UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE UNA RED CORPORATIVA CON SERVICIOS NAT, DHCP Y VLANS SIMULANDO LA NUBE FRAME RELAY CON UN ROUTER

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

VICTOR LORENZO ALAYO SALAZAR

PROMOCIÓN
2003- I
LIMA – PERÚ
2008

DISEÑO DE UNA RED CORPORATIVA CON SERVICIOS NAT, DHCP Y VLANS SIMULANDO LA NUBE FRAME RELAY CON UN ROUTER

A mis padres quienes con su grandes enseñanzas me han enseñado los verdaderos valores de la vida.

SUMARIO

El presente trabajo muestra el diseño y la configuración de una red de datos de una empresa, con 4 sedes, cada una con un router, tres de las cuales se conectarán mediante enlaces seriales de línea dedicada. La cuarta oficina (Arequipa), se conectará mediante Frame Relay por cuestiones de costo. La oficina en Arequipa utiliza RIP V2 para el enrutamiento, las otras tres oficinas utilizarán OSPF, aquí se verá la manera en que las rutas RIP se deben redistribuir al proceso de enrutamiento OSPF.

La oficina de Surco, posee una LAN grande y compleja. Debido a su tamaño y complejidad, se crearán algunas VLAN para controlar broadcast, aumentar la seguridad y agrupar los usuarios de forma lógica. Además se usarán direcciones privadas y DHCP en toda la WAN. Se implementará NAT para permitir la conexión a Internet.

Para utilizar eficientemente y minimizar el desperdicio en el espacio de direcciones, se utilizarán mascaras de subred de longitud variable.

INDICE

PROLOGO

El propósito del presente trabajo, es mostrar la implementación de una red a nivel LAN y WAN, asi como los servicios y ventajas que se pueden implementar en un router y switches.
Se mostrará el direccionamiento IP V4, partiendo de una dirección IP dada, se detallara el proceso de configuración de un router, de acuerdo a lo que se requiera, asi como la creación de VLANS en un switch.
En el Capitulo I se describe la Ingeniería del Problema, enunciando lo solicitado, objetivos que se alcanzan y las limitaciones del mismo.
En el Capitulo II, se presenta la base teórica sobre la cual se sustenta dicho trabajo, definiciones de términos usados, formas de configuración de los dispositivos, asi como las ventajas y desventajas en el uso de estas tecnologías.
En el Capitulo III, se hace el diseño de la red, empezando a elaborar lo solicitado por medio de cálculos y consideraciones a tomar en cuenta al direccionar la red a partir de un numero IP asignado a la empresa.
Finalmente en el Capitulo IV se realizan las configuraciones necesarias para lograr los objetivos trazados en el problema, ingresando comandos usuales de configuración en routers y switches.

CAPITULO I
PLANTEAMIENTO DE INGENIERIA DEL PROBLEMA

1.1. Descripción del problema

Se muestra el gráfico (Figura 1.1) del problema planteado.

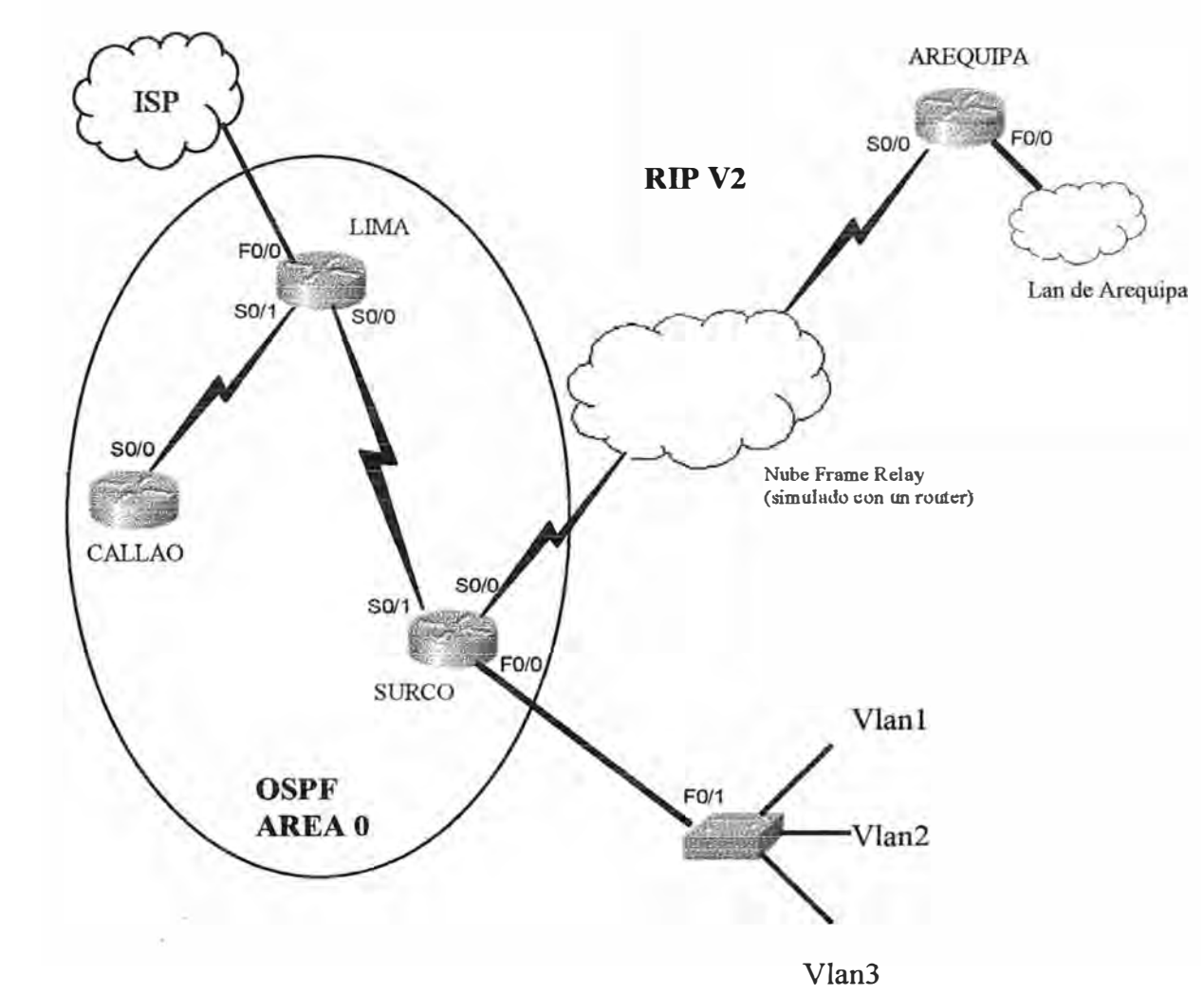


Fig. 1.1 Diagrama Completo

Una empresa necesita que se diseñe e implemente una red. La empresa tiene oficinas en cuatro ubicaciones: Lima, Callao, Surco y Arequipa. Callao. Lima y Surco se conectarán mediante enlaces seriales de linea dedicada. Una cuarta oficina, Arequipa, se conectara mediante Frame Relay por cuestiones de costo.

Se debe usar la dirección de clase B 172.16.0.0 fullclass para el direccionamiento interno.

Anteriormente , la empresa utilizaba RIP V2 en Arequipa, y por el momento desea seguir usando esta opción. Sin embargo, las otras tres oficinas usarán OSPF, de manera que las rutas RIP se deben redistribuir al proceso de enrutamiento OSPF y viceversa.

Surco, posee una LAN grande y compleja con 750 dispositivos. Debido a su tamaño y complejidad, la empresa desea crear algunas VLANs para controlar el broadcast, aumentar la seguridad y agrupar los usuarios de forma lógica.

La empresa también desea usar direcciones privadas y DHCP en Arequipa que debe tener capacidad para 512 dispositivos.

Se desea implementar NAT con traducción dinámica para permitir a conexión a Internet, en el router de Lima, el conjunto NAT que le entrega el Proveedor de Internet es 192.168.1.6 / 30, y sólo deben permitirse la salida a las direcciones internas (172.16.0.0 / 16) y negarse todo el trafico restante, para lo cual debe configurarse una Lista de acceso. Además el tiempo de espera de NAT debe ser de 120 segundos. Se simulará al servidor ISP con una computadora conectada al puerto Fastethernet del router Lima, en la red 10.0.0.0 / 8 .

Aunque se usarán direcciones privadas (RFC 1918), la empresa aprecia la eficiencia y la conservación de direcciones en el diseño. Para minimizar el desperdicio en el espacio de direcciones, han pedido que se utilicen mascaras de subred de longitud variable cuando resulte apropiado.

Se debe configurar las interfaces S0 de los routers Surco y Arequipa para usar el encapsulamiento Frame Relay.

Se simulará la nube Frame Relay con un router

1.2. Objetivos del trabajo

- Establecer la configuración física de la red, de acuerdo al diagrama y la descripción correspondiente.
- Configurar correctamente la OSPF (primero la ruta libre mas corta) de área única.
- Configurar correctamente las VLANs y la agregación de enlaces 802.1q.
- Configurar correctamente el Frame Relay
- Configurar correctamente DHCP.
- Configurar correctamente NAT
- Crear y activar listas de control de acceso en los routers e interfaces pertinentes.
- Verificar que todas las configuraciones sean operacionales y funcionen según las pautas de la situación.

1.3. Evaluación del problema

Para la solución de este diseño se usaran routers de la marca CISCO de la serie 2600. No obstante, se pueden usar routers de las series 800, 1600, 1700.

Para la simulación de la nube Frame Relay, se usará un Router CISCO serie 2500.

El switch usado es un switch de la serie 2950.

1.4 Limitaciones del Trabajo

El presente trabajo es implementado solo en laboratorio, usando routers y switches reales, simulando las conexiones seriales reales con cables V35 y simulando el MODEM con el comando clock rate del router en modo DCE, en la realidad el MODEM, es el que da la señal de reloj. La nube Frame Relay será simulada con un router, buscando que se de la comunicación solicitada. Los resultados del presente trabajo, se pueden simular con el uso de un simulador de Networking, como Boson o RouterSim.

CAPITULO II
MARCO TEORICO CONCEPTUAL

2.1. DIRECCIONAMIENTO IP

Para que dos sistemas se comuniquen, se deben poder identificar y localizar entre sí. Aunque las direcciones de la Figura 2.1 no son direcciones de red reales, representan el concepto de agrupamiento de las direcciones. Este utiliza A o B para identificar la red y la secuencia de números para identificar el host individual.

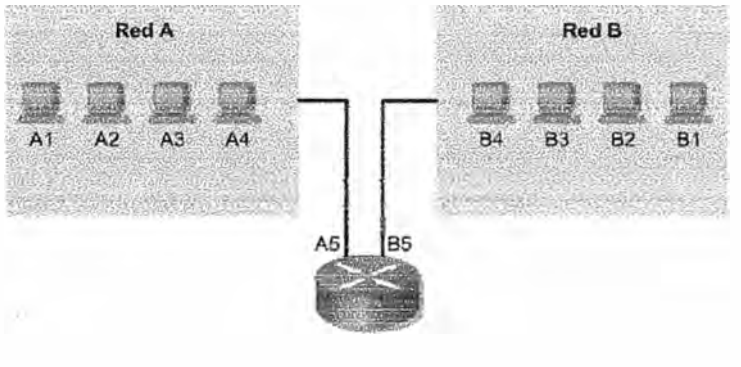


Fig. 2.1. Comunicación entre dos hosts

La combinación de letras (dirección de red) y el número (dirección del host) crean una dirección única para cada dispositivo conectado a la red. Cada computador conectado a una red TCP/IP debe recibir un identificador exclusivo o una dirección IP. Esta dirección, que opera en la Capa 3, permite que un computador localice otro computador en la red. Todos los computadores también cuentan con una dirección física exclusiva, conocida como dirección MAC. Estas son asignadas por el fabricante de la tarjeta de interfaz de la red. Las direcciones MAC operan en la Capa 2 del modelo OSI.

2.1.1. DIRECCIÓN IP

Una **Dirección IP** (dirección del *Internet Protocol*), es como un DNI para máquinas, es un número único que utilizan los dispositivos para identificarse y comunicarse entre ellos en una red que utiliza el estándar del Internet Protocol.

Una dirección IP (IP es acrónimo de Internet Protocol) es una secuencia de unos y ceros de 32 bits. La Figura 2.2 muestra un número de 32 bits de muestra.

Fig. 2.2 Numero de 32 bits

Para que el uso de la dirección IP sea más sencillo, en general, la dirección aparece escrita en forma de cuatro números decimales separados por puntos. Por ejemplo, la dirección IP de un computador es 192.168.1.2. Otro computador podría tener la dirección 128.10.2.1. Esta forma de escribir una dirección se conoce como formato decimal punteado. En esta notación, cada dirección IP se escribe en cuatro partes separadas por puntos. Cada parte de la dirección se conoce como octeto porque se compone de ocho dígitos binarios. Por ejemplo:

La dirección IP 192.168.1.8 sería
11000000.10101000.00000001.00001000 en una notación binaria.

La notación decimal punteada es un método más sencillo de comprender que el método binario de unos y ceros. Esta notación decimal punteada también evita que se produzca una gran cantidad de errores por transposición, que sí se produciría si sólo se utilizaran números binarios. El uso de decimales separados por puntos permite una mejor comprensión de los patrones numéricos. Tanto los números binarios como los decimales de la Figura representan a los mismos valores, pero resulta más sencillo apreciar la notación decimal punteada. Este es uno de los problemas frecuentes que se encuentran al trabajar directamente con números binarios. Las largas cadenas de unos y ceros que se repiten hacen que sea más probable que se produzcan errores de transposición y omisión.

Para poder clasificar las direcciones IP se dividen en grupos llamados clases. A esto se le conoce como direccionamiento "classfull". Toda dirección IP completa de 32 bits, se compone de dos partes: parte de Red y parte de Host. (Figura 2.3)

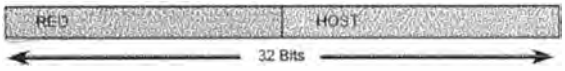


Fig. 2.3 Partes de una dirección IP

2.1.2. CLASES DE DIRECCIONES IP

Un bit o una secuencia de bits al inicio de la dirección IP, determina su clase. Se tienen cinco clases (Figura 2.4):

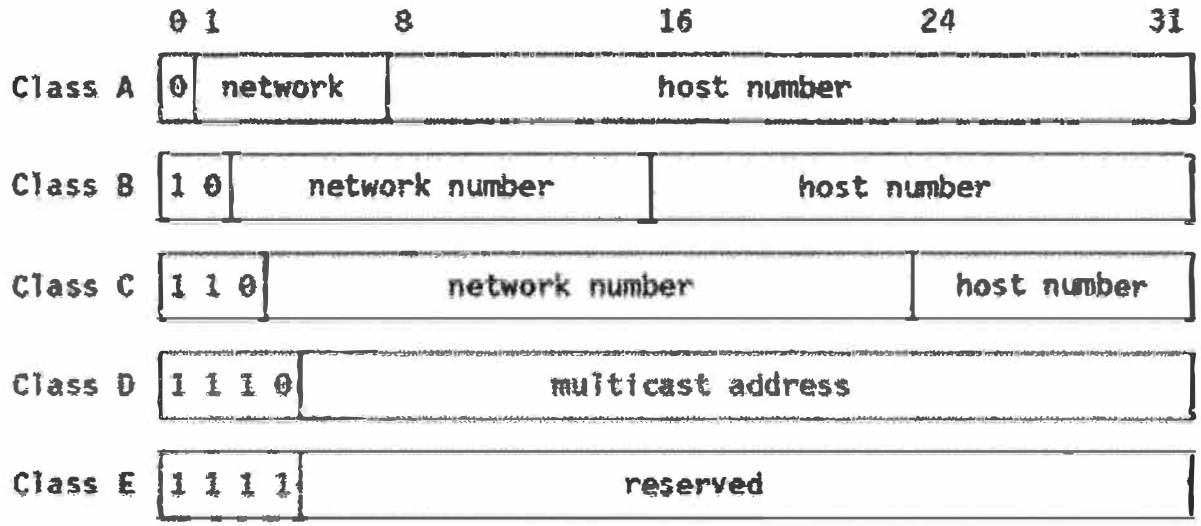


Fig. 2.4 Clases de direcciones IP

La dirección Clase A se diseñó para admitir redes de tamaño extremadamente grande, de más de 16 millones de direcciones de host disponibles. Las direcciones IP Clase A utilizan sólo el primer octeto para indicar la dirección de la red. Los tres octetos restantes son para las direcciones host.

El primer bit de la dirección Clase A siempre es 0. Con dicho primer bit, que es un 0, el menor número que se puede representar es 00000000, 0 decimal. El valor mas alto que se puede representar es 01111111, 127 decimal. Estos números 0 y 127 quedan reservados y no se pueden utilizar como direcciones de red. Cualquier dirección que comience con un valor entre 1 y 126 en el primer octeto es una dirección Clase A.

La red 127.0.0.0 se reserva para las pruebas de loopback. Los Routers o las máquinas locales pueden utilizar esta dirección para enviar paquetes nuevamente hacia ellos mismos. Por lo tanto, no se puede asignar este número a una red.

La dirección Clase B se diseñó para cumplir las necesidades de redes de tamaño moderado a grande. Una dirección IP Clase B utiliza los primeros dos de los cuatro octetos para indicar la dirección de la red. Los dos octetos restantes especifican las direcciones del host.
Los primeros dos bits del primer octeto de la dirección Clase B siempre son 10. Los seis bits restantes pueden poblarse con unos o ceros. Por lo tanto, el menor número que puede representarse en una dirección Clase B es 10000000, 128 decimal. El número más alto que puede representarse es 10111111, 191 decimal. Cualquier dirección que comience con un valor entre 128 y 191 en el primer octeto es una dirección Clase B.

