible, se reemplazan con un puente para incrementar el desempeño. En la figura 4-41(b) los puentes reemplazaron a todos los hubs excepto uno.

También se pueden conectar distintos tipos de cables a un puente. Por ejemplo, el cable que conecta el puente B1 con el puente B2 en la figura 4-41(b) podría ser un enlace de fibra óptica de larga distancia, mientras que el cable que conecta los puentes con las estaciones podría ser una línea de par trenzado de corta distancia. Esta disposición es útil para conectar redes LAN mediante puentes en distintos edi- ficios.

Ahora consideremos lo que ocurre dentro de los puentes. Cada puente opera en modo promiscuo; es decir, acepta cada una de las tramas que transmiten las estaciones conectadas a cada uno de sus puertos.



El puente debe decidir si va a reenviar o desechar cada trama y, en caso de que sea la primera opción, también debe decidir por qué puerto enviar la trama. Esta decisión se basa en la dirección de destino. Como ejemplo, considere la topología de la figura 4-41(a). Si la estación A envía una trama a la estación B, el puente B1 recibirá la trama en el puerto 1. Esta trama se puede desechar de inmediato sin más preámbulos, debido a que ya se encuentra en el puerto correcto. Sin embargo, suponga que en la topología de la figura 4-41(b) la estación A envía una trama a D. El puente B1 recibirá la trama en el puerto 1 y la enviará por el puerto

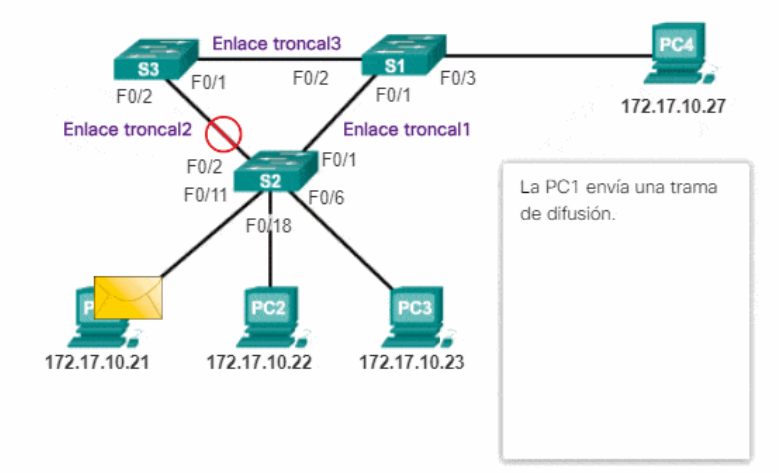
4. Después el puente B2 recibirá la trama en su puerto 4 y la enviará por el puerto 1.

Una forma simple de implementar este esquema es mediante una gran tabla (hash) dentro del puente. La ta- bla puede listar cada posible destino y a qué puerto de salida pertenece. Por ejemplo, en la figura 4-41(b), la tabla en B1 listaría a D como perteneciente al puerto 4, ya que todo lo que B1 tiene que saber es por qué puerto enviar las tramas para llegar a D. El que, de hecho, se lleven a cabo más reenvíos posteriormente cuando la trama llegue a B2 no es de interés para B1.

Cuando se conectan por primera vez los puentes, todas las tablas de hash están vacías. Ninguno de los puentes sabe dónde se encuentran los destinos, por lo que utilizan un algoritmo de inundación: todas las tramas que llegan con un destino desconocido se envían por todos los puertos a los que está conectado el puente, excepto por el que llegaron. Con el paso del tiempo, los puentes aprenden dónde están los des- tinos. Una vez conocido un destino, las tramas destinadas para él se colocan sólo en el puerto apropiado; no se inundan

2.6 Puentes con árbol de expansión

El protocolo de árbol de extensión (STP) protege los dominios de difusión de capa 2 de las tormentas de difusión. Establece los links en modo de espera para evitar loops. Los loops ocurren cuando existen rutas alternativas entre los hosts. Estos bucles en una red extendida pueden hacer que los switches de Capa 2 reenvíen tráfico una cantidad infinita de veces, lo que da lugar a una mayor carga de tráfico y a una menor eficiencia de la red. STP proporciona una topología de árbol para cualquier arreglo de links y switches de Capa 2 mediante la creación de una ruta única entre estaciones finales en una red. Estas rutas individuales eliminan la posibilidad de loops. El usuario en un escenario en tiempo real puede configurar el STP para evitar loops y, por lo tanto, evitar un gran flujo de tráfico de ida y vuelta en la red. Este documento explica cómo configurar STP en los switches apilables de la serie Sx500.



2.7 Repetidores

Un repetidor es un dispositivo electrónico que recibe una señal débil o de bajo nivel y la retransmite a una potencia o nivel más alto, de tal modo que se puedan cubrir distancias más largas sin degradación o con una degradación tolerable.

En telecomunicaciónes, el término repetidor tiene los siguientes significados normalizados:

• Un dispositivo analógico que amplifica una señal de entrada, independientemente de su naturaleza (analógica o digital).

• Un dispositivo digital que amplifica, conforma, retemporiza o lleva a cabo una combinación de cualquiera de estas funciones sobre una señal digital de entrada para su retransmisión.

En el caso de señales digitales el repetidor se suele denominar regenerador porque, de hecho, la señal de salida es una "señal regenerada" a partir de la de entrada.

En el modelo de referencia OSI, el repetidor opera en el nivel físico. Los repetidores se utilizan a menudo en los cables transcontinentales y transoceánicos porque la atenuación (pérdida de señal) en tales distancias sería completamente inaceptable sin ellos. Los repetidores se utilizan tanto en cables de cobre portadores de señales eléctricas como en cables de fibra óptica portadores de luz. Los repetidores se utilizan también en los servicios de radiocomunicación. Un subgrupo de estos son los repetidores usados por los radioaficionados. Asimismo, se utilizan repetidores en los enlaces de telecomunicación punto a punto mediante radioenlaces que funcionan en el rango de las microondas, como los utilizados para distribuir las señales de televisión entre los centros de producción y los distintos emisores o los utilizados en redes de telecomunicación para la transmisión de telefonía. Los repetidores telefónicos consisten en un receptor (auricular) acoplado mecánicamente a un micrófono de carbón, fueron utilizados antes de la invención de los amplificadores electrónicos dotados de tubos de vacío. En comunicaciones ópticas el término repetidor se utiliza para describir un elemento del equipo que recibe una señal óptica, la convierte en eléctrica, la regenera y la retransmite de nuevo como señal óptica.

Dado que estos dispositivos convierten la señal óptica en eléctrica y nuevamente en óptica, estos dispositivos se conocen a menudo como repetidores electro-ópticos. 0.1 Repetidor wifi Un repetidor wifi o también llamado amplificador wifi cumple con las características de funcionalidad de un repetidor por lo que recoge la señal que recibe y la amplifica con el fin de ampliar el rango de la señal. La peculiaridad de estos dispositivos es que están destinados a propagar la señal wifi recibida por parte de un emisor, habitualmente suele ser un router wireless.

2.8 Puerta de enlace

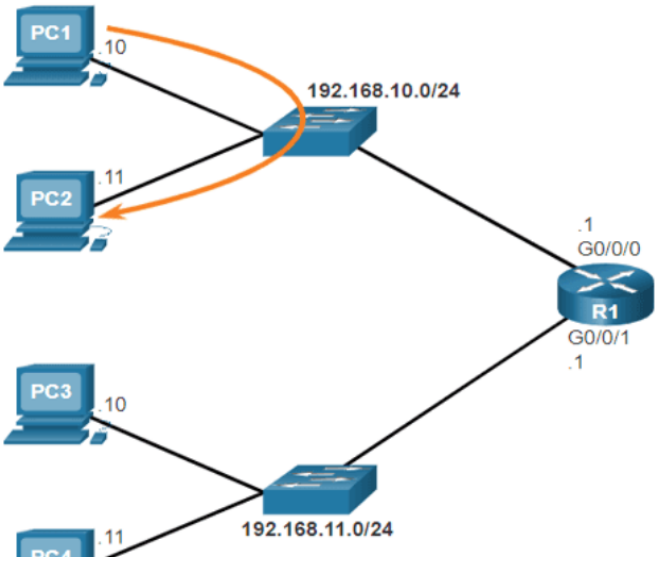
Si tu red local sólo tiene un Router, será el Router de puerta de enlace y todos los hosts y switches de su red deben estar configurados con esta información. Si la red local tiene varios routers, debes

seleccionar uno de ellos para que sea el router de puerta de enlace predeterminado. En este tema se explica cómo configurar la puerta de enlace predeterminada en hosts y switches.

Para que un dispositivo final se comunique a través de la red, debe configurarse con la información de dirección IP correcta, incluida la dirección de puerta de enlace predeterminada. La puerta de enlace predeterminada solo se usa cuando el host desea enviar un paquete a un dispositivo en otra red. La dirección de la puerta de enlace predeterminada es generalmente la dirección de la interfaz del Router conectada a la red local del host. La dirección IP del dispositivo host y la dirección de la interfaz del Router deben estar en la misma red.

Por ejemplo, imagna una topología de red IPv4 que consiste en un Router que interconecta dos LAN separadas. G0/0/0 está conectado a la red 192.168.10.0, mientras que G0/0/1 está conectado a la red 192.168.11.0. Cada dispositivo host está configurado con la dirección de puerta de enlace predeterminada apropiada.

En este ejemplo, si la PC1 envía un paquete a la PC2, no se usa la puerta de enlace predeterminada. En cambio, la PC1 direcciona el paquete con la dirección IPv4 de la PC2 y reenvía el paquete directamente a la PC2 a través del Switch.



¿Qué pasa si la PC1 envió un paquete a la PC3? PC1 direccionará el paquete con la dirección IPv4 de PC3, pero reenviará el paquete a su puerta de enlace predeterminada, que es la interfaz G0/0/0 de R1. El Router acepta el paquete y accede a su tabla de enrutamiento para determinar que G0/0/1

es la interfaz de salida adecuada según la dirección de destino. R1 luego reenvía el paquete fuera de la interfaz apropiada para llegar a PC3.

Puerta de Enlace Predeterminada en un Switch

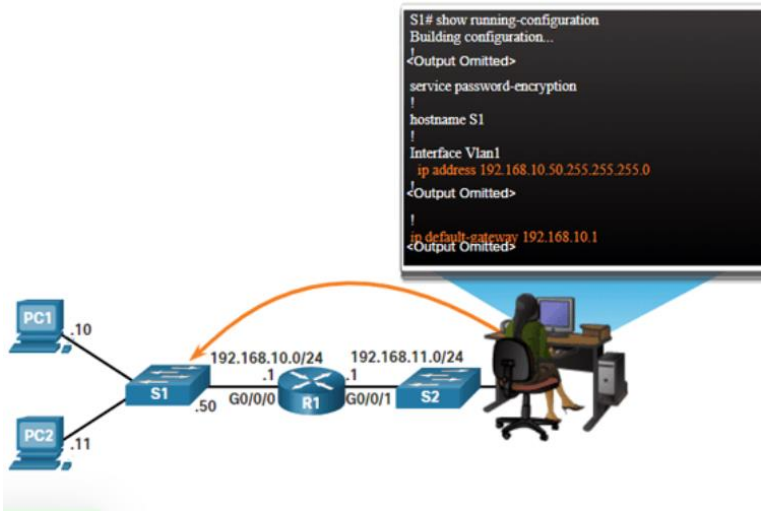
Un Switch que interconecta computadoras cliente es típicamente un dispositivo de Capa 2. Como tal, un Switch de capa 2 no requiere una dirección IP para funcionar correctamente. Sin embargo, se puede configurar una configuración de IP en un Switch para dar a un administrador acceso remoto al Switch.

Para conectarse y administrar un Switch a través de una red IP local, debe tener una interfaz virtual de Switch (SVI) configurada. El SVI está configurado con una dirección IPv4 y una máscara de subred en la LAN local. El Switch también debe tener una dirección de puerta de enlace predeterminada configurada para administrar de forma remota el Switch desde otra red.

La dirección de puerta de enlace predeterminada generalmente se configura en todos los dispositivos que se comunicarán más allá de su red local.

Para configurar una puerta de enlace predeterminada IPv4 en un Switch, use el comando de configuración global ip default-gateway ip-address . La dirección IP configurada es la dirección IPv4 de la interfaz del Router local conectada al Switch.

La imagen muestra un administrador que establece una conexión remota para cambiar S1 en otra red.



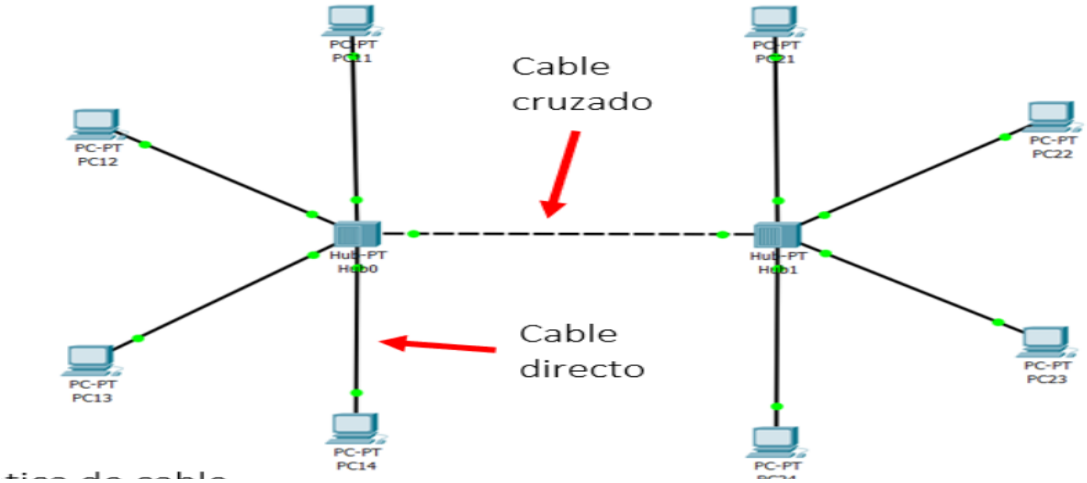
En este ejemplo, el host administrador usaría su puerta de enlace predeterminada para enviar el paquete a la interfaz G0/0/1 de R1. R1 reenviaría el paquete a S1 fuera de su interfaz G0/0/0. Debido a que la dirección IPv4 de origen del paquete provenía de otra red, S1 requeriría una puerta de enlace predeterminada para reenviar el paquete a la interfaz G0/0/0 de R1. Por lo tanto, S1 debe configurarse con una puerta de enlace predeterminada para poder responder y establecer una conexión SSH con el host administrativo.

2.9 Concepto de Hub

El hub es el dispositivo más sencillo de todos. Un Hub tiene la función de interconectar los ordenadores de una red local. Comparado con el switch y el router, es mucho más simple, ya que sólo se dedica a recibir datos procedentes de un ordenador para transmitirlo a los demás. Digamos que se trata de un punto central de conexión en una red. Normalmente son usados para conectar segmentos de una red LAN a través de sus diferentes puertos. "Cuando un paquete es recibido en un puerto, es copiado a todos los demás puertos, para que cualquier nodo conectado a la red pueda verlo"

En el momento en que esto ocurre, ningún switch puede enviar una señal. Su liberación surge después que la señal anterior haya sido completamente distribuida.

