ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"ANALISIS, DISEÑO Y OPTIMIZACION DE UNA RED LOCAL CON INTERVLANS TRONCALIZADAS Y SEGURIDAD DE ACCESO MEDIANTE LA APLICACIÓN DE ACLS"

TESIS DE GRADO

Previa a la obtención del título de:

INGENIERO EN ELECTRONICA Y TELECOMUNICACIONES

Presentado por

María Auxiliadora Desiderio Rodrigo
Pedro José Solís Sánchez

Guayaquil – Ecuador

2005

Agradecimiento

“Agradezco a todos los miembros de mi familia, por haberme apoyado en todo momento, por haber contado con cada uno de ellos en las etapas de mi carrera universitaria, gracias a todos.”

María Auxiliadora Desiderio Rodrigo

“Agradezco a mi padre celestial sobre todas las cosas, por brindarme su ayuda incondicional, por estar siempre conmigo y ser mi roca fuerte, agradezco a mi querida madre por brindarme toda su ayuda, y a pesar de estar lejos supo llenar el vacío de su ausencia, agradezco a mi familia toda por ser también el eje principal de este logro tan importante en mi vida, a mis amigos por sus sabios consejos y estar conmigo en las buenas y malas, a la Ingeniera Ivonne Martín por brindarnos su ayuda incondicional en el desarrollo de esta tesis y al Ingeniero Carlos Salazar por creer en mí”

Pedro José Solís Sánchez

Dedicatoria

“Dedico esta tesis, a mi Dios todopoderoso que siempre me guió y supo darme fuerzas cuando me faltaban, el estuvo conmigo desde el inicio de mi carrera y supo cuidarme siempre, y a mi amada madre que supo ayudarme y siempre oro por mí”

María Auxiliadora Desiderio Rodrigo

“Dedico esta tesis a Dios Todopoderoso, a mi querida madre la Señora Yolanda Sánchez, a mis amados hermanos Junior y Carolita, a mis abuelitos Oliva y Enrique, gracias por sus dulces desayunos en las madrugadas de estudio, a mi padre y a Mariuxi una gran amiga”

Pedro José Solís Sánchez

TRIBUNAL DE GRADUACION

Ing. Miguel Yapur Ahuad
Presidente

Ing. Rebeca Estrada Pico
Miembro Principal

Ing. Pedro Vargas
Miembro Principal

Ing. Ivonne Martín Moreno
Director

DECLARACION EXPRESA

“La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral”

María Auxiliadora Desiderio Rodrigo

Pedro José Solís Sánchez

Resumen

En esta tesis diseñamos una red local con 3 VLANS, las cuales se comunican entre ellas de manera troncalizada, para este propósito empleamos un router que permite la comunicación entre ellas. Sobre nuestro diseño implementamos los 4 principales protocolos de enrutamiento que existen en la actualidad que son: RIP V1, RIP V2, IGRP, y, EIGRP, siendo estos dos últimos protocolos propietarios de la marca CISCO.

Realizamos pruebas de conectividad entre los distintos dispositivos que conformaron nuestra red, aplicando cada uno de los protocolos de enrutamiento detallados en este resumen, escogimos el mejor en base a la escalabilidad y convergencia, sobre la configuración de los routers con el protocolo seleccionado se aplicaron ACLS a las interfases tanto físicas como virtuales de los routers, con lo cual comprobamos el correcto funcionamiento de las ACLS.

También se efectuaron pruebas de redundancia aplicando Etherchannel, tecnología propietaria de CISCO, se simularon caídas de enlace, verificando de esta manera la continuidad de la conectividad de nuestra red.

INDICE GENERAL

INDICE GENERAL

INDICES DE ABREVIATURAS

ACL Access Control List.

BID Bridge ID.

BPDU Bridge Protocol Data Unit.

CIDR Classless Inter-Domain Routing

CLI Configuration Line Interface.

CO Central Office.

CDP CISCO Discovery Protocol.

DHCP Dynamic Host Configuration Protocol.

DOT1Q InterVLAN protocol of CISCO.

DUAL Difuse Update Algoritm.

EIGRP Enhanced Interior Gateway Routing Protocol.

ID Identification.

IDF Intermediate Distribution Frame.

IEEE Institute of Engineer Electrics and Electronics..

IGP Interior Gateway Protocol.

IGRP Interior Gateway Routing protocol.

IOS Image Operative System.

IP Internet Protocol.

INDICES DE ABREVIATURAS

IPX Internetwork Exchange Packet.

ISL Inter-Switch Link**.**

ISP Internet Service Provider.

LAcP Link Aggregation Control Protocol.

LAN Local Area Network.

LLC Logical Link Control.

LSA Link State Advertisement.

MAC Medium Access Control.

MDF Main Distribution Frame.

NVRAM No Volatile RAM.

OSPF Short Path First.

PAcp Port Aggregation Control Protocol.

RAM Random Access Memory.

RIP V1 Routing Information Protocol.

RIP V2 Routing Information Protocol version 2.

RFC Request For Comments.

SNAP Subnet Access Protocol.

INDICES DE ABREVIATURAS

SPF Short Path First.

SPT Spanning-Tree Protocol.

STD Standar de Internet.

TFTP Trivial File Transfer Protocol.

VLAN Virtual Local Area Network.

VLSM Variable Length Subset Mask.

VTP VLAN Trunking Protocol.

WAN Wide Area Network.

INDICES DE FIGURAS

Pág.

Capítulo 1

Capítulo 2

INDICES DE FIGURAS

Capítulo 3

Capítulo 4

INDICES DE TABLAS

Pág.

INTRODUCCION

Una red de área local virtual (VLAN) es un segmento de red conmutado que está lógicamente segmentado por función, proyecto o aplicación sin importar la ubicación física de los usuarios, las VLANS tienen los mismos atributos que las LAN físicas , los puertos que pertenecen a la misma VLAN pueden recibir los paquetes unicast, multicast y broadcast, cada VLAN se considera un segmento lógico separado de la red , la tecnología VLAN brinda varias ventajas, entre ellas: el control del trafico de broadcast, y, mejorar la seguridad de la red, sin embargo, las VLAN tienen una limitación importante, éstas operan en Capa de enlace, lo que significa que los dispositivos en distintas VLAN no se pueden comunicar, si es que en la red no existe un router que permita el enrutamiento entre ellos.

Por otra parte, se debe anticipar y manejar el crecimiento físico de la red De forma eficiente. Es posible que esto implique la creación de otro nodo de comunicación, por ende la necesidad adicional tanto de espacio físico como equipos de red tal como: bastidores, paneles de conexión, switches, routers, entre otros. También se debe elegir esquemas de direccionamiento que permitan el crecimiento de la red.

La máscara de subred de longitud variable (VLSM) se utiliza para crear esquemas de direccionamiento eficientes y escalables.

Existen dos tipos de protocolos de enrutamiento interior: Protocolos de vector- distancia y de estado de enlace. Ambos tipos de protocolos de enrutamiento buscan rutas a través de sistemas autónomos, y, utilizan distintos métodos para realizar las mismas tareas. Los algoritmos de enrutamiento del estado de enlace, también conocidos como “algoritmos de primero la ruta libre más corta” (SPF), mantienen una compleja base de datos de información de topología, incluyendo una información completa sobre routers lejanos y su interconexión. Por otra parte, los algoritmos de vector-distancia proporcionan información no específica sobre redes distantes.

La redundancia en una red es fundamental, porque permite que las redes sean tolerantes a las fallas. Las topologías redundantes proporcionan protección a la falta de disponibilidad de la red, esto puede deberse a la falla de un enlace, puerto o dispositivo de red, pero la redundancia es susceptible a las tormentas de broadcast, transmisiones de múltiples tramas e inestabilidad de la base de datos de direcciones MAC (dirección de control de acceso al medio), para esto existe el protocolo Spanning-Tree que se usa en redes conmutadas para crear una topología lógica sin lazos a partir de una topología física con lazos.

El enlace troncal de VLAN al definirse varias VLAN, permite que estas sean transportadas por toda una gran red conmutada a través de un enlace troncal, común. El enlace troncal de VLAN se basa en estándares, siendo el protocolo de enlace troncal de la IEEE, el **802.1Q**, un estándar abierto, que se basa en etiquetar las tramas con un ID para saber a que VLAN pertenece, en cambio el enlace Inter-Switch (**ISL**) que es un protocolo de enlace troncal propietario de Cisco, se basa en el filtrado de tramas, gracias a unas tablas que manejan los switches.

Los objetivos de la tesis son:

1. Optimizar el direccionamiento de los dispositivos, permitiendo la escalabilidad de la red, evitando el desperdicio de direcciones lógicas (direcciones de capa de red).

2. Diseñar una red segura, restringiendo el acceso a información clasificada a miembros de la red no autorizados.

3. Optimizar la conectividad de los usuarios mediante el correcto protocolo de enrutamiento que cumpla con todos los requerimientos de la red.

4. Diseñar una red escalable y económica mediante la implementación de InterVLAN en la red, agrupando de esta manera a los miembros de la red por departamentos para que ellos compartan aplicaciones y recursos.

5. Aplicar un método seguro, y confiable de conectividad entre VLAN permitiendo la convergencia de la red ante cualquier cambio topológico.

Se van a realizar pruebas de:

- Conectividad con los siguientes protocolos de enrutamiento: RIPV1 (Protocolo de información de enrutamiento), IGRP (Protocolo de enrutamiento de gateway interior), RIPV2 (RIP versión 2) y EIGRP (IGRP avanzado) sobre la misma red de prueba.

- Aplicación de listas de acceso, para la seguridad de la información de la red.