El espacio de direccionamiento Clase C es el que se utiliza más frecuentemente en las clases de direcciones originales. Este espacio de direccionamiento tiene el propósito de admitir redes pequeñas con un máximo de 254 hosts.
Una dirección Clase C comienza con el binario 110. Por lo tanto, el menor número que puede representarse es 11000000, 192 decimal. El número más alto que puede representarse es 11011111, 223 decimal. Si una dirección contiene un número entre 192 y 223 en el primer octeto, es una dirección de Clase C.

La dirección Clase D se creó para permitir multicast en una dirección IP. Una dirección multicast es una dirección exclusiva de red que dirige los paquetes con esa dirección destino hacia grupos predefinidos de direcciones IP. Por lo tanto, una sola estación puede transmitir de forma simultánea una sola corriente de datos a múltiples receptores.
El espacio de direccionamiento Clase D, en forma similar a otros espacios de direccionamiento, se encuentra limitado matemáticamente. Los primeros cuatro bits de una dirección Clase D deben ser 1110. Por lo tanto, el primer rango de octeto para las direcciones Clase D es 11100000 a 11101111, o 224 a 239. Una dirección IP que comienza con un valor entre 224 y 239 en el primer octeto es una dirección Clase D.

Se ha definido una dirección Clase E. Sin embargo, la Fuerza de tareas de ingeniería de Internet (IETF) ha reservado estas direcciones para su propia investigación. Por lo tanto, no

se han emitido direcciones Clase E para ser utilizadas en Internet. Los primeros cuatro bits de una dirección Clase E siempre son 1s. Por lo tanto, el rango del primer octeto para las direcciones Clase E es 11110000 a 11111111, o 240 a 255.

Si consideramos una dirección IP como : X.Y.Z.W , donde X,Y,Z,W representan octetos binarios, podemos resumir lo anterior en el siguiente cuadro mostrado en la figura 2.5:

Clase	Valor de w	Identificador de red	Identificador de host	Número de redes	Número de hosts por red
A	1-126	*w*	*x.y.z*	126	16,777,214
B	128-191	*w.x*	*y.z*	16,384	65,534
C	192-223	*w.x.y*	*z*	2,097,152	254
D	224-239	Reservado para direcciones de multidifusión	No disponible	No disponible	No disponible
E	240-254	Reservado para uso experimental	No disponible	No disponible	No disponible

Fig. 2.5 Clases de direcciones IP

2.1.3. TIPOS DE DIRECCIONES IP: PÚBLICAS Y PRIVADAS

Las direcciones IP públicas constituyen las direcciones de Internet, son asignadas para ser globalmente únicas, este tipo de direcciones son únicas en Internet por cada host (computador o servidores), este es un requerimiento absoluto el cual garantiza que cada dispositivo en el Internet puede ser identificado de manera única. El principal propósito de este espacio de direcciones es permitir la comunicación sobre Internet.

Estos números son indispensables para instalar servicios en la red pública como servidores web, correos, FTP, etc.

Los IPs privados son números no usados en la red Internet, son rangos de direcciones IP que han sido reservados para la operación de redes privadas que usan el protocolo IP. Cualquier organización puede usar estas direcciones IP en sus redes privadas sin la necesidad de solicitarlo a algún registro de Internet. La principal condición establecida para el uso de direcciones IP privadas es que los dispositivos que usen estas direcciones IP no necesiten ser alcanzados desde Internet.

Existen muchas redes privadas junto con las redes públicas. Sin embargo, no es recomendable que una red privada utilice una dirección cualquiera debido a que, con el tiempo, dicha red podría conectarse a Internet. El RFC 1918 asigna tres bloques de la dirección IP para uso interno y privado. Estos tres bloques consisten en una dirección de Clase A, un rango de direcciones de Clase B y un rango de direcciones de Clase C, como se muestra en la figura 2.6.

Clase	Redes
A	10.0.0.0 hasta 10.255.255.255
B	172.16.0.0 hasta 172.31.0.0
C	192.168.0.0 hasta 192.168.255.0

Fig. 2.6 Rango de direcciones IP

Las direcciones que se encuentran en estos rangos no se enrutan hacia el backbone de la Internet. Los Routers de Internet descartan inmediatamente las direcciones privadas. Si se produce un direccionamiento hacia una intranet que no es pública, un laboratorio de prueba o una red doméstica, es posible utilizar las direcciones privadas en lugar de direcciones exclusivas a nivel global. Las direcciones IP privadas pueden entremezclarse, como muestra el gráfico, con las direcciones IP públicas. Así, se conservará el número de direcciones utilizadas para conexiones internas.

La conexión de una red que utiliza direcciones privadas a la Internet requiere que las direcciones privadas se conviertan a direcciones públicas. Este proceso de conversión se conoce como Traducción de direcciones de red (NAT). En general, un Router es el dispositivo que realiza la NAT.

2.2. ENRUTAMIENTO Y PROTOCOLOS DE ENRUTAMIENTO OSPF Y RIP

2.2.1 ENRUTAMIENTO

El enrutamiento no es otra cosa que instrucciones para ir de una red a otra. Estas instrucciones, también conocidas como rutas, pueden ser dadas a un router por otro de forma dinámica, o pueden ser asignadas al router por el administrador de forma estática.

Se toma en cuenta muchos aspectos al seleccionar un protocolo de enrutamiento dinámico. El tamaño de la red, el ancho de banda de los enlaces disponibles, la capacidad de procesamiento de los routers, las marcas y modelos de los routers de la red y los protocolos que ya se encuentran en uso en la red son todos factores a considerar a la hora de elegir un protocolo de enrutamiento.

El enrutamiento es el proceso usado por el router para enviar paquetes a la red de destino. Un router toma decisiones en función de la dirección de IP de destino de los paquetes de datos. Todos los dispositivos intermedios usan la dirección de IP de destino para guiar el paquete hacia la dirección correcta, de modo que llegue finalmente a su destino. A fin de tomar decisiones correctas, los routers deben aprender la ruta hacia las redes remotas. Cuando los routers usan enrutamiento dinámico, esta información se obtiene de otros routers. Cuando se usa enrutamiento estático, el administrador de la red configura manualmente la información acerca de las redes remotas.

Debido a que las rutas estáticas deben configurarse manualmente, cualquier cambio en la topología de la red requiere que el administrador agregue o elimine las rutas estáticas afectadas por dichos cambios. En una red de gran tamaño, el mantenimiento manual de las tablas de enrutamiento puede requerir de una enorme cantidad de tiempo de administración. En redes pequeñas, con pocos cambios, las rutas estáticas requieren muy poco mantenimiento. Debido a los requisitos de administración adicionales, el enrutamiento estático no tiene la escalabilidad o capacidad de adaptarse al crecimiento del enrutamiento dinámico. Aun en redes de gran tamaño, a menudo se configuran rutas estáticas, cuyo objetivo es satisfacer requerimientos especificos, junto con un protocolo de enrutamiento dinámico.

2.2.2 INTRODUCCIÓN A LOS PROTOCOLOS DE ENRUTAMIENTO

Los protocolos de enrutamiento son diferentes a los protocolos enrutados tanto en su función como en su tarea.

Un protocolo de enrutamiento es el esquema de comunicación entre routers. Un protocolo de enrutamiento permite que un router comparta información con otros routers, acerca de las redes que conoce así como de su proximidad a otros routers. La información que un router obtiene de otro, mediante el protocolo de enrutamiento, es usada para crear y mantener las tablas de enrutamiento.

Ejemplos de protocolos de enrutamiento:
Protocolo de información de enrutamiento (RIP)
Protocolo de enrutamiento de gateway interior (IGRP)
Protocolo de enrutamiento de gateway interior mejorado (EIGRP)
Protocolo "Primero la ruta más corta" (OSPF)

Un protocolo enrutado se usa para dirigir el tráfico generado por los usuarios. Un protocolo enrutado proporciona información suficiente en su dirección de la capa de red, para permitir que un paquete pueda ser enviado desde un host a otro, basado en el esquema de direcciones.

Ejemplos de protocolos enrutados:

-Protocolo Internet (IP)
-Intercambio de paquetes de intemetwork (IPX)

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.
Cuando todos los routers de una red se encuentran operando con la misma información, se dice que la red ha hecho convergencia. Una rápida convergencia es deseable, ya que reduce el período de tiempo durante el cual los routers toman decisiones de enrutamiento erróneas.

Los sistemas autónomos (SA) permiten la división de la red global en subredes de menor tamaño, más manejables. Cada SA cuenta con su propio conjunto de reglas y políticas, y con un único número SA que lo distingue de los demás sistemas autónomos del mundo.

2.2.3 SISTEMA AUTÓNOMO

Un sistema autónomo (SA) es un conjunto de redes bajo una administración común, las cuales comparten una estrategia de enrutamiento común (Figura 2.7) . Para el mundo exterior, el AS es una entidad única. El SA puede ser administrado por uno o más operadores, a la vez que presenta un esquema unificado de enrutamiento hacia el mundo exterior.

Los números de identificación de cada SA son asignados por el Registro estadounidense de números de la Internet (ARIN), los proveedores de servicios o el administrador de la red. Este sistema autónomo es un número de 16 bits. Los protocolos de enrutamiento tales como el IGRP de Cisco, requieren un número único de sistema autónomo.

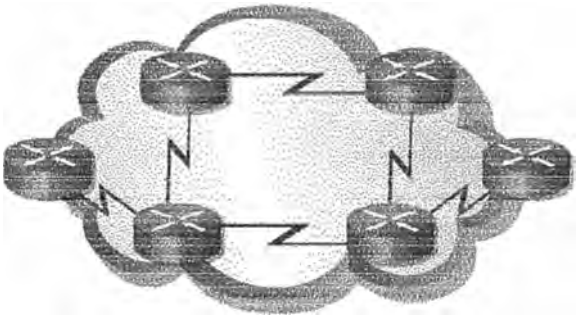


Fig. 2.7 Sistema Autónomo: Routers bajo una administración común

2.2.4. CLASES DE PROTOCOLOS DE ENRUTAMIENTO

La mayoría de los algoritmos de enrutamiento pertenecen a una de estas dos categorías:

-Vector-distancia
-Estado del enlace

El método de enrutamiento por vector-distancia determina la dirección (vector) y la distancia hacia cualquier enlace en la red. El método de estado del enlace, también denominado

"primero la ruta más corta", recrea la topología exacta de toda la red. Algunos ejemplos de protocolo de enrutamiento:

- **RIP:** Un protocolo de enrutamiento interior por vector-distancia.
- **IGRP:** El protocolo de enrutamiento interior por vector-distancia de Cisco.
- **OSPF:** Un protocolo de enrutamiento interior de estado del enlace
- **EIGRP:** El protocolo mejorado de enrutamiento interior por vector-distancia de Cisco.
- **BGP:** Un protocolo de enrutamiento exterior por vector-distancia

2.2.5 PROTOCOLO RIP

Uno de los protocolos de routing más antiguos es el Routing Information Protocol o más comúnmente llamado RIP. RIP utiliza algoritmos de vector distancia para calcular sus rutas. Este tipo de algoritmos para calcular rutas fueron utilizados durante décadas en sus distintas variantes. De hecho los algoritmos de vector distancia utilizados por RIP están basados en aquellos algoritmos utilizados por ARPANET en el año 1969.

Los protocolos vector distancia fueron descritos académicamente por: R.E. Bellman, L.R. Ford Jr y D.R. Fulkerson .

La primera organización que implementó un protocolo de vector distancia fue la compañía Xerox en su protocolo GIP (Gateway Information Protocol), este protocolo estaba incluido dentro de la arquitectura XNS (Xerox Network Systems). GIP se utilizaba para intercambiar información de routing entre redes o sistemas autónomos no adyacentes. Pero claro, Xerox había implementado su propio protocolo propietario.

Poco después la University of California en Berkeley creo una variante llamada "routed ", esta variante del GIP introdujo novedades como modificación del campo de direccionamiento, que se consiguió más flexible , también se añadió un temporizador que limitaba a 30 segundos el tiempo máximo de actualización, es decir, el tiempo máximo permitido sin saber la información de los vecinos, y por supuesto se integró dentro de UNIX, con lo cual pasó a ser abierto.

El protocolo RIP, tal cual lo conocemos actualmente, fue descrito por primera vez en el RFC 1058 (http://www.rfc-editor.org/rfc/rfc1058.txt) por C. Hedrick de la Rutgers University en Junio de 1988, y posteriormente fue mejorado en la RFC 2453 (http://www.rfc-editor.org/rfc/rfc2453.txt) por G.Malkin de la compañía Bay Networks en Noviembre de 1998.

Desde el año 1998 el protocolo RIP se ha mantenido estable, aunque posteriormente salió la versión para Ipv6, la cual tiene su propio capítulo.

RIP es un protocolo de routing de vector distancia muy extendido en todo el Mundo por su simplicidad en comparación a otros protocolos como podrían ser OSPF, IS-IS o BGP. RIP se trata de un protocolo abierto a diferencia de otros protocolos de routing como por ejemplo IGRP y EIGRP propietarios de Cisco Systems o VNN propietario de Lucent Technologies.

RIP está basado en el algoritmo de Bellman Ford y busca su camino óptimo mediante el conteo de saltos, considerando que cada router atravesado para llegar a su destino es un salto.

RIP, al contar únicamente saltos, como cualquier protocolo de vector distancia no tiene en cuenta datos tales como por ejemplo ancho de banda o congestión del enlace.

RFC 1058: Routing Information Protocol

En Junio de 1988, C. Hedrick publicó el RFC 1058 correspondiente a RIP versión 1, y lo encabezó de la siguiente manera:

"This RFC describes an existing protocol for exchanging routing information among gateways and other hosts. It is intended to be used as a basis for developing gateway software for use in the Internet community. Distribution of this memo is unlimited."

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

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

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

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

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

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

Tabla de routing de RIP

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

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

Para obtener esta tabla, el protocolo de routing RIP utiliza el siguiente procedimiento para mantener actualizada la tabla de routing de cada uno de los nodos o routers de la red:
Mantener una tabla con una entrada por cada posible destino en la red. La entrada debe contener la distancia D al destino, y el siguiente salto S del router a esa red. Conceptualmente también debería de existir una entrada para el router mismo con métrica 0, pero esta entrada no existirá.
Periódicamente se enviará una actualización de la tabla a cada uno de los vecinos del router mediante la dirección de broadcast. Esta actualización contendrá toda la tabla de routing.

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

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

Dirección de destino

La dirección de destino en la tabla de routing de RIP será la red de destino, es decir, la red final a la que deseamos acceder, esta red en la versión 1 del protocolo RIP tendrá que ser obligatoriamente clasfull, es decir tendrá que tener en cuenta la clase, es decir, no se permite el subneting en RIP versión 1, por ejemplo si la red de destino es la 192.168.4.0, sabemos que al ser RIP classfull la red de destino tiene 256 direcciones, de las cuales 254 son útiles, una vez descontada la dirección de red y la dirección de broadcast, ya que la red 192.168.4.0 es de clase C, es decir que los 24 primeros bits de la dirección IP identifican la red y los 8 últimos identifican los hosts de dentro de la red.

Siguiente salto

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

Interfaz de salida del router

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

Métrica

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

Temporizador

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

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

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

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

RFC 2453: RIP Versión 2

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

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

-Autenticación para la transmisión de información de RIP entre vecinos.
-Utilización de mascaras de red, con lo que ya es posible utilizar VLSM
-Utilización de máscaras de red en la elección del siguiente salto, lo cual nos puede permitir la utilización de arquitecturas de red discontinuas.
-Envío de actualizaciones de tablas de RIP mediante la dirección de multicast 224.0.0.9.
-Inclusión de RIPv2 en los bloques de información de gestión (MIB).
-Por supuesto además de estas mejoras RIPv2 nos permite la redistribución de rutas externas aprendidas por otros protocolos de routing.

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

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

2.2.6 PROTOCOLO OSPF

OSPF (Open Shortest Path First) es un protocolo de enrutamiento del estado de enlace basado en estándares abiertos. Se describe en diversos estándares de la Fuerza de Tareas de Ingeniería de Internet (IETF). El término "libre" en "Primero la ruta libre más corta" significa que está abierto al público y no es propiedad de ninguna empresa.
En comparación con RIP v1 y v2, OSPF es el IGP preferido porque es escalable. RIP se limita a 15 saltos, converge lentamente y a veces elige rutas lentas porque pasa por alto ciertos factores críticos como por ejemplo el ancho de banda a la hora de determinar la ruta. Una desventaja de usar OSPF es que solo soporta el conjunto de protocolos TCP/IP. OSPF ha superado estas limitaciones y se ha convertido en un protocolo de enrutamiento sólido y escalable adecuado para la redes modernas. OSPF se puede usar y configurar en una sola área en las redes pequeñas. También se puede utilizar en las redes grandes. Tal como se muestra en la Figura 2.8, las redes OSPF grandes utilizán un diseño jerárquico.