Específicamente, los hubs se utilizan para la creación de redes locales con topología tipo estrella, en los cuáles se interconectan el resto de los equipos, así como para realizar análisis de redes, ya que al solamente repetir y repartir los mismos datos, se puede analizar fácilmente el tráfico e información que fluye por la red.



La configuración IP es la siguiente:

PC11: 192.168.1.1

PC12: 192.168.1.2

PC13: 192.168.1.3

PC14: 192.168.1.4

PC21: 192.168.2.1

PC22: 192.168.2.2

PC23: 192.168.2.3

PC24: 192.168.2.4

La máscara de red es la misma en todos los PC: 255.255.255.0

2.10 Concepto de router

Los routers guían y dirigen los datos de red mediante paquetes que contienen varios tipos de datos, como archivos, comunicaciones y transmisiones simples como interacciones web.

Los paquetes de datos tienen varias capas o secciones; una de ellas transporta la información de identificación, como emisor, tipo de datos, tamaño y, aún más importante, la dirección IP (protocolo de Internet) de destino. El router lee esta capa, prioriza los datos y elige la mejor ruta para cada transmisión.

Los routers también pueden proporcionar seguridad. El software de firewall y filtrado de contenido integrado proporciona una protección adicional contra el contenido no deseado y los sitios web maliciosos, sin que esto afecte la experiencia en línea.

No obstante, un router no solo sirve para la transmisión de datos o las conexiones a Internet. La mayoría de los routers permiten conectar discos duros y usarlos como servidores de uso compartido de archivos, o impresoras a las que pueden acceder todos los usuarios de la red.

Tipos de routers

Router principal

Los routers principales son los que suelen usar los proveedores de servicios (es decir, AT&T, Verizon, Vodafone) o los proveedores de la nube (es decir, Google, Amazon, Microsoft). Proporcionan el máximo ancho de banda para conectar routers o switches adicionales. La mayoría de las empresas no necesitan routers principales. Pero las empresas muy grandes que tienen muchos empleados que trabajan en varios edificios o ubicaciones pueden usar los routers principales como parte de la arquitectura de red.

Router perimetral

Un router perimetral, también llamado router de puerta de enlace o "puerta de enlace" para abreviar, es el punto de conexión más externo de la red con las redes externas, incluida Internet.

Los routers perimetrales están optimizados para el ancho de banda y están diseñados para conectarse a otros routers a fin de distribuir los datos a los usuarios finales. Los routers perimetrales no suelen ofrecer Wi-Fi ni la capacidad de administrar redes locales de manera completa. Por lo general, solo tienen puertos Ethernet; una entrada para conectarse a Internet y varias salidas para conectar otros routers.

Los términos router perimetral y módem se usan casi de manera indistinta, aunque el segundo término ya no suelen usarlo con frecuencia los fabricantes ni los profesionales de TI para referirse a los routers perimetrales.

Router de distribución

Un router de distribución o router interior recibe datos del router perimetral (o la puerta de enlace) mediante una conexión cableada y los envía a los usuarios finales, por lo general por Wi-Fi, aunque el router también suele incluir conexiones físicas (Ethernet) para conectar usuarios o routers adicionales.

Router inalámbrico

Los routers inalámbricos o puertas de enlace residenciales combinan las funciones de los routers perimetrales y los routers de distribución. Estos routers son comunes en las redes domésticas y para el acceso a Internet.

La mayoría de los proveedores de servicios proporcionan routers inalámbricos con funciones completas como equipo estándar. Aunque tenga la opción de usar el router inalámbrico del ISP en su pequeña empresa, puede que prefiera usar un router de nivel empresarial para aprovechar el mejor rendimiento inalámbrico, los mayores controles de conectividad y la seguridad.

Router virtual

Los routers virtuales son programas de software que permiten virtualizar algunas funciones del router en la nube para prestarlas como servicio. Estos routers son ideales para las grandes empresas con necesidades de red complejas. Ofrecen flexibilidad, escalabilidad simple y menor costo de entrada. Otra ventaja de los routers virtuales es la reducción de la carga de administración de hardware de red local.

CONFIGURACIÓN BÁSICA ROUTER

Router#erase startup-config

R1(config)#no ip domain-lookup

R1(config-line)#enable password cisco

R1(config)#line console 0

R1(config-line)#password cisco

R1(config-line)#logging synchronous

R1(config)#line vty 0 4

R1(config-line)#password cisco

R1(config-line)#logging synchronous

R1(config)#banner login «Personal autorizado»

R1(config)#banner motd «Revision 1»

CONFIGURACIÓN VLAN EN ROUTER

R1(config)#interface FastEthernet0/1

R1(config-if)#no shutdown

R1(config)#interface f0/1.10

R1(config-subif)#encapsulation dot1Q 10

R1(config-subif)#ip address 192.168.10.1 255.255.255.0

R1(config-subif)#exit

R1(config)#interface f0/1.12

R1(config-subif)#encapsulation dot1Q 12

R1(config-subif)#ip address 10.12.12.1 255.255.255.0

R1(config-subif)#exit

R1(config)#interface f0/1.13

R1(config-subif)#encapsulation dot1Q 13

R1(config-subif)#ip address 10.13.13.1 255.255.255.0

R1(config-subif)#exit

R1(config)#interface s0/0/0

R1(config-if)#ip address 10.1.1.1 255.255.255.252

R1(config-if)#clock rate 64000

R1(config-if)#no shutdown

R1(config-subif)#exit

R1#copy running-config startup-config

R2(config)#interface fa 0/1

R2(config-if)#no shutdown

R2(config)#interface fa0/1.12

R2(config-subif)#encapsulation dot1Q 12

R2(config-subif)#ip address 10.12.12.2 255.255.255.0

R2(config)#interface fa0/1.20

R2(config-subif)#encapsulation dot1Q 20

R2(config-subif)#ip address 192.168.20.1 255.255.255.0

R2(config)#interface s0/0/0

R2(config-if)#ip address 10.1.1.2 255.255.255.252

R2(config-if)#no shutdown

R2(config)#interface s0/0/1

R2(config-if)#ip address 10.2.2.1 255.255.255.252

R2(config-if)#no shutdown

R2#copy running-config startup-config

R3(config)#interface fa 0/1

R3(config-if)#no shutdown

R3(config)#interface fa0/1.13

R3(config-subif)#encapsulation dot1Q 13

R3(config-subif)#ip address 10.13.13.3 255.255.255.0

R3(config)#interface fa0/1.30

R3(config-subif)#encapsulation dot1Q 30

R3(config-subif)#ip address 192.168.30.1 255.255.255.0

R3(config)#interface s0/0/1

R3#copy running-config star

R3(config-if)#ip address 10.2.2.2 255.255.255.252

R3(config-if)#no shutdown

_____

VERIFICACIONES

R1#show ip route

R1#show ip interface

R1#show interfaces fa0/1

2.11 Conceptos de switches.

Switch es un dispositivo que permite que la conexión de computadoras y periféricos a la red para que puedan comunicarse entre sí y con otras redes.

Switch es una palabra en inglés usada en el área de informática para referirse al controlador de interconexión entre varios dispositivos. En este sentido, *switch* se traduce en español como conmutador. Los *switches* se utilizan para conectar varios dispositivos a través de la misma red. De esta manera, un *switch* puede conectar varias computadoras,

impresoras y servidores para crear una red de servicios compartidos dentro de una oficina o edificio.

El *switch* actúa como un controlador que permite que diferentes dispositivos compartan información entre sí. Existen dos tipos de *switches*:

- ***Switches* administrados**: son aquellos programables. Se puede ajustar de forma remota o local para controlar el tráfico de red y los accesos a la red.
- ***Switches* no administrados:** funcionan automáticamente y no permiten cambios. Estos son los *switches* más comunes usados en las redes domésticas.

Diferencia entre *switch* y *Router*

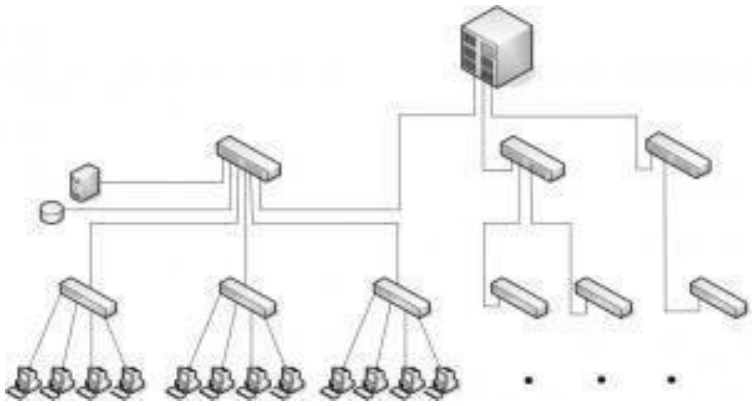
El *switch* y el *router* permiten la conexión de las computadoras y sus dispositivos periféricos a la red. El *router* liga los aparatos a la red, mientras que el *switch* los interconecta.

Tipos de switches.

La clasificación final aquí propuesta parte de dos parejas de términos que se expondrán a continuación:

- **Switch troncal / switch perimetral**

El término **switch troncal** se refiere a los que se utilizan en el núcleo central (core) de las grandes redes. Es decir, a estos switches están conectados otros de jerarquía inferior, además de servidores, routers WAN, etc. Por otro lado, el término **switch perimetral** se refiere a los utilizados en el nivel jerárquico inferior en una red local y a los que están conectados los equipos de los usuarios finales.



- **Switch gestionable (managed) / switch no gestionable (unmanaged)**

El término **gestionable (managed)** se refiere a los switches que ofrecen una serie de características adicionales que requieren de configuración y gestión. Por el contario los switches **no gestionables (unmanaged)** suelen ser los que ofrecen funcionalidades básicas que no requieren procedimiento de configuración o gestión.

En base a todo lo anterior se ofrece la clasificación propuesta, seguida de la explicación de las características de cada tipo.

- Desktop
- Perimetrales no gestionables
- Perimetrales gestionables
- Troncales de prestaciones medias
- Troncales de altas prestaciones

Switches

desktop

Este es el tipo de switch más básico que ofrece la función de conmutación básica sin ninguna característica adicional. Su uso más habitual es en redes de ámbito doméstico o en pequeñas empresas para la interconexión de unos pocos equipos, por lo que no están preparados para su montaje en rack 19". Estos switches no requieren ningún tipo de configuración, ya que utilizan el modo de *autoconfiguración* de Ethernet para configurar los parámetros de cada puerto. Las características más habituales en este tipo son:

- Número de puertos: 4 -8 puertos

RJ-45.

• Configuración de los puertos: normalmente admiten 10BASE-T y 100BASE-TX tanto en modo half-dúplex como full-dúplex. Su configuración se lleva a cabo por negociación mediante la característica de *autonegociación* que proporciona el estándar **IEEE 802.3**.

• Los switches más actuales de este tipo pueden incluir la característica *Auto MDI/MDI- X*.

Switches perimetrales no gestionables

Este tipo de switches se utilizan habitualmente para constituir redes de pequeño tamaño de prestaciones medias. No admiten opciones de configuración y suelen tener características similares a los switches desktop pero incrementando el número de puertos y ofreciendo la posibilidad de montaje en rack 19“.

- El número de puertos de este tipo de switch puede ser típicamente de 4, 8, 16 o 24 puertos.
- Suelen ser puertos 10/100 RJ-45 que admiten *autonegociación* y *Auto MDI/MDI-X*.

  Existen algunos modelos con puertos 10/100/1000.
- En algunos casos pueden presentar puertos adicionales de rendimiento superior al resto de puertos.
- Existen modelos no gestionables que proporcionan *Power Over Ethernet* (**PoE**).
- Preparados para su montaje en rack de 19“.

Switches perimetrales gestionables

Este tipo se utiliza para la conexión de los equipos de los usuarios en redes de tamaño medio y grande, y se localizan en el nivel jerárquico inferior. Es necesario que estos switches ofrezcan características avanzadas de configuración y gestión. Sus características más habituales son:

- EL número de puertos fijos que ofrecen oscila entre 16 y 48 puertos.
- Existen modelos con puertos 10/100 y otros con puertos 10/100/1000, todos con soporte *Auto MDI/MDI-X*.
- Incluyen puertos adicionales de mayores prestaciones o puertos modulares (**GBIC** o **SFP**) para la conexión con un switch troncal.
- Características avanzadas de gestión por **SNMP**, puerto de consola, navegador web, ssh, monitorización *Port Mirroring*.
- Características avanzadas de configuración en el nivel 2 como *Port Trunking*, *Spanning*

  Tree, *IEEE 802.1x*, *QoS, VLAN*, soporte de tramas *Jumbo*, etc.
- Algunos modelos pueden ofrecer *Power Over Ethernet* en todos los puertos.

Switches troncales de prestaciones medias

Este tipo de switches están diseñados para formar el núcleo o troncal de una red de tamaño medio. Proporcionan altas prestaciones y funcionalidades avanzadas. Una de las principales diferencias con los switches perimetrales es que ofrecen características de nivel 3 como enrutamiento IP. A continuación, se exponen sus características más representativas:

- Características avanzadas de configuración de nivel 2 similares a los switches perimetrales gestionables.
- Habitualmente ofrecen entre 24 y 48 puertos fijos 10/100 con conector RJ-45 con algunos puertos modulares adicionales para Gigabit Ethernet y 10GbE para cable y fibra. Existen también modelos con puertos de altas prestaciones 10/100/1000 o incluso puertos 10GbE.
- Permiten expandir sus capacidades mediante la apelación de switches.
- Niveles 2/3. Además de cubrir funciones de conmutación avanzadas del nivel 2 también proporcionan funciones de enrutamiento y gestión en el nivel 3.

Switches troncales de altas prestaciones

La principal característica de este tipo, además de su alto rendimiento, es su alta modularidad. El formato habitual es de tipo *chasis* donde se instalan los módulos que se necesitan. Se utilizan en grandes redes corporativas o de campus, e incluso se utilizan por los operadores para constituir sus redes metropolitanas. Sus principales características son:

• Altamente modulares mediante un chasis con un número variable de slots donde se insertan módulos con los elementos requeridos. Normalmente suelen admitir la inserción de módulos en caliente (*hot swappable*) de forma que no hay que desconectar el switch para realizar dicha operación, garantizando así una alta disponibilidad.

• Niveles 2/3/4. Además de cubrir funciones de conmutación avanzadas del nivel 2 también proporcionan funciones de enrutamiento y gestión en los niveles 3 y 4.

• Fuentes de alimentación redundantes.

• Admiten módulos con todos los tipos de puertos, tanto de cobre como de fibra con velocidades 10/100/1000 Mbps hasta 10Gbps.

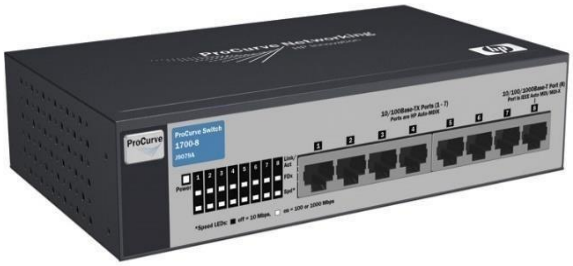
• Alta densidad de puertos. Pueden llegar a más de 500 puertos 10/100, hasta 200 puertos Gigabit o sobre unos 25 puertos 10GbE.

• Características avanzadas de configuración y gestión en el nivel 2.

• Enrutamiento en el nivel 3 (IPv4 e IPv6).