- Convergencia sobre enlaces troncalizados

Todas las configuraciones, y comandos utilizados en esta tesis son de equipos **CISCO.**

CAPITULO 1

COMUNICACIÓN ENTRE LANS VIRTUALES.

En este capítulo trataremos el concepto de VLAN, como operan en la red, el beneficio de implementarlas y el tipo de VLAN que existen en la actualidad. También citaremos los comandos de configuración para un tipo en especial de VLAN: las VLAN estáticas, y mencionaremos el concepto, operación, y funcionamiento de las ACLS.

1.1 VLAN.

1.1.1 Concepto y Clasificación.

Una VLAN es una agrupación lógica de dispositivos de red que no se limita a un segmento de LAN físico, esto nos facilita la administración de los equipos que se pueden comunicar como si estuviesen en el mismo segmento, las VLAN segmentan de manera lógica las redes conmutadas dependiendo de las necesidades de la organización, sin importar la ubicación física de los usuarios ni de las conexiones físicas de la red, en otras palabras las VLAN ayudan a gestionar los dominios broadcast. En la figura 1.1 se muestra una red con dos VLANS y la comunicación entre ellas a través del router de manera troncalizada(véase Bibliografía 1).

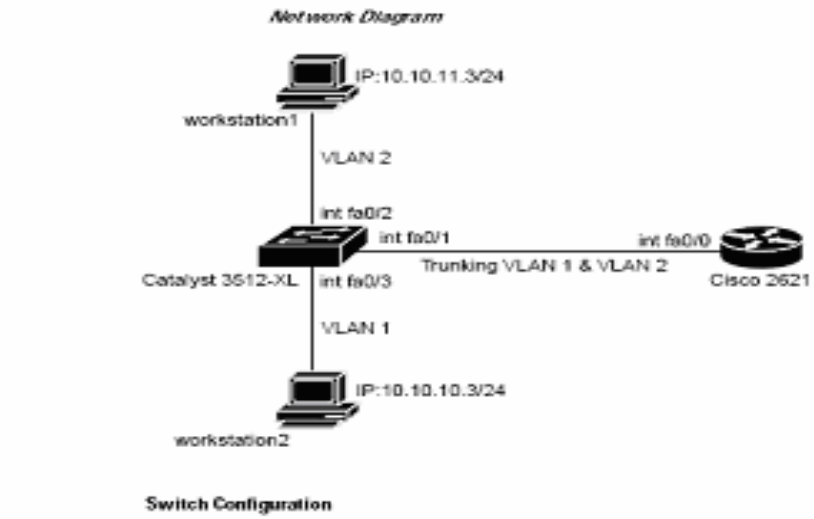

Figura 1.1 Estructura de una red local con 2 VLAN.

La configuración de las VLAN se logra mediante software. Por lo tanto, no se requiere que los equipos de la red se trasladen o se conecten físicamente en otro lugar, las VLAN segmentan de forma lógica la red en diferentes dominios de broadcast, de tal manera que los paquetes sólo conmutan entre los puertos que se asignan a la misma VLAN. Las VLAN se crean para brindar servicios de segmentación proporcionados tradicionalmente por routers ubicados en las configuraciones de la red local. 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 transmiten ningún tráfico entre VLAN, dado que esto viola la integridad del dominio de broadcast de las VLAN. El tráfico sólo debe enrutarse entre VLAN(véase Bibliografía 4).

Una VLAN es un dominio de broadcast que se crea en uno o más switches, dependiendo el número de puertos que necesitemos en cada VLAN. El enrutamiento permite que el router mande los paquetes a dominios de broadcast diferentes. El switch es el encargado de enviar tramas a las interfaces del router cuando se presentan ciertas circunstancias:

1 Si es una trama de broadcast.
2 Si está en la ruta a una de las direcciones MAC del router.

La implementación de VLAN en un switch hace que se produzcan ciertas acciones:

1 El switch mantiene una tabla de puenteo separada para cada VLAN.
2 Cuando se recibe la trama, el switch agrega la dirección origen a la tabla de puenteo si es desconocida en el momento.
3 Se verifica el destino para que se pueda tomar una decisión de envío.

Las VLAN estáticas, se configuran puerto por puerto, cada puerto está asociado a una VLAN, se llaman VLAN de asociación de puerto central y basadas en puerto. Cuando un dispositivo entra a la red, se debe asignar una dirección IP de la VLAN a la cual pertenece el puerto que se conecta, esta asignación puede ser de forma manual o dinámica.

En la asociación de VLAN de puerto central y basada en puerto, el puerto se asigna a una VLAN específica independiente del usuario. Al utilizar este método de asociación, todos los usuarios del mismo puerto deben estar en la misma VLAN. Un solo usuario, o varios usuarios pueden estar conectados a un puerto y no darse nunca cuenta de que existe una VLAN. Este método es fácil de manejar porque no se requieren tablas de búsqueda complejas para la segmentación de VLAN(véase Bibliografía 6).

Las VLAN de asociación dinámica son creadas mediante software de administración de red, en el caso de equipos CISCO tenemos: CiscoWorks 2000 o CiscoWorks for Switched Internetworks. Las VLAN dinámicas

permiten la asociación basada en la dirección MAC del dispositivo conectado al puerto del switch, los puertos pueden dinámicamente calcular su configuración de VLAN. Cuando un dispositivo entra a la red, el switch al que está conectado consulta una base de datos que contiene un mapeo de direcciones MAC a VLAN, que el administrador de red debe configurar previamente(véase Bibliografía 9).

Los usuarios conectados al mismo segmento compartido, comparten el ancho de banda de ese segmento. Por cada usuario adicional conectado al medio compartido implica que el ancho de banda se reduce. 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 manejar el switch. Todos los demás puertos en el switch pueden reasignarse a una distinta VLAN.

Los puentes filtran el tráfico que no necesita ir a los segmentos, salvo el segmento destino. Si una trama necesita atravesar un puente y la dirección MAC destino es conocida, el puente sólo envía la trama al puerto de puente correcto. Si la dirección MAC es desconocida, inunda la trama a todos los puertos en el dominio de broadcast, o la VLAN, salvo el puerto origen donde

se recibió la trama. Los switches se consideran como puentes multipuerto. Existen 3 asociaciones básicas de VLAN que se usan para determinar y controlar la manera de asignar un paquete(ver figura 1.2).

1 VLAN basadas en puerto.
2 VLAN basadas en direcciones MAC.
3 VLAN basadas en protocolo.

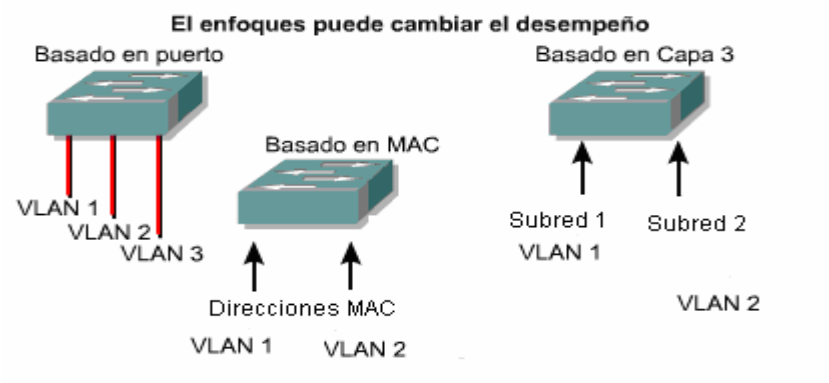

Figura 1.2 Tipos de asociaciones básicas de VLAN.

Alguna de las características de la membresía por puerto son: máxima seguridad entre las VLAN, los paquetes no se filtran a otros dominios y hay un control en toda la red, este método se aplica cuando tenemos servidores DHCP (protocolo de configuración dinámica de host), los cuales asignan dinámicamente las direcciones IP a los usuarios.

Dentro de la membresía por dirección MAC tenemos: flexibilidad, pero la administración, el diagnostico de fallas y la gestión son difíciles de manejar.

El sistema basado en capa de red ofrece: seguridad y gestión adicional, los routers controlan el acceso a las VLAN, ya no es común este sistema actualmente debido a la implementación de servidores DHCP en la red. La cantidad de VLAN en un switch varía según diversos factores:

1 Patrones de tráfico.
2 Tipos de aplicaciones.
3 Necesidades de administración de red.
4 Aspectos comunes del grupo.

El esquema de direccionamiento es otra consideración importante a la hora de definir la cantidad de VLAN en un switch, aunque es recomendable la correspondencia de uno a uno entre las VLAN y las subredes IP, se recomienda que las VLAN no se extiendan fuera del dominio de la capa de enlace del switch de distribución.

En un entorno conmutado, una estación de trabajo sólo recibe tráfico dirigido a ella. Como los switches filtran el tráfico de red, las estaciones de trabajo en un entorno conmutado envían y reciben datos con ancho de banda completo y dedicado. Al contrario de lo que ocurre con un sistema de hubs, en el que sólo una estación puede transmitir a la vez, una red conmutada permite varias transmisiones simultáneas en un dominio de broadcast. Este proceso no afecta directamente a las demás estaciones dentro o fuera de un dominio de broadcast. Cada VLAN debe tener una dirección única de subred asignada a ella.

Las VLAN pueden existir como redes de extremo a extremo, o pueden existir dentro de las fronteras geográficas, una red VLAN de extremo a extremo tiene varias características, entre ellas tenemos: la asociación a las VLAN para los miembros se basan en la función dentro de la organización mas no de su ubicación física, cada miembro debe de tener el mismo patrón de flujo de tráfico 80/20, cada VLAN tiene un conjunto común de requisitos de seguridad para todos los miembros, además se proporcionan puertos de switch para cada usuario en la capa de acceso. El etiquetado de tramas se utiliza para transportar información desde múltiples VLAN entre los switches de la capa de acceso y los switches de la capa de distribución, los servidores de grupos de trabajo operan de acuerdo con un modelo de cliente/servidor. Por este motivo, se asigna a los usuarios la misma VLAN que el servidor usa para maximizar el desempeño de la conmutación en la red y mantener el tráfico localizado, un router de capa núcleo se utiliza para el enrutamiento.