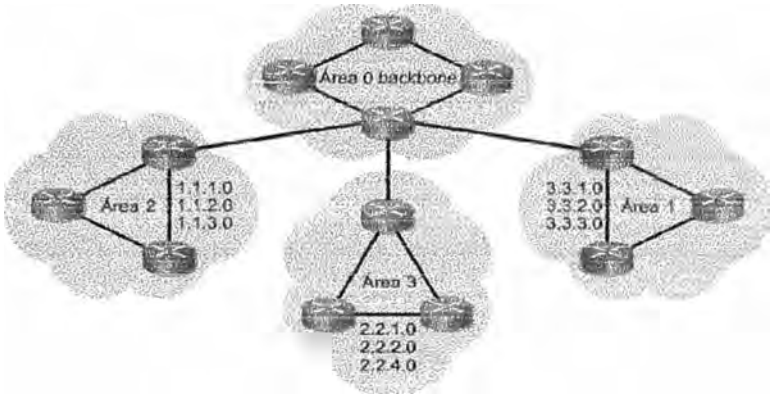


Fig. 2.8. OSPF configurado en redes grandes

Varias áreas se conectan a un área de distribución o a un área 0 que también se denomina backbone. El enfoque del diseño permite el control extenso de las actualizaciones de enrutamiento. La definición de área reduce el gasto de procesamiento, acelera la convergencia, limita la inestabilidad de la red a un área y mejora el rendimiento. Además los cambios de estado de enlace son invisibles fuera del área.

RIP es adecuado para pequeñas redes y la mejor ruta se basa en el menor número de saltos. OSPF es apropiado para internetworks grandes y escalables y la mejor ruta se determina a base de la velocidad del enlace. RIP, así como otros protocolos de vector-distancia, utiliza algoritmos sencillos para calcular las mejores rutas. El algoritmo SPF es complejo. Los routers que implementan los protocolos de vector-distancia necesitan menos memoria y menos potencia de procesamiento que los que implementan el protocolo OSPF.

OSPF selecciona las rutas en base al costo, lo que se relaciona con la velocidad. Cuanto mayor sea la velocidad, menor será el costo de OSPF del enlace.

OSPF selecciona la ruta más rápida y sin bucles del árbol SPF como la mejor ruta de la red.

OSPF garantiza un enrutamiento sin bucles. Los protocolos de vector-distancia pueden provocar bucles de enrutamiento.

Si los enlaces son poco estables, la inundación de la información del estado de enlace puede provocar publicaciones del estado de enlace no sincronizadas y decisiones incoherentes entre los routers.

OSPF ofrece soluciones a los siguientes problemas:

-Velocidad de convergencia
-Admite la Máscara de subred de longitud variable (VLSM)
-Tamaño de la red
-Selección de ruta.
-Agrupación de miembros

En las redes grandes, la convergencia de RIP puede tardar varios minutos dado que la tabla de enrutamiento de cada router se copia y se comparte con routers directamente conectados. Después de la convergencia OSPF inicial, el mantenimiento de un estado convergente es más rápido porque se inundan los otros routers del área con los cambios en la red.

OSPF admite VLSM y por lo tanto se conoce como un protocolo sin clase. RIP v1 no admite VLSM, pero RIP v2 sí la admite.

RIP considera inalcanzable a una red que se encuentra a más de 15 routers de distancia porque el número de saltos se limita a 15. Esto limita el RIP a pequeñas topologías. OSPF no tiene límites de tamaño y es adecuado para las redes intermedias a grandes.

RIP selecciona una ruta hacia una red agregando uno al número de saltos informado por un vecino. Compara los números de saltos hacia un destino y selecciona la ruta con la distancia más corta o menos saltos. Este algoritmo es sencillo y no requiere ningún router poderoso ni demasiada memoria. RIP no toma en cuenta el ancho de banda disponible en la determinación de la mejor ruta.

OSPF selecciona la ruta mediante el costo, una métrica basada en el ancho de banda. Todos los routers OSPF deben obtener información acerca de la redes de cada router en su totalidad para calcular la ruta más corta. Éste es un algoritmo complejo. Por lo tanto, OSPF requiere routers más poderosos y más memoria que RIP.

RIP utiliza una topología plana. Los routers de una región RIP intercambian información con todos los routers. OSPF utiliza el concepto de áreas. Una red puede subdividirse en grupos de routers. De esta manera, OSPF puede limitar el tráfico a estas áreas. Los cambios en un

área no afectan el rendimiento de otras áreas. Este enfoque jerárquico permite el eficiente crecimiento de una red.

Protocolo HELLO de OSPF

Cuando un router inicia un proceso de enrutamiento OSPF en una interfaz, envía un paquete hello y sigue enviando hellos a intervalos regulares. Las reglas que gobiernan el intercambio de paquetes hello de OSPF se denominan protocolo Hello.

En la capa 3 del modelo OSI, los paquetes hello se direccionan hacia la dirección multicast 224.0.0.5. Esta dirección equivale a "todos los routers OSPF". Los routers OSPF utilizan los paquetes hello para iniciar nuevas adyacencias y asegurarse de que los routers vecinos sigan funcionando. Los Hellos se envían cada 10 segundos por defecto en las redes multiacceso de broadcast y punto a punto. En las interfaces que se conectan a las redes NBMA, como por ejemplo Frame Relay, el tiempo por defecto es de 30 segundos.
En las redes multiacceso el protocolo Hello elige un router designado (DR) y un router designado de respaldo (BDR).
Aunque el paquete hello es pequeño, consiste en un encabezado de paquete OSPF. Para el paquete hello, el campo de tipo se establece en 1.
El paquete hello transmite información para la cual todos los vecinos deben estar de acuerdo antes de que se forme una adyacencia y que se pueda intercambiar información del estado de enlace.

2.3. LANs VIRTUALES (VLAN)

Una VLAN es un agrupamiento lógico de estaciones y dispositivos de red. Las VLAN se pueden agrupar por función laboral o departamento, sin importar la ubicación física de los usuarios. El tráfico entre las VLAN está restringido. Los switches y puentes envían tráfico unicast, multicast y broadcast sólo en segmentos de LAN que atienden a la VLAN a la que pertenece el tráfico. En otras palabras, los dispositivos en la VLAN sólo se comunican con los dispositivos que están en la misma VLAN. Los routers suministran conectividad entre diferentes VLAN.

Las empresas con frecuencia usan las VLAN como una manera de garantizar que un conjunto determinado de usuarios se agrupen lógicamente más allá de su ubicación física. Las organizaciones usan las VLAN para agrupar usuarios en el mismo departamento. Por ejemplo, los usuarios del departamento de Mercadotecnia se ubican en la VLAN de Mercadotecnia, mientras que los usuarios del Departamento de Ingeniería se ubican en la VLAN de Ingeniería, un ejemplo de ello, se puede ver en la figura 2.9.

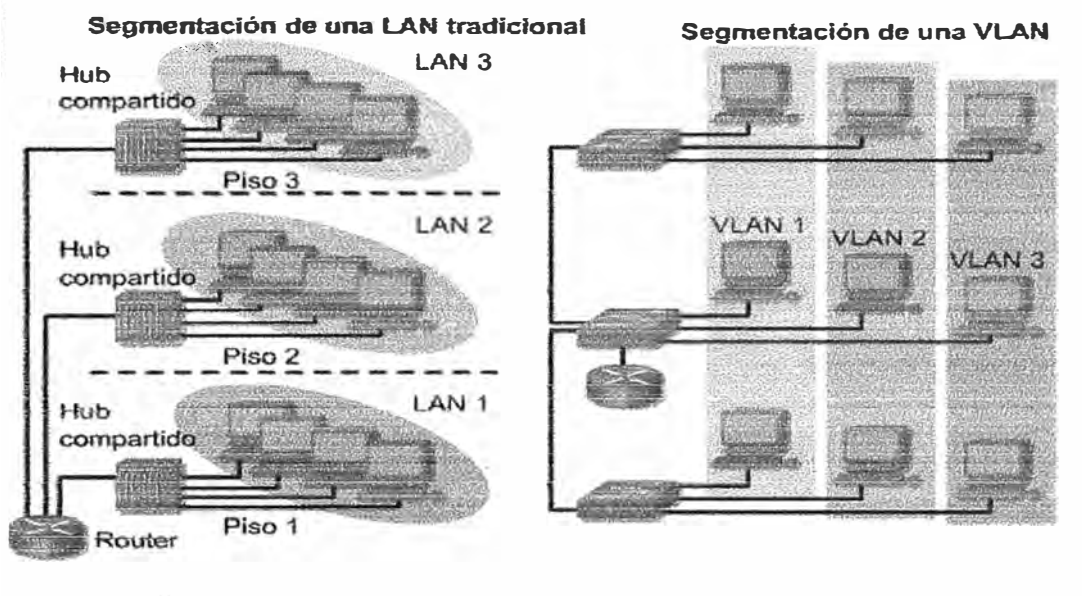


Fig. 2.9 Segmentación mediante VLANs

Las VLAN se crean para brindar servicios de segmentación proporcionados tradicionalmente por routers físicos en las configuraciones de LAN. Las VLAN se ocupan de la escalabilidad, seguridad y gestión de red. Los routers en las topologías de VLAN proporcionan filtrado de broadcast, seguridad y gestión de flujo de tráfico. Los switches no puentean ningún tráfico entre VLAN, dado que esto viola la integridad del dominio de broadcast de las VLAN. El tráfico sólo debe enrutarse entre VLAN.

Una VLAN se compone de una red conmutada que se encuentra lógicamente segmentada. Cada puerto de switch se puede asignar a una VLAN. Los puertos asignados a la misma VLAN comparten broadcasts. Los puertos que no pertenecen a esa VLAN no comparten esos broadcasts. Esto mejora el desempeño de la red porque se reducen los broadcasts innecesarios. Las VLAN de asociación estática se denominan VLAN de asociación de puerto

central y basadas en puerto. Cuando un dispositivo entra a la red, da por sentado automáticamente que la VLAN está asociada con el puerto al que se conecta.

Los usuarios conectados al mismo segmento compartido comparten el ancho de banda de ese segmento. Cada usuario adicional conectado al medio compartido significa que el ancho de banda es menor y que se deteriora el desempeño de la red. Las VLAN ofrecen mayor ancho de banda a los usuarios que una red Ethernet compartida basada en hubs. La VLAN por defecto para cada puerto del switch es la VLAN de administración. La VLAN de administración siempre es la VLAN 1 y no se puede borrar. Por lo menos un puerto debe asignarse a la VLAN 1 para poder gestionar el switch. Todos los demás puertos en el switch pueden reasignarse a VLAN alternadas.

Las VLAN de asociación dinámica son creadas mediante software de administración de red. Las VLAN dinámicas permiten la asociación basada en la dirección MAC del dispositivo conectado al puerto de switch. Cuando un dispositivo entra a la red, el switch al que está conectado consulta una base de datos en el Servidor de Configuración de VLAN para la asociación de VLAN.

2.3.1 VENTAJAS DE USAR VLANS

Las VLAN permiten que los administradores de red organicen las LAN de forma lógica en lugar de física. Ésta es una ventaja clave. Esto permite que los administradores de red realicen varias tareas:

-Trasladar fácilmente las estaciones de trabajo en la LAN

-Agregar fácilmente estaciones de trabajo a la LAN

-Cambiar fácilmente la configuración de la LAN

-Controlar fácilmente el tráfico de red

-Mejorar la seguridad

2.3.2 CREACIÓN DE VLANS ESTATICAS

Basado en un Switch Cisco serie 2900, se deben tener las siguientes pautas:

- La cantidad máxima de VLAN depende del switch.
- Una de las VLAN por defecto de fábrica es VLAN1.
- La VLAN Ethernet por defecto es VLAN1.
- Se envían publicaciones del Protocolo de Descubrimiento de Cisco (CDP) y Protocolo de Enlace Troncal de VLAN (VTP) en la VLAN 1.
- La dirección IP del switch se encuentra por defecto en el dominio de broadcast de la VLAN 1.
- El switch debe estar en el modo de servidor VTP para crear, agregar o borrar VLAN.

La configuración seria:

```
Switch#vlan database
Switch(vlan)#vlan vlan_number
Switch(vlan)#exit
```

Luego se requiere asignar puertos del switch a la VLAN creada:

```
Switch(config)#interface fastethernet 0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan vlan_number
Switch(config-if)#end
```

Para verificar la configuración:

Mostrar VLANs configuradas y los puertos asignados, además del estado:

```
Switch#show vlan
```

Muestra mas resumida:

```
Switch#show vlan brief
```

2.3.3 ENLACES TRONCALES

En una red conmutada, un enlace troncal es un enlace punto a punto que admite varias VLAN. El propósito de un enlace troncal es conservar los puertos cuando se crea un enlace entre dos dispositivos que implementan las VLAN. La Figura 2.10 muestra dos VLAN compartidas entre los switches Sa y Sb. Cada switch usa dos enlaces físicos de modo que cada puerto transporta tráfico para una sola VLAN. Ésta es una forma sencilla de implementar la comunicación entre las VLAN de diferentes switches, pero no funciona bien a mayor escala.

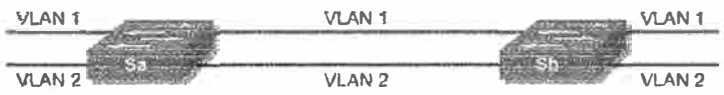


Fig. 2.10 Comunicación entre 2 VLAN

La adición de una tercera VLAN requiere el uso de dos puertos adicionales, uno para cada switch conectado. Este diseño también es ineficiente en lo que se refiere al método de compartir la carga. Además, el tráfico en algunas de las VLAN puede no justificar un enlace dedicado. El enlace troncal agrupa múltiples enlaces virtuales en un enlace físico. Esto permite que el tráfico de varias VLAN viaje a través de un solo cable entre los switches (Figura 2.11).

Fig. 2.11 Comunicación por una interface

Protocolos de Enlace Troncal

Los protocolos de enlace troncal se desarrollaron para administrar la transferencia de tramas de distintas VLAN en una sola línea física de forma eficaz. Los protocolos de enlace troncal establecen un acuerdo para la distribución de tramas a los puertos asociados en ambos entremos del enlace troncal.

Los dos tipos de mecanismos de enlace troncal que existen son el filtrado de tramas y el etiquetado de tramas. La IEEE adoptó el etiquetado de tramas como el mecanismo estándar de enlace troncal.

Los protocolos de enlace troncal que usan etiquetado de tramas logran un envío de tramas más veloz y facilitan la administración.

El único enlace físico entre dos switches puede transportar tráfico para cualquier VLAN (Figura 2.12). Para poder lograr esto, se rotula cada trama que se envía en el enlace para identificar a qué VLAN pertenece. Existen distintos esquemas de etiquetado. Los dos esquemas de etiquetado más comunes para los segmentos Ethernet son ISL y 802.1Q:

- ISL : Un protocolo propietario de Cisco
- 802.1Q : Un estándar IEEE que es el punto central de esta sección.

Los dos tipos de mecanismos de enlace troncal estándar que existen son el etiquetado de tramas y el filtrado de tramas. El estándar IEEE 802.1Q establece el etiquetado de tramas como el método para implementar las VLAN.

El etiquetado de trama de VLAN se ha desarrollado específicamente para las comunicaciones conmutadas. El etiquetado de trama coloca un identificador único en el encabezado de cada trama a medida que se envía por todo el backbone de la red. El identificador es comprendido y examinado por cada switch antes de enviar cualquier broadcast o transmisión a otros switches, routers o estaciones finales. Cuando la trama sale del backbone de la red, el switch elimina el identificador antes de que la trama se transmita a la estación final objetivo. El etiquetado de trama funciona a nivel de Capa 2 y requiere pocos recursos de red o gastos administrativos (Figura 2.12).

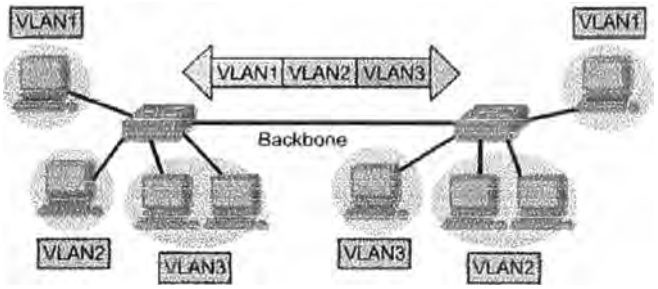


Fig. 2.11 Varias VLAN por un enlace troncal

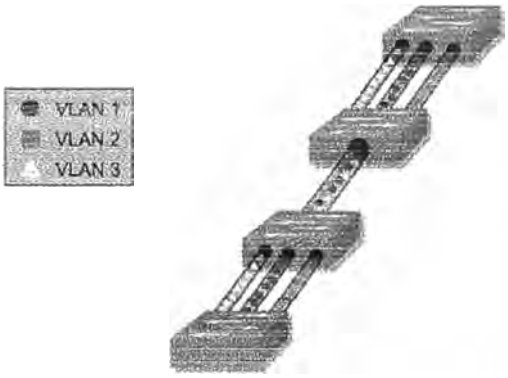


Fig. 2.12 Etiquetado de tramas

Es importante entender que un enlace troncal no pertenece a una VLAN específica. Un enlace troncal es un conducto para las VLAN entre los switches y los routers.

ISL es un protocolo que mantiene la información de VLAN a medida que el tráfico fluye entre los switches. Con ISL, la trama Ethernet se encapsula con un encabezado que contiene un identificador de VLAN.

Como las VLANS crean diferentes dominios de broadcast, y cuando el host en un dominio de broadcast desea comunicarse con un host en otro dominio de broadcast, debe utilizarse un router.

El puerto 1 en un switch forma parte de la VLAN 1 y el puerto 2 forma parte de la VLAN 200. Si todos los puertos de switch formaran parte de la VLAN 1, es posible que los hosts conectados a estos puertos puedan comunicar entre sí. Sin embargo, en este caso, los puertos forman parte de distintas VLAN, la VLAN 1 y la VLAN 200. Se debe utilizar un router si los hosts de las distintas VLAN necesitan comunicarse entre si (Figura 2.13).