Finalmente recordar que en base al carácter no científico de esta clasificación podemos

encontrar modelos que no encajen en un solo tipo. Por ejemplo, el siguiente modelo de switch:



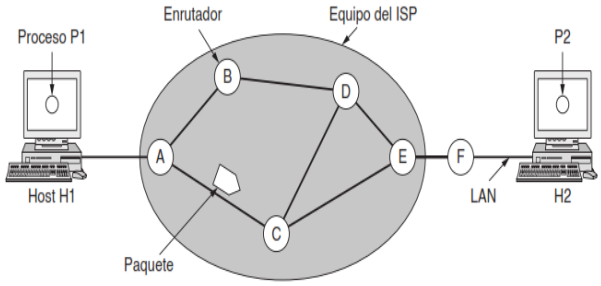
Este es un switch gestionable de características avanzadas pero que sin embargo cuenta con tan sólo 8 puertos, 7 de ellos a 10/100 y uno a 10/100/1000. En fin, lo que podríamos llamar, un híbrido.

UNIDAD III CONFIGURACIÓN DE SWITCHES

3.1 Conmutación de paquetes de almacenamiento y reenvío

Antes de empezar a explicar los detalles sobre la capa de red, vale la pena volver a exponer el contexto en el que operan los protocolos de esta capa. En la figura 5-1 podemos ver este con texto. Los componentes principales de la red son el equipo del Provedor del Servicio de Internet (ISP) (enrutadores conectados mediante líneas de transmisión), que se muestra dentro del óvalo sombreado, y el equipo de los clientes, que se muestra fuera del óvalo. El host *H1* está conectado de manera directa a un enrutador del ISP, *A*, tal vez en forma de una computadora en el hogar conectada a un módem DSL.

En contraste, *H2* se encuentra en una LAN (que podría ser una Ethernet de oficina) con un enrutador, *F*, el cual es propiedad del cliente, quien lo maneja. Este enrutador tiene una línea alquilada que va al equipo del ISP. Mostramos a *F* fuera del óvalo porque no pertenece al ISP. Sin embargo y para los fines de este capítulo, los enrutadores locales de los clientes se consideran parte de la red del ISP debido a que ejecutan los mismos algoritmos que los enrutadores del ISP (y nuestro principal interés aquí son los algoritmos)



Este equipo se utiliza de la siguiente manera. Un host que desea enviar un paquete lo transmite al enrutador más cercano, ya sea en su propia LAN o a través de un enlace punto a punto que va al ISP. El paquete se almacena ahí hasta que haya llegado por completo y el enlace haya terminado su procesa miento mediante la comprobación de la suma de verificación. Después se reenvía al siguiente enrutador de la ruta hasta que llega al host de destino, en donde se entrega. Este mecanismo se denomina conmutación de almacenamiento y envío, como hemos visto en capítulos anteriores.

3.2 Servicios proporcionados a la capa de transporte

La capa de red proporciona servicios a la capa de transporte en la interfaz entre la capa de red y de transporte. Una pregunta importante es qué tipo de servicios proporciona precisamente la capa de red a la capa de transporte. Hay que diseñar los servicios de manera cuidadosa, con los siguientes objetivos en mente:

1. Los servicios deben ser independientes de la tecnología del enrutador.
2. La capa de transporte debe estar aislada de la cantidad, tipo y topología de los enrutadores presentes.
3. Las direcciones de red disponibles para la capa de transporte deben usar un plan de numeración uniforme, incluso a través de redes LAN y WAN. Un bando (representado por la comunidad de Internet) declara que la tarea de los enrutadores es mover paquetes de un lado a otro, y nada más. Desde su punto de vista (basado en casi 40 años de experiencia con una red de computadoras real), la red es de naturaleza no confiable, sin importar su diseño.

Por lo tanto, los hosts deben aceptar este hecho y efectuar ellos mismos el control de errores (es decir, detección y corrección de errores) y el control de flujo.

Este punto de vista conduce a la conclusión de que el servicio de red debe ser sin conexión y debe contar tan sólo con las primitivas SEND PACKET y RECEIVE PACKET. En particular, no debe efectuarse ningún ordenamiento de paquetes ni control de flujo, pues de todos modos los hosts lo van a efectuar y por lo general se obtiene poca ganancia al hacerlo dos veces. Este razonamiento es un ejemplo del argumento extremo a extremo (end-to-end argument), un principio de diseño que ha sido muy influyente para dar forma a Internet.

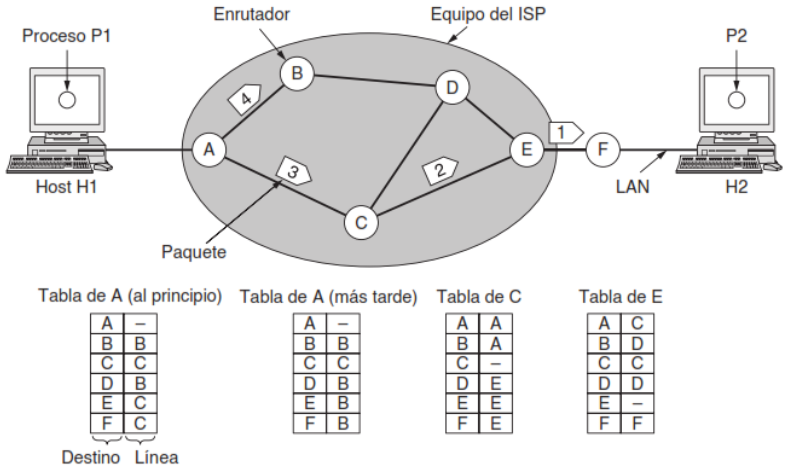
(Saltzer y colaboradores, 1984). Además, cada paquete debe llevar la dirección de destino completa, porque cada paquete enviado se transporta de manera independiente a sus antecesores, si los hay.

3.3 Implementación del servicio sin conexión

Puesto que ya vimos las dos clases de servicios que la capa de red puede proporcionar a sus usuarios, es tiempo de analizar el funcionamiento interno de esta capa. Se pueden realizar dos formas de organización distintas, dependiendo del tipo de servicio ofrecido. Si se ofrece el servicio sin conexión, los paquetes se transmiten por separado en la red y se enrutan de manera independiente. No se necesita una configuración por adelantado.

Ahora veamos cómo funciona una red de datagramas. Suponga que el proceso *P1* de la figura 5-2 tiene un mensaje largo para *P2*. Dicho proceso entrega el mensaje a la capa de transporte y le indica

a ésta que lo envíe al proceso *P2* en el host *H2*. El código de la capa de transporte se ejecuta en *H1*, por lo general entro del sistema operativo. Dicho código agrega un encabezado de transporte al frente del mensaje y entrega el resultado a la capa de red, que quizá sólo sea otro procedimiento dentro del sistema operativo.



Supongamos para este ejemplo que el mensaje es cuatro veces más largo que el tamaño máximo de paquete, por lo que la capa de red tiene que dividirlo en cuatro paquetes: 1, 2, 3 y 4; y enviar cada uno por turnos al enrutador *A* mediante algún protocolo punto a punto; por ejemplo, PPP. En este momento entra en acción el ISP. Cada enrutador tiene una tabla interna que le indica a dónde enviar paquetes para cada uno de los posibles destinos. Cada entrada en la tabla es un par que consiste en un destino y la línea de salida que se utilizará para ese destino. Sólo se pueden utilizar líneas conectadas en forma directa. Por ejemplo, en la figura, *A* sólo tiene dos líneas de salida (a *B* y a *C*), por lo que cada paquete entrante se debe enviar a uno de estos enrutadores, incluso si el destino final es algún otro enrutador. En la figura 5-2, la tabla de enrutamiento inicial de *A* se muestra bajo la leyenda "al principio.

En *A*, los paquetes 1, 2 y 3 se almacenan unos momentos, después de haber llegado por el enlace entrante y de haber comprobado sus sumas de verificación. Después cada paquete se reenvía de acuerdo con la tabla de *A*, por el enlace de salida a *C* dentro de una nueva trama. Después, el paquete 1 se reenvía a *E* y después a *F*. Cuando llega a *F*, se envía dentro de una trama a *H2* a través de la LAN.

Los paquetes 2 y 3 siguen la misma ruta.

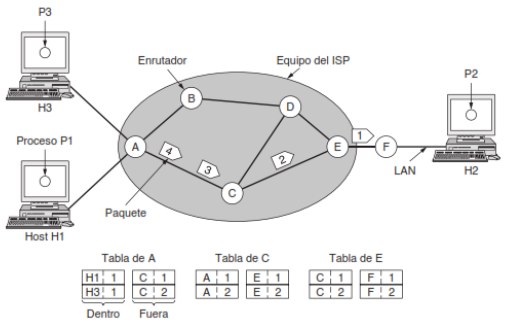
Sin embargo, ocurre algo diferente con el paquete 4. Cuando llega a *A* se envía al enrutador *B*, aun cuando también está destinado a *F*. Por alguna razón, *A* decidió enviar el paquete 4 por una ruta diferente a la de los primeros tres paquetes. Tal vez se enteró de que había alguna congestión de tráfico en alguna parte de la ruta *ACE* y actualizó su tabla de enrutamiento, como se muestra bajo la leyenda "más tarde". El algoritmo que maneja las tablas y realiza las decisiones de enrutamiento se conoce como **algoritmo de enrutamiento**. Los algoritmos de enrutamiento son uno de los principales temas que estudiaremos en este capítulo. Hay distintos tipos de ellos, como veremos más adelante.

3.4 Implementación del servicio orientado a conexión

Para el servicio orientado a conexión necesitamos una red de circuitos virtuales. Veamos ahora cómo funciona. La idea detrás de los circuitos virtuales es evitar la necesidad de elegir una nueva ruta para cada paquete enviado, como en la figura. Cuando se establece una conexión, se elige una ruta de la máquina de origen a la máquina de destino como parte de la configuración de conexión y se almacena en tablas dentro de los enrutadores. Esa ruta se utiliza para todo el tráfico que fluye a través de la conexión, de la misma forma en que funciona el sistema telefónico.

Como ejemplo, considere la situación que se muestra en la figura 5-3. En ésta, el host *H1* ha establecido

Una conexión 1 con el host *H2*. Esta conexión se recuerda como la primera entrada en cada una de las tablas de enrutamiento. La primera línea de la tabla *A* indica que si un paquete con el identificador de conexión 1 viene de *H1*, se enviará al enrutador *C* y se le dará el identificador de conexión 1. De manera similar, la primera entrada en *C* enruta el paquete a *E*, también con el identificador de conexión 1.



Ahora consideremos lo que sucede si *H3* también desea establecer una conexión con *H2*. Elige el identificador de conexión 1 (debido a que está iniciando la conexión y a que ésta es su única conexión) y le indica a la red que establezca el circuito virtual. Esto nos lleva a la segunda fila de las tablas. Observe que aquí surge un problema, pues aunque *A* sí puede saber con facilidad cuáles paquetes de conexión 1 provienen de *H1* y cuáles provienen de *H3*, *C* no puede hacerlo. Por esta razón, *A* asigna un identificador de conexión diferente al tráfico de salida para la segunda conexión. Evitar conflictos de este tipo es la razón por la cual los enrutadores necesitan la habilidad de reemplazar identificadores de conexión en los paquetes de salida.

3.5 Comparación entre las redes de circuitos virtuales y las redes de datagrama

Tanto los circuitos virtuales como los datagramas tienen sus seguidores y sus detractores. Ahora intentaremos resumir los argumentos de ambos bandos. Los aspectos principales se listan en la figura, aunque es probable que los puristas puedan encontrar ejemplos contrarios para todo lo indicado en la figura:

Asunto	Red de datagramas	Red de circuitos virtuales
Configuración del circuito.	No necesaria.	Requerida.
Direccionamiento.	Cada paquete contiene la dirección de origen y de destino completas.	Cada paquete contiene un número de CV corto.
Información de estado.	Los enrutadores no contienen información de estado sobre las conexiones.	Cada CV requiere espacio de tabla del enrutador por cada conexión.
Enrutamiento.	Cada paquete se enruta de manera independiente.	La ruta se elije cuando se establece el CV; todos los paquetes siguen esa ruta.
Efecto de fallas del enrutador.	Ninguno, excepto para paquetes perdidos durante una caída.	Terminan todos los CVs que pasaron por el enrutador defectuoso.
Calidad del servicio.	Difícil.	Fácil si se pueden asignar suficientes recursos por adelantado para cada CV.
Control de congestión.	Difícil.	Fácil si se pueden asignar suficientes recursos por adelantado para cada CV.

Dentro de la red existen ventajas y desventajas entre los circuitos virtuales y los datagramas. Una de ellas tiene que ver con el tiempo de configuración y el tiempo de análisis de la dirección. El uso de circuitos virtuales requiere una fase de configuración que necesita tiempo y recursos. Sin embargo, una vez que se paga este precio, es fácil averiguar qué hacer con un paquete de datos en una red de circuitos virtuales: el enrutador sólo usa el número de circuito para buscar en una tabla

y encontrar hacia dónde va el paquete. En una red de datagramas no se requiere configuración, pero se requiere un procedimiento más complicado para localizar la entrada correspondiente al destino.

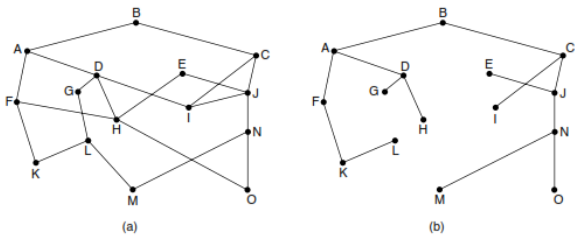
Un aspecto relacionado es que las direcciones de destino que se utilizan en las redes de datagramas son más largas que los números de los circuitos que se utilizan en las redes de circuitos virtuales, ya que tienen un significado global. Si los paquetes tienden a ser bastante cortos, incluir una dirección de destino completa en cada paquete puede representar una cantidad considerable de sobrecarga y, por ende, un desperdicio de ancho de banda.

3.6 Principio de optimización

Antes de entrar en algoritmos específicos, puede ser útil señalar que es posible hacer una postulado general sobre las rutas óptimas sin importar la topología o el tráfico de la red. Este postulado se conoce Como **principio de optimización** (Bellman, 1957) y establece que si el enrutador *J* está en la ruta óptima del enrutador *I* al enrutador *K*, entonces la ruta óptima de *J* a *K* también está en la misma ruta.

Para ver esto, llamemos r_1 a la parte de la ruta de *I* a *J* y r_2 al resto de la ruta. Si existiera una ruta mejor que *r* entre *J* y *K*, se podría concatenar con *r* para mejorar la ruta de *I* a *K*, lo cual contradice nuestro postulado de que $r_1 r_2$ es óptima.

Como consecuencia directa del principio de optimización, podemos ver que el grupo de rutas óptimas de todos los orígenes a un destino dado forman un árbol con raíz en el destino. Dicho árbol se conoce como **árbol sumidero** (o **árbol divergente**) y se ilustra en la figura, donde la métrica de distancia es el número de saltos. El objetivo de todos los algoritmos de enrutamiento es descubrir y usar los árboles sumidero para todos los enrutadores.