La red se diseña sobre la base de los patrones de flujo de tráfico, para que tengan el 80 por ciento del tráfico contenido en una VLAN, y el 20 por ciento restante atraviesa el router a los servidores de la empresa, y al Internet, es decir permite que los dispositivos se agrupen según el uso de recursos. Esto incluye parámetros como el uso de servidores, equipos de proyecto y departamentos. El objetivo de las VLAN de extremo a extremo es mantener el 80 por ciento del tráfico en la VLAN local. A medida que se desea

centralizar recursos, las VLAN de extremo a extremo se vuelven más difíciles de mantener.

El cambio en la asignación y uso de recursos requiere que se creen las VLAN en torno de límites geográficos en lugar de límites de aspectos comunes. En una estructura geográfica, es típico encontrar en uso la nueva norma 20/80. Esto significa que el 20 por ciento del tráfico permanece dentro de la VLAN local y 80 por ciento del tráfico de la red viaja fuera. Aunque esta topología significa que los servicios desde los recursos deben viajar a través de un dispositivo de capa de red, este diseño permite que la red aplique un método inteligente en el acceso a recursos.

1.1.2 Configuración de VLAN estáticas.

Las VLAN estáticas son puertos en un switch que se asignan manualmente a una VLAN. Esto se hace con una aplicación de administración de VLAN o configurarse directamente en el switch mediante la CLI (configuración mediante consola). Estos puertos mantienen su configuración de VLAN asignada hasta que se cambien manualmente. Este tipo de VLAN funciona bien en las redes, todos los movimientos son controlados y gestionados.

Algunas consideraciones en el momento de configuración de VLAN son:

1. La máxima cantidad de VLAN depende del modelo del switch.
2. La VLAN por defecto de fábrica es VLAN1, la cual no se puede borrar, la dirección IP del switch se encuentra en la VLAN1, protocolos como CDP (protocolo de descubrimiento de CISCO) y VTP (protocolo de enlace troncal de VLAN), que son propietario de CISCO, es decir que solo corren en equipos CISCO, son necesarios, el primero para descubrir nuevos hosts y el segundo administrar correctamente las VLAN, es necesario configurar una dirección IP en el switch para poder monitorearlo en la red(ver APENDICE A).

Los comandos que se utilizan para la creación de una VLAN de manera estática en el switch CISCO Catalyst 2950 son:

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

Switch(config)#interface fastethernet 0/Port number



Switch(config-if)#switchport  mode access
Switch(config-if)#switchport access vlan vlan_number
```

En la primera línea: del modo privilegiado se accede al modo de configuración de las VLAN, en la segunda línea: se crea una VLAN, donde tenemos "***vlan_number***" ponemos el número que debe ser de modo secuencial de creación, para llevar un orden, tomando en cuenta que Vlan 1,

que es la Vlan administrativa, ya está creada por defecto, y no se la debe tomar en cuenta de nuevo, o la programación, nos va a dar un error, en ***vlan-name*** ponemos el nombre de la vlan, para darle una referencia, ponemos un ejemplo. Puede ser: profesor, alumno, etc. Hay que recordar que a la vlan 1 no se le puede asignar ningún nombre, al automáticamente digitar enter y luego el comando "exit", estamos grabando esta configuración en la NVRAM del switch sin recurrir al típico comando en modo privilegiado "***copy running-config startup-config***", en la cuarta, quinta y sexta línea vamos a asociar un puerto del switch a la VLAN creada.

Una VLAN creada permanece sin usar hasta que se la asigna a puertos del switch, por defecto de fábrica todos los puertos del switch pertenecen a la VLAN1.

Por motivos de seguridad los valores de configuración del switch se pueden copiar en un servidor TFTP con el comando ***copy running-config tftp***. Para tener un respaldo de las configuraciones. También, se puede usar la función de captura de HyperTerminal junto con los comandos ***show running-config*** y ***show vlan*** para guardar los valores de configuración.

El comando ***show vlan*** nos permite ver todo el detalle de las VLAN hasta ese momento creadas, el comando ***show vlan brief*** nos brinda lo más

importante de esos detalles es decir, un resumen de las VLAN creadas hasta ese momento. En la figura 1.3 vemos la salida en un switch al comando ***show vlan brief***, podemos apreciar que los puertos 1, 2, y 4 pertenecen a VLAN 1, que los puertos 3, 5, 6, y 7 pertenecen a VLAN 2, y que los puertos 8, 9, 10, 11 y 12 pertenecen a VLAN 3, las VLAN 1002, 1003, 1 004 Y 1005 están presentes por defecto.

```
SydneySwitch#show vlan brief

VLAN Name                 Status    Ports
---- -------------------- --------- -------------------------------
1    default              active    Fa0/1, Fa0/2, Fa0/4
2    VLAN2                active    Fa0/3, Fa0/5, Fa0/6, Fa0/7
3    VLAN3                active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                    Fa0/12
1002 fddi-default         active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active
```

Figura 1.3 Salida brindada al comando show vlan brief.

El comando que se detalla debajo de este párrafo se utiliza para eliminar una VLAN de un switch, cuando se elimina una VLAN, todos los puertos asignados a esa VLAN quedan inactivos. Los puertos, sin embargo, quedan asociados a la VLAN eliminada hasta que se los asigna a una nueva VLAN.