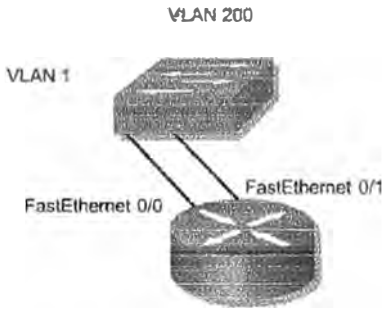


Fig. 2.13 Uso del router para enrutar VLANs

2.4 PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOST (DHCP)

El Protocolo de configuración dinámica del host (DHCP) funciona en el modo cliente/servidor. DHCP permite que los clientes DHCP de una red IP obtengan sus configuraciones de un servidor DHCP. Es menos trabajoso administrar una red IP cuando se utiliza DHCP (Figura 2.14). La opción de configuración más significativa que el cliente recibe del servidor es su dirección IP. El protocolo DHCP se describe en RFC 2131.

Un cliente DHCP está incluido en la mayoría de los sistemas operativos modernos, inclusive en varios sistemas operativos de Windows, Novell Netware, Sun Solaris, Linux y MAC OS. El cliente pide valores de direccionamiento al servidor DHCP de red. Este servidor administra la asignación de las direcciones IP y responde a las peticiones de configuración de los clientes. El servidor DHCP puede responder a las peticiones provenientes de muchas subredes. DHCP no está destinado a la configuración de routers, switches y servidores. Estos tipos de hosts necesitan contar con direcciones IP estáticas.

La función de DHCP es brindar un proceso para que el servidor pueda asignar información IP a los clientes. Los clientes alquilan la información de los servidores por un período definido administrativamente. Cuando el período de alquiler se termina, el cliente debe pedir otra dirección, aunque en general, se le reasigna la misma dirección.

Los administradores en general prefieren que los servidores de red ofrezcan servicios DHCP porque estas soluciones facilitan el crecimiento y la administración. Los routers de Cisco pueden utilizar un conjunto de funciones Cisco IOS, que se llama Easy IP, para ofrecer un servidor DHCP opcional con todas las funciones. Easy IP alquila las configuraciones por 24 horas por defecto. Esto resulta muy útil en las oficinas pequeñas y para aquellos que trabajan en sus casas, donde el usuario puede aprovechar DHCP y NAT sin contar con un servidor NT o UNIX.

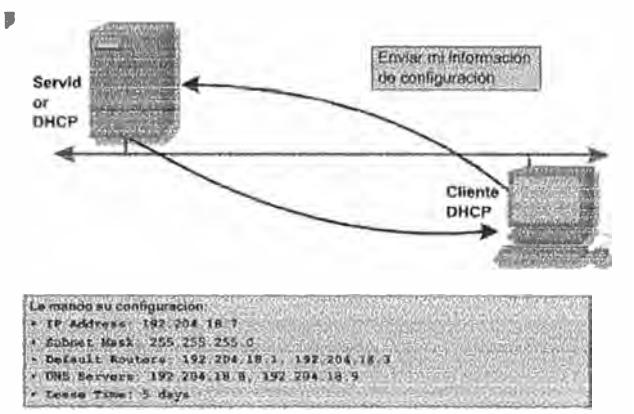


Fig. 2.14 Asignacion DHCP

Los administradores configuran los servidores DHCP para asignar direcciones de conjuntos predefinidos. Los servidores DHCP pueden ofrecer otra información, tal como direcciones del servidor DNS, direcciones del servidor WINS y nombres de dominios. La mayoría de los servidores DHCP también permiten que el administrador defina de forma específica cuáles direcciones MAC de cliente se pueden servir y asignarles cada vez la misma dirección IP de forma automática.

DHCP utiliza el Protocolo de datagrama del usuario (UDP) como su protocolo de transporte. El cliente envía mensajes al servidor en el puerto 67. El servidor envía mensajes al cliente en el puerto 68

Operación de DHCP

El proceso de configuración de un cliente DHCP consta de los siguientes pasos Figura 2.15):

1.- Un cliente debe tener DHCP configurado al comenzar su proceso de participación en la red. El cliente envía una petición al servidor para obtener una configuración IP. Algunas veces el cliente sugiere la dirección IP que quiere, como cuando pide una extensión de un alquiler DHCP. El cliente ubica el servidor DHCP enviando un broadcast llamado DHCPDISCOVER.

2.- Cuando un servidor recibe el broadcast, determina si puede servir esa petición de su propia base de datos. Si no puede, es posible que el servidor envíe la petición a otro servidor DHCP. Si puede, el servidor DHCP ofrece al cliente información de configuración IP como

DHCPOFFER unicast DHCPOFFER es una configuración propuesta que puede incluir direcciones IP, direcciones de servidores DNS y tiempo de alquiler.

3.- Si el cliente encuentra que la propuesta es buena, envía otro broadcast, un DHCPREQUEST, pidiendo de forma específica aquellos parámetros IP en particular. ¿Por qué un cliente envía la petición en forma broadcast en lugar de enviarla en unicast directamente al servidor? Se utiliza un broadcast porque el primer mensaje, el DHCPDISCOVER, pudo haber llegado a más de un servidor DHCP. Si más de un servidor realiza una oferta, el DHCPREQUEST enviado permite que los otros servidores sepan cuál oferta se aceptó. Por lo general, la oferta que se acepta es la primera que se recibe.

4.- El servidor que recibe el DHCPREQUEST formaliza la configuración mandando un recibo unicast, el DHCPACK. Es posible, aunque muy poco probable, que el servidor no envíe el DHCPACK. Esto puede ocurrir porque entretanto, el servidor pudo haber alquilado esa información a otro cliente. La recepción del mensaje DHCPACK permite que un cliente comience a utilizar la dirección asignada de inmediato.

5.- Si el cliente detecta que la dirección ya está en uso en el segmento local, envía un mensaje DHCPDECLINE y el proceso vuelve a comenzar. Si el cliente recibe un DHCPNACK del servidor luego de enviar el DHCPREQUEST, entonces comienza el proceso nuevamente.

6.- Si el cliente ya no desea la dirección IP, envía un mensaje DHCPRELEASE al servidor.

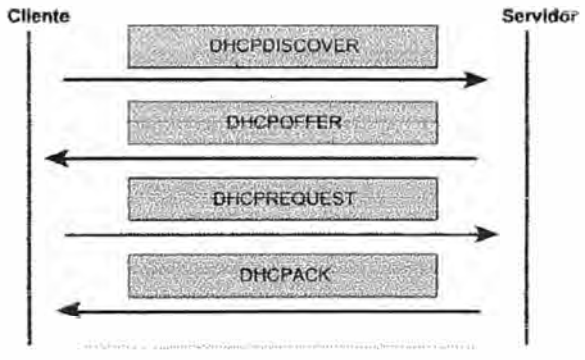


Fig. 2.15 Proceso DHCP

2.5. TRADUCCIÓN DE DIRECCIONES DE RED (NAT)

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

Estas direcciones privadas e internas se convierten en direcciones públicas enrutables. Esto se logra mediante el uso de dispositivos de internetwork que ejecutan un software NAT especializado, el cual puede aumentar la privacidad de la red al esconder las direcciones IP internas. Un dispositivo que ejecuta NAT generalmente opera en la frontera de una red stub. Una red stub es una red que posee una sola conexión a su red vecina. Cuando un host dentro de una red stub desea hacer una transmisión a un host en el exterior, envía el paquete al router del gateway fronterizo. El router del gateway fronterizo realiza el proceso de NAT, traduciendo la dirección privada interna de un host a una dirección pública, enrutable y externa (Figura 2.16).

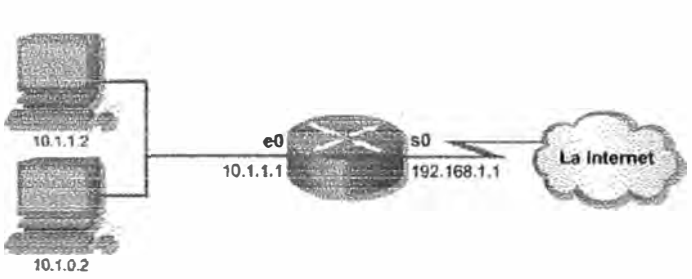


Fig. 2.16 Traduccion NAT

En la terminología de NAT, la red interna es el conjunto de redes que están sujetos a traducción. La red externa se refiere a todas las otras direcciones.

Cisco define los siguientes términos NAT:

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

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

Dirección local externa: la dirección IP de un host externo, como la conocen los hosts en la red interna.
Dirección global externa: la dirección IP asignada a un host en la red externa. El dueño del host asigna esta dirección.

Las traducciones NAT se pueden usar para una variedad de propósitos y pueden asignarse de manera dinámica o estática. NAT estática está diseñada para permitir que cada dirección local se mapee a su correspondiente dirección global. Esto resulta particularmente útil para los hosts que deban tener una dirección constante que esté accesible desde la Internet. Estos hosts internos pueden ser servidores de empresas o dispositivos de networking.
NAT dinámica está diseñada para mapear una dirección IP privada a una dirección pública. Cualquier dirección IP de un conjunto de direcciones IP públicas se asigna a un host de red. La sobrecarga, o Traducción de direcciones de puerto (PAT), mapea varias direcciones IP privadas a una sola dirección IP pública. Se pueden mapear varias direcciones a una sola dirección porque cada dirección privada se diferencia por el número de puerto.
PAT utiliza números únicos de puerto origen en la dirección IP global interna para distinguir entre las traducciones. El número de puerto se codifica en 16 bits. En teoría, el número total de direcciones internas que se pueden traducir a una dirección externa podría ser hasta 65,536 por dirección IP . En realidad, el número de puertos que se pueden asignar a una sola dirección IP es aproximadamente 4000. PAT intenta preservar el puerto origen original. Si el puerto origen está en uso, PAT asigna el primer número de puerto disponible comenzando desde el principio del grupo de puertos correspondiente 0-511, 512-1023, o 1024-65535. Cuando no hay más puertos disponibles y hay más de una dirección IP externa configurada, PAT utiliza la próxima dirección IP para tratar de asignar nuevamente el puerto origen original. Este proceso continúa hasta que no haya puertos ni direcciones IP externas disponibles.

NAT ofrece las siguientes ventajas:
- Elimina la reasignación de una nueva dirección IP a cada host cuando se cambia a un nuevo ISP. NAT elimina la necesidad de re-direccionar todos los hosts que requieran acceso externo, ahorrando tiempo y dinero.
- Conserva las direcciones mediante la multiplexión a nivel de puerto de la aplicación. Con PAT, los hosts internos pueden compartir una sola dirección IP pública para toda

comunicación externa. En este tipo de configuración, se requieren muy pocas direcciones externas para admitir muchos hosts internos, y de este modo se conservan las direcciones IP - Protege la seguridad de la red. Debido a que las redes privadas no publican sus direcciones o topología interna, ellas son razonablemente seguras cuando se las utiliza en conjunto con NAT para tener un acceso externo controlado.

Desventajas de NAT

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

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

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

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

NAT también hace que algunas aplicaciones que utilizan el direccionamiento IP dejen de funcionar, porque esconde las direcciones IP de extremo a extremo. Las aplicaciones que utilizan las direcciones físicas en vez de un nombre de dominio calificado no llegarán a los

destinos que se traducen en el router NAT. Algunas veces, este problema puede evitarse implementando mapeos NAT estáticos.

2.6 FRAME RELAY

La tecnología Frame Relay es un estándar del Sector de Normalización de Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T) y del Instituto Nacional Americano de Normalización (ANSI). Frame Relay es un servicio WAN de conmutación de paquetes, orientado a conexión. Opera en la capa de enlace de datos del modelo de referencia OSI. Frame Relay utiliza un subconjunto del protocolo de Control de enlace de datos de alto nivel (HDLC) llamado Procedimiento de acceso a enlaces para Frame Relay (LAPF) Las tramas transportan datos entre los dispositivos de usuarios, llamados equipo terminal de datos (DTE), y el equipo de comunicaciones de datos (DCE) en la frontera de la WAN.

Una red Frame Relay puede ser privada, pero es más común que se use los servicios de una compañía de servicios externa. Una red Frame Relay consiste, en general, de muchos switches Frame Relay esparcidos geográficamente, los cuales se interconectan mediante líneas troncales.

Con frecuencia, se usa Frame Relay para la interconexión de LANs. En estos casos, un router en cada una de las LANs será el DTE. Una conexión serial, como una línea arrendada T1/E1, conecta el router al switch Frame Relay de la compañía de servicio en su punto de presencia más cercano al router. El switch Frame Relay es un dispositivo DCE. Las tramas se envían y entregan desde un DTE a otro DTE utilizando la red de Frame Relay creada por los DCE de la compañía de servicios (Figura 2.17).

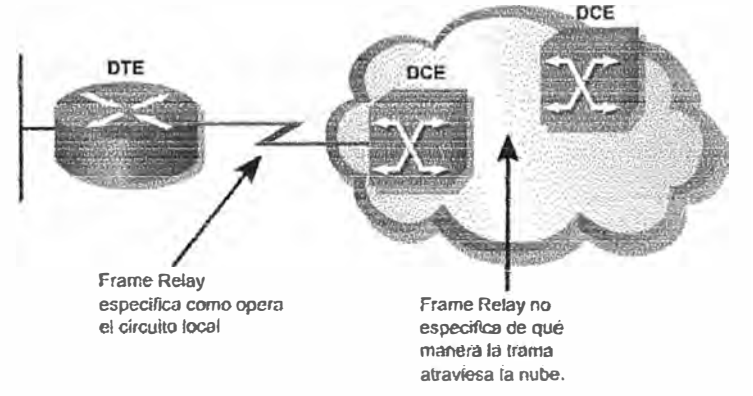


Fig. 2.17 Frame Relay

Frame Relay no tiene mecanismos de recuperación de errores, porque fue diseñada para operar en lineas digitales de alta calidad. Si un nodo detecta un error en la trama, se descarta sin notificación.

2.6.1 TERMINOLOGÍA FRAME RELAY

CIRCUITO VIRTUAL (VC): Es la conexión lógica entre dos DTEs a través de la red Frame Relay. Hay dos tipos de VC : Circuito Virtual Conmutado (SVC) y el Circuito Virtual Permanente (PVC). Un VC se crea al almacenar la información de asignación de puerto de entrada a puerto de salida en la memoria de cada switch y así se enlaza un switch con otro hasta que se identifica la ruta de un extremo a otro.

SVC: Se establecen mediante el envío de mensajes de señalización a través a la red. No son muy comunes.

PVC: Son circuitos previamente configurados por la compañía de servicios.

FRAD (Dispositivo De Acceso Frame Relay): Cualquier dispositivo de red que permita establecer la conexión entre una LAN a una WAN Frame Relay. En muchos casos el router juega el papel de FRAD.

DLCI (Identificador de Canal de Enlace de Datos): Sirve para identificar un determinado circuito virtual dentro de la única línea de acceso (la cual puede tener varios VCs configurados). Este DLCI tiene significado local y puede ser diferente en cada extremo de un VC (Figura 2.18).

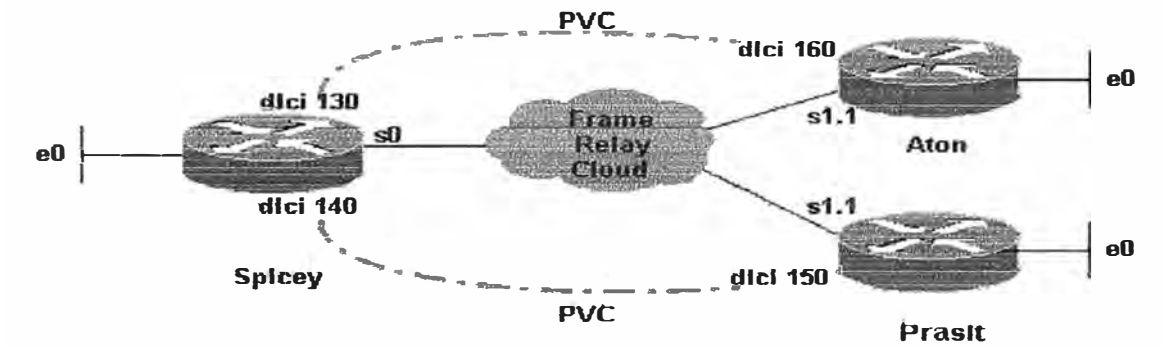


Fig. 2.18 DLCIs en una configuración Frame Relay

La conexión serial de acceso a la red Frame Relay por lo general es mediante una línea arrendada. La velocidad de línea es la velocidad de acceso o velocidad de puerto. Por lo general son 64 Kbps y 4 Mbps, aunque algunos proveedores ofrecen velocidades de hasta 45 Mbps.

En un solo enlace físico hay varios PVCs operando y cada VC tiene un ancho de banda dedicado, la cual es llamado Velocidad de Información Suscrita (CIR).

CIR (Velocidad de Información Suscrita): Es la velocidad a la que el proveedor acuerda aceptar bits en el VC.

Cada CIR de cada VC son por lo general menores a la velocidad del puerto, pero la suma de todas, por lo general es superior a la velocidad del puerto y llega algunas veces hasta 2 o 3 veces 3 la velocidad máxima. Estadísticamente las comunicaciones son usualmente en ráfagas, lo que hace improbable que todos los canales estén trabajando a su máxima velocidad de transmisión al mismo tiempo.

EIR (Velocidad de Información en Exceso): Es la diferencia entre la CIR y la Velocidad máxima ya sea que el máximo sea la velocidad del puerto o sea menor (que es un valor que algunos proveedores imponen como máximo para cada VC)

Tc (Tiempo suscrito): Es el intervalo de tiempo con el cual se calculan las velocidades.

Bc (Ráfaga Suscrita): Es la cantidad de bits suscritos durante un periodo Tc.