Cabe mencionar que un árbol sumidero no necesariamente es único; pueden existir otros árboles con las mismas longitudes de rutas. Si permitimos que se elijan todas las posibles rutas, el árbol se convierte en una estructura más general conocida como **DAG** (**Gráfico Acíclico Dirigido**, del inglés *Directed Acyclic Graph*). Los DAG no tienen ciclos. Usaremos los árboles sumidero como un método abreviado conveniente para ambos casos, que también dependen del supuesto técnico de que las rutas no interfieren entre sí; por ejemplo, un congestionamiento de tráfico en una ruta no provocará que se desvíe a otra ruta.

Puesto que un árbol sumidero ciertamente es un árbol, no contiene ciclos, por lo que cada paquete se entregará en un número de saltos finito y limitado. En la práctica, la vida no es tan fácil. Los enlaces y los enrutadores pueden fallar y recuperarse durante la operación, así que distintos enrutadores pueden tener de las diferentes sobre la topología actual. Además, hemos evadido la cuestión de si cada enrutador tiene que adquirir de manera individual la información en la cual basa su cálculo del árbol sumidero, o si debe obtener esta información por otros medios.

3.7 Algoritmo de la ruta más corta

Empecemos nuestro estudio de los algoritmos de enrutamiento con una técnica simple para calcular las rutas óptimas con base en una imagen completa de la red. Estas rutas son las que queremos que encuentre un algoritmo de enrutamiento distribuido, aun cuando no todos los enrutadores conozcan todos los detalles de la red.

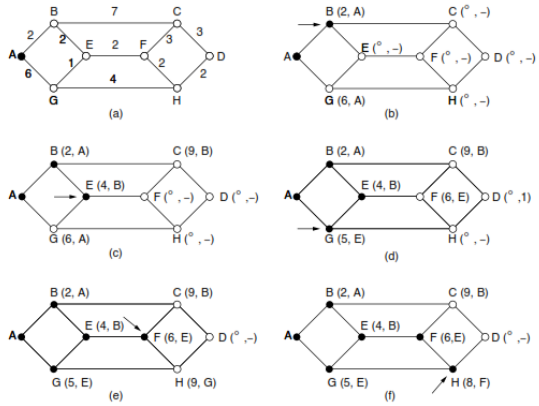
La idea es construir un grafo de la red, en donde cada nodo del grafo representa un enrutador y cada arco del grafo representa una línea o enlace de comunicaciones. Para elegir una ruta entre un par específico de enrutadores, el algoritmo simplemente encuentra la ruta más corta entre ellos en el grafo.

El concepto de la **ruta más corta** merece una explicación. Una manera de medir la longitud de una ruta es mediante el número de saltos. Con base en esta métrica, las rutas *ABC* y *ABE* en la figura son igual de largas. Otra métrica es la distancia geográfica en kilómetros, en cuyo caso *ABC* es sin duda mucho más larga que *ABE* (suponiendo que la figura esté dibujada a escala).

Sin embargo, también son posibles muchas otras métricas además de los saltos y la distancia física. Por ejemplo, cada arco se podría etiquetar con el retardo promedio de un paquete de prueba

estándar, determinado por una serie de pruebas cada hora. Con estas etiquetas en el grafo, la ruta más corta es la ruta más rápida, en lugar de la ruta con menos arcos o kilómetros.
En el caso general, las etiquetas de los arcos se podrían calcular como una función de la distancia, ancho de banda, tráfico promedio, costo de comunicación, retardo promedio y otros factores. Al cambiar la función de ponderación, el algoritmo calcularía la ruta "más corta" de acuerdo con cualquiera de estos criterios, o una combinación de ellos.

Se conocen varios algoritmos para calcular la ruta más corta entre dos nodos de un grafo. Uno de éstos se debe a Dijkstra (1959), el cual encuentra las rutas más cortas entre un origen y todos los destinos en una red. Cada nodo se etiqueta (entre paréntesis) con su distancia desde el nodo de origen a través de la mejor ruta conocida. Las distancias no deben ser negativas, como lo serán si se basan en cantidades reales como ancho de banda y retardo.



Comenzamos por marcar el nodo *A* como permanente, lo cual se indica mediante un círculo relleno. Después examinamos, por turno, cada uno de los nodos adyacentes a *A* (el nodo de trabajo) y reetiquetamos cada uno de ellos con la distancia a *A*. Cada vez que reetiquetamos un nodo, también lo etiquetamos con el nodo desde el que se hizo la prueba, para poder reconstruir más tarde la ruta final. Si la red tuviera más de una ruta más corta de *A* a *D* y quisiéramos encontrarlas todas tendríamos que recordartodos los nodos de prueba que podrían llegar a un nodo con la misma distancia.

Una vez que terminamos de examinar cada uno de los nodos adyacentes a *A*, examinamos todos los nodos etiquetados tentativamente en el grafo completo y hacemos permanente el de la etiqueta más pequeña, como se muestra en la figura 5-7(b). Éste se convierte en el nuevo nodo de trabajo.
Ahora comenzamos por *B* y examinamos todos los nodos adyacentes a él. Si la suma de la etiqueta en *B* y la distancia desde *B* hasta el nodo en consideración es menor que la etiqueta de ese nodo, tenemos una ruta más corta, por lo que reetiquetamos ese nodo.

3.8 Enrutamiento por difusión

En algunas aplicaciones, los hosts necesitan enviar mensajes a varios o a todos los hosts en la red. Por ejemplo, el servicio de distribución de informes sobre el clima, la actualización de los precios de la bolsa o los programas de radio en vivo podrían funcionar mejor si se difunden a todas las máquinas para dejar que las personas interesadas lean los datos. El envío simultáneo de un paquete a todos los destinos se llama **difusión** (*broadcasting*). Se han propuesto varios métodos para llevarla a cabo.

Ya hemos visto una mejor técnica de enrutamiento por difusión: la inundación. Cuando se implementa con un número de secuencia por cada origen, la inundación usa los enlaces de manera eficiente con una regla de decisión en los enrutadores que es relativamente simple. Aunque la inundación es poco adecuada para la comunicación punto a punto ordinaria, para difusión puede merecer que se le considere con seriedad.
La idea del **reenvío por ruta invertida** (*reverse path forwarding*) es elegante y excepcionalmente sencilla una vez planteada (Dalal y Metcalfe, 1978). Cuando llega un paquete difundido a un enrutador, éste lo revisa para ver si llegó por el enlace que se usa por lo común para enviar paquetes *hacia* el origen de la difusión. De ser así, hay excelentes posibilidades de que el paquete difundido haya seguido la mejor ruta desde el enrutador y, por lo tanto, sea la primera copia en llegar al enrutador. Si éste es el caso, el enrutador reenvía copias del paquete a todos los enlaces, excepto a aquel por el que llegó.

Nuestro último algoritmo de difusión mejora el comportamiento del reenvío por ruta invertida. Usa de manera explícita el árbol sumidero (o cualquier otro árbol de expansión conveniente) para el enrutador que inicia la difusión. Un **árbol de expansión** es un subconjunto de la red que incluye

todos los enrutadores pero no contiene ciclos. Los árboles sumidero son árboles de expansión. Si cada enrutador sabe cuáles de sus líneas pertenecen al árbol de expansión, puede copiar un paquete de difusión entrante en todas las líneas del árbol de expansión, excepto en aquella por la que llegó. Este método utiliza de manera óptima el ancho de banda, ya que genera el número mínimo absoluto de paquetes necesarios para llevar a cabo el trabajo.
El único problema es que cada enrutador debe tener conocimiento de algún árbol de expansión para que este método pueda funcionar. Algunas veces esta información está disponible (por ejemplo, con el enrutamiento por estado del enlace, todos los enrutadores conocen la topología completa, por lo que pueden calcular un árbol de expansión), pero a veces no (por ejemplo, con el enrutamiento por vector de distancia).

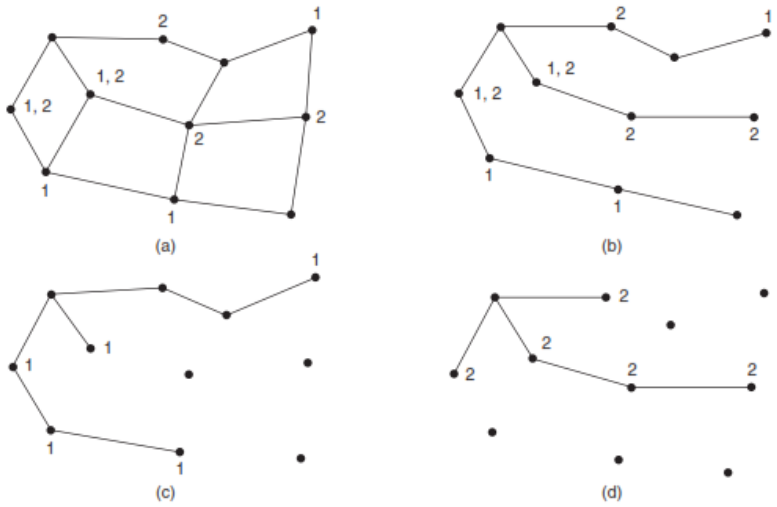
3.9 Enrutamiento multidifusión

Algunas aplicaciones, como un juego multijugador o un video en vivo de un evento deportivo que se transmite por flujo continuo a muchas ubicaciones, envían paquetes a múltiples receptores. A menos que el grupo sea muy pequeño, es costoso enviar un paquete distinto a cada receptor. Por otro lado, sería un desperdicio difundir un paquete si el grupo consiste en, por decir, 1000 máquinas en una red con un millón de nodos, de tal forma que la mayoría de los receptores no están interesados en el mensaje (o peor aún, están en definitiva interesados pero se supone que no deben verlo). Por lo tanto, necesitamos una manera de enviar mensajes a grupos bien definidos que sean grandes en número, pero pequeños en comparación con la totalidad de la red.

El proceso de enviar un mensaje a uno de tales grupos se denomina **multidifusión** (*multicasting*); el algoritmo de enrutamiento que se utiliza es el **enrutamiento por multidifusión**. Todos los esquemas de multidifusión requieren alguna forma de crear y destruir grupos, además de identificar qué enrutadores son miembros de un grupo. La forma de realizar estas tareas no le concierne al algoritmo de enrutamiento.
Por ahora vamos a suponer que cada grupo se identifica mediante una dirección de multidifusión y que los enrutadores conocen los grupos a los que pertenecen.

Si el grupo es denso, la difusión es un buen comienzo debido a que transmite de manera eficiente el paquete a todas las partes de la red. Pero la difusión llegará a algunos enrutadores que no sean

miembros del grupo, lo cual es un desperdicio. La solución explorada por Deering y Cheriton (1990) es recortar el árbol de expansión de difusión, mediante la eliminación de enlaces que no conducen a los miembros. El resultado es un árbol de expansión de multidifusión eficiente



Con el enrutamiento por vector de distancia se puede seguir una estrategia de recorte diferente. El algoritmo básico es el reenvío por ruta invertida. Sin embargo, cuando un enrutador sin hosts interesados en un grupo en particular y sin conexiones con otros enrutadores recibe un mensaje de multidifusión para ese grupo, responde con un mensaje PRUNE (de recorte) para indicar al vecino emisor que no envíe más multidifusiones para ese grupo. Cuando un enrutador que no tiene miembros del grupo entre sus propios hosts recibe uno de tales mensajes por todas las líneas a las que envía la multidifusión, también puede responder con un mensaje PRUNE.

3.10 Elementos de un switch.

Los puertos son los elementos del switch que permiten la conexión de otros dispositivos al mismo. Como por ejemplo un PC, portátil, un router, otro switch, una impresora y en general cualquier dispositivo que incluya una interfaz de red Ethernet. El número de puertos es una de las características básicas de los switches. Aquí existe un abanico bastante amplio,

desde los pequeños switches de 4 puertos hasta switches troncales que admiten varios cientos de puertos.

El estándar Ethernet admite básicamente dos tipos de medios de transmisión cableados: **el cable de par trenzado** y **el cable de fibra óptica**. El conector utilizado para cada tipo lógicamente es diferente así que otro dato a tener en cuenta es de qué tipo son los puertos. Normalmente los switches básicos sólo disponen de puertos de cable de par trenzado (cuyo conector se conoce como **RJ-45**) y los más avanzados incluyen puertos de fibra óptica (el conector más frecuente aunque no el único es el de tipo **SC**).

Velocidad

Dado que Ethernet permite varias velocidades y medios de transmisión, otra de las características destacables sobre los puertos de los switches es precisamente la velocidad a la que pueden trabajar sobre un determinado medio de transmisión. Podemos encontrar puertos definidos como 10/100, es decir, que pueden funcionar bajo los estándares **10BASE-T** (con una velocidad de 10 Mbps) y **100BASE-TX**(velocidad: 100 Mbps). Otra posibilidad es encontrar puertos 10/100/1000, es decir, añaden el estándar **1000BASE-T** (velocidad 1000 Mbps). También se pueden encontrar puertos que utilicen fibra óptica utilizando conectores hembra de algún formato para fibra óptica. Existen puertos **100BASE-FX** y **1000BASE-X**. Por último, los switches de altas prestaciones pueden ofrecer puertos que cumplan con el estándar **10GbE**, tanto en fibra como en cable UTP.

Puertos modulares: GBIC y
SFP

La mayor parte de los switches de gamas media y alta ofrecen los llamados puertos modulares. Estos puertos realmente no tienen ningún conector específico si no que a ellos se conecta un módulo que contiene el puerto. De esta forma podemos adaptar el puerto al tipo de medio y velocidad que necesitemos. Es habitual que los fabricantes ofrezcan módulos de diferentes tipos con conectores RJ-45 o de fibra óptica. Los puertos modulares proporcionan flexibilidad en la configuración de los switches.

Puertos modulares SFP y GBIC

Existen dos tipos de módulos para conectar a los puertos modulares: el primer tipo de módulo que apareció es el módulo **GBIC** (*Gigabit Interface Converter*) diseñado para ofrecer flexibilidad en la elección del medio de transmisión para Gigabit Ethernet. Posteriormente apareció el módulo **SFP** (*Small Form-factor Puggable*) que es algo más pequeño que GBIC (de hecho también se denomina **mini-GBIC**) y que ha sido utilizado por los fabricante para ofrecer módulos tanto Gigabit como 10GbE en fibra o en cable UTP.

Power Over Ethernet (*Alimentación eléctrica por Ethernet*), también conocido como **PoE**, es una tecnología que permite el envío de alimentación eléctrica junto con los datos en el cableado de una red Ethernet. La primera versión de esta tecnología se publicó en el estándar **IEEE802.3af** en 2003 y en el año 2009 se publicó una revisión y ampliación en el estándar **IEEE 802.3at**.

La tecnología PoE permite suministrar alimentación eléctrica a dispositivos conectados a una red Ethernet, simplificando por tanto la infraestructura de cableado para su funcionamiento. Un dispositivo que soporte PoE obtendrá tanto los datos como la alimentación por el cable de red Ethernet.

Los dispositivos que utilizan esta característica son puntos de acceso inalámbricos Wi-Fi, cámaras de video IP, teléfonos de VoIP, switches remotos y en general cualquier dispositivo que esté conectado a una red Ethernet, que no tenga un consumo energético muy elevado y que su ubicación física dificulte la instalación de cableado.

En el mercado podemos encontrar multitud de modelos de switches que incluyen puertos con PoE. En dichos puertos podemos conectar un dispositivo que admita esta característica y recibirá la alimentación eléctrica por el propio cable Ethernet.

3.11.- Proceso de arranque del switch.