Be (Ráfaga en Exceso): Es el numero de bits adicionales que excede la Bc, hasta la velocidad máxima de acceso.

Aunque el switch acepta el tráfico de tramas que excede la CIR, el switch activa (es decir, coloca en "1") el bit elegible de descarte (DE) en el campo de la dirección a todas las tramas que se excedan.

El bit de Notificación explícita de congestión hacia adelante (FECN) se activa en cada trama que el switch recibe en el enlace congestionado. El bit de Notificación explícita de congestión hacia atrás (BECN) se configura en cada trama que el switch coloca en el enlace congestionado. Se espera que los DTE que reciben tramas con el grupo de bits ECN activos intenten reducir el flujo de tramas hasta que la congestión desaparezca.

Los bits DE, FECN y BECN forman pare del campo de dirección de las tramas LAPF, como se puede apreciar en el esquema anterior.

La figura 2.19 muestra el formato de una trama Frame Relay

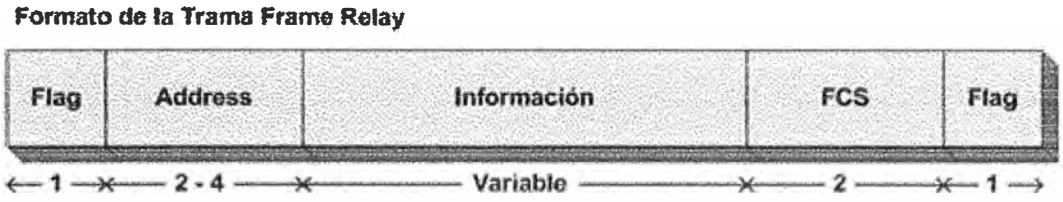


Fig. 2.19 Formato de la trama Frame Relay

La figura 2.20 muestra el detalle del campo de dirección en la trama Frame Relay

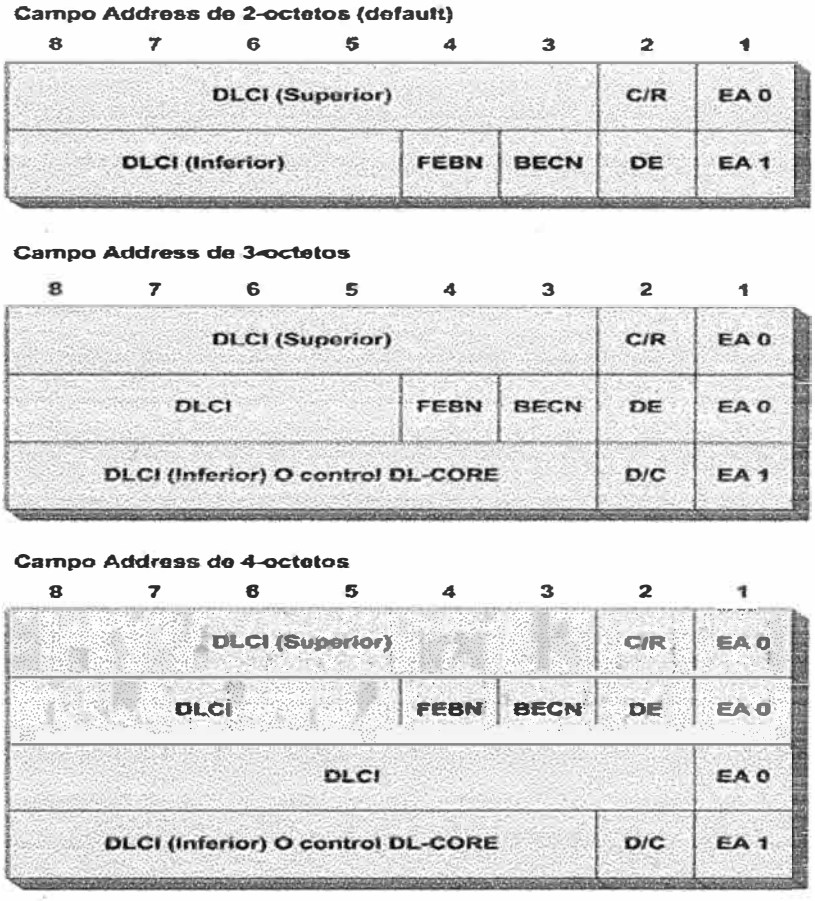


Fig. 2.20 Detalle del campo de direccion

2.6.2 TOPOLOGÍAS FRAME RELAY

Es improbable que Frame Relay sea económica cuando sólo se necesita interconectar dos lugares mediante una conexión punto a punto. Frame Relay resulta más atractiva económicamente cuando se requiera interconectar múltiples lugares.

Con frecuencia, las WAN se interconectan mediante una topología en estrella (Figura 2.21).

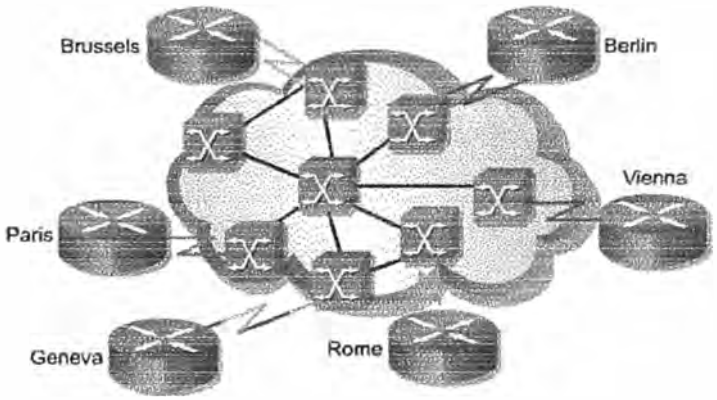


Fig. 2.21 Nube Frame Relay, en topología estrella. Cada enlace físico lleva 5 circuitos virtuales

Otras topologías, se muestran en las figuras 2.22 y 2.23

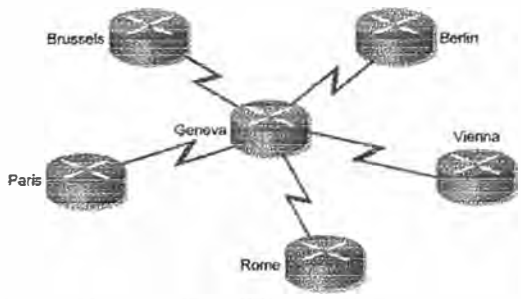


Fig. 2.22 Estrella con un nodo central y líneas arrendadas. La ubicación del nodo central se elige de manera que el costo sea menor para dichas líneas arrendadas.

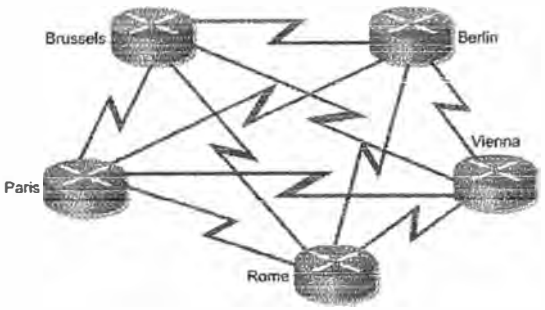


Fig. 2.23 Malla completa. 5 nodos que requieren 10 enlaces

No importa cuál sea la topología subyacente de la red física, todos los FRAD o routers necesitan una vinculación entre las direcciones Frame Relay de la capa de enlace de datos y las dirección de la capa de red, por ejemplo: las direcciones IP. Principalmente, el router necesita saber cuáles redes se pueden alcanzar más allá de una interfaz en particular. Existe el mismo problema si una línea arrendada ordinaria se conecta a una interfaz. La diferencia es que el extremo remoto de una línea arrendada se conecta directamente a un único router. Las tramas del DTE viajan a través de la línea arrendada hasta el switch de la red, donde pueden esparcirse a muchos routers, hasta 1000. El DLCI de cada VC debe estar vinculado a la dirección de red de su router remoto. La información se puede configurar de forma manual mediante los comandos de asignaciones. El DLCI puede configurarse de manera automática mediante el protocolo ARP inverso.

2.6.3 INTERFASE DE ADIMINISTRACION LOCAL (LMI)

Es muy importante conocer como hablan entre sí los dos equipos de Frame Relay, esto lo hacen con el LMI (Local Management Interface). El LMI proporciona la comunicación entre el cliente Frame Relay y el Frame Relay switch. Los mensajes de estado ayudan a verificar la integridad de los enlaces físico y lógico. Esta información resulta fundamental en un entorno de enrutamiento, ya que los protocolos de enrutamiento toman decisiones según la integridad del enlace.

Es fundamental conocer como funciona el LMI y conocer los tipos de LMI que existen, porque aunque el LMI sea autoconfigurable desde la IOS 11.3 de Cisco, las versiones anteriores no lo son y hay que realizarlo manualmente mediante comandos, además algunos equipos necesitan que se configure.

Tipos:

Cisco
ANSI
ITU-T Q922

La comunicación del LMI tiene lugar durante el intervalo del keepalive del serial que por defecto es cada 10 segundos, así que cada 10 segundo se envía una query de LMI al LMI switch y se obtiene una respuesta, de esta forma se consigue la continuidad de DLCIs.

Cada 6 LMI paquetes se llama full LMI status y se produce cuando el FR switch confirma toda la información de sus DLCIs.
Los mensajes de estado LMI combinados con los mensajes del ARP inverso permiten que un router vincule direcciones de capa de red con direcciones de la capa de enlace de datos.

Operación de los LMIs

Cuando un router que está conectado a una red Frame Relay arranca, envía un mensaje de consulta de estado LMI a la red. La red contesta con un mensaje de estado LMI que contiene detalles de cada VC configurado en el enlace de acceso (Figura 2.24).
Periódicamente el router repite la consulta de estado, pero las respuestas siguientes sólo incluyen los cambios en el estado. Después de un determinado número de respuestas abreviadas, la red enviará un mensaje de estado completo.

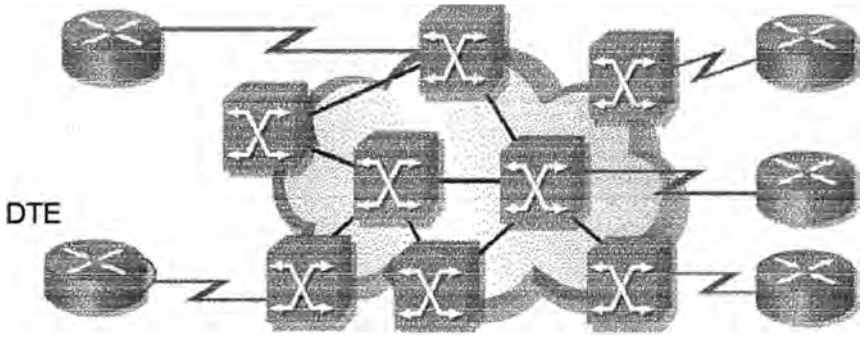


Fig. 2.24 Operación de los DLCIs
DTE (router) envía un mensaje de consulta al DCE (switch FR)
DCE responde con un mensaje de estado que incluye los DCLIs configurados.
DTE descubre los VCs que posee

Si el router necesita asignar los VC a direcciones de capa de red, enviará un mensaje ARP inverso desde cada VC. El mensaje ARP inverso incluye la dirección de capa de red del router, de modo que el DTE o el router remoto, pueda realizar la vinculación. La respuesta ARP inversa permite que el router haga los registros necesarios en su tabla de asignaciones de direcciones a DLCIs. Si el enlace soporta varios protocolos de capa de red, se enviarán mensajes ARP inversos para cada uno de ellos.

2.6.4 CONFIGURACIÓN FRAME RELAY

Se detalla la configuración de un PVC básico en una interfaz serial y equipos Cisco. Para nosotros lo importante de Frame Relay va a ser la parte cliente (DTE) y no la nube Frame Relay.

En Frame Relay es muy importante conocer la relación entre el cliente de Frame Relay y el switch. Si miramos en la parte de cliente tendremos que fijarnos tanto en el nivel 1 y en el nivel 2.En el nivel físico tendremos que ver si tenemos que proporcionar el clocking al interfaz, que esto podemos hacerlo aunque seamos el cliente de nivel 2.En el nivel 2 tendremos que ver la encapsulacion, DTE si somos el cliente o DCE si somos el Frame Relay Switch (situación que no suele ocurrir).También tenemos que fijamos que no hay relación directa entre el nivel 1 y el nivel 2 en el caso de DCE ya que aunque se esté proporcionando el reloj esto no implica que sea el Frame Relay switch

Frame Relay se configura en una interfaz serial. Se debe especificar el tipo de trama Frame Relay de capa 2. El tipo de encapsulamiento por defecto es una versión propietaria de Cisco del HDLC. Se puede cambiar el encapsulamiento de Frame Relay.

```
Router#configure terminal
Router(config)#interface serial 0
Router(config-if)#encapsulation frame-relay [ cisco / ietf ]
```

cisco Usa el encapsulamiento Frame Relay propietario de Cisco. Use esta opción para conectarse a otro router Cisco. Muchos dispositivos de otras marcas también soportan este tipo de encapsulamiento. Esta es la opción por defecto.

ietf Establece el método de encapsulamiento para cumplir con el estándar de la Fuerza de Tareas de Ingeniería de Internet (IETF) RFC 1490. Elija ésta si se conecta a un router que no es Cisco.

-Asignar una dirección IP:

```
Router(config-if)#ip address ip_number mask
```

-Establecer un ancho de banda:

```
Router(config-if)#bandwidth valor_en_Kbps
```

Este comando se usa para notificar al protocolo de enrutamiento que el ancho de banda del enlace se configuró estáticamente. El Protocolo de enrutamiento de gateway interior (IGRP), el Protocolo de enrutamiento de gateway interior mejorado (EIGRP) y el protocolo Primero la ruta libre más corta (OSPF) utilizan el valor del ancho de banda para determinar la métrica de los enlaces

-Establecer el tipo de LMI

```
Router(config-if)#frame-relay lmi-type [ansi/cisco/q333a]
```

Este comando establece y configura la conexión LMI. Este comando es necesario sólo si se usa el Cisco IOS Release 11.1 o una versión anterior. Con la versión 11.2 del software Cisco IOS o posterior, el tipo LMI se detecta automáticamente (que tomara el LMI usado por el switch Frame Relay) y no se requiere configuración. El tipo de LMI por defecto es Cisco. El tipo LMI se configura interfaz por interfaz y se muestra en la resultado del comando `show interfaces`.

2.6.5 MAPEO ESTATICO FRAME RELAY

Se debe asignar de forma estática el DLCI local a la dirección de capa de red de un router remoto cuando el router remoto no soporte el protocolo ARP inverso. Esto también es válido cuando se deba controlar el tráfico de broadcast y de multicast a través de un PVC. Este método de asignación de DLCI se denominan en Frame Relay asignaciones estáticas.

```
Router(config-if)#frame-relay map protocolo direccion_protocolo dlci [broadcast]
```

2.6.6 SUBINTERFACES EN FRAME RELAY

Para permitir el envío de las actualizaciones broadcast de enrutamiento en una topología Frame Relay en estrella, se configura el router de la central con interfaces asignadas lógicamente. Estas interfaces reciben el nombre de subinterfaces. Las subinterfaces son subdivisiones lógicas de una interfaz física.

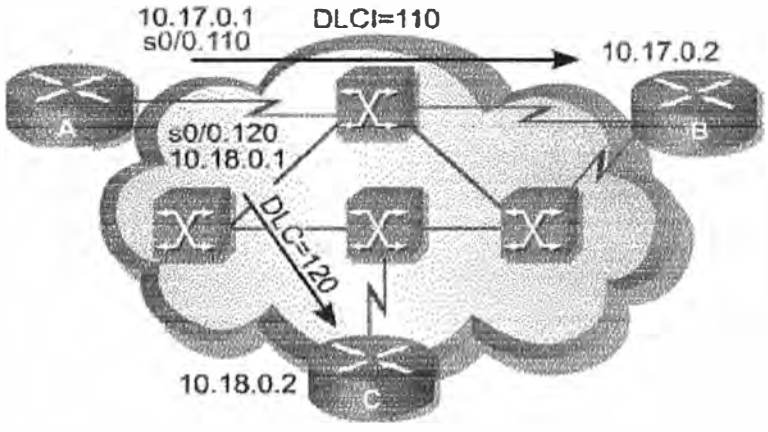


Fig. 2.25 Subinterfaces en Frame Relay

Configuración de Subinterfaces en Frame Relay

En la figura 2.25 , el Router A tiene dos subinterfaces punto a punto. La subinterfaz s0/0.110 se conecta al router B y la subinterfaz s0/0.120, al router C. Cada subinterfaz se encuentra en una subred diferente.

Comandos:

En la interfaz física S0/0 del router A, se configuran dos subinterfaces para dos PVCs

```
Router(config-if)#interface serial s0.110 point-to-point
Router(config-if)#description PVC hacia Router B, DLCI 110
Router(config-if)#ip address 10.17.0.1 255.255.0.0
Router(config-if)#frame-relay interface-dlci  110

Router(config-if)#interface serial s0.120 point-to-point
Router(config-if)#description PVC hacia Router C, DLCI 120
Router(config-if)#ip address 10.18.0.1 255.255.0.0
Router(config-if)#frame-relay interface-dlci  120
```

2.6.7 CONCLUSIONES FRAME RELAY

Frame Relay no es un protocolo especialmente diseñado para soportar tráfico multimedia, audio y vídeo en tiempo real. No hay garantías sobre el retardo de tránsito, pero en la práctica las redes suelen estar bien dimensionadas y el retardo de tránsito es pequeño y no varía apreciablemente.