Una vez que se enciende el switch Cisco, lleva a cabo la siguiente secuencia de arranque:

1. Primero, el switch carga un programa de autodiagnóstico al encender (POST) almacenado en la memoria ROM. El POST verifica el subsistema de la CPU. Esta comprueba la CPU, la memoria DRAM y la parte del dispositivo flash que integra el sistema de archivos flash.

2. A continuación, el switch carga el software del cargador de arranque.

El cargador de arranque es un pequeño programa almacenado en la memoria ROM que se ejecuta inmediatamente después de que el POST se completa correctamente.

3. El cargador de arranque lleva a cabo la inicialización de la CPU de bajo nivel. Inicializa los registros de la CPU, que controlan dónde está asignada la memoria física, la cantidad de memoria y su velocidad.

4. El cargador de arranque inicia el sistema de archivos flash en la placa del sistema.

5. Por último, el cargador de arranque ubica y carga en la memoria una imagen del software del sistema operativo IOS predeterminado y le cede el control del switch al IOS.

3.12 Conceptos

Post, (Power OnSelf Test): la rutina de autocomprobación que el sistema BIOS de un ordenador realiza al ser encendido.

BIOS (siglas en inglés de Basic Input Output System, es decir, Sistema Básico de Entrada y Salida),

RX, Receiver (o Receive) Data Datos del receptor (o recibidor) TX, Transmitter o Transmit Data Transmisor o transmirit datos CPU, (Siglas de central processing unit, unidad central de proceso) RAM: Random Access Memory(memoria de acceso aleatorio) ROM: Read Only Memory (Memoria de solo lectura)

HD- disco duro (del inglés Hard Disk)

IOS significa Sistema Operativo de Internet (Internet Operating System)

BIOS (siglas en inglés de Basic Input Output System, es decir, Sistema Bástico de Entrada y salida).

DCD (Data Carrier Detect) DTR (Data Terminal Ready) GND(ground)

DSR (Data Sheet Ready)

RTS (Request To Send) CTS (Clear To Send)

RI (Ring Indicator)

RX - Receiver (o Receive) Data , Datos del receptor (o recibidor). TX - (Transmitter o Transmit Data ,Transmisor o transmitir datos) TFTP (Trivial File Transfer Protocol)

3.13 Ingreso a la consola del switch.

Los routers Cisco y ciertos switches soportan la conectividad fuera de banda (sobre todo para la recuperación de catástrofes) mediante un módem que conecta con el puerto auxiliar o el puerto de consola. Los switches Cisco Catalyst no tienen puertos auxiliares. Por lo tanto, El módem conecta solamente con el puerto de consola. Tenga presente que la configuración de los puertos de la consola en los switches Catalyst está diseñada para un acceso fácil y rápido a través de cualquier dispositivo DTE RS-232 estándar (por ejemplo, un PC). Sin embargo, el diseño de los puertos de la consola no es para una accesibilidad remota con un DCE, como un módem. Este documento proporciona un procedimiento para marcar en el puerto de la consola de los switches de Catalyst.

Nota: La conexión de los módems al puerto de la consola de un conmutador tiene algunas desventajas. Hay también problemas de seguridad cuyo ser consciente. Algunos ejemplos son los siguientes:

- El puerto de la consola no utiliza el control del módem RS232 (detección de la portadora DSR/Data [DCD], [DTR] listo del terminal de datos). Por lo tanto, cuando la sesión de EXEC termina (fin de comunicación), la conexión del módem no cae automáticamente; el usuario necesita desconectar manualmente la sesión.
- Más seriamente, si la conexión del módem cae, la sesión de EXEC no reajusta automáticamente. Este error reajustar presenta a una brecha en la seguridad; una llamada posterior en ese módem puede tener acceso a la

consola sin la entrada de una contraseña. Usted puede hacer el agujero más pequeño si usted fija un tiempo de espera de EXEC corto en la línea. Sin embargo, en caso que la seguridad sea importante, utilice un módem que proporcione un mensaje de indicación de contraseña.

Si usted planea conectar un módem con el puerto de la consola de cualquier conmutador del catalizador, primero refiera a la sección de los *problemas del puerto de la consola de la* guía para la conexión del módem-router. El documento proporciona a los riesgos y las limitaciones, así como las ventajas de este procedimiento.

La información en este documento se aplica a este Switches del catalizador:

- Software de las 4500/4000 Series del catalizador (OS del software o del catalizador de Cisco que se ejecuta IOS® [CatOS])
- Switches de las 5500/5000 Series del catalizador
- Switches de las 6500/6000 Series del catalizador (software o CatOS del Cisco IOS que se ejecuta)
- Switches de configuración fija del catalizador, que incluyen el catalizador 2900/3500XL, 2940, 2950, 2955, 2960, 2970, 3550, 3560, y 3750 Series Switch.
- Catalyst 8500 Series Switch Switches de las Catalyst 1900 y 2820 Series.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Cables y conectores

El Switches del catalizador viene normalmente con kit accesorio. El equipo contiene el cable y los adaptadores que usted necesita conectar una terminal (generalmente una PC que funciona con el software de emulación de terminal) o un módem con el puerto de la consola. En algunos casos, los adaptadores individuales son opcionales y usted necesita pedir los adaptadores por separado. Controle la documentación sobre hardware para que su conmutador esté seguro.

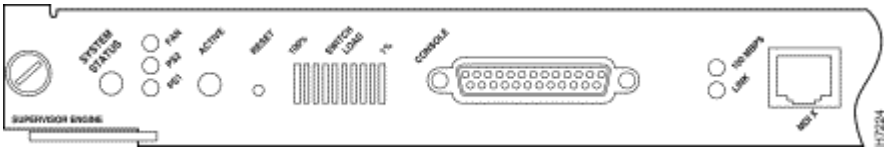
Kit acceso rio

Usted puede ser que necesite para pedir algunos items por separado.

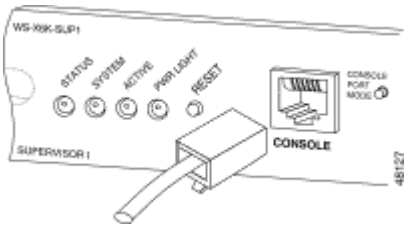
Los cables y los adaptadores en esta tabla son los mismos que envían con los Cisco 2500 Series

Router y los otros productos de Cisco. Tipos de puerto de consola común. Todo el conmutador del catalizador o puertos de consola de Supervisor Engine tiene los conectores hembra RJ-45 o DB-25.

Figura 1: Motor I e II del supervisor del catalizador 5500/5000 panel frontal



El cuadro 2 muestra un motor del supervisor con un conector del puerto de la consola RJ-45.



Switch de modo del puerto de la consola

Algunos puertos de consola de Supervisor Engine tienen un switch de modo. El switch de modo del puerto de la consola (los motores del supervisor del catalizador 5500/5000 y del catalizador 6500/6000 solamente) tiene dos modos. El modo I es –enll la posición (valor por defecto), y el modo 2 es –hacia fueralI coloca. El modo I permite que usted conecte una terminal o el módem con el puerto de la consola con el uso del cable transpuesto de consola del valor por defecto. El cable viene con kit accesorio.

Usted puede ser que no tenga kit accesorio (véase los cables y los conectores) o usted puede ser que haya colocado mal el cable transpuesto de consola. En este caso, el modo 2 le da la opción para utilizar un cable de conexión directa estándar RJ-45 para conectar una terminal.

El switch de modo del puerto de la consola está adentro (por abandono), que es la posición que el procedimiento paso a paso de este documento utiliza. Para más información sobre la señalización y los pinouts para estos dos modos específicamente, refiera al conector y a las especificaciones del cable del documento.

El comando set system baud cambia la velocidad de los puertos de la consola de un poco de Switches (ese funcionamiento CatOS). Usted puede cambiar la velocidad a hasta 38,400 bits por segundo (los BPS). Sin embargo, usted no debe realizar esta acción.

Primero, algunos puertos de la consola del conmutador no utilizan las velocidades más arriba de 9600 BPS. Con el propósito de este documento, usted debe dejar a la velocidad del puerto de la consola en el valor por defecto 9600 BPS.

Comand set system modem

El catalizador 4500/4000, 5500/5000, y 6500/6000 del Switches que ejecuta CatOS tiene el comando set system modem opcional **{permiso | neutralización}**. Este comando activa el control de flujo de hardware (uso de la petición de enviar [RTS] /Clear para enviar [CTS] las señales) en el puerto de la consola. Usted configura el comando a ambos lados de la conexión. (Véase su manual del módem para el Hayes-compatible EN los comandos del ["attention"].)

El control de flujo de hardware es útil para proteger la pérdida de datos a velocidades más altas. Sin embargo, puesto que usted debe dejar la velocidad del puerto de la consola en el valor por defecto de 9600, el control de flujo de hardware no es necesario. Con el propósito de este documento, usted debe dejar este comando en la configuración por defecto de la **neutralización del módem del sistema del conjunto**.

Recomendaciones de la configuración

Algunos puertos de la consola proporcionan a la señalización DTE mientras que otros proporcionan al DCE. Para evitar la confusión, utilice estos escenarios de configuración:

- Si el conmutador tiene un puerto RJ-45, utilice un cable rodado RJ-45-to-RJ-45 (CAB500RJ=) y un adaptador macho RJ-45-to-DB-25 (CAB-25AS-MMOD) para conectar el cable rodado con el puerto DB-25 en el módem.

- Si el conmutador tiene un puerto DB-25, utilice un cable rodado RJ-45-to-RJ-45 (CAB-

  500RJ=) con los adaptadores DB-25-to-RJ-45 que son –módem marcadoII (CAB-25AS- MMOD) en los **ambos extremos**. En vez de esta combinación, usted puede también utilizar un cable del módem nulo DB-25F-to-DB25M RS232.

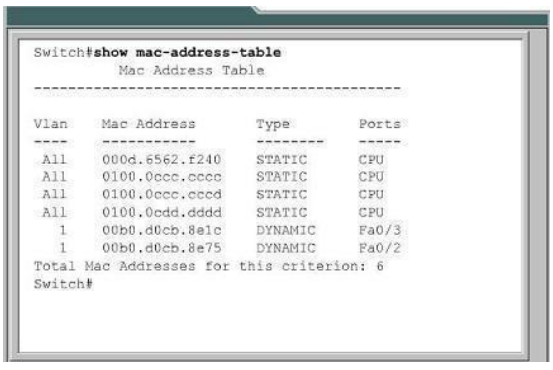
Otras combinaciones de cables y de adaptadores son posibles. Usted puede también hacer sus propios cables, aunque esto no se recomiende. Para más información sobre la señalización del puerto de la consola, los pinouts, y el cableado para todo el Switches del catalizador, refieren al documento que conecta una terminal con el puerto de la consola en el Switches del catalizador.

3.14.- administración de la tabla de direcciones MAC.

Manera en que los switches crean y administran las tablas de direcciones MAC

Los switches examinan la dirección origen de las tramas que se reciben en los puertos para aprender la dirección MAC de las estaciones de trabajo o las PC conectadas a éstos. Estas direcciones MAC aprendidas se registran luego en una tabla de direcciones MAC. Las tramas que tienen una dirección MAC destino, que se ha registrado en la tabla, se pueden conmutar hacia la interfaz correcta.

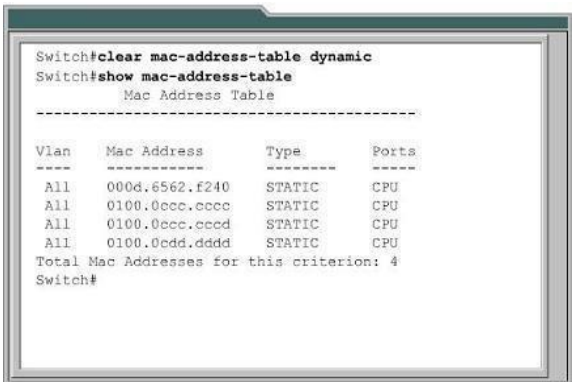
El comando show mac-address-table se puede introducir en el modo EXEC privilegiado para examinar las direcciones que un switch ha aprendido.



Un switch aprende en forma dinámica y mantiene miles de direcciones MAC. Para preservar la memoria y para una operación óptima del switch, las entradas aprendidas se pueden descartar de la tabla de direcciones MAC. Es posible que se hayan eliminado máquinas de un puerto, se hayan apagado o trasladado a otro puerto en el mismo switch o en un switch diferente. Esto puede provocar confusión al momento de enviar las tramas. Por todas estas razones, si no se ven tramas con una dirección aprendida anteriormente, la entrada de direcciones MAC se descarta automáticamente o expiran después de 300 segundos.

En lugar de esperar que una entrada dinámica expire, los administradores de red pueden utilizar el comando clear mac-address-table en el modo EXEC privilegiado.

Las entradas de direcciones MAC configuradas por los administradores de red también se pueden eliminar con este comando. Este método para borrar entradas de tabla permite eliminar de forma inmediata las direcciones no válidas.



3.15.- configuración de direcciones MAC.

Al contrario de lo que puede parecer, una dirección MAC no sólo hace referencia a ordenadores de Mac. También de los de Microsoft.

Se trata de un identificador de 48 bits (6 números hexadecimales) que está presente en todo dispositivo de red. Viene asignado por el fabricante.

Un ejemplo de **dirección MAC** podría ser el siguiente: 00:1B:44:11:3A:B7.

En este post vamos hablarte un poco de las direcciones MAC, cómo puedes identificar tus direcciones MAC en una red de dispositivos y qué es un filtro de direcciones MAC y cómo puedes hacer uno.

Direcciones Mac ¿qué son?

Son las siglas en inglés de *Media Access Control*, lo que traducido sería –control de acceso al medio**ll**. Las direcciones MAC son únicas en todo el mundo. Se escriben en el hardware, de forma binaria, en el momento de llevarse a cabo la fabricación del dispositivo.

Los primeros 24 bits (los tres primeros bloques hexadecimales) están configurados por el IEEE (**Instituto de Ingeniería Eléctrica y Electrónica**) y los otros 24 por el fabricante del dispositivo.

Enrutadores, tarjetas de red, impresoras, tarjetas inalámbricas, tablets… todos los dispositivos tienen una dirección MAC, única e irrepetible.

Generalmente no vas a necesitar **conocer tu dirección MAC** para las operaciones habituales, como configurar una conexión a Internet por cable, o crear una red doméstica de ordenadores.

Sin embargo, sí puede ser muy útil conocerla si, por ejemplo, quisiéramos que nuestro punto de acceso a Internet permita que sólo unas direcciones MAC determinadas tuvieran conexión a Internet.

Qué es un filtro de direcciones MAC

El filtrado de MAC te da la oportunidad de permitir o impedir que determinados ordenadores con determinadas tarjetas de red se conecten a Internet a través de tu red. Se trata de un sistema de control de acceso que te ayudará a mejorar la seguridad en el acceso a Internet.

De esta forma, como la conexión a Internet estará restringida a determinadas direcciones

MAC, nadie conectarse sin tu
permiso.

El **filtro de direcciones MAC** es mucho más efectivo en las redes cableadas que en las redes inalámbricas, ya que en estas últimas un atacante puede escuchar las transmisiones.

El filtrado de MAC también suele utilizarse en oficinas con puntos de acceso múltiples. De este modo, podemos evitar que los ordenadores cliente puedan comunicarse con otros clientes inalámbricos y sólo lo hagan con la puerta de enlace determinada. Así se mejora la eficiencia y el rendimiento del acceso a la red.