Además la disponibilidad de estas redes es muy alta, y por todo ello muchas compañías usan redes FR para cursar este tipo de tráfico. En general se considera que son suficientemente buenas para cursar tráfico telefónico, en el que lo más importante (más que la probabilidad de error) es tener una elevada disponibilidad.

CAPITULO III
DISEÑO DE LA RED

3.1 GRAFICO COMPLETO (figura 3.1)

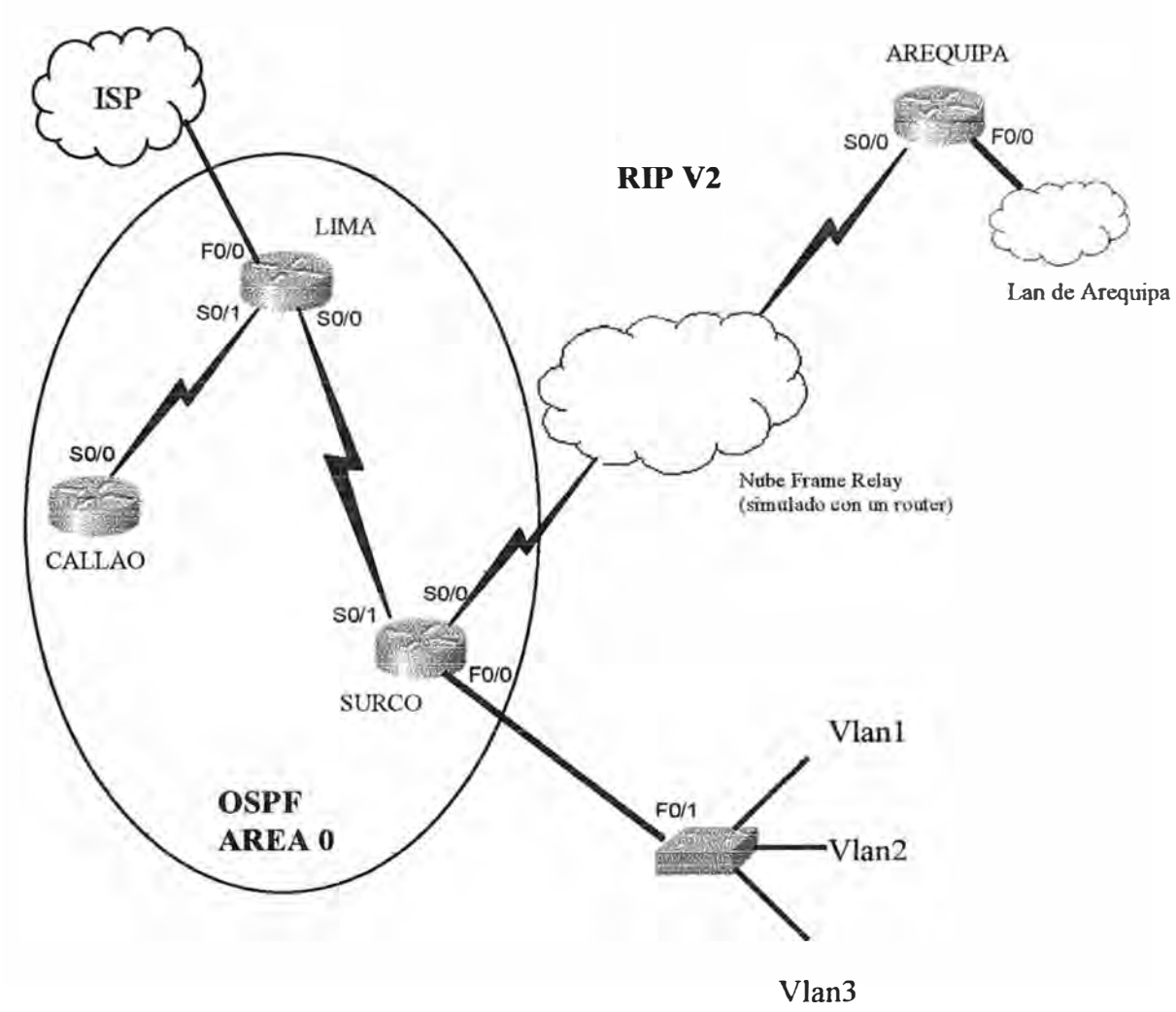


Fig. 3.1 Gráfico completo de la red

3.2 DISEÑO IP DE LA RED

Tenemos como direccion IP: 172.16.0.0 (clase B, fullclass)
Mask: 255.225.0.0 (/16)

Según lo requerido, Surco requiere la mayor cantidad de hosts (750), empezamos el diseño con esta cantidad para crear las subredes.

Aplicamos: $2^n \geq 750$
n = 10

nueva mask: 11111111.11111111.111111**00**.00000000 = 255.255.252.0 = /22
($n = 10$)

De esta manera se obtiene $2^6 = 64$ subredes

Las subredes obtenidas con este subneteo con mascara = /22 serán:

RED 1
172.16.0.0 /22
172.16.0.1

172.16.3.254
172.16.3.255

RED2
172.16.4.0 /22
172.16.4.1

172.16.7.255
172.16.7.255

RED 3
172.16.8.0 /22
172.16.8.1

172.16.11.254
172.16.11.255

RED 4
172.16.12.0 /22
172.16.12.1

172.16.15.254
172.16.15.255

RED 5
172.16.16.0 /22
172.16.16.1

172.16.19.254
172.16.19.255

RED 63
172.16.248.0 /22
172.16.248.1

172.16.251.254
172.16.251.255

RED 64
172.16.252.0 /22
172.16.252.1

172.16.255.254
172.16.255.255

3.2.1 ASIGNACIÓN DE REDES A LAS LAN

Para la LAN de SURCO asignamos la Red 2 (No se usan la Red 1 ni la Red 64 porque contienen la IP de la Red completa así como la IP de Broadcast respectivamente, además así lo recomienda la RFC 950 para una buena implementación de red) :

RED2
172.16.4.0 /22
172.16.4.1
.
.
172.16.7.255
172.16.7.255

Para la red de AREQUIPA asignamos la Red 3, que será el conjunto DHCP a aplicar en su LAN.

RED 3
172.16.8.0 /22
172.16.8.1
.
.
172.16.11.254
172.16.11.255

3.3 DISEÑO DE LOS ENLACES SERIALES

Como solo se requiere 2 ips útiles para los enlaces seriales, vamos a subnetear la penúltima red (RED 63)

RED 63
172.16.248.0
172.16.248.1
.
.
172.16.251.254
172.16.251.255

Para 2 ips útiles: $2^n > 2$ por lo tanto n = 2

Nueva mask: 11111111.11111111.11111111.11111100 = 255.255.255.252 = /30

n = 2

De esta manera se obtienen 2^8 = 256 subredes

Ahora las subredes obtenidas con mascara = /30 serán:

SUBRED 1
172.16.248.0 / 30
172.16.248.1
172.16.248.2
172.16.248.3

SUBRED 2
172.16.248.4 /30
172.16.248.5
172.16.248.6
172.16.248.7

SUBRED 3
172.16.248.8 /30
172.16.248.9
172.16.248.10
172.16.248.11

SUBRED 4
172.16.248.12 /30
172.16.248.13
172.16.248.14
172.16.248.15

SUBRED 256
172.16.251.252 /30
172.16.251.253
172.16.251.254
172.16.251.255

Asignamos lo siguiente (según criterio RFC 950):
Para el enlace Callao – Lima: la Subred 2:

SUBRED 2
172.16.248.4 /30
172.16.248.5
172.16.248.6
172.16.248.7

Para el enlace Lima – Surco: la Subred 3:

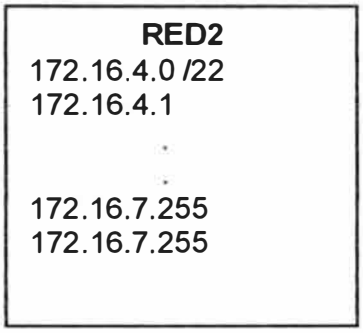
SUBRED 3
172.16.248.8 /30
172.16.248.9
172.16.248.10
172.16.248.11

Para la simulación en Frame Relay (Surco – Arequipa), la Subred 4:

SUBRED 4
172.16.248.12 /30
172.16.248.13
172.16.248.14
172.16.248.15

3.4 DISEÑO DE LAS VLANs

Se tiene la red 172.16.4.0 /22



asignada a la LAN de SURCO, en la cual hay 1024 direcciones IPs, entonces crearemos 4 subredes para las 3 VLANs solicitadas.

Para 4 subredes : $2^n \geq 4$, entonces n = 2

Nueva mask: 11111111.11111111.11111111.00000000 = 255.255.252.0 = /24

n = 2

Con lo cual habrá 2^8 = 256 direcciones Ips por cada subred

Las subredes serán:

SUBRED 1

172.16.4.0 /24
172.16.4.1

172.16.4.254
172.16.4.255

SUBRED 2

172.16.5.0 /24
172.16.5.1

172.16.5.254
172.16.5.255

SUBRED 3
172.16.6.0 /24
172.16.6.1

172.16.6.254
172.16.6.255

SUBRED 4

172.16.7.0 /24
172.16.7.1

172.16.7.254
172.16.7.255

*Tomamos para la VLAN 1 (administrativa) la Subred 1:

SUBRED 1

172.16.4.0 /24
172.16.4.1
172.16.4.2
.
.
172.16.4.254
172.16.4.255

De aquí : 172.16.4.1 → Interfase Ethernet del Router (Default Gateway)
172.16.4.2 → IP para el SWTICH_SURCO

*Tomamos para la VLAN 2, la Subred 2:

SUBRED 2

172.16.5.0 /24
172.16.5.1
.
.
172.16.5.254
172.16.5.255

*Tomamos para la VLAN 3, la Subred 3:

SUBRED 3
172.16.6.0 /24
172.16.6.1
.
.
172.16.6.254
172.16.6.255

Luego, el direccionamiento quedaría como se muestra en la figura 3.2

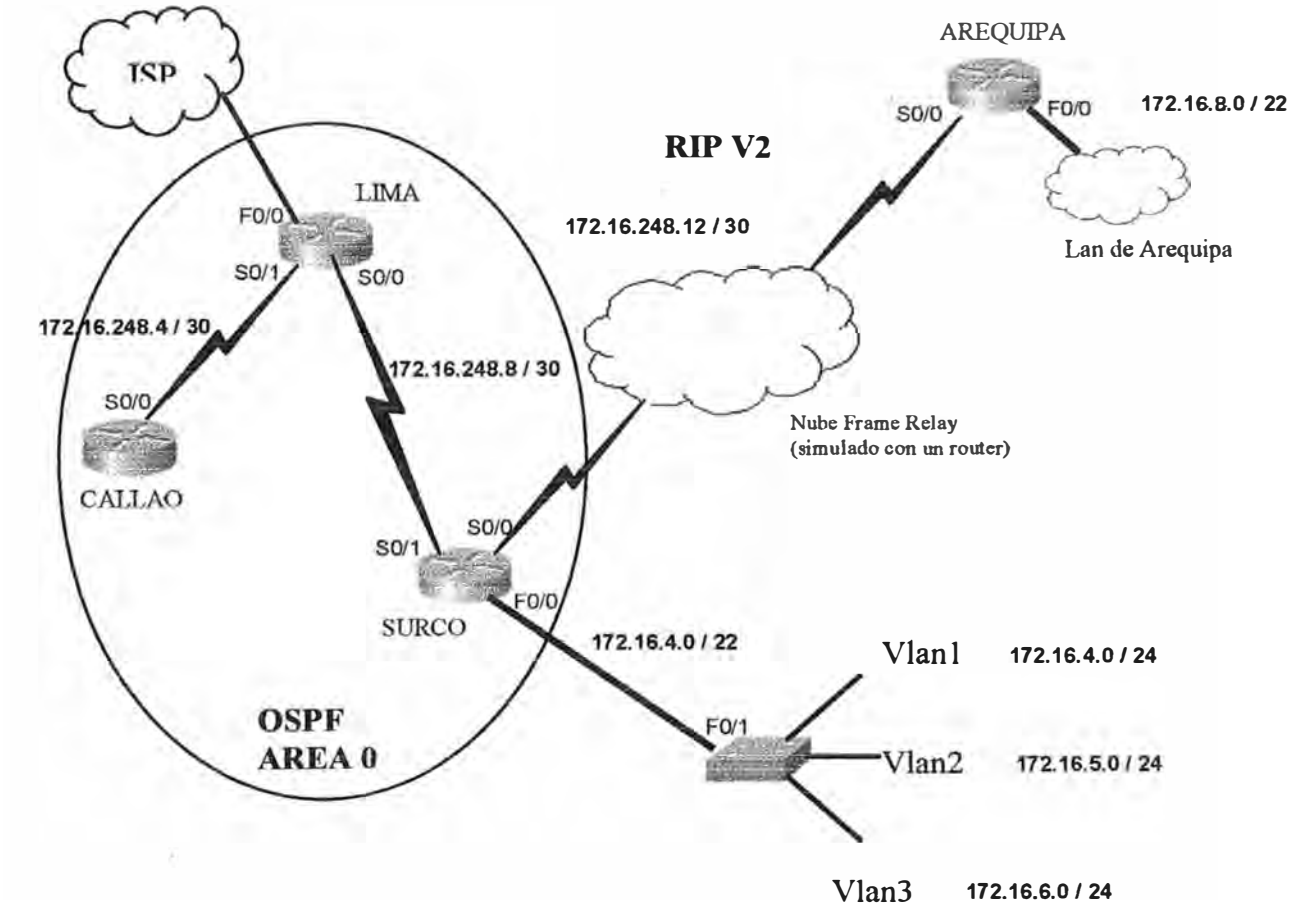


Fig. 3.2 Direccionamiento de la red

CAPITULO IV

CONFIGURACIÓN Y PRESENTACIÓN DE RESULTADOS

4.1 DIRECCIONAMIENTO COMPLETO

El gráfico y tabla resumen completo se muestra en la figura 4.1 y la tabla 4.1 respectivamente.

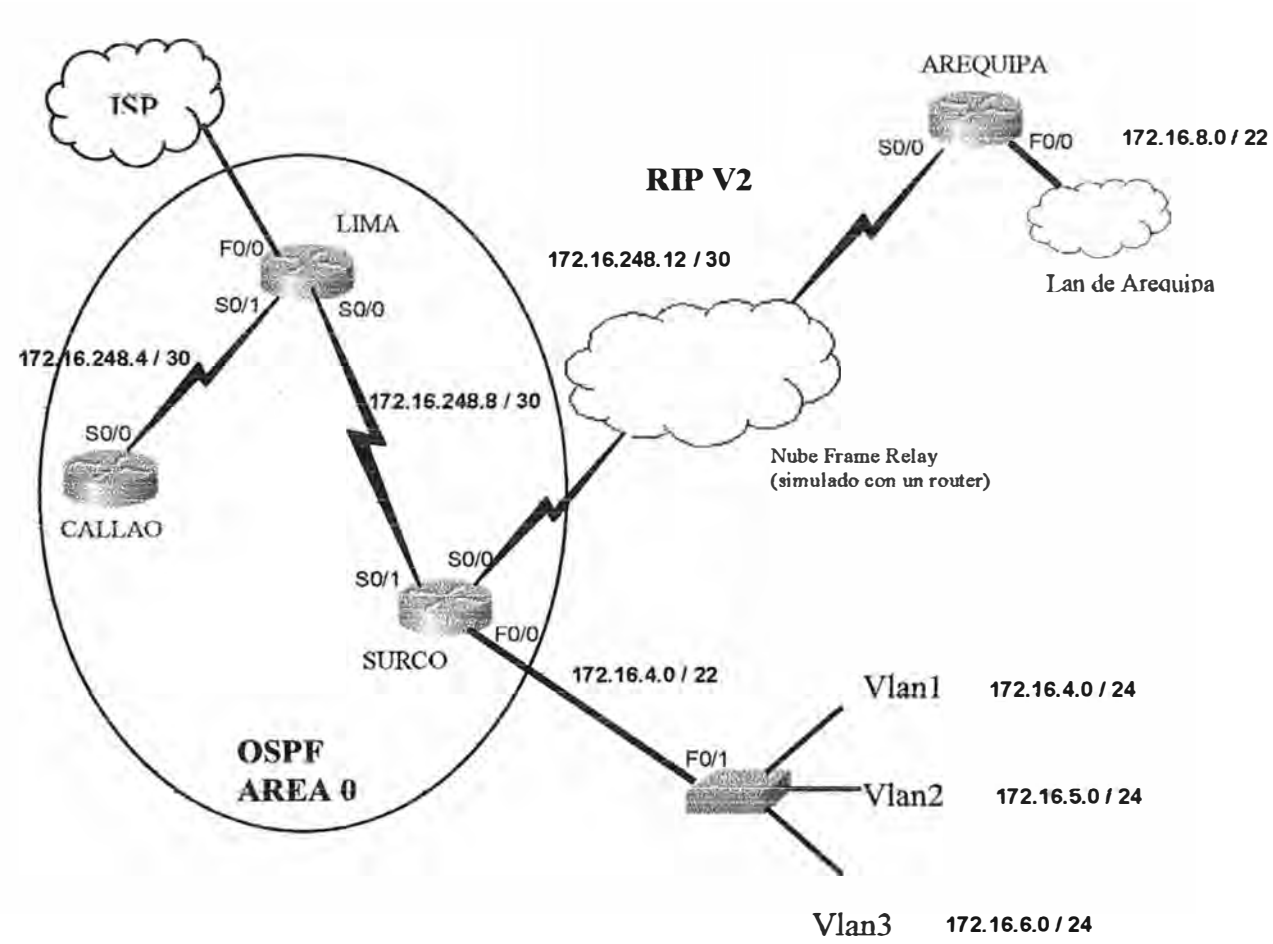


Fig. 4.1 Direccionamiento completo de la red

Nombre Router	Interfaz	IP y mascara de subred
Lima	F0/0	10.0.0.1 /8
Lima	S0/0	172.16.248.9 / 30
Lima	S0/1	172.16.248.5 / 30
Callao	S0/0	172.16.248.6 / 30
Surco	S0/1	172.16.248.10 / 30
Surco	S0/0.102	172.16.248.13 / 30
Surco	F0/0.1	172.16.4.1 / 24
Surco	F0/0.2	172.16.5.1 / 24
Surco	F0/0.3	172.16.6.1 / 24
Arequipa	S0/0.201	172.16.248.14 / 30
Arequipa	F0/0	172.16.8.1 / 22
Pool DHCP Arequipa		172.16.8.0 / 22
LAN SURCO	3 VLAN	172.14.4.0 - 172.16.7.0 / 22
254 Host	VLAN 1	172.16.4.0 – 172.16.4.255 / 24
254 Host	VLAN 2	172.16.5.0 – 172.16.5.255 / 24
254 Host	VLAN 3	172.16.6.0 – 172.16.6.255 / 24

Tabla 4.1 Resumen del direccionamiento IP

4.2 CONFIGURACIÓN DE NOMBRES Y PASSWORD DE LOS ROUTERS

Para configurar el nombre y passwords (consola, vía telnet, y la contraseña enable) se usan

CONFIGURACIÓN DE LIMA

```
Router>en
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname LIMA
LIMA(config)#line console 0
LIMA(config-line)#password amil753123
LIMA(config-line)#login
LIMA(config-line)#exit
LIMA(config)#line vty 0 4
LIMA(config-line)#password amil753123
LIMA(config-line)#login
LIMA(config-line)#exit
LIMA(config)#enable secret amil753123
LIMA(config)#service password-encryption
```

CONFIGURACIÓN DE SURCO

```
Router>en
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname SURCO
SURCO(config)#line console 0
SURCO(config-line)#password ocrus753123
```

```
SURCO(config-line)#login
SURCO(config-line)#exit
SURCO(config)#line vty 0 4
SURCO(config-line)#password ocrus753123
SURCO(config-line)#login
SURCO(config-line)#exit
SURCO(config)#enable secret ocrus753123
SURCO(config)#service password-encryption
```

CONFIGURACIÒN DE CALLAO

```
Router>en
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname CALLAO
CALLAO(config)#line console 0
CALLAO(config-line)#password oallac753123
CALLAO(config-line)#login
CALLAO(config-line)#exit
CALLAO(config)#line vty 0 4
CALLAO(config-line)#password oallac753123
CALLAO(config-line)#login
CALLAO(config-line)#exit
CALLAO(config)#enable secret oallac753123
CALLAO(config)#service password-encryption
```

4.3 CONFIGURACIÓN DE INTERFACES SERIALES Y ETHERNET

LIMA

```
LIMA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
LIMA(config)#interface serial 0/1
LIMA(config-if)#ip address 172.16.248.5 255.255.255.252
LIMA(config-if)#no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to
up
%LINK-3-UPDOWN:  Interface Serial0/1, changed state to up

LIMA(config)#interface serial 0/0
LIMA(config-if)#ip address 172.16.248.9 255.255.255.252
LIMA(config-if)#no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to
up
%LINK-3-UPDOWN:  Interface Serial0/0, changed state to up
LIMA(config-if)#clock rate 56000
```

CALLAO

```
CALLAO#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CALLAO(config)#interface serial 0/0
```

```
CALLAO(config-if)#ip address 172.16.248.6 255.255.255.252
CALLAO(config-if)#no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to
up
%LINK-3-UPDOWN:  Interface Serial0/0, changed state to up
CALLAO(config-if)#clock rate 56000
```

SURCO

```
SURCO#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SURCO(config)#interface serial 0/1
SURCO(config-if)#ip address 172.16.248.10 255.255.255.252
SURCO(config-if)#no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to
up
%LINK-3-UPDOWN:  Interface Serial0/1, changed state to up
```

No se considera aún la configuración de S0/0 de SURCO, pues se verá al configurar el Circuito Virtual (PVC) del Frame Relay entre SURCO y AREQUIPA. Tampoco la configuración de E0 pues como se formarán VLANs para esta LAN, primero debemos crearlas.

4.4 CONFIGURACIÓN DEL SWITCH

```
Switch>en
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SWITCH_SURCO
SWITCH_SURCO(config)#password surco
SWITCH_SURCO(config)#login
SWITCH_SURCO(config)#line vty 0 15
SWITCH_SURCO(config)#password surco
SWITCH_SURCO(config)#login
SWITCH_SURCO(config)#interface vlan 1
SWITCH_SURCO(config-if)#ip address 172.16.4.2 255.255.255.0
SWITCH_SURCO(config-if)#ip default-gateway 172.16.4.1
```

4.5 CREACION DE LAS VLANS

```
SWITCH_SURCO#vlan database
SWITCH_SURCO(vlan)#vlan 2 name vlan2
SWITCH_SURCO(vlan)#exit
```

```
SWITCH_SURCO#vlan database
SWITCH_SURCO(vlan)#vlan 3 name vlan3
SWITCH_SURCO(vlan)#exit
```

4.6 ASIGNAR PUERTOS A LAS VLANS

4.6.1 ASIGNAR PUERTOS A LA VLAN 2

```
SWITCH_SURCO#configure terminal
SWITCH_SURCO(config)#interface fastethernet 0/9
SWITCH_SURCO(config-if)#switchport mode access
SWITCH_SURCO(config-if)#switchport access vlan 2

SWITCH_SURCO(config)#interface fastethernet 0/10
SWITCH_SURCO(config-if)#switchport mode access
SWITCH_SURCO(config-if)#switchport access vlan 2

SWITCH_SURCO(config)#interface fastethernet 0/11
SWITCH_SURCO(config-if)#switchport mode access
SWITCH_SURCO(config-if)#switchport access vlan 2

SWITCH_SURCO(config)#interface fastethernet 0/12
SWITCH_SURCO(config-if)#switchport mode access
SWITCH_SURCO(config-if)#switchport access vlan 2

SWITCH_SURCO(config)#interface fastethernet 0/13
SWITCH_SURCO(config-if)#switchport mode access
SWITCH_SURCO(config-if)#switchport access vlan 2

SWITCH_SURCO(config)#interface fastethernet 0/14
SWITCH_SURCO(config-if)#switchport mode access
SWITCH_SURCO(config-if)#switchport access vlan 2

SWITCH_SURCO(config)#interface fastethernet 0/15
SWITCH_SURCO(config-if)#switchport mode access
SWITCH_SURCO(config-if)#switchport access vlan 2
```

4.6.2 ASIGNAR PUERTOS A LA VLAN 3

```
SWITCH_SURCO#configure terminal
SWITCH_SURCO(config)#interface fastethernet 0/16
SWITCH_SURCO(config-if)#switchport mode access
SWITCH_SURCO(config-if)#switchport access vlan 3

SWITCH_SURCO(config)#interface fastethernet 0/17
SWITCH_SURCO(config-if)#switchport mode access
SWITCH_SURCO(config-if)#switchport access vlan 3
```

```
SWITCH_SURCO(config)#interface fastethernet 0/18
SWITCH_SURCO(config-if)#switchport mode access
SWITCH_SURCO(config-if)#switchport access vlan 3
SWITCH_SURCO(config)#interface fastethernet 0/19
SWITCH_SURCO(config-if)#switchport mode access
SWITCH_SURCO(config-if)#switchport access vlan 3

SWITCH_SURCO(config)#interface fastethernet 0/20
SWITCH_SURCO(config-if)#switchport mode access
SWITCH_SURCO(config-if)#switchport access vlan 3

SWITCH_SURCO(config)#interface fastethernet 0/21
SWITCH_SURCO(config-if)#switchport mode access
SWITCH_SURCO(config-if)#switchport access vlan 3

SWITCH_SURCO(config)#interface fastethernet 0/22
SWITCH_SURCO(config-if)#switchport mode access
SWITCH_SURCO(config-if)#switchport access vlan 3

SWITCH_SURCO(config)#interface fastethernet 0/23
SWITCH_SURCO(config-if)#switchport mode access
SWITCH_SURCO(config-if)#switchport access vlan 3

SWITCH_SURCO(config)#interface fastethernet 0/24
SWITCH_SURCO(config-if)#switchport mode access
SWITCH_SURCO(config-if)#switchport access vlan 3
```

4.7 CONFIGURANDO EL ENLACE TRONCAL PARA LA CONEXIÓN ENTRE EL SWITCH Y EL ROUTER (en el puerto e0/1 del switch)

```
SWITCH_SURCO#configure terminal
SWITCH_SURCO(config)#interface fastethernet 0/1
SWITCH_SURCO(config-if)#switchport mode trunk
SWITCH_SURCO(config-if)#end
```

4.8 CONFIGURACION PARA EL ROUTER CON DHCP

```
Router>en
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname AREQUIPA
AREQUIPA(config)#line console 0
AREQUIPA(config-line)#password apiuqe753123
AREQUIPA(config-line)#login
AREQUIPA(config-line)#exit
AREQUIPA(config)#line vty 0 4
```

AREQUIPA(config-line)#password apiuqe753123
AREQUIPA(config-line)#login
AREQUIPA(config-line)#exit
AREQUIPA(config)#enable secret apiuqe753123
AREQUIPA(config)#service password-encryption

AREQUIPA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AREQUIPA(config)#interface fastethernet 0/0
AREQUIPA(config-if)#ip address 172.16.8.1 255.255.252.0
AREQUIPA(config-if)#no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
%LINK-3-UPDOWN: Interface Serial0/0, changed state to up

AREQUIPA(config)#ip dhcp pool DHCPAREQUIPA
AREQUIPA(dhcp-config)#network 172.18.8.0 255.255.252.0
AREQUIPA(dhcp-config)#default-router 172.16.8.1
AREQUIPA(dhcp-config)#domain-name DATACENTER.COM

Excluir la dirección del Gateway (e0)

AREQUIPA(config)#ip dhcp excluded-address 172.16.8.1 172.16.8.1

4.9 CONFIGURACIÓN DEL ENRUTAMIENTO EN EL AREA 0

CALLAO

CALLAO#configure terminal
CALLAO(config)#router ospf 1
CALLAO(config-router)#network 172.16.248.4 0 0.0.0.3 area 0

LIMA

LIMA#configure terminal
LIMA(config)#router ospf 1
LIMA(config-router)#network 172.16.248.4 0 0.0.0.3 area 0
LIMA(config-router)#network 172.16.248.8 0 0.0.0.3 area 0

SURCO : Se definieron las VLANs, se crearan las subinterfaces (f0/0.1 , f0/0.2 , f0/0.3) asociadas a cada VLAN y se procede al enrutamiento entre ellas

```
SURCO#configure terminal
SURCO(config)#interface fastethernet 0/0.1
SURCO(config-subif)#description Subinterfaz f0/0.1 – Gateway para VLAN1, VLAN administrativa
SURCO(config-subif)#encapsulation dot1Q 1  {Define el encapsulamiento de las tramas en VLAN1
SURCO(config-subif)#ip address 172.16.4.1 255.255.255.0

SURCO(config)#interface fastethernet 0/0.2
SURCO(config-subif)#description Subinterfaz f0/0.2 – Gateway para VLAN2, Administra la VLAN 2
SURCO(config-subif)#encapsulation dot1Q 2
SURCO(config-subif)#ip address 172.16.5.1 255.255.255.0

SURCO(config)#interface fastethernet 0/0.3
SURCO(config-subif)#description Subinterfaz f0/0.3 – Gateway para VLAN3, Administra la VLAN 3
SURCO(config-subif)#encapsulation dot1Q 3
SURCO(config-subif)#ip address 172.16.6.1 255.255.255.0


*Definiendo el enrutamiento entre con los demás routers
SURCO(config)#router ospf 1
SURCO(config-router)#network 172.16.4.0  0 0.0.0.255 area 0
SURCO(config-router)#network 172.16.5.0  0 0.0.0.255 area 0
SURCO(config-router)#network 172.16.6.0  0 0.0.0.255 area 0
SURCO(config-router)#network 172.16.248.8 0.0.0.3 area 0
```

En este router se debe configurar la redistribución de rutas entre OSPF y RIP para lo cual previamente configuraremos RIP.

4.10 CONFIGURACION RIP

Además se debe configurar en el router SURCO el enrutamiento RIP V2 pues con este protocolo intercambiara tablas de ruteo con Arequipa según lo propuesto en el diseño.

```
Surco(config)# router rip
Surco(config-router)#version 2
Surco(config-router)#network 172.16.248.12
```

AREQUIPA: Se incluye en el ruteo su respectiva red LAN

```
Arequipa(config)#router rip
Arequipa(config-router)#version 2
Arequipa(config-router)#network 172.16.248.12
Arequipa(config-router)#network 172.16.8.0
```

4.11 REDISTRIBUCIÓN DE RUTAS

Según lo propuesto, existen 2 zonas que usan protocolos de encaminamiento distinto, y para que pueda funcionar correctamente toda la red, deben poder intercambiar correctamente sus tablas de ruteo. En este caso en el Área 0 : Callao, Lima y Surco intercambian tablas de rutas mediante OSPF, mientras que Surco y Arequipa lo hacen mediante RIP V2. Hay que inyectar las rutas que se aprenden de un protocolo a otro. A este proceso se le llama "Redistribución de rutas". Lo lógico es que en una red corra un único protocolo de ruteo, pero imaginar que se unen dos redes con protocolos distintos y tienen que convivir (pueden incluso estar administrados por distintos departamentos).

El punto más importante es que las métricas de los protocolos son distintas, RIP usa saltos ("hops") y OSPF usa "bandwitdh".

4.11.1 REDISTRIBUCIÓN DE RIP DENTRO DE OSPF

```
Surco(config)#router ospf 1
Surco(config-router)#redistribute rip subnets    {redistribuye redes classfull y classless,
                                                   anuncia las rutas obtenidas por RIP en el
                                                   proceso OSPF
```

4.11.2 REDISTRIBUCIÓN DE OSPF DENTRO DE RIP

```
Surco(config)#router rip
Surco(config-router)#version 2
Surco(config-router)#redistribute ospf 1 match internal external 1 external 2
                                                    {Anuncia las rutas obtenidas
                                                     por OSPF en el proceso RIP

Surco(config-router)#default-metric 17
```

4.12 CONFIGURACIÓN DE NAT

El router Lima ejecutará NAT, el conjunto NAT consiste de una sola dirección de 192.168.1.6 / 30 . Se debe permitir el tráfico a Internet de todas las direcciones internas (172.16.0.0 / 16) y se debe denegar todo el tráfico restante, además el tiempo de espera NAT será de 120 segundos. Se simulará el Servidor ISP con una PC conectada al puerto ethernet del router, con IP 10.0.0.2 / 8. (Figura 4.2)

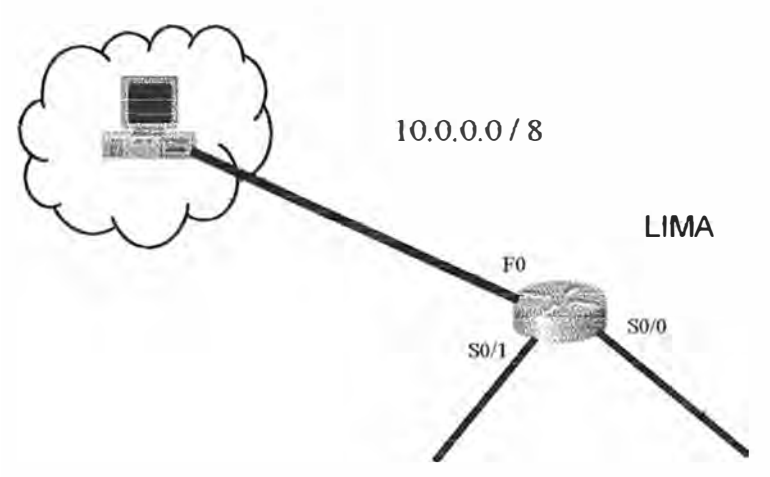


Fig. 4.2 Implementar NAT

Lima#configure terminal
Lima(config)#interface f0/0
Lima(config-if)#description Interfaz de conexión con el ISP
Lima(config-if)#ip address 10.0.0.1 255.0.0.0
Lima(config-if)#exit

Lima(config)#access-list 1 172.16.0.0 0.0.255.255 {crea la lista de acceso

Lima(config)#ip nat pool Publico 192.168.1.6 192.168.1.6 netmask 255.255.255.252
{crea el pool (1) de direcciones NAT

Lima(config)#ip nat incide source list 1 pool Publico overload {sobrecarga, todas se traducen
a 192.168.1.6