¿Cómo averiguar tu dirección MAC?

Según el sistema operativo del que estemos hablando, el método para comprobar cuál es la dirección MAC de tu tarjeta de red puede ser diferente. Veamos:

1. Entra en –Preferencias del sistema (System Preferences)
2. Selecciona –Red (Network)
3. Pulsa –Wifi en el panel izquierdo y pulsa en –Avanzado
4. En la ficha Hardware, mira donde dice –Dirección Wifi.

Como hacer un filtrado Mac en tu enrutador

Si lo que quieres es hacer un filtrado MAC para que sólo las direcciones MAC que tú desees puedan conectarse a través de tu red, se puede hacer de la siguiente manera.

Hay que entrar en la página web de administrador de tu router. Para eso, sólo tienes que escribir la **dirección IP** en tu navegador e identificarte con tu usuario y contraseña.

Para poder hacer la configuración, antes de este paso necesitas averiguar y apuntarte las direcciones MAC a las que sí deseas permitirle el acceso. En caso de que quieras crear una lista negra, puedes utilizar un programa llamado **Wireless Network Watcher** para ver qué dispositivos están conectados a Internet a través de tu red.

Cuando hayas anotado las direcciones MAC con las que vas a trabajar, ve al apartado Wireless y busca el submenú filtrado de MAC (o MAC filter).

Precauciones de seguridad con direcciones MAC

Por último, es importante que no des tu dirección MAC a nadie que no sea de confianza. Se trata de un dato privado que sólo concierne por razones de seguridad al administrador de tus ordenadores.

Si quieres llevar a cabo ésta y otras opciones en la mejora de la seguridad de tu red informática, te invitamos a que te pongas en contacto con nuestros expertos.

UNIDAD IV: VLANS

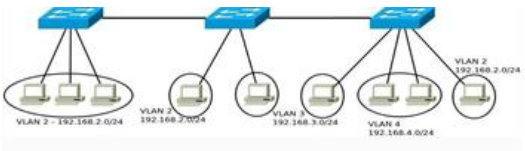
4.1.- Introducción a las VLANS

Una VLAN (virtual LAN) es, conceptualmente, una red de área local formada a nivel lógico. Dada esta particularidad, las VLANs proveen una forma de separar grupos de hosts con objetivos diferentes aunque estos se encuentren conectados al mismo switch. A su vez, en este punto, nos permite optimizar los puertos de switch.

Debajo pueden verse dos topologías que dan como resultado una misma red a nivel lógico. La primera de ellas no utiliza VLANs, con lo cual necesita de diferentes switches para garantizar una correcta separación entre las redes. La segunda utiliza el mismo switch pero con un esquema de VLANs.

Si vemos la configuración del switch en la figura 2 podemos abstraerlo en tres switches diferentes, como muestra la figura 3.

Por su naturaleza, una VLAN puede formarse también a partir de múltiples segmentos de LAN. Esto permiten que estaciones de trabajo ubicadas físicamente en lugares diferentes pueden trabajar en la misma red lógica (es decir, con el mismo direccionamiento de red), como si estuvieran conectadas al mismo switch. La figura 4 muestra un ejemplo de este caso.



Funcionamiento de las VLAN

Hasta ahora hemos visto que un switch es capaz de separar los hosts de las diferentes VLANs como si los grupos de puertos fueran efectivamente switches diferentes. Que

funcione dicha separación trabajando con un único switch no es, a priori, difícil. El trabajo que debe hacer el switch es comunicar sólo entre sí los hosts que pertenezcan a una misma VLAN. Con indicarleen su configuración a qué VLAN pertenece cada puerto el inconveniente estaría solucionado.

El problema surge cuando deseamos que la separación se mantenga entre diferentes switches, permitiendo aún la comunicación entre hosts de la misma VLAN. Veamos la figura 4. Es claro, como ya dije anteriormente, que dentro de un mismo switch no hay problema. ¿Pero qué ocurre cuando el tráfico de un switch pasa a los siguientes? En el primer switch hay tres hosts en la VLAN 2 que se comunican con un host de la VLAN 2 en el segundo switch y uno en el tercero. No obstante, en estos dos últimos hay hosts que pertenecen a otras VLANs y también deben comunicarse entre sí. Si el lector es observador notará que entre cada switch hay un único cable, lo que supone que tanto el tráfico de la VLAN 2 como el de la VLAN 3 se mezclan en dicho cable. No obstante, los switches son capaces de garantizar la separación de las VLANs y la comunicación entre los hosts. Veamos cómo ocurre esto.

Para la comunicación entre switches se utiliza un protocolo estándar definido por la IEEE. Se trata de 802.1q, cuya función es la de encapsular las tramas Ethernet en una nueva estructura. Así, a la trama Ethernet tradicional se le agregan 4 bits en la cabecera que conforman el identificador de VLAN. De esta manera, el tráfico va todo junto en el mismo cable pero es fácilmente identificable.

Tipos de puertos

Un switch que utiliza VLANs puede tener dos tipos de puertos: puertos de acceso y puertos de trunk. A continuación se da una explicación de cada uno de ellos.

- Puertos de acceso: este tipo de puertos son los que conectan hosts finales. Trabajan con las tramas clásicas de Ethernet, sin el agregado de las etiquetas de VLAN.
- Puertos de trunk: los puertos de trunk tienen una función especial que es la de conectar

switches entre sí o un switch con un router. Cuando llega tráfico a un puerto de trunk proveniente desde el propio switch, éste es etiquetado con el identificador de VLAN y enviado por el puerto. El equipo que lo recibe, desencapsula la trama Ethernet (quitándole la etiqueta) y lo envía al puerto que corresponda.

4.2.- Configuración de las VLAN.

Una Virtual LAN (VLAN) es una división lógica del dominio de Broadcast a nivel de la Capa 2 del modelo OSI. También podemos decir que una VLAN es una agrupación lógica de dispositivos que se pueden comunicar en sí.

Los dispositivos que pertenecen a VLANs diferentes NO se pueden comunicar entre sí. En el Real World la tecnología de VLAN se implementa en los switch de la red.

A continuación, presentamos el procedimiento sobre cómo podemos implementar la tecnología de VLAN en un Cisco Catalyst Switch:

Paso #1: Cómo Mostrar en pantalla las VLANs

SW1>**enable**

Entra al modo privilegiado

SW1#**show vla**

Muestra en pantalla las VLANs creadas en el Cisco IOS **Paso #2: Cómo crear una VLAN** SW1#**configure terminal**

Entra al modo privilegiado

SW1(config)#**vlan 10**

Crear la VLAN 10

SW1(config-vlan)#**name CAPACITY**

Configura la etiqueta "CAPACIY" a la VLAN 10

SW1(config)#**vlan 10**

Crear la VLAN 10

SW1(config-vlan)#**name CAPACITY**

Configura la etiqueta "CAPACIY" a la VLAN 10

SW1(config-vlan)#**exit**

Sale al modo de configuración anterior

SW1(config)#**vlan 20**

Crear la VLAN 20

SW1(config-vlan)#**name CISCO**

Configura la etiqueta "CISCO" a la VLAN 20

SW1(config-vlan)#**exit**

Sale al modo de configuración anterior

SW1(config)#**vlan 30**

Crear la VLAN 30

SW1(config-vlan)#**name ENGLISHENVIVO**

Configura la etiqueta "ENGLISHENVIVO" a la VLAN 30

SW1(config-vlan)#**exit**

Sale al modo de configuración anterior

Paso #3: Cómo asignar un puerto a una VLAN

SW1(config)#**interface f0/1**

Entra al modo de configuración de interface

SW1(config-if)#**switchport mode access**

Configura la interface en el modo "access"

SW1(config-if)#**switchport access vlan 20**

Asigna la interface a la VLAN 20

SW1(config-if)#**no**
shutdown *Inicializa la interface de switch*
SW1(config-if)#**exit**

SW1(confi
g)#**exit**

Paso #4: Cómo borrar una VLAN

SW1#**configure**
terminal *Entra al modo privilegiado*
SW1(config)#**no**
vlan 10

Borra la VLAN 10

Si quieres borrar todas las VLANs creados en un Cisco Switch solo debes de borrar el archivo **vlan.dat** almacenado en la memoria flash del Swtich.

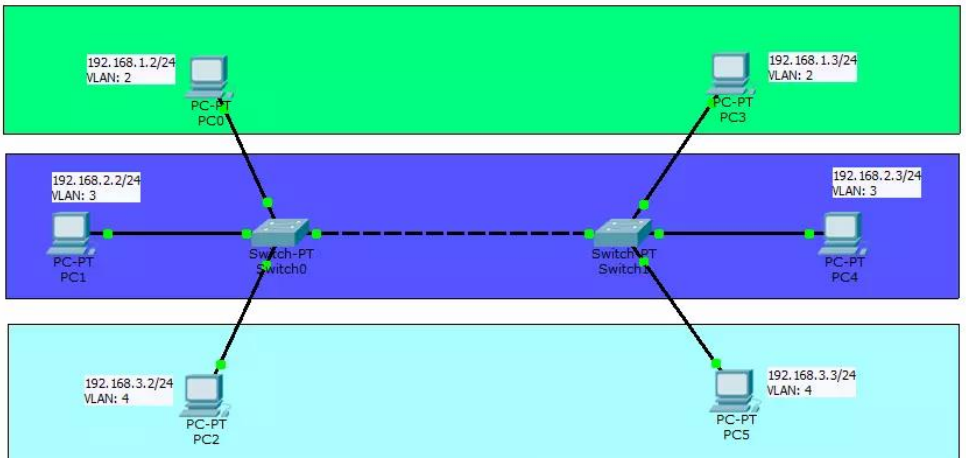
SW1#**delete**
flash:vlan.dat

4.3 VLAN en packet tracer

Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4).

Una VLAN consiste en dos o más redes de computadoras que se comportan como si estuviesen conectados al mismo PCI, aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local (LAN). Los administradores de red configuran las VLAN mediante software en lugar de hardware, lo que las hace extremadamente fuertes.

Para el ejemplo siguiente, es necesario crear desde el GUI el siguiente esquema de red. Es bastante sencillo e intuitivo, por lo que no explicaré esta parte. Nuestra red constará de 6 ordenadores, 2 switches y la red la dividiremos en 3 VLANs. Cada equipo solo podrá acceder a equipos de su misma VLAN.



En la siguiente tabla muestro como he realizado el conexionado de los SWITCHES y los PCs. Los switches se conectan por la interfaz Fa3/1 de cada uno de ellos, con cable cruzado y en modo trunk (ver explicación más abajo):

COMPUTER	IP ADDRESS	SWITCH	NIC	SWITCH PORT	VLAN
PC0	192.168.1.2	Switch0	Fa0	Fa0/1	2
PC1	192.168.2.2	Switch0	Fa0	Fa1/1	3
PC2	192.168.3.2	Switch0	Fa0	Fa2/1	4
PC3	192.168.1.3	Switch1	Fa0	Fa0/1	2
PC4	192.168.2.3	Switch1	Fa0	Fa1/1	3
PC5	192.168.3.3	Switch1	Fa0	Fa2/1	4

Para asignar las IPs y la máscara de Red de nuestros equipos, haremos doble click en la interfaz gráfica en cada de uno de ellos y en **IP Configuration** introducimos la IP y su máscara de red. El Gateway y DNS no son necesarios para este ejemplo. En nuestro caso usaremos una **máscara** de red /24, por tanto 255.255.255.0

SWITCH0

Creamos las 3 VLANs necesarias. Le asignaremos un nombre a cada una de ellas: 2=oficina1,

```
Switch#config
Configuring from terminal, memory, or network [terminal]? terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name oficina1
Switch(config-vlan)#vlan 3
Switch(config-vlan)#name oficina2
Switch(config-vlan)#vlan 4
Switch(config-vlan)#name oficina3
Switch(config-vlan)#
```

3=oficina2 y 4=oficina3:

Ahora podemos hacer un listado de las VLANs que tenemos creadas. Podemos ver que no tienen a Switch#show vlan

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1, Fa1/1, Fa2/1, Fa3/1

Fa4/1, Fa5/1

2 oficina1 active

3 oficina2 active

4 oficina3 active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup signado ningún puerto:

Asignaremos los puertos a cada VLAN. En nuestro caso es un puerto por cada VLAN:

Switch#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#interface FastEthernet 0/1

Switch(config-if)#switchport access vlan 2

Switch(config)#interface FastEthernet 1/1

Switch(config-if)#switchport access vlan 3

Switch(config-if)#interface FastEthernet 2/1

Switch(config-if)#switchport access vlan 4

Para que ambos Switches compartan la información de sus VLANS, las interfaces que interconectan ambos switches debe estar en modo **Trunk**:

Switch(config)#interface FastEthernet 3/1

Switch(config-if)#switchport mode trunk

Switch(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet3/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet3/1, changed state to up

Tras configurar las interfaces y las VLANs, podemos ver que cada VLAN ahora tiene un puerto asignado:

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa4/1, Fa5/1
2    oficina1                         active    Fa0/1
3    oficina2                         active    Fa1/1
4    oficina3                         active    Fa2/1
```

SWITCH1

Repetimos los mismos pasos del SWITCH0 **teniendo en cuenta** el conexionado de la tabla del principio del "ejercicio".

Creamos las 3 VLANs necesarias. Le asignaremos un nombre a cada una de ellas: 2=oficina1, 3=oficina2 y 4=oficina3:

```
Switch#config

Configuring from terminal, memory, or network [terminal]? terminal

Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Switch(config)#vlan 2
Switch(config-vlan)#name oficina1
Switch(config-vlan)#vlan 3
Switch(config-vlan)#name oficina2
Switch(config-vlan)#vlan 4
Switch(config-vlan)#name oficina3
Switch(config-vlan)#
```

Ahora podemos hacer un listado de las VLANs que tenemos creadas. Podemos ver que no tienen asignado ningún puerto:

```
Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa1/1, Fa2/1, Fa3/1
                                                 Fa4/1, Fa5/1
2    oficina1                          active
3    oficina2                          active
4    oficina3                          active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Asignaremos los puertos a cada VLAN. En nuestro caso es un puerto por cada VLAN:

```
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport access vlan 2
Switch(config)#interface FastEthernet 1/1
Switch(config-if)#switchport access vlan 3
Switch(config-if)#interface FastEthernet 2/1
Switch(config-if)#switchport access vlan 4
```

Para que ambos Switches compartan la información de sus VLANS, las interfaces que interconectan ambos switches debe estar en modo **Trunk**:

```
Switch(config)#interface FastEthernet 3/1
Switch(config-if)#switchport mode trunk


Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet3/1, changed state to down


%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet3/1, changed state to up
```

Tras configurar las interfaces y las VLANs, podemos ver que cada VLAN ahora tiene un puerto asignado:

```
Switch#show vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa4/1, Fa5/1
2    oficina1                          active    Fa0/1
3    oficina2                          active    Fa1/1
```

```
4    oficina3                    active    Fa2/1
```

Ahora podremos ver que desde PC0 solo podemos hacer PING a PC3, desde PC1 a PC4 y desde PC2 a PC4 y viceversa.