-Definimos las interfaces internas y externas

Lima(config)#interface serial 0/0
Lima(config-if)#ip nat inside

Lima(config)#interface serial 0/1
Lima(config-if)#ip nat inside

Lima(config)#interface fastethernet 0/0
Lima(config-if)#ip nat outside

Lima#ip nat translation 120 {Tiempo de espera NAT

4.13 CONFIGURACIÓN FRAME RELAY Y CREACIÓN DE SUBINTERFACES

Nos apoyamos en la figura 4.3

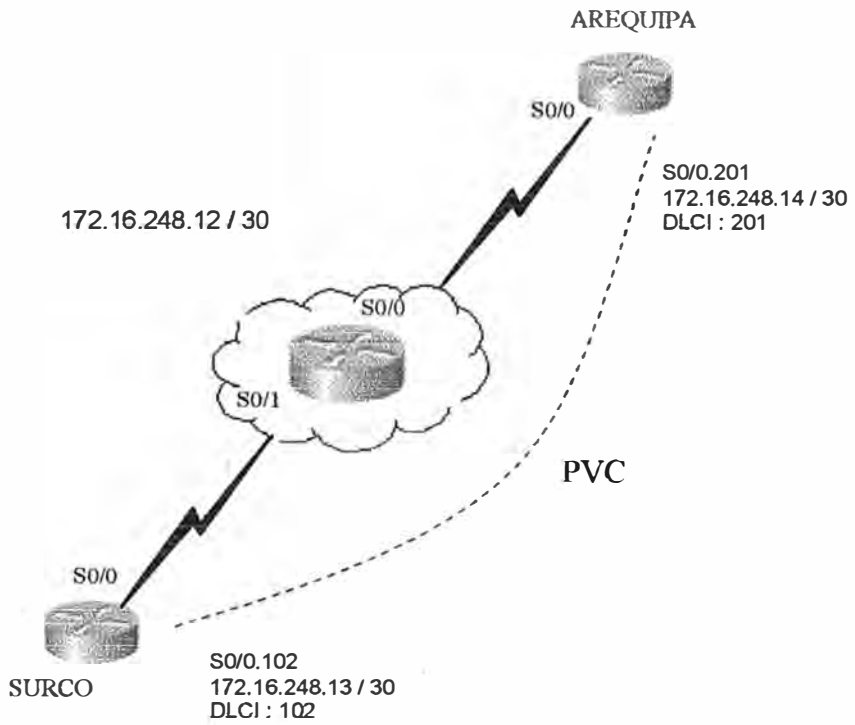


Fig. 4.3 Nube Frame Relay

ROUTER SURCO:

Configuración Frame Relay: Trabajamos en la interface serial 0/0

```
Surco#configure terminal
Surco(config)#interface serial 0/0
Surco(config-if)#encapsulation frame-relay ietf
Surco(config-if)#frame-relay lmi-type ansi
Surco(config-if)#no shutdown
Surco(config-if)#end
```

Creación de Subinterfaces y PVCs : Trabajamos en la interface serial 0/0

```
Surco(config)#interface serial 0/0.102 point-to-point
Surco(config-if)#description PVC hacia Arequipa, DLCI 102
Surco(config-if)#ip address 172.16.248.13 255.255.255.252
Surco(config-if)#frame-relay interface-dlci 102
Surco(config-if)#end
```

ROUTER AREQUIPA:
Configuración Frame Relay

```
Arequipa#configure terminal
Arequipa(config)#interface serial 0/0
Arequipa(config)#encapsulation frame-relay ietf
Arequipa(config)#frame-relay lmi-type ansi
Arequipa(config)#no shutdown
Arequipa(config)#end
```

Creación de Subinterfaces y PVCs : Trabajamos en la interface serial 0/0

```
Arequipa(config)#interface serial 0/0.201 point-to-point
Arequipa(config-if)#description PVC hacia Surco, DLCI 201
Arequipa(config-if)#ip address 172.16.248.14 255.255.255.252
Arequipa(config-if)#frame-relay interface-dlci 201
Arequipa(config-if)#end
```

4.14 SIMULACIÓN DE NUBE FRAME RELAY CON UN ROUTER

Activamos la opción de Switch Frame Relay en el modo de configuración global:

```
Router_sw(config)#frame-relay switching
```

Además para en cada interface serial debemos especificar que dichas interfaces serán DCE

También usamos el comando de configuración de interface : ***frame-relay route***, para rutear el DLCI entrante a la interface saliente y al DLCI saliente:

frame-relay route *dlci_entrante* **interface** *interface_saliente dlci_saliente*

Ingresamos a la interface serial 0/0 y configuramos:

```
Router_sw(config)#interface s0/0
Router_sw(config-if)#encapsulation frame-relay ietf
Router_sw(config-if)#clock rate 56000
Router_sw(config-if)#no shutdown
Router_sw(config-if)#frame-relay intf-type dce
Router_sw(config-if)#frame-relay lmi-type ansi
Router_sw(config-if)#frame-relay route 201 interface s0/1 102
```

Ingresamos a la interface serial 0/1 y configuramos

```
Router_sw(config)#interface s0/1
Router_sw(config-if)#encapsulation frame-relay ietf
Router_sw(config-if)#clock rate 56000
Router_sw(config-if)#no shutdown
Router_sw(config-if)#frame-relay intf-type dce
Router_sw(config-if)#frame-relay lmi-type ansi
Router_sw(config-if)#frame-relay route 102 interface s0/0 201
```

Para verificar el contenido de las tablas de rutas Frame Relay:

```
Router_sw#show frame-relay route
```

CONCLUSIONES Y RECOMENDACIONES

1.- Se recomienda, en todo diseño de red, seguir las instrucciones de las Request For Comments (RFC), acerca del tema en desarrollo.

2.- Se concluye que cuando mas servicios se activen en el router, decrece su performance y eficiencia.

3.- Se recomienda, en la medida de lo posible, hacer uso de servidores DHCP en el diseño de red, ya que esto minimizaria los errores por asignación de direcciones IP, así como la mejor administración de dichos recursos.

4.- Se recomienda que antes de realizar una implementación física de dicha red, primero se debe realizar una simulación mediante software, del diseño realizado, pues permitiría analizar los resultados, y poder modificar la red si hubiesen errores.

5.- Se concluye que el uso de VLANs en un diseño de red, permite trasladar y agregar fácilmente las estaciones de trabajo, asi como controlar el tráfico de la red.

6.- Si se utiliza al router como servidor DHCP, se recomienda configurar este servicio en cada router, para asi evitar que las peticiones broadcast DHCP inunden toda la WAN.

7.- Se recomienda el uso de NAT ya que de esta manera, ahorramos direcciones IP utilizables para salir a Internet.

ANEXOS

ANEXO A

COMANDOS USUALES EN ROUTERS Y SWITCHES

Configuración del Hostname

Router#configure terminal
Router(config)#hostname *[Nombre]*
Nombre(config)#Ctrl + z
Nombre#

Configuración de Password

1.- Enable Password

Nombre#configure terminal
Nombre(config)#enable password *[password]*
Nombre(config)#Ctrl + z
Nombre#

2.- Enable Secret

Nombre#configure terminal
Nombre(config)#enable secret *[password]*
Nombre(config)#Ctrl + z
Nombre#

3.- Terminal

Nombre#configure terminal
Nombre(config)#line vty 0 4
Nombre(config-line)#login
Nombre(config-line)#password *[password]*
Nombre(config-line)#Ctrl + z
Nombre#

4.- Consola

Nombre#configure terminal
Nombre(config)#line console 0
Nombre(config-line)#login
Nombre(config-line)#password *[password]*
Nombre(config-line)#Ctrl + z
Nombre#

5.- Auxiliar

Nombre#configure terminal
Nombre(config)#line auxiliary 0
Nombre(config-line)#login
Nombre(config-line)#password *[password]*
Nombre(config-line)#Ctrl + z
Nombre#

Configuración de Mensaje del día

Nombre#configure terminal
Nombre(config)#banner motd #
Enter TEXT message. End with the carácter '#'
Mensaje #
Nombre(config)#Ctrl+z
Nombre#

Configuración de Mensaje del día

Nombre#configure terminal
Nombre(config)#banner login #
Enter TEXT message. End with the carácter '#'
Mensaje #
Nombre(config)#Ctrl+z
Nombre#

Configuración de la descripción de las Interfaces

Nombre#configure terminal
Nombre(config)#interface *[interface]*
Nombre(config-if)#description *[descripción]*
Nombre(config-if)#Ctrl + z
Nombre#

Configuración del Registro de Configuración

Nombre#configure terminal
Nombre(config)config-register *[registro]*
Nombre(config)#Ctrl + z
Nombre#

Configuración de las Direcciones de las Interfaces

Nombre#configure terminal
Nombre(config)#interface *[interface]*
Nombre(config-if)#ip address *[dirección] [máscara]*
Nombre#config-if)#no shutdown
Nombre(config-if)#Ctrl + z
Nombre#

Configuración del Protocolo

Nombre#configure terminal
Nombre(config)#router rip
Nombre#config-router)#Ctrl.+z
Nombre#

Configuración de Rutas Estáticas

Nombre#configure terminal
Nombre(config)#ip router ip_*[red_origen] [máscara_destino] [ip_interface_destino]*
Nombre(config)#Ctrl.+z
Nombre#

Configuración de redes Directamente Conectadas

Nombre#configure terminal
Nombre(config)#router *[protocolo]*
Nombre(config-router)#network *[dirección]*
Nombre(config-router)#Ctrl+z
Nombre#

Configuración de la Secuencia de Arranque

Nombre# configure terminal
Nombre(config)#boot system flash gsnew-image
Nombre(config)#boot system tftp test.exe dirección
Nombre(config)#boot system rom
Nombre(config)#Ctrl+z
Nombre#

Configuración de Hosts

Nombre#configure terminal
Nombre(config)#ip host *[nombre][direcciones]*
Nombre(config)#ctrl.+z
Nombre#

Comandos ACL estándar

Paso 1 Definir la ACL

Router(config)# **access-list** *[access-list-number]* {**permit** | **deny**} *{test-conditions}*

Paso2: Aplicar la ACL a una interface

Router(config-if)# *{protocol}* **access-group** *[access-list-number]*

Comandos any

Router(config)# **access-list** 1 permit 0.0.0.0 255.255.255.255
cualquier IP máscara wildcard

Se puede usar esto:

Router(config)# access-list 1 permit any

Comando host

Router(config)# **access-list** 1 permit 172.30.16.29 0.0.0.0
dirección IP máscara wildcard

se puede usar esto:

Router(config)# **access-list** 1 permit host 172.30.16.29

Comando para ver las ACL

Router(config)# **show access-list** *[access-list-number]*

Comandos ACL extendidas

Router(config)# **access-list** *[access-list-number]* {**permit** | **deny**} *[protocol] [source-address] [source-mask] [destination-adress] [destination-mask]* **operator** *[operand]* [established]

Router(config-if)# *{protocol}* **access-group** *[access-list-number]* {**in** | **out**}

Comandos ACL nombradas

Router(config)# **ip access-list** {**standard** | **extended**} *[name]*

El Comandos deny

deny {source *[source-wildcard]* | **any**}

Comandos Show

Router# show running-config
Router# show startup-config
Router# show memory
Router# show stacks
Router# show buffers
Router# show arp
Router# show processes
Router# show nvram
Router# show flas
Router# show version
Router# show processes cpu
Router# show tech-support

Comandos Copy

Router# copy running-config tftp
Router# copy tftp running-config
Router# copy flsh tftp
Router# copy tftp flash

Comandos de Inicio

Router(config)# config-register 0x2102
Router(config)# boot system flash igs-j-1.111-5
Router(config)# boot system tftp igs-j-1.111-5

Encapsulamiento PPP

Router(config)# interface Serial 0
Router(config-if)# encapsulation ppp
Router# show interface s 0

PPP con autenticación PAP

Router(config)# interface Serial 0
Router(config-if)# encapsulation ppp
Router(config-if)# ppp authentication pap
Router(config-if)# ppp pap sent-username LabB password class

PPP con autenticación CHAP

Router(config)# interface Serial 0
Router(config-if)# encapsulation ppp
Router(config-if)# ppp authentication chap
Router# username LabB password class

Comandos Para Frame Relay
Router-1

```
Router-1(config)# interface s 1
Router-1(config-if)# ip add 100.16.0.1 255.255.255.0
Router-1(config-if)# encapsulation frame-relay
Router-1(config-if)# bandwidth 56
Router-1(config-if)# frame-relay map ip 10.16.0.2 110 broadcast ietf
Router-1(config-if)# frame-relay lmi-type ansi (Se necesita para versiones anteriores a 11.0
                                                IOS 11.0 soporta sensor LMI automático)
Router-1(config)# router rip
Router-1(config-router)# network 10.0.0.0
```

Router-2

```
Router-2(config)# interface s 1
Router-2(config-if)# ip add 10.16.0.2 255.255.255.0
Router-2(config-if)# encapsulation frame-relay
Router-2(config-if)# bandwidth 56
Router-1(config-if)# frame-relay map ip 10.16.0.1 110 broadcast ietf
Router-1(config-if)# frame-relay lmi-type ansi (Se necesita para versiones anteriores a 11.0
                                                IOS 11.0 soporta sensor LMI automático)
Router-1(config)# router rip
Router-1(config-router)# network 10.0.0.0
```

Ejemplo de configuración de subinterfaces multipunto

```
Router-1(config)# interface s2
Router-1(config-if)# no ip address
Router-1(config-if)# encapsulation frame-relay
Router-1(config-if)# exit
Router-1(config)# interface s2.2 multipoint
Router-1(config-if)# ip add 10.17.0.1 255.255.255.0
Router-1(config-if)# bandwhidth 64
Router-1(config-if)# frame-relay map ıp 10.17.0.2 broadcast ietf
Router-1(config-if)# frame-relay map ıp 10.17.0.3 broadcast ietf
Router-1(config-if)# frame-relay map ıp 10.17.0.4 broadcast ietf

Router-1(config)# router rip
Router-1(config-if)# network 10.0.0.0
```

Ejemplo de configuración de subinterfaces punto a punto

```
Router-1(config)# interface s2
Router-1(config-if)# no ip address
```

```
Router-1(config-if)# encapsulation  frame-relay
Router-1(config-if)# exit
Router-1(config)# interface  s2.2  point-to-point
Router-1(config-if)# ip add  10.17.0.2  255.255.255.0
Router-1(config-if)# bandwhidth  64
Router-1(config-if)#  frame-relay  interface-dlci  200  broadcast  cisco
Router-1(config-if)#  exit
Router-1(config)# interface  s2.3  point-to-point
Router-1(config-if)# ip add  10.18.0.3  255.255.255.0
Router-1(config-if)# bandwhidth  64
Router-1(config-if)#  frame-relay  interface-dlci  300  broadcast  cisco
Router-1(config-if)#  exit
Router-1(config)# interface  s2.4  point-to-point
Router-1(config-if)# ip add  10.20.0.3  255.255.255.0
Router-1(config-if)# bandwhidth  64
Router-1(config-if)#  frame-relay  interface-dlci  400  broadcast  cisco

Router-1(config)#  router rip
Router-1(config-if)#  network  10.0.0.0
```

Monitoreo de Frame-Relay

Router# show frame-relay pvc	Muestra estadísticas acerca de los PVC para las interfaces Frame Relay
Router# show frame-relay map	Muestra la entrada de asignación Frame Relay actuales e información acerca de estas conexiones
Router# show frame-relay lmi	Muestra estadísticas acerca de la interface de administración local (LMI)
Router# debug frame-relay events	Muestra los sucesos de paquetes Frame Relay
Router# debug frame-relay lmi	Muestra los intercambios LMI de Frame Relay con el proveedor de servicio
Router# debug frame-relay packet	Muestra los paquetes Frame Relay
Router# debug frame-relay nli	Muestra la interface de capa de red Frame Relay

Comandos de configuración de VLAN

Los comandos son similares a los de Cisco IOS

Switch 1900 - Borrar Archivo de Configuración

1900-A#delete NVRAM
1900-A#delete vtp (hay que marcar los dos)
1900-A#show ip (muestra la IP de administración. Es una sola. ¡OJO! la IP y la VLAN en la misma red)

Switch Catalyst 1900 - Crear VLAN

1900-A#config t
1900-A(config)# vlan *[vlan-number (1-999)]* name *[vlan-name]*

Para trunk 100000 (SAID) + Número de VLAN

1900-A(config)# interface fastethernet 0/4 a 27 (trunk on)
1900-A(config-if)# vlan-membership *[static] [vlan-number]*

1900-A(config)# show vlan
vlan *[vlan-number]*
vlan *membership*

Switch Catalyst 2950 - Borrar Archivo de Configuración

2950-A# erase startup-config
2950-A# vlan database
2950-A# no vlan *[vlan-number]* se debe borrar una por una

2950-A(config)# interface *[vlan-number]*
2950-A(config-if)# ip address *[IP-address] [IP-mask]* Una IP por cada VLAN Management
2950-A(config-if)# ip default-gateway *[IP-address]*

Switch Catalyst 2950 - Crear VLAN

2950-A# vlan database
2950-A(vlan)# vlan *[vlan-number]* name *[vlan-name]*
2950-A(vlan)# exit

Switch Catalyst 2950 - Asignar puertos

2950-A# interface fastethernet 0/4
2950-A(config-if)# switchport mode *[access | trunk]*
2950-A(config-if)# switchport access vlan *[vlan-number]*
2950-A(config-if)# switchport alloed-vlan *[desde-hasta]*
2950-A(vlan)# CTRL + Z

Switch Catalyst 2950 - Para ver VLAN

2950-A# show vlan *[all | vlan-number]*

BIBLIOGRAFÍA

1.- Redes de Computadoras, Andrew Tanenbaum, 4ta Edición, Editorial Prentice may México.

2.- Guía del primer año, Academia de Networking Cisco, Editorial Cisco Press

3.- Guía del segundo año, Academia de Networking Cisco, Editorial Cisco Press

4.- Interconexión de dispositivos Cisco, Editorial Cisco Press

5.- Fundamentos de seguridad de redes, Editorial Cisco Press

6.- Pagina oficial de la Academia de Networking de Cisco:
http://www.cisco.com/web/leaming/netacad/index.html

7.- Wikipedia en español
http://es.wikipedia.org/wiki/Portada

8. Documentos de los estándares que se encuentran dentro de los RFC
http://www.rfc-editor.org/

9.- RFC de la IETF
http://www.ietf.org/rfc.html

10.- Tutorial sobre Frame relay
http://www.consulintel.es/Html/Tutoriales/Articulos/tutorial_fr.html