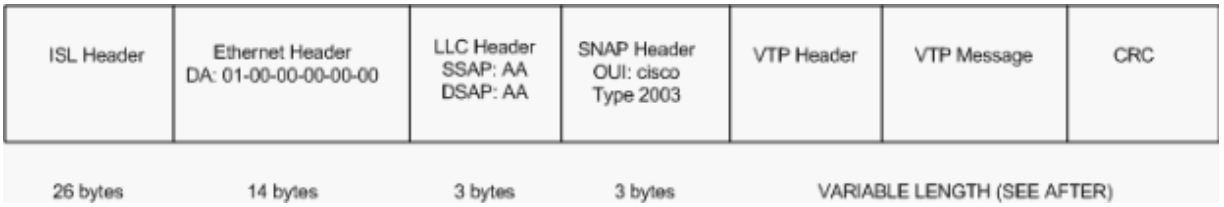
4.4.- VTP.

El VLAN Trunk Protocol (VTP) reduce la administración en una red de switch. Al configurar una VLAN nueva en un servidor VTP, se distribuye la VLAN a través de todos los switches del dominio. Esto reduce la necesidad de configurar la misma VLAN en todas partes. VTP es un protocolo de propiedad de Cisco que está disponible en la mayoría de los productos de la serie Cisco Catalyst.

Mensajes VTP en detalle

Los paquetes VTP se envían en las tramas de Inter-Switch Link (ISL) o en las tramas de IEEE 802.1Q (dot1q). Estos paquetes se envían a la dirección MAC de destino 01-00-0C-CC-CC- CC con un código de control de link lógico (LLC) de Subnetwork Access Protocol (SNAP)

(AAAA) y un tipo de 2003 (en el encabezado SNAP). A continuación, se presenta el formato de un paquete VTP encapsulado en tramas ISL:



Por supuesto, puede tener un paquete VTP dentro de tramas 802.1Q. En ese caso, el encabezado ISL y la verificación por redundancia cíclica (CRC) es sustituido por el etiquetado dot1q.

Ahora considere el detalle de un paquete VTP. El formato de encabezado VTP puede variar, en función del tipo de mensaje VTP. Pero, todos los paquetes VTP contienen estos campos en el :

- Versión del protocolo VTP: 1, 2, o 3
- Tipos de mensaje VTP:
- Anuncios de resumen
- Anuncio de subgrupos
- Solicitudes de anuncio
- Mensajes de unión VTP
- Extensión del dominio de administración
- Nombre de dominio de administración

Número de Revisión de la Configuración

El número de revisión de configuración es un número de 32 bit que indica el nivel de revisión para un paquete VTP. Cada dispositivo VTP rastrea el número de revisión de configuración VTP que se asigna a él. La mayor parte de los paquetes VTP contienen el número de revisión de la configuración VTP del remitente.

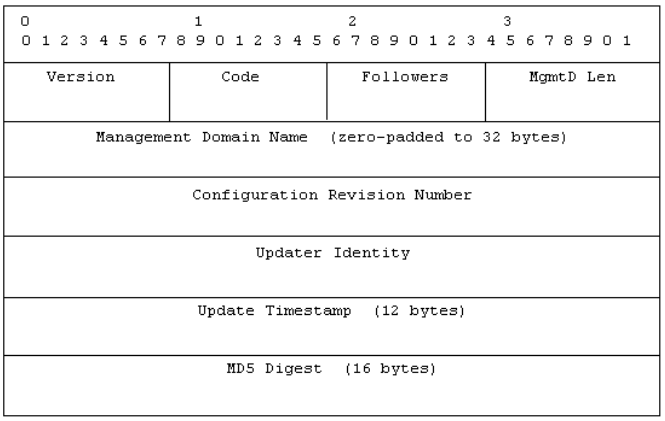
Esta información se usa para determinar si la información recibida es más reciente que la versión actual. Cada vez que modifica la VLAN en un dispositivo VTP, la revisión de la configuración se incrementa en uno. Para reiniciar la revisión de configuración en un switch, cambie el nombre del dominio VTP y después vuelva a cambiarlo e ingrese el nombre original.

Anuncios del Resumen

Los switches Catalyst emiten anuncios de resumen en aumentos de 5 minutos de forma predeterminada. Los anuncios de resumen le informan a los Catalyst adyacentes el nombre de dominio VTP actual y el número de revisión de la configuración.

Cuando el switch recibe un paquete de anuncio de resumen, el switch compara el nombre de dominio VTP con su propio nombre de dominio VTP. Si el nombre es diferente, el switch simplemente ignora el paquete. Si el nombre es el mismo, el switch compara la revisión de la configuración con su propia revisión. Si su revisión de configuración es más alta o igual, se ignora el paquete. Si es inferior, se envía una solicitud de anuncio.

Summary Advert Packet Format:



La lista siguiente explica el significado del campo en el paquete de anuncios:

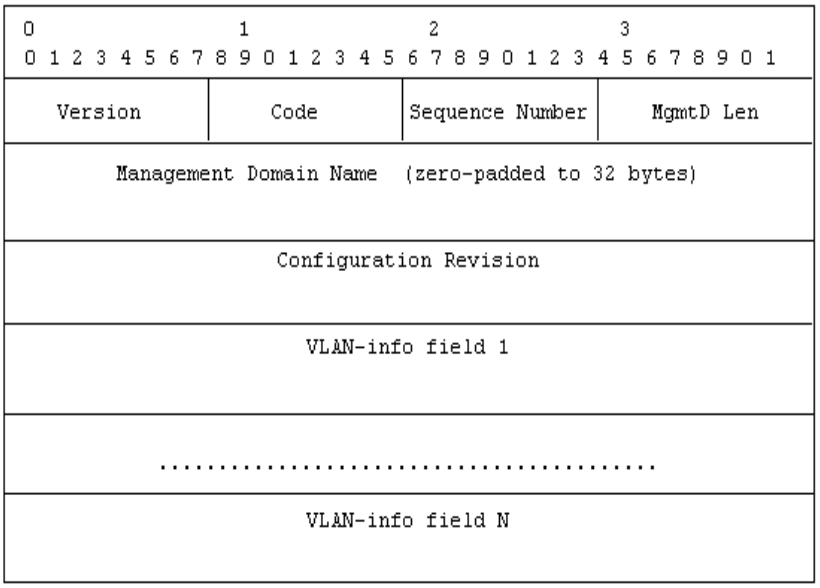
El campo de Seguidores indica que este paquete es seguido por un paquete de Anuncio de Subgrupo.

- La identidad que actualiza es la dirección de IP del switch que sea el último en haber incrementado la revisión de su configuración.
- El Fechado de Actualización es la fecha y la hora del último incremento de la revisión de configuración.
- Message Digest 5 (MD5) lleva la contraseña del VTP si se configuró y usó para autentificar la validación de una actualización del VTP.

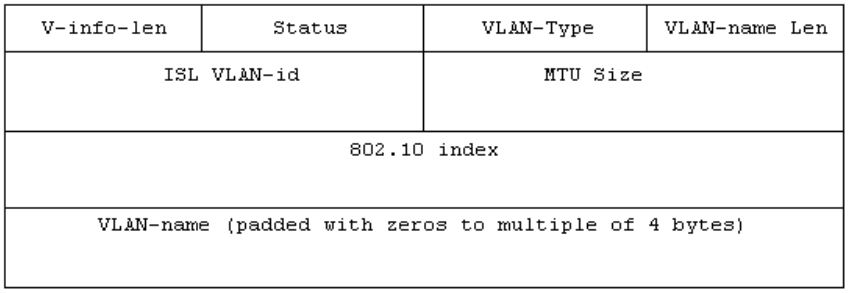
Anuncios de subgrupos

Cuando agrega, elimina o cambia una VLAN en un Catalyst, el servidor Catalyst aumenta la revisión de configuración donde ser realizaron los cambios y emite un anuncio de resumen, seguido de uno o varios anuncios de subconjuntos. Uno o varios avisos de subconjunto siguen el anuncio de resumen. Un anuncio de subconjuntos contiene una lista de información VLAN. Si existen varias VLAN, es posible que se requiera más de un anuncio de subgrupos para anunciar todas las VLAN.

Subset Advert Packet Format:



El siguiente ejemplo formateado muestra que cada campo de información VLAN contiene información para una VLAN diferente. Se ha ordenado de manera que los ID de VLAN ISL aparezcan primero:

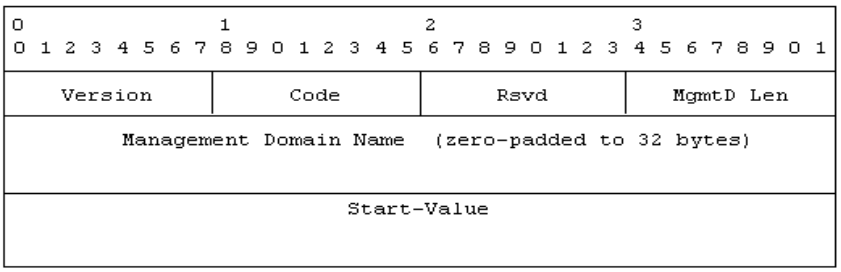


La mayoría de los campos de este paquete son fáciles de entender. Las siguientes son dos aclaraciones:

- **Código** —El formato que corresponde es 0x02 para el anuncio de subgrupo.
- **Número de secuencia**: esta es la secuencia del paquete en el flujo de paquetes posterior a un anuncio de resumen. La secuencia comienza con 1.

Solicitudes de Anuncio

- Un switch requiere una solicitud de anuncio de VTP en las siguientes situaciones:
- El switch fue restablecido.
- Se ha cambiado el Domain Name VTP.
- El switch ha recibido un anuncio de resumen VTP con una revisión de la configuración mayor.
- Cuando se recibe una solicitud de anuncio, un dispositivo VTP envía un anuncio de resumen. Uno o varios anuncios de subgrupos siguen el anuncio de resumen. Aquí tiene un ejemplo:



- **Código**: el formato que corresponde es 0x03 para el anuncio de subconjunto.

- **Start-Value**: esto se utiliza en los casos en los que existen diversos anuncios de subconjuntos. Si el primer anuncio de subconjunto (n) se ha sido recibido y el subsiguiente, (*n+1*) no se ha recibido, el Cataslyst sólo solicita anuncios de (*n+1*) .

4.5 Modos VTP

Se puede configurar la mayoría de los switches para que funcionen en cualquiera de estos modos de VTP:

• **Servidor:** En el modo de servisor VTP, puede crear, modificar y eliminar VLAN, y especificar otros parámetros de configuración, como la versión VTP y el recorte VTP, para el dominio completo de VTP. Los servidores VTP anuncian su configuración VLAN a los otros switches en el mismo dominio VTP y sincronizan su configuración VLAN con otros switches en función de los avisos recibidos en los links de trunk. El servidor VTP es el modo predeterminado.

- Cliente: los clientes VTP se comportan de la misma manera que los servidores VTP, pero no pueden crear, cambiar, o eliminar las VLAN en un cliente VTP.
- Transparente: los switches VTP transparente no participan en VTP. Un switch VTP transparente no anuncia su configuración VLAN y no sincroniza su configuración VLAN en función de los anuncios recibidos; sin embargo, en la versión 2 VTP, los switches transparentes reenvían anuncios VTP que reciben los switches por sus puertos de trunk.
- Desconectado (configurable solo en los switches CatOS): en los tres modos descritos, se reciben y se transmiten los avisos VTP tan pronto como el switch ingrese el estado

• Desconectado (configurable solo en los switches CatOS): en los tres modos descritos, se reciben y se transmiten los avisos VTP tan pronto como el switch ingrese el estado del dominio de administración. En el modo de VTP desconectado, Los switches que funcionan en modo transparente descartan los anuncios VTP si no están en el mismo dominio VTP.

VTP V2 y VTP V1 no son muy diferentes. La diferencia principal es que VTP V2 introduce el soporte para las VLAN de Token Ring. Si utiliza las VLAN de Token Ring, debe habilitar VTP V2. De otra manera, no hay razón para usar VTP V2. Cambiar la versión de VTP de 1 a 2, no hará que switch se recargue.

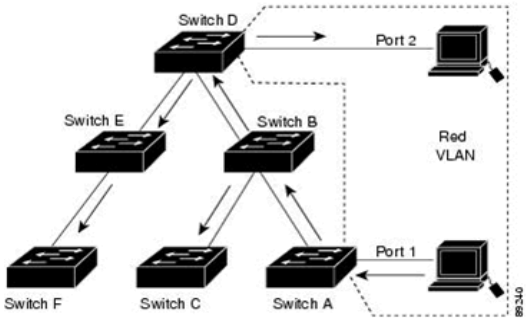
Contraseña VTP

Si configura una contraseña para el VTP, debe configurar la contraseña en todos los switches en el dominio VTP. La contraseña debe ser la misma contraseña en todos esos switches. La contraseña VTP que configura se traduce mediante un algoritmo en una palabra de 16 bytes (valor MD5) que figura en todos los paquetes de anuncios de resumen VTP.

Recorte vtp

El VTP se asegura de que todos los switches en el dominio de VTP tengan en cuenta a todas las VLAN. En ocasiones, sin embargo, VTP puede crear tráfico innecesario. Todos las unicasts y broadcasts que se producen en VLAN se inundan en toda la VLAN. Todos los switches de la red reciben todos los broadcasts, incluso en situaciones en las que sean pocos los usuarios conectados a esa VLAN. Los recortes VTP son una función que utiliza para eliminar o *recortar* este tráfico innecesario.

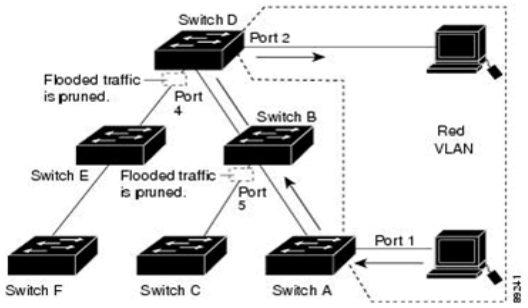
Tráfico de broadcast en una red de switch sin recorte



Esta figura muestra una red de switch sin los recortes VTP habilitados. El puerto 1 en el Switch A y el puerto 2 en el Switch D se asignan a la VLAN Roja. Si se envía un broadcast del host conectado al Switch A, el Switch A inunda el broadcast y cada switch en la red lo recibe, aunque los Switches C, E, y F no tienen puertos en la VLAN Roja.

Tráfico de broadcast en una red de switch con recorte

Esta figura muestra la misma red de switch con los recortes VTP habilitados. El tráfico de broadcast del Switch A no se reenvía a los switches C, E, y F porque el tráfico para la VLAN roja se ha recortado en los links mostrados (el Puerto 5 en el Switch B y el Puerto 4 en el Switch D).



Cuando los recortes VTP se habilitan en un servidor VTP, el recorte se habilita para el dominio de administración completo. Hacer que las VLAN sean elegibles o no para el recorte afecta la elegibilidad del recorte para estas VLAN en ese trunk solamente (no todos los switches en el dominio VTP). Los recortes VTP surten efecto varios segundos después de que los habilite. Los recortes VTP no recortan el tráfico de las VLAN que no son elegibles para el recorte. Las VLAN1 y las VLAN 1002 a 1005 no son eleglibles nunca para el recorte; el tráfico de estas VLAN no puede ser recortado. Las VLAN de rango extendido (ID de VLAN mayores de 1005) tampoco son elegibles para el recorte.

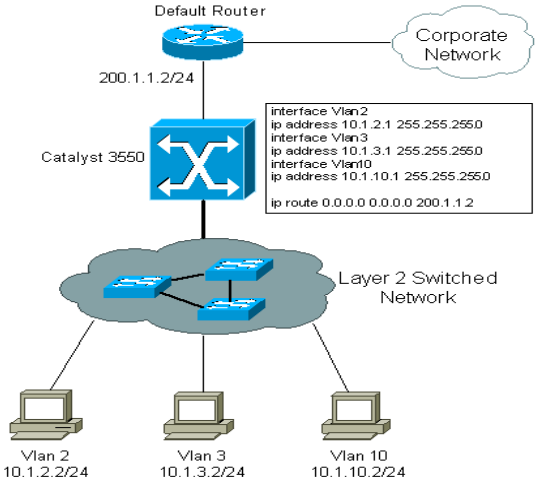
4.6 Utilizar el VTP en una Red

De manera predeterminada, todos los switches son configurados para ser servidores VTP. Esta configuración es conveniente para las redes a escala reducida en las que los tamaños de la información de VLAN son pequeños y la información se almacena fácilmente en todos los switches (en el NVRAM). En las redes de gran escala, el administrador de la red debe decidir en algún momento cuándo el almacenamiento NVRAM que es necesario resulta inútil por estar duplicado en cada switch. En este momento, el administrador de red debe seleccionar unos pocos switches bien equipados y mantenerlos como servisores VTP. Todos los demás dispositivos que

participen en el VTP se convertirán en clientes. La cantidad de servidores VTP debería seleccionarse para determinar el grado de redundancia que se espera que tenga la red.

4.6.- Ruteo entre VLANS.

Este diagrama lógico explica un escenario sencillo de ruteo entre VLAN. El escenario se puede ampliar para incluir un entorno del multi-Switch si usted primero configura y prueba la Conectividad del inter-Switch a través de la red antes de que usted configure la capacidad de ruteo. Para tal escenario, donde se utiliza un Catalyst 3550, consulte Configuración del Ruteo InterVLAN con Catalyst 3550 Series Switches.



Instrucciones paso a paso

Complete estos pasos para configurar un Switch para realizar el InterVLAN Routing.

• Habilite el encaminamiento en el Switch con el **comando ip routing**. Incluso si se habitó previamente el ruteo IP, este paso garantiza que estará activado. Switch(config)#**ip routing**

• Anote las VLAN entre las que desea rutear. En este ejemplo, se desea rutear el tráfico entre las VLAN 2, 3 y 10.

• Utilice el **comando show vlan** para verificar que los VLA N existen en la base de datos de VLAN. Si no existen, agréguelas al switch. Este ejemplo muestra la adición de los VLA N 2,3, y 10 a la base de datos de VLAN del Switch

1. Switch#**vlan database**
2. Switch(vlan)#**vlan 2**
3. VLAN 2 added:
4. Name: VLAN0002
5. Switch(vlan)#**vlan 3**
6. VLAN 3 added:
7. Name: VLAN0003
8. Switch(vlan)#**vlan 10**
9. VLAN 10 added:
10. Name: VLAN0010
11. Switch(vlan)#**exit**
12. APPLY completed.

    Exiting....

Determine las direcciones IP que desee asignar a la interfaz de VLAN en el switch. Para que el switch pueda rutear entre las VLAN, las interfaces de VLAN deben estar configuradas con una dirección IP. Cuando el Switch recibe un paquete destinado para otro subnet/VLAN, el Switch mira la tabla de ruteo para determinar donde remitir el paquete. Luego, el paquete se pasa a la interfaz de VLAN del destino. Se envía, a su vez, al puerto donde se conecta el dispositivo extremo.

• Configure las interfaces de VLAN con la dirección IP identificada en el paso 4.

Switch#**configur**

e terminal

Enter configuration commands, one per line. End with

CNTL/Z. Switch(config)#**interface Vlan2**

Switch(config-if)#**ip address 10.1.2.1**

255.255.255.0

Switch(config-if)#**no**

shutdown

Repita este proceso para todas las VLAN que se identificaron en

el paso 1.

- Configure la interfaz al router predeterminado. En este caso, cuenta con un puerto

FastEthernet

de Capa 3.

1. Switch(config)#**interface**

FastEthernet 0/1

2. Switch(config-if)#**no switchport**
3. Switch(config-if)#**ip address 200.1.1.1 255.255.255.0**

   Switch(config-if)#**no shutdown**

- Configure la ruta predeterminada para el switch. Switch(config)#**ip route 0.0.0.0 0.0.0.0 200.1.1.2**

En la sección Tarea del diagrama, note que la dirección IP del router predeterminado es 200.1.1.2. Si el switch recibe un paquete para una red que no se encuentra en la tabla de ruteo, lo reenviará al gateway predeterminado para un procesamiento adicional. En el switch, verifique que usted pueda hacer ping con el router predeterminado.

• Configure los dispositivos extremos para utilizar la respectiva interfaz de VLAN del Catalyst 3550 como su gateway predeterminado. Por ejemplo, los dispositivos en la VLAN 2 deben utilizar la dirección IP de la interfaz de VLAN 2 como su gateway predeterminado. Para obtener más información sobre cómo designar el gateway predeterminado, consulte la guía de configuración de cliente correspondiente.

4.7 Algoritmos de control de congestión

Es un concepto más amplio que el control de flujo. Comprende todo un conjunto de técnicas para detectar y corregir los problemas que surgen cuando no todo el tráfico ofrecido a una red puede ser cursado, con los requerimientos de retardo, u otros, necesarios desde el punto de vista de la calidad del servicio. Por tanto, es un concepto global, que involucra a toda la red, y no sólo a un remitente y un destinatario de información, como es el caso del control de flujo.

El control de flujo es una más de las técnicas para combatir la congestión. Se consigue con ella parar a aquellas fuentes que vierten a la red un tráfico excesivo. Sin embargo, como veremos, hay otros mecanismos. Una vez hecha esta distinción, en los sucesivos apartados veremos características del retardo y del caudal, veremos distintas causas de aparición de congestión, analizaremos las soluciones que se proponen para este problema y acabaremos viendo distintos algoritmos de control de congestión.

Ventana de congestion: Al establecer una conexión, el emisor asigna a la ventana de congestión el tamaño de segmento máximo usado por la conexión; entonces envía un segmento máximo. Si se recibe la confirmación de recepción de este segmento antes de que expire el temporizador, el emisor agrega el equivalente en bytes de un segmento a la ventana de congestión para hacerla de dos segmentos de tamaño máximo, y envía dos segmentos. A medida que se confirma cada uno de estos segmentos, se aumenta el tamaño de la ventana de congestión en un segmento máximo. Cuando la ventana de congestión es de n segmentos, si de todos los n se reciben confirmaciones de recepción a tiempo, se aumenta el tamaño de la ventana de

congestión en la cuenta de bytes correspondiente a n segmentos. De hecho, cada ráfaga confirmada duplica la ventana de congestionamiento.

Algoritmo de control de congestión de Internet. Este algoritmo requiere de un parámetro llamado umbral, inicialmente de 64 KB, además de las ventanas de recepción y congestión. Al ocurrir una expiración del temporizador, se establece el umbral en la mitad de la ventana de congestión actual, y la ventana de congestión se restablece a un segmento máximo. Luego se usa el arranque lento para determinar lo que puede manejar la red, excepto que el crecimiento exponencial termina al alcanzar el umbral. A partir de este punto, las transmisiones exitosas aumentan linealmente.

Control de Flujo

El control de flujo es el proceso de gestionar la tasa de transmisión de datos entre dos nodos. El objetivo de esto es prevenir que un transmisor rápido exceda a un receptor lento. Provee mecanismos para que el receptor controle la velocidad de transmisión, haciendo que el nodo receptor no se sature con los datos entrantes. El control de flujo debe distinguirse del control de congestión, el cual es usado para controlar el flujo de datos cuando la congestión ya está ocurriendo. Éste es muy importante porque un emisor puede llegar a enviar datos mucho más rápido de lo que un emisor puede recibirlos y procesarlos, ya que puede generar pérdida de información.

En este método, el receptor indica su disposición a recibir los datos para cada trama, el mensaje se divide en múltiples marcos. Los emisores espera para un ACK (reconocimiento) después de cada cuadro por el tiempo especificado (llamado tiempo de espera). Se envía a asegurar que el receptor ha recibido la trama correctamente. A continuación, enviar el siguiente fotograma sólo después de que se haya recibido el ACK. Operaciones

- Remitente: Transmite un solo cuadro a la vez.
- Receptor: Transmite acuse de recibo (ACK), ya que recibe una trama.
- Remitente recibe ACK dentro de tiempo de espera.
- Vaya al paso 1.

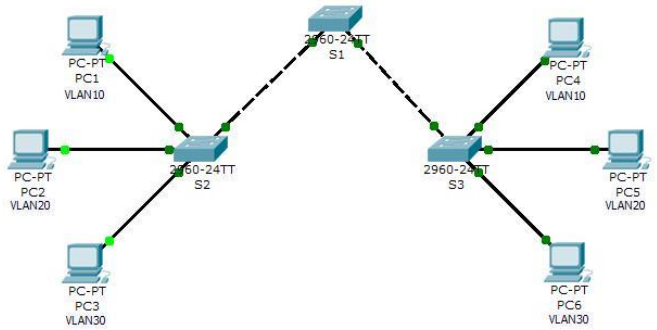
Si se pierde un marco o ACK durante la transmisión, entonces tiene que ser transmitidos de nuevo por el remitente. Este proceso se conoce como retransmisión ARQ (petición de repetición automática). El problema con Stop-and espera es que sólo un fotograma se puede transmitir a la vez, y que a menudo conduce a la transmisión ineficiente, ya que hasta el remitente

recibe el ACK no puede transmitir cualquier nuevo paquete. Durante este tiempo tanto el emisor y el canal son no utilizados.

4.8 Configuración VTP

En esta actividad, practicará la configuración del VTP. Cuando Packet Tracer se abre por primera vez los switches ya contienen una configuración parcial, por eso recomiendo descargar el archivo .pka situado abajo del todo.

Partiendo de la siguiente topología procederemos a:



Paso 1. Verifique la configuración en ejecución actual de los switches.

¿Qué configuraciones ya están presentes en los switches?

Paso 2. Muestre las VLAN actuales de cada switch.

¿Hay alguna VLAN presente? Las VLAN, ¿las crea el usuario o son VLAN por defecto?

```
S1#show vlan brief
VLAN Name                Status    Ports
---- ----------------------- --------- -------------------------------
1    default                 active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                       Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                       Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                       Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                       Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                       Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                       Gig1/1, Gig1/2
```

```
1002 fddi-default              active
1003 token-ring-default        active
1004 fddinet-default           active
1005 trnet-default             active
```

Al final de esta tarea, el porcentaje de finalización debe ser del 0%.

4.9 Configuración servidor VTP

Paso 1. Configure el comando del modo VTP.

El S1 es el servidor para el VTP. Establezca el S1 en modo servidor.

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#
```

Observe que el switch ya está establecido para el modo servidor por defecto. Sin embargo, es importante que usted configure este comando de manera explícita para asegurarse que el switch esté en modo servidor.

Paso 2. Configure el nombre del dominio VTP.

Configure el S1 con **CCNA** como nombre de dominio VTP. Recuerde que los nombres de dominio VTP distinguen mayúsculas de minúsculas.

```
S1(config)#vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S1(config)#
```

Paso 3. Configure la contraseña de dominio VTP.

Configure el S1 con **cisco** como contraseña de dominio VTP. Recuerde que las contraseñas de dominio VTP distinguen mayúsculas de minúsculas.

```
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#
```

Paso 4. Confirme los cambios de configuración.

Utilice el comando **show vtp status** del S1 para confirmar que el modo y el dominio VTP se configuraron correctamente.

```
S1#show vtp status
```

VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 64
Number of existing VLANs : 5
VTP Operating Mode : Server
VTP Domain Name : CCNA
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x8C 0x29 0x40 0xDD 0x7F 0x7A 0x63
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Para verificar la contraseña VTP, utilice el comando **show vtp password**.

S1#**show vtp password** VTP Password: cisco
S1#

Paso 5. Verifique los resultados.

Su porcentaje de finalización debe ser del 8%. De lo contrario, haga clic en **Check Results** para saber cuáles son los componentes requeridos que aún no se completan.

.

4.10 Configuración clientes VTP

Paso 1. Configure el comando del modo VTP.

El S2 y el S3 son clientes VTP. Establezca estos dos switches en modo cliente.

Paso 2. Configure el nombre del dominio VTP.

Antes de que S2 y S3 acepten las publicaciones VTP desde S1, deben pertenecer al mismo dominio VTP. Configure S2 y S3 con **CCNA** como el nombre de dominio de VTP. Recuerde que los nombres de dominio VTP distinguen mayúsculas de minúsculas.

Paso 3. Configure la contraseña de dominio VTP.

Además, S2 y S3 deben utilizar la misma contraseña antes de que puedan aceptar las publicaciones VTP del servidor VTP. Configure S2 y S3 con **cisco** como la contraseña de dominio de VTP. Recuerde que las contraseñas de dominio VTP distinguen mayúsculas de minúsculas.

Paso 4. Confirme los cambios de configuración.

Utilice el comando **show vtp status** de cada switch para confirmar que el modo y el dominio VTP se configuraron correctamente. Aquí se muestra el resultado para el S3.

S3#**show vtp status**

```
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x8C 0x29 0x40 0xDD 0x7F 0x7A 0x63
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Observe que el número de revisión de la configuración es 0 en los tres switches. ¿Por qué?

Para verificar la contraseña VTP, utilice el comando **show vtp password**.

```
S3#show vtp password
VTP Password: cisco
S3#
```

Paso 5. Verifique los resultados.

Su porcentaje de finalización debe ser del 31%. De lo contrario, haga clic en **Check Results** para saber cuáles son los componentes requeridos que aún no se completan.

4.11 Configurar las VLAN en VTP

Las VLAN se pueden crear en el servidor VTP y distribuir a otros switches en el dominio VTP. En esta tarea, usted crea 4 VLAN nuevas en el servidor VTP del S1. Estas VLAN se distribuyen al S2 y al S3 por medio del VTP.

Paso 1. Cree las VLAN.

Para efectos de calificación en Packet Tracer, los nombres de las VLAN distinguen mayúsculas de minúsculas.

- VLAN 10 con el nombre **Faculty/Staff**
- VLAN 20 con el nombre **Students**
- VLAN 30 con el nombre **Guest(Default)**
- VLAN 99 con el nombre **Management&Native**

Paso 2. Verifique las VLAN.

Utilice el comando **show vlan brief** para verificar las VLAN y sus nombres.

```
S1#show vlan brief
VLAN Name                    Status    Ports
---- ------------------------ --------- -------------------------------
1    default                  active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                        Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                        Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                        Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                        Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                        Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                        Gig1/1, Gig1/2
10   Faculty/Staff            active
20   Students                 active
30   Guest(Default)           active
99   Management&Native        active
1002 fddi-default             active
1003 token-ring-default       active
1004 fddinet-default          active
1005 trnet-default            active
```

Si usted ingresa el mismo comando en S2 y S3, observa que las VLAN no se encuentran en su base de datos VLAN. ¿Por qué no?

Paso 3. Verifique los resultados.

Su porcentaje de finalización debe ser del 46%. De lo contrario, haga clic en **Check Results** para saber cuáles son los componentes requeridos que aún no se completan.

Bibliografía

TITULO	AUTOR	EDITORIAL
Redes de computadoras	Tanenbaum	Pearseon
Redes de computadoras	Olifer, Natalia	Digital
Transmision de datos y redes de computadoras	Forouzan	McGraw Hill