```
Switch#vlan database
Switch(vlan)#no vlan vlan_number
```

1.2 Conectividad dentro de una VLAN.

1.2.1 Protocolos.

Los protocolos de conectividad dentro de una red permiten que se definan varias VLAN, el **802.1Q** es un mecanismo de etiquetado de VLAN de la IEEE, es de estándar abierto , esto significa que es implementado en varios equipos independientes de la marca, y consiste en que se agregan etiquetas especiales a las tramas para saber a que VLAN pertenecen. Este etiquetado permite que varias VLAN sean transportadas por toda una gran red conmutada a través de un enlace troncal, común, este método logra el envío de tramas a mayor velocidad y facilita la administración, 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, el etiquetado de trama funciona a nivel de capa de enlace y requiere pocos recursos de red o gastos administrativos. En la siguiente página se detalla cada campo del etiquetado con el 802.1Q en la tabla I, y en la figura 1.4 apreciamos toda la trama ethernet con la inserción del campo del protocolo 802.1Q(bloque de color morado), el cual es la agrupación de los 4 campos detallados en la tabla I(véase Bibliografía 10).

Campo IEEE 802.1q	Descripción
TPID	Son 16-bit y son el identificador del protocolo de etiquetado, el cual indica que sigue a continuación un etiquetado 802.1q.
Priority	Son 3-bit IEEE 802.1p y son de prioridad, el cual provee 8 niveles de prioridad.
CFI	Es el indicador del formato canónico, el cual indica si las direcciones MAC están en formato canónico (0), o formato no canónico (1).
VID	Son 12-bits y es indicador que permite 4096 valores únicos para las VLAN; Los números VLAN 0,1 y 4095 son reservados.

Tabla I Campos del etiquetado del protocolo 802.1Q

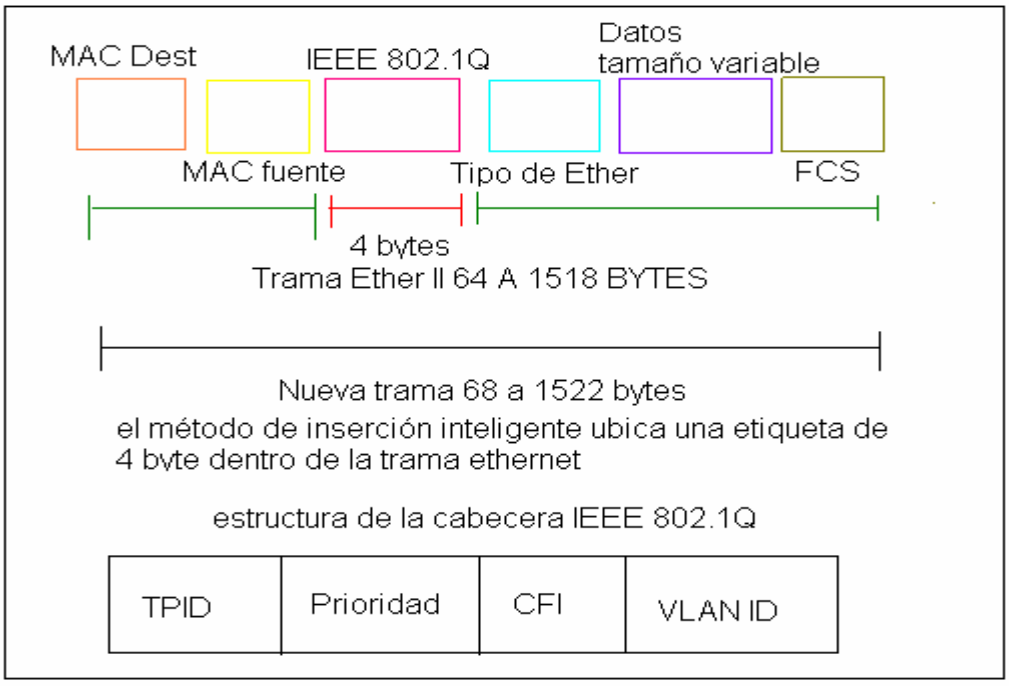

Figura 1.4 Estructura de la trama 802.1q

En cambio el enlace Inter-Switch (**ISL**) es un protocolo de enlace troncal propietario de Cisco, que mantiene información de las VLAN, a medida que el tráfico fluye entre switches y routers, este protocolo filtra las tramas, cada switch tiene una tabla de filtrado, el switch comparte la información de la tabla de direcciones, las entradas de la tabla se compara con las tramas, de acuerdo a eso el switch realiza la acción correspondiente, con **ISL**, la trama Ethernet se encapsula con un encabezado que contiene un identificador de VLAN. A medida que aumenta la cantidad de VLAN que viajan a través del enlace troncal, las decisiones de envío se tornan más lentas y más difíciles de administrar dado que las tablas de conmutación de mayor tamaño tardan más en procesarse(véase Bibliografía 17).

En la siguiente página indicamos todos los campos de la trama del protocolo ISL gracias a la Tabla II, y en la Figura 1.5 apreciamos toda la estructura de un paquete Ethernet con el campo del protocolo ISL.

Campos ISL	Descripción
DA	40-bit dirección destino, se establece en la dirección multicast: 0x01 00 c0 00 00.
Type	4-bit valor que indica el tipo de la trama fuente con los siguientes valores:
	0000 = Ethernet
	0001 = Token Ring
	0010 = FDDI
	0011 = ATM
User	4-bits, usualmente establecidos a cero, pero puede extender el significado del campo **Type**.
SA	48-bit la dirección MAC fuente.
LEN	16-bit de longitud del dato del usuario y encabezado ISL, excluyendo los campos: DA, T, U, SA, LEN, y CRC
SNAP	3-byte campo establecido a 0xAAAA03.
HSA	Mayor de 3 bytes, la identificación del fabricante, del campo SA ; debe contener el valor de: 0x00_00_0C.
VLAN ID	15-bit ID de la VLAN.
BPDU	1-bit establecidos para todos los BPDU encapsulados por ISL.
INDX	16-bit index indica el Puerto fuente del paquete.
RES	16-bit campo reservado se establece a cero para Ethernet..
Encapsulated	
Frame	Encapsulacion Ethernet, Token Ring, FDDI, o ATM frame, incluyendo su propio CRC, completamente sin cambios.
CRC	32-bit el valor CRC calculado en la trama entera encapsulada desde el campo DA hasta el campo encapsulated.

Tabla II Campos de la trama ISL

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

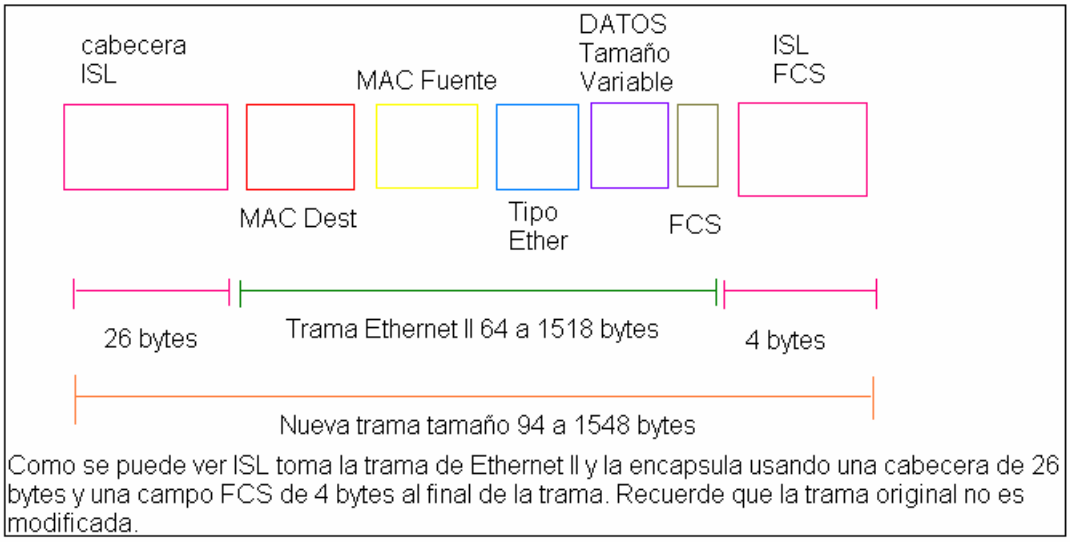

Figura 1.5 Estructura de la trama ISL

1.2.2 Solución a problemas de conectividad.

Los siguientes pasos explican como se aísla un problema en una red conmutada:

- Comience con una sola configuración en un switch y prosiga el proceso hacia afuera.
- Verifique el enlace de Capa 1(capa física del modelo OSI).
- Verifique el enlace de Capa 2(capa de enlace del modelo OSI).

Al efectuar el diagnóstico de posibles fallas, verifique si el problema se presenta varias veces en vez de una falla aislada. Algunos problemas repetitivos ocurren por un crecimiento de la demanda de servicios por parte de las estaciones de trabajo que exceden en aplicaciones.

Muchas LAN se enfrentan a patrones de tráfico de red impredecibles resultantes de la combinación de tráfico de intranet, el uso creciente de aplicaciones multicast, entre otras. La antigua norma de 80/20, que establecía que sólo el 20 por ciento del tráfico de la red pasaba por el backbone, es obsoleta (VLAN extremo a extremo). La exploración de Web interna ahora permite que los usuarios localicen y accedan a la información desde cualquier lugar en la intranet corporativa. Los patrones de tráfico están determinados por la ubicación de los servidores y no por las configuraciones del grupo de trabajo físico con el que se agrupan. Si una red presenta con frecuencia síntomas de cuello de botella, como desbordes excesivos, tramas descartadas y retransmisiones, es posible que haya demasiados puertos en un solo enlace troncal o demasiados requerimientos de recursos globales y

acceso a los servidores de intranet, otra razón es que este tráfico se ve obligado a atravesar el backbone.

Se produce una tormenta de broadcast cuando se recibe una gran cantidad de paquetes de broadcast en un puerto. Esto produce que la red se haga más lenta. El control de tormentas se configura para el switch como un todo, pero opera por puerto. El control de tormentas se encuentra inhabilitado por defecto de fábrica. La prevención de las tormentas de broadcast mediante el establecimiento de valores demasiado altos o bajos del umbral descarta el tráfico MAC excesivo de broadcast, multicast o unicast.

Los problemas de STP(spanning- tree protocol) incluyen tormentas de broadcast, lazos, y paquetes descartados(ver APENDICE A). Para realizar el diagnóstico de fallas de la operación de la conexión troncal entre el router y los switches, es necesario asegurarse de que la configuración de interfaz del router está completa y correcta. Verifique que no se haya configurado una dirección IP en la interfaz Ethernet. Las direcciones IP se configuran en cada subinterfaz de una conexión de VLAN. Verifique que la configuración de conectividad duplex en el router coincida con el puerto/interfaz correspondiente en el switch, en ambos tanto en el interfaz del router y en el interfaz del switch deben estar configurados para transmitir en modo full duplex y a la misma velocidad.

El comando ***show vlan*** muestra información de todas las VLAN en el router. El comando ***show vlan*** seguido por el número de VLAN muestra información específica de esa VLAN en el router.

Un problema que se presenta al tener dos o más switches conectados en cascada ocurre cuando los puertos que se a signan a una VLAN en un switch no están presentes en los otros switches , otro problema adicional que se presenta es cuando los switches tienen distintos protocolos de enlace interVLAN, la solución es manejar el mismo protocolo, un problema de conectividad se presenta cuando las VLAN no están activadas todas en cada switch, para este propósito son útiles los comandos ***show*** y ***debug.***

1.3 Enrutamiento InterVLAN.

1.3.1 Concepto y operación de un sistema Trunking.

El enlace troncal de VLAN permite que se definan varias VLAN, agregando etiquetas especiales a las tramas identificando a la VLAN a la cual pertenecen. Este etiquetado permite que varias VLAN sean transportadas a través de un enlace común(véase Bibliografía 29).

La configuración y el mantenimiento manual del protocolo de enlace troncal virtual (VTP) tiene sus ventajas como es: la automatización de varias de las tareas de configuración de la VLAN una vez que VTP se configura en la red(ver APENDICE A).

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. Cada switch utiliza un puerto por cada VLAN de modo que cada puerto transporta tráfico para cada una de ellas. Esta es una forma sencilla de implementar la comunicación entre las VLAN en diferentes switches, pero no funciona bien a mayor escala. Y si se añade más VLAN estaríamos ocupando un puerto en cada switch para esa VLAN adicional. En la figura 1.6 vemos como cada VLAN tiene su propio puerto en cada Switch para la comunicación InterVLAN.

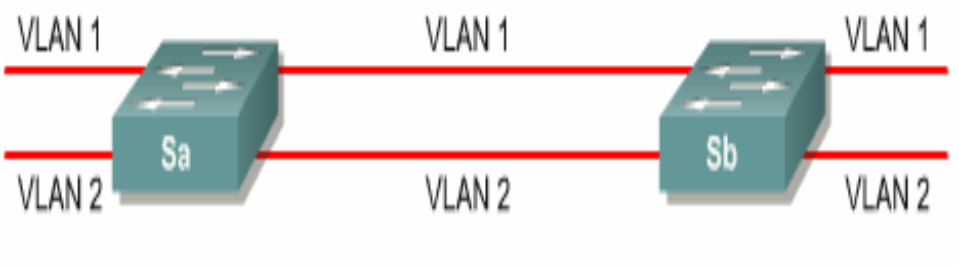

Figura 1.6 Enlace VLAN sin aplicar Trunking.

Las tablas de conmutación en ambos extremos del enlace troncal se pueden usar para tomar decisiones de envío basadas en las direcciones MAC destino de las tramas. A medida que aumenta la cantidad de VLAN que viajan a través del enlace troncal, las decisiones de envío se tornan más lentas y más difíciles de administrar. El proceso de decisión se torna más lento dado que las tablas de conmutación de mayor tamaño tardan más en

procesarse.

Dentro del modo de configuración global del switch ingresamos a configurar la VLAN administrativa con el siguiente comando:

Switchport trunk encapsulation mode, donde ***mode* e**s dot1q si queremos establecer el protocolo **802.1q**, o, **isl**, si queremos establecer el protocolo ISL de Cisco, pero, no todos los switches poseen la característica de tener los dos modos, depende del sistema operativo del switch, hay que destacar que tanto el switch como el router deben de manejar el mismo protocolo, en nuestras pruebas utilizamos el switch CISCO Catalyst 2950, el cual solo trabaja con el protocolo 802.1Q.

Cuando se conectan las VLAN entre sí, surgen algunos problemas técnicos. Dos de los problemas más comunes que pueden surgir en un entorno de Varias VLAN son los siguientes:

1. La necesidad de que los dispositivos de usuario final alcancen hosts no locales.
2. La necesidad de que los hosts en distintas VLAN se comuniquen entre sí.

Cuando un router necesita realizar una conexión a un host remoto, verifica su tabla de enrutamiento para determinar si existe alguna ruta conocida. Si el host remoto entra en una subred que sabe como llegar al destino, el sistema verifica si puede conectarse a través de esta interfaz. Si todas las rutas conocidas fallan, el sistema tiene una última opción, la ruta gateway y por lo

general es la única que está presente en el sistema. En un router, un asterisco (*) permite indicar que existe una ruta por defecto cuando utilizamos el comando ***show ip route***.

Las rutas por defecto se implementan usando el comando ***ip route***:

```
Router(Config)# ip route 0.0.0.0  0.0.0.0  172.16.2.1
```

En nuestra red, la IP privada 172.16.2.1 es el gateway. La conectividad entre VLAN se puede lograr a través de una conectividad lógica o física. Por cada VLAN se va a particionar lógicamente en subinterfases a la conexión física entre el router y el switch. La ventaja principal del uso del enlace troncal es una reducción en la cantidad de puertos de router y switch que se utiliza. Esto no sólo permite un ahorro de dinero sino también reduce la complejidad de la configuración.

Cada subinterfaz admite una VLAN y se le asigna una dirección IP. Para que varios dispositivos en una misma VLAN se puedan comunicar, las direcciones IP de todas las subinterfases deben encontrarse en la misma red o subred. En la figura 1.7 vemos que el router tiene 3 subinterfases para las VLAN que el conecta, y así permitir la comunicación troncalizada entre ellas.

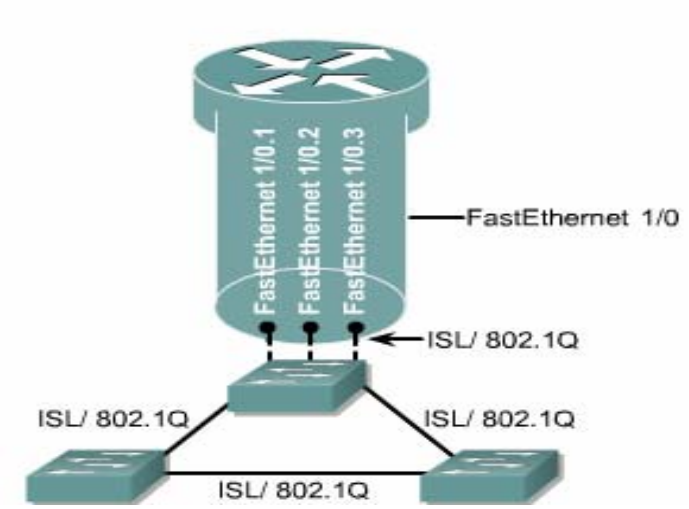

Figura 1.7 Subinterfases en el router.

Para identificar la interfaz utilice el comando ***interface*** en el modo de configuración global:

```
Router(config)#interface fastethernet port-number. subinterface-number
```

port-number identifica la interfaz física y ***subinterface-number*** identifica la interfaz virtual.

El router debe poder comunicarse con el switch utilizando un protocolo de enlace troncal estandarizado. Esto significa que ambos dispositivos conectados entre sí deben comprenderse, esto se logra con el siguiente comando:

```
Router(config-if)#encapsulation dot1q vlan-number
```

vlan-number identifica la VLAN para la cual la subinterfaz transportará el tráfico. Se agrega un ID de VLAN a la trama sólo cuando la trama está destinada a una red no local.

Cada paquete de VLAN transporta el ID de VLAN dentro del encabezado del paquete. Para asignar una dirección IP a la interfaz, introduzca el siguiente comando en el modo de configuración de interfaz:

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

ip-address y ***subnet-mask*** son la dirección y la máscara de red de 32 bits de la interfaz específica, respectivamente.

1.3.2 Posibles fallas en enrutamiento Trunking.

Cuando existan dificultades con una conexión de enlace troncal entre un Switch y un router, tenga en cuenta las siguientes causas posibles:

- Hay que asegurarse de que el puerto esté conectado y no reciba ningún error de capa física. Esto puede hacerse con el comando ***show interface*** en el switch.
- Debe Verificarse de que el duplex y la velocidad se encuentren correctamente configurados entre el switch y el router. Esto puede hacerse con el comando ***show interface status*** en el switch o el comando ***show interfaces*** en el router.

- Configure la interfaz física del router con una subinterfaz por cada VLAN que enrute el tráfico. Verifique esto introduciendo el comando IOS ***show interfaces***. Asegúrese también de que cada subinterfaz en el router tenga el tipo de encapsulamiento, número de VLAN, dirección IP y máscara de subred correctos configurado. Esto puede hacerse con los comandos IOS ***show interfaces*** *o* ***show running-config***.
- Confirme que el router esté ejecutando una versión del IOS que admita enlaces troncales. Esto se puede realizar con el comando ***show version***.

1.4 Seguridad de Acceso en la red.

1.4.1 Concepto y Configuración de ACLS.

Los routers ofrecen funciones del filtrado básico de tráfico, como el bloqueo del tráfico de Internet, mediante el uso de las listas de control de acceso (ACLs). Una ACL es una lista secuencial de sentencias de permiso o rechazo que se aplican a direcciones o protocolos de capa superior a la capa de red.

Las ACLs son listas de condiciones que se aplican al tráfico que viaja a través de la interfaz del router, estas le informan al router el tipo de de paquetes que debe aceptar o denegar. La aceptación y rechazo se pueden basar en ciertas condiciones específicas. Las ACLs permiten la administración del tráfico y aseguran el acceso exterior o interior a una red. Podemos aplicar ACLs en un interfaz lógico o físico, el bloqueo del tráfico puede ser de entrada o salida de la interfase.

La figura 1.8 nos muestra la ubicación que llevan las ACLS en una red (por lo general van en las interfases de los routers principales de la red).

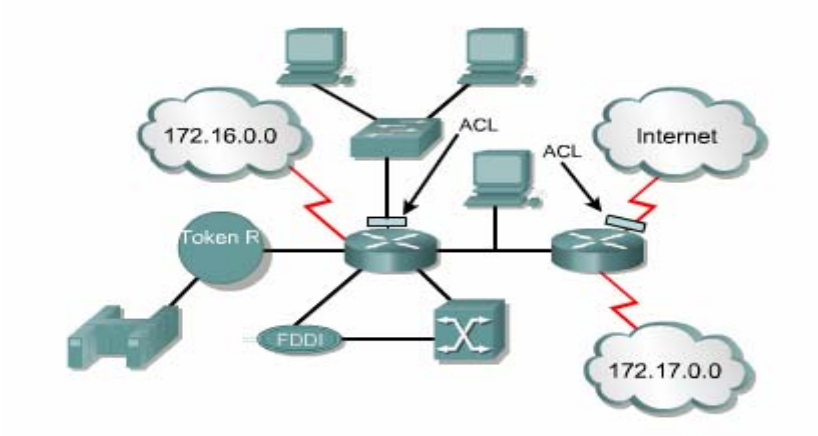

Figura 1.8 Una red con ACLs.

Las ACLs filtran el tráfico de red, controlando si los paquetes enrutados se envían o se bloquean en las interfaces del router. El router examina cada paquete y lo enviará o lo descartará, según las condiciones especificadas en la ACL. Algunos de los puntos de decisión de ACL son direcciones origen y destino, protocolos y números de puerto de capa superior. Si las ACLs no están configuradas en el router, todos los paquetes que pasen a través del router tendrán acceso a todas las partes de la red.

Las ACLs se definen según el protocolo, la dirección o el puerto. Para controlar el flujo de tráfico en una interfaz, se debe definir una ACL para cada protocolo habilitado en la interfaz. Las ACLs controlan el tráfico en una dirección por vez, en una interfaz. Se necesita crear una ACL por separado para cada dirección, una para el tráfico entrante y otra para el saliente.

Las razones principales de la aplicación de ACLs es debido a:

1. Sirven para limitar el tráfico en la red y mejorar el rendimiento de la misma.
2. Las ACL pueden restringir el envío de las actualizaciones de enrutamiento. Si no se necesitan actualizaciones, se preserva el ancho de banda.
3. Proporcionan un nivel básico de seguridad para el acceso a la red. Por ejemplo, las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro acceda a la misma área.
4. Restringir la capacidad de hacer TELNET al acceder a un router.
5. Cambiar distancias administrativas de los routers.

Clasificación.

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

Las **ACL extendidas** se utilizan con más frecuencia que las ACL estándar porque ofrecen un mayor control. Las ACL extendidas verifican las direcciones de paquetes de origen y destino, y también los protocolos y números de puerto. Esto ofrece mayor flexibilidad para permitir o rechazar el acceso de los paquetes según el lugar donde se originó el paquete y su destino así como el tipo de protocolo y direcciones de puerto. Algunos protocolos devuelven un paquete al emisor, indicando que el destino era

inalcanzable. Es posible configurar múltiples sentencias en una sola ACL. Cada una de estas sentencias debe tener el mismo número de lista de acceso, para poder relacionar las sentencias con la misma ACL. Puede haber tanta cantidad de sentencias de condición como sean necesarias, siendo la única limitación la memoria disponible en el router. Por cierto, cuantas más sentencias se establezcan, mayor será la dificultad para comprender y administrar la ACL. Las extendidas filtran según la IP de origen y/o destino, según el puerto usado y según el protocolo usado, sea TCP, IP, UDP, ICMP o varios de ellos al mismo tiempo. Es importante poner la instrucción más restrictiva en primero orden y la menos restrictiva en último orden. No se puede modificar una instrucción de una ACL existente.

Las **ACL nombradas IP** se introdujeron en el software Cisco IOS Versión 11.2, permitiendo que las ACL extendidas y estándar tuvieran nombres en lugar de números. Las ventajas que ofrece una lista de acceso nombrada son las siguientes:

1. Identifica intuitivamente las ACLs usando un nombre alfanumérico.
2. El IOS no limita el número de las ACLs nombradas que se pueden configurar.
3. Las ACL nombradas tienen la capacidad de modificar las ACL sin tener que eliminarlas y luego reconfigurarlas. Cabe notar que las listas de acceso nombradas permiten eliminar sentencias pero sólo permiten que las sentencias se agreguen al final de la lista. Aún con las ACL nombradas, se recomienda utilizar un editor de textos para crearlas.

Restricción de acceso al Terminal virtual.

Las listas de acceso extendidas y estándar se aplican a paquetes que viajan a través de un router. No están diseñadas para bloquear paquetes que se originan dentro del router.

Del mismo modo que hay puertos físicos o interfaces, como Fa0/0 y S0/0 en el router, también hay puertos virtuales. Estos puertos virtuales se denominan líneas VTY. Existen cinco líneas vty, numeradas del 0 al 4, Por razones de seguridad, es posible negar o permitir, a los usuarios, el acceso a la Terminal virtual del router.

El objetivo de restringir el acceso vty es aumentar la seguridad de la red. También se logra el acceso a vty utilizando el protocolo Telnet para realizar una conexión no física con el router. Como resultado, hay solo un tipo de lista de acceso vty. Es necesario imponer idénticas restricciones a todas las líneas vty, ya que no es posible controlar a qué línea se conectará el usuario.

El proceso de creación de una lista de acceso vty es igual al descrito para una interfaz. Sin embargo, para aplicar la ACL a una línea Terminal se necesita el comando ***access-class*** en vez del ***access-group***. Cuando configure las listas de acceso en las líneas VTY tenga en consideración lo siguiente:

1. Cuando controle el acceso a una interfaz, es posible utilizar un número o un nombre.
2. Sólo se pueden aplicar listas de acceso numeradas a las líneas virtuales.
3. Imponga restricciones idénticas a todas las líneas de Terminal virtual, porque el usuario puede querer conectarse a cualquiera de ellas.

Configuración de ACLS.

Debemos de definir la ACL con el siguiente comando:

```
(config)#access-list access-list-number [permit / deny]  (test-conditons)
```

Sentencia global que identifica la ACL, específicamente se reserva para IP estándar el intervalo del 1 al 99, ***permit*** o ***deny*** indican que se hace con los paquetes de esa interfase.

Es necesario aplicar las ACLs en un interfaz mediante el comando ***access-group***:

```
Router(config-if)#{protocol} access-group access-list-number
```

Todas las sentencias ACLs identificadas con ***access-list-number*** están relacionadas con una o más interfaces. Cualquier paquete que pase las condiciones de prueba de la ACL tiene permiso de usar cualquier interfaz en el grupo de acceso de las interfases.

```
Para borrar una ACL: no access-list   list-number
```

Hay dos palabras clave especiales que se utilizan en las ACL, las opciones ***any*** y ***host***. Para explicarlo de forma sencilla, la opción ***any*** reemplaza la dirección IP con 0.0.0.0 y la máscara wildcard por 255.255.255.255. Esta

opción concuerda con cualquier dirección con la que se la compare. La máscara 0.0.0.0 reemplaza la opción ***host***.

Con los comandos ***show ip interface*** o ***show running config*** se puede verificar si alguna ACL se ha aplicado a alguna interface. Con ***show access-lists*** vemos en detalle todas las ACLs creadas en el router.

1.4.2 Modo de operación de ACLS.

Una lista ACL es un grupo de sentencias que definen si se aceptan o rechazan los paquetes en interfaces entrantes o salientes. Estas decisiones se toman haciendo coincidir una sentencia de condición en una lista de acceso y luego realizando la acción de aceptación o rechazo definida en la sentencia.

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

El principio del proceso de comunicaciones es el mismo, ya sea que las ACL se usen o no. A medida que una trama ingresa a una interfaz, el router verifica si la dirección de capa de red concuerda o si es una trama de broadcast.

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

CAPITULO 2

PROTOCOLOS DE ENRUTAMIENTO A IMPLEMENTAR EN LA RED.

En este capítulo, trataremos el concepto de enrutamiento, explicaremos el significado de una ruta estática y los comandos para crearla en el router CISCO 2600, también revisaremos el concepto de rutas dinámicas y la manera que los routers las manejan.

Nos enfocaremos en explicar detalladamente el concepto y funcionamiento de los protocolos de enrutamiento tanto los de estado de enlace como los protocolos vector distancia, luego entraremos a un profundo estudio de los protocolos que se implementaron en la red de prueba: **RIP V1**, **IGRP**, **RIP V2**, y **EIGRP**, se revisarán los comandos para configurarlos en las interfases del router y para verificar el correcto funcionamiento de los mismos.

Introducción.

El enrutamiento no es más que ordenes para la comunicación entre redes. Esto se logra gracias a rutas, que pueden ser dinámicas o estáticas. Se debe de tomar en cuenta varios aspectos al seleccionar un protocolo de enrutamiento dinámico: El tamaño de la red, el ancho de banda de los enlaces presentes, la robustez de los routers, entre otros.

El enrutamiento es el procedimiento utilizado por el router, dispositivo de capa de red, para enviar paquetes a una red destino. Un router efectúa el enrutamiento en base de la dirección IP destino de los paquetes. Todos los dispositivos intermedios usan la dirección de IP de destino para guiar el paquete hacia la dirección correcta. A fin de tomar las decisiones acertadas, los routers deben aprender la ruta hacia redes remotas. Cuando los routers utilizan enrutamiento dinámico, esta información se obtiene de otros routers. En cambio si utilizamos el enrutamiento estático, las rutas hacia una red remota se configuran de manera manual, el router las instala en la tabla de enrutamiento, y ante un cambio topológico, se debe actualizar de manera manual, en una red grande esto se puede tornar tedioso, en cambio en redes pequeñas las redes estáticas requieren poco mantenimiento, por esto el enrutamiento estático no es escalable, ni capaz de adaptarse a un crecimiento dinámico(véase Bibliografía 11).

El comando**: *ip route red destino máscara de subred interfaz local / próximo salto***, en el modo privilegiado es el que nos permite ingresar una ruta estática. La distancia administrativa es un parámetro que nos brinda una medida del nivel de confiabilidad de una ruta. Un valor menor de la distancia administrativa indica una ruta más confiable. Por lo tanto, es preferible instalar rutas de distancia administrativa menor antes que una ruta idéntica de distancia administrativa mayor. En una ruta estática la distancia administrativa es de valor 1. En la tabla de enrutamiento se observará la ruta estática indicando la interfaz de salida, como si hubiera conexión directa. Esto a veces confunde, ya que las redes directamente conectadas tienen distancia 0. La distancia administrativa de una ruta en particular se puede ver, usando el comando ***show ip route address***, la dirección ip de dicha ruta se inserta en la opción ***address***.

Si se desea una distancia administrativa diferente a la distancia por defecto, se introduce un valor entre 0 y 255 después de la interfaz de salida o el siguiente salto, como se muestra a continuación, el valor de **80** se introduce como distancia:

```
routerA(config)#ip route 172.16.4.0 255.255.255.0 172.16.4.2  80
```

Si el router no puede llegar a la interfaz de salida que se indica en la ruta, éste no instalará la ruta estática en la tabla de enrutamiento. Por lo general, las rutas estáticas se utilizan como rutas de respaldo, la cual sólo se usará en caso de fallas en la ruta dinámicamente conocida. Para utilizar una ruta estática de esta forma, simplemente fije la distancia administrativa en un valor superior a la proporcionada por el protocolo de enrutamiento dinámico en uso. Se debe guardar la configuración activa en la NVRAM mediante el comando ***copy running-config startup-config***. Las rutas por defecto sirven para enviar paquetes a destinos que no coinciden con ninguno de las otras rutas en la tabla de enrutamiento. Generalmente, los routers están configurados con una ruta por defecto para el tráfico que se dirige a la Internet. En realidad, una ruta por defecto es una ruta estática especial que utiliza este formato:

```
ip route 0.0.0.0  0.0.0.0  [dirección-del-siguiente-salto | interfaz de salida]
```

La máscara 0.0.0.0, cuando se ejecuta el AND lógico hacia la dirección de IP de destino del paquete, siempre obtiene la red 0.0.0.0. Si el paquete no coincide con una ruta más específica en la tabla de enrutamiento, será enviado hacia la red 0.0.0.0, es preferible especificar la dirección IP del router del siguiente salto, y se debe de guardar la configuración en la NVRAM.

Para verificar si las rutas fueron ingresadas correctamente se utilizan los comandos: ***show running-config*** y ***show ip route*** Para corregir alguna falla en la conectividad se utilizan los comandos ping y traceroute, ejecutados desde el modo privilegiado(véase Bibliografía 12).

Existen dos tipos de protocolos dinámicos: Protocolos de enrutamiento interiores y exteriores, dentro de los protocolos de enrutamiento Interiores tenemos: protocolos de estado de enlace y vector distancia. 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**).

En cambio 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 internetwork (IPX).

Los protocolos de enrutamiento por vector-distancia envían copias periódicas de las tablas de enrutamiento de un router a otro (solo entre routers vecinos).

Estas actualizaciones periódicas entre routers informan de los cambios de topología. Finalmente acumulan información acerca de las distancias de la red, esto le permite mantener una base de datos de la topología de la misma. Sin embargo, los routers sólo conocen la información del router vecino. Cada router que aplica el enrutamiento por vector-distancia empieza por identificar sus propios vecinos. La interfaz que conduce a las redes conectadas directamente tiene una distancia de 0. A medida que el proceso de descubrimiento de la red continua, los routers descubren la mejor ruta hacia las redes de destino, de acuerdo a la información de vector-distancia que reciben de cada vecino. Cada una de las redes de destino en la tabla de enrutamiento tiene una cantidad total de vector-distancia, la cual indica la distancia a la que se encuentra dicha red por una ruta determinada. Las actualizaciones de las tablas de enrutamiento se producen al haber cambios en la topología. Las actualizaciones de cambios de topología avanzan paso a paso, de un router a otro. Los algoritmos de vector-distancia hacen que cada router envíe su tabla de enrutamiento completa a cada uno de sus vecinos adyacentes, en otras palabras es lenta la convergencia.

En la figura 2.1 vemos el modo de propagación de la información de enrutamiento entre los routers manejando los dos tipos de protocolos: vector distancia y estado de enlace(véase Bibliografía 13).

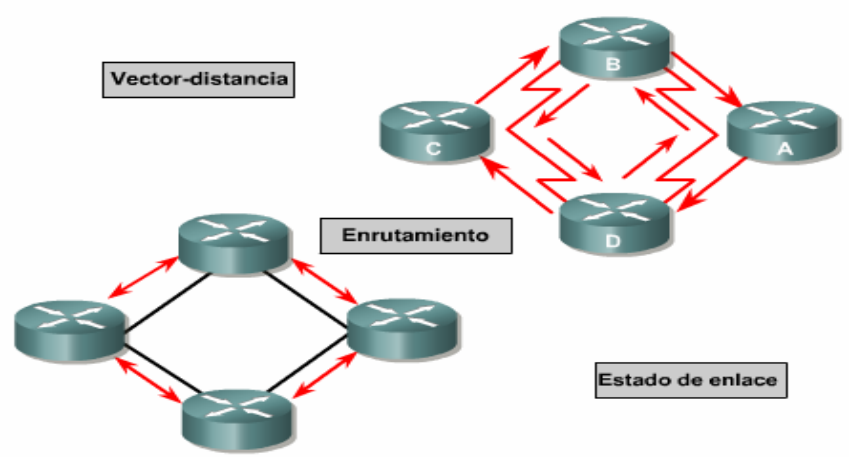

Figura 2.1 Esquema de los protocolos de enrutamiento.

Los algoritmos de estado del enlace también conocidos como algoritmos Dijkstras o SPF, mantienen una base de datos compleja, con la información de la topología de la red. Este algoritmo mantiene información completa sobre routers lejanos y su interconexión.

El enrutamiento de estado del enlace emplea:

1. **Publicaciones de estado del enlace (LSA):** paquete pequeño de información sobre el enrutamiento, el cual es enviado de router a router.
2. **Base de datos topológica:** información que se ha reunido mediante las LSA.
3. **Algoritmo SPF:** realiza cálculos en la base de datos, y el resultado es el árbol SPF.
4. **Tablas de enrutamiento:** una lista de las rutas e interfases conocidas.

El intercambio de LSAS empieza en las redes que se encuentran directamente conectadas al router, de las cuales se tiene información directa. Cada router, en paralelo con los demás, genera una base de datos

topológica que contiene toda la información recibida por intercambio de LSAS(véase Bibliografía 14)

El algoritmo SPF determina la conectividad de la red. El router fabrica la topología lógica en forma de árbol, con él mismo como raíz, y cuyas ramas son todas las rutas posibles hacia cada subred de la red. Luego ordena dichas rutas, y coloca las ruta más cortas primero . El router elabora una lista de las mejores rutas a las redes de destino, y de las interfases que permiten llegar a ellas. Esta información se incluye en la tabla de enrutamiento.

Los routers que utilizan protocolos de estado de enlace requieren de más memoria y exigen más esfuerzo al procesador, que los que usan protocolos de enrutamiento por vector-distancia. Los routers deben tener la memoria suficiente para almacenar toda la información de las diversas bases de datos, el árbol de topología y la tabla de enrutamiento. La cantidad de LSAS que ocurre al encender un router consume una porción del ancho de banda, ya que envían LSAS a todos los demás routers. Esta acción genera un gran volumen de tráfico y reduce temporalmente el ancho de banda disponible para el tráfico enrutado de los usuarios. Después de esta disminución inicial de la eficiencia de la red, los protocolos de enrutamiento del estado del enlace generalmente consumen un ancho de banda mínimo, sólo para enviar

las ocasionales LSAS que informan de algún cambio en la topología.

2.1 RIP V1

2.1.1Concepto y funcionamiento.

El Protocolo de información de enrutamiento (RIP) es un protocolo de enrutamiento por vector-distancia, y está en uso en miles de redes alrededor del mundo, la versión moderna del protocolo de estándar abierto RIP, a menudo denominado RIP IP, se describe formalmente en dos documentos distintos. El primero es el la Solicitud de comentarios 1058 (RFC 1058) y el segundo el Estándar de Internet 56 (STD 56). El hecho de que RIP se base en estándares abiertos y que sea de fácil implementación hace que resulte atractivo, aunque RIP carece de la capacidad y de las características de los protocolos de enrutamiento más avanzados. Por su simplicidad, RIP es un buen protocolo para redes pequeñas. Su distancia administrativa es de 120. Es uno de los IGP (Interior Gateway Protocol) más ampliamente utilizados.

Sus características principales son las siguientes:

1. Por defecto, las actualizaciones de enrutamiento son enviadas cada 30 segundos.
2. Utiliza el número de saltos como métrica para la selección de rutas, no puede ser mayor a 15 caso contrario el paquete es descartado.
3. Es un protocolo de enrutamiento por vector-distancia.

RIP evita que los bucles de enrutamiento se prolonguen en forma indefinida, mediante la fijación de un límite en el número de saltos permitido en una ruta, desde su origen hasta su destino. El número máximo de saltos permitido en una ruta es de 15. Cuando un router recibe una actualización de enrutamiento que contiene una entrada nueva o cambiada, el valor de la métrica aumenta en 1, para incluir el salto correspondiente a sí mismo. Si este aumento hace que la métrica supere la cifra de 15, se considera que es infinita y la red de destino se considera fuera de alcance. RIP incluye diversas características las cuales están presentes en otros protocolos de enrutamiento. Por ejemplo, RIP implementa los mecanismos de espera y horizonte dividido para prevenir la propagación de información de enrutamiento errónea, Cuando se utilizan horizontes divididos, un router registra la interfaz por la que ha recibido una ruta particular y no difunde la información acerca de la ruta de regreso sobre la misma interfaz. Con esto evitamos que la información "negativa" no sea difundida con rapidez.

Una de las técnicas finales para resolver el problema de la convergencia lenta se conoce como Poison Reverse. Una vez que una conexión desaparece, el router anuncia la conexión conservando la entrada de información por varios periodos de actualización e incluye un costo infinito en la difusión. Para hacer el Poison Reverse más efectivo, se debe combinar con las Triggered Updates (actualizaciones activadas) que obligan al router

a que envíe una difusión inmediatamente al recibir "malas noticias", en lugar de esperar el próximo periodo de difusión. Al enviar una actualización inmediatamente, un router minimiza el tiempo en que es vulnerable por recibir "buenas noticias"(véase Bibliografía 12).

La mayoría de los protocolos de enrutamiento usan una combinación de actualizaciones causadas por eventos (event-driven) o por tiempo (time-driven). RIP es time-driven, pero la implementación en la marca CISCO de RIP envía actualizaciones tan pronto se detectan cambios. Una vez que se haya actualizado la tabla de enrutamiento por cambios en la configuración, el router comienza inmediatamente a transmitir las actualizaciones de enrutamiento, a fin de informar de estos cambios a los routers vecinos. Estas actualizaciones, denominadas actualizaciones generadas por eventos, se envían independientemente de las actualizaciones periódicas que envían los routers RIP a intervalos regulares.

2.1.2 Comandos más importantes.

El comando ***router rip*** habilita el protocolo de enrutamiento RIP. Luego se ejecuta el comando ***network*** para informar al router acerca de las interfases donde RIP estará activo. A continuación, el proceso de enrutamiento asocia las interfases específicas con las direcciones de red y comienza a enviar y a recibir actualizaciones RIP en estas interfases. La configuración se realiza en

el modo global del router. Los routers RIP conservan sólo la mejor ruta hacia un destino pero pueden conservar más de una ruta al mismo destino si el costo de todas es igual.

Para habilitar RIP, ejecute los siguientes comandos desde el modo de configuración global:

- ***Router(config)#router rip***: habilita el proceso de enrutamiento RIP.
- ***Router(config-router)#network*** *número-de-la-red* : asocia una red al proceso de enrutamiento RIP.

El siguiente comando se utiliza para inhabilitar el horizonte dividido:

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

El temporizador de espera es otro de los mecanismos que se puede efectuar algún cambio. Los temporizadores de espera ayudan a prevenir la cuenta al infinito, pero también aumentan el tiempo de convergencia. La espera por defecto en el protocolo RIP es de 180 segundos. Esto evita que una ruta menos conveniente ingrese en la tabla de enrutamiento pero también puede evitar que se instale una ruta alternativa válida. Es posible reducir el lapso del temporizador de espera, para hacer la convergencia más ágil pero esto se debe hacer con cautela. El ajuste ideal es que se fije el temporizador con una duración apenas mayor al lapso máximo de actualización posible de la red. Por ejemplo, si el bucle consta de tres routers. Si cada router tiene un lapso de actualización de 30 segundos, el bucle más largo posible es de 90

segundos. Por lo tanto, el temporizador de espera debe ser apenas mayor a 90 segundos. En la Figura 2.2 se muestra un ejemplo.

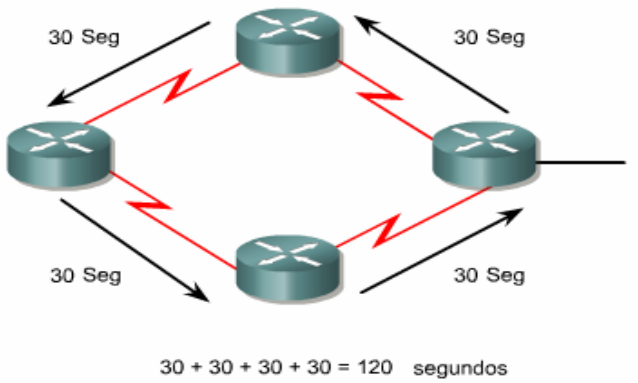

Figura 2.2 Ejemplo del temporizador de espera.

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

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

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

La publicación indeseada de actualizaciones de enrutamiento desde una

interfaz en particular, otro detalle que se puede manejar, para este efecto se puede inhabilitar el envío de actualizaciones desde la o las interfases que escoja. Para ello se usa el comando ***passive-interface.***

En algunos routers se puede configurar que se envíe con una versión de RIP y que se reciba con otra versión RIP, o la misma, esto se logra con el comando ***versión 1| 2*** dentro del modo RIP se configura al software para recibir o enviar paquetes RIP versión 1 o versión 2, si queremos que un interfaz en especifico envíe paquetes RIP en alguna versión se debe entrar a esa interfaz y utilizar el comando: ***ip rip send version {1|2},*** y si queremos que reciba se utiliza el comando: ***ip rip receive version {1|2}.***

El comando ***show ip protocols*** muestra cuáles son los protocolos que Transportan tráfico IP en el router. Este resultado puede utilizarse para Verificar la configuración del protocolo RIP. Algunos de los aspectos de la configuración más comunes que deben ser verificados son: si el router publica las redes completas, si en las interfases configuradas se están recibiendo las actualizaciones RIP.

El comando ***show ip route*** se utiliza para verificar que rutas se han aprendido por RIP(estas son marcadas con una “R”).

Otros comandos para verificar la configuración del protocolo RIP son los

siguientes:

```
show interface interface
show ip interface interface
show running-config
```

La mayoría de las fallas a la hora de manejar RIP son: comandos de red incorrectos, subredes discontinuas u horizontes divididos, y redes duplicadas. Para este efecto es muy útil el comando: ***debug ip rip***.

El comando ***debug ip rip*** muestra las actualizaciones de enrutamiento RIP a medida que se las envía y recibe. Después de recibir y procesar la actualización, el router envía la información recientemente actualizada hacia sus interfases RIP.

Otros comandos adicionales para diagnosticar fallas son:

```
show ip rip database
show ip protocols {sumario}
show ip route
debug ip rip {eventos}
show ip interface brief
```

Resumen de RIP V1

- Las actualizaciones, se envían por medio de Broadcast.
- Se esperan actualizaciones de los routers directamente conectados, si no se reciben de forma oportuna se eliminaran la ruta aprendidas.
- El número de saltos máximos son de 15.
- Una ruta que falle se publica por un tiempo, con una métrica infinita (16).
- Los routers envían a los routers vecinos su tabla de enrutamiento.
- No soporta VLSM, ni CIDR.
- Maneja horizonte divido, rutas envenenadas, cuenta al infinito para el control de bucles.
- Su distancia administrativa es 120.
- Envía actualizaciones cada 30 segundos.
- La única métrica es el número de salto.

2.2 IGRP.

2.2.1 Concepto y funcionamiento.

IGRP es un protocolo de enrutamiento de gateway interior (IGP) por vector-distancia, propietario de CISCO. Su distancia administrativa es de 100.

IGRP envía actualizaciones de enrutamiento a intervalos de 90 segundos, las cuales publican las redes de un sistema autónomo en particular. Las características más importantes de IGRP son:

1. La versatilidad al manejar automáticamente topologías indefinidas y complejas.
2. La flexibilidad necesaria para segmentarse con distintas características de ancho de banda y de retardo.
3. La escalabilidad para operar en redes de gran tamaño y complejas.

El algoritmo utilizado para calcular la métrica de enrutamiento para IGRP se define con el valor de las métricas K1 a K5 donde k1=k3=1 el resto son cero, y el máximo número de saltos es de 255. La métrica K1 representa el ancho de banda y la métrica K3 representa el retardo. Esta métrica compuesta es más precisa que la métrica del número de saltos que usa RIP para elegir una ruta hacia un destino. La ruta de menor valor métrico es la mejor.

tanto IGRP como EIGRP utilizan el siguiente calculo de metrica:
* metrica = [K1 * ancho de banda + (K2 * ancho de banda) / (256 - carga) + (K3 * retardo)] * [K5 / (confiabilidad + k4)]
los siguientes son los valores por defecto de las constantes:
* K1 = 1 , K2 = 0 , K3 = 1 , K4 = 0 , K5 = 0
* metrica = ancho de banda + retardo
cuando K4 y K5 son 0, la porcion [K5 / (confiabilidad + K4)] de la ecuacion no forman parte del calculo de la metrica. Por tanto, utilizando los valores por defecto de las constantes, la ecuacion de la metrica es:
Ancho de banda + retardo
IGRP y EIGRP utilizan las siguientes ecuaciones para determinar los valores usados en el calculo de la metrica (observe que EIGRP multiplica el valor por 256):
* ancho de banda para IGRP = (10000000 / ancho de banda)
* ancho de banda para EIGRP = (10000000 / ancho de banda) * 256
* retardo para IGRP = retardo / 10
* retardo para EIGRP = retardo / 10 * 256

Tabla III Fórmula de la métrica de IGRP

Las métricas que utiliza el protocolo IGRP son (ver Tabla III):

1. **Ancho de banda:** el menor valor de ancho de banda en la ruta.
2. **Retardo:** el retardo acumulado de la interfaz a lo largo de la ruta.
3. **Confiabilidad:** la confiabilidad del enlace hacia el destino, según sea determinada por el intercambio de mensajes de actividad (keepalives).
4. **Carga:** la carga sobre un enlace hacia el destino, medida en bits por segundos.

IGRP publica tres tipos de rutas (ver Figura 2.3):

1. Interiores: Son rutas entre subredes de la red conectada a una interfaz de un router. Si la red que está conectada a un router no está dividida en subredes, IGRP no publica rutas interiores
2. Del sistema: Son rutas hacia redes ubicadas dentro de un sistema autónomo Las rutas de sistema no incluyen información acerca de las subredes
3. Exteriores: Son rutas hacia redes fuera del sistema autónomo, las cuales se tienen en cuenta al identificar un gateway de último recurso.

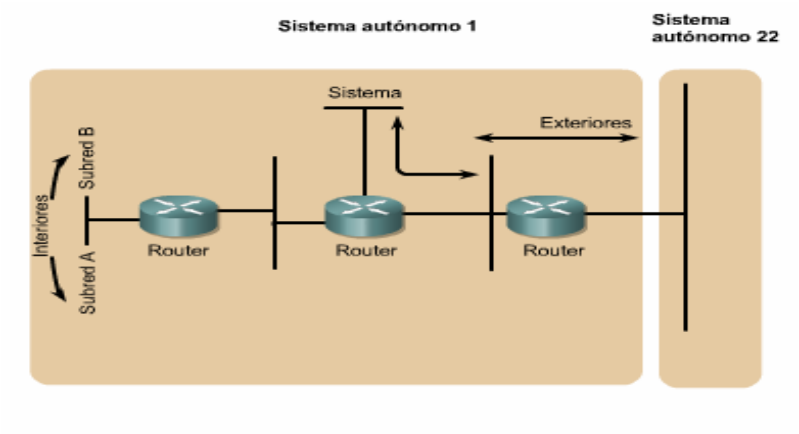

Figura 2.3 Clases de rutas que publica IGRP.

IGRP ofrece una serie de funciones diseñadas para mejorar su estabilidad, por ejemplo:

1. Lapsos de espera.
2. Horizontes divididos.
3. Actualizaciones inversas envenenadas.

Lapsos de espera.

IGRP también mantiene un cierto número de temporizadores y de variables que contienen los intervalos de tiempo. Estos incluyen un temporizador de actualizaciones, un temporizador de caída del servicio, un temporizador de espera y un temporizador de purga. IGRP envía actualizaciones por defecto cada 90 segundos(véase Bibliografía 13).

El temporizador de caída del servicio especifica cuánto tiempo debe esperar un router ante la ausencia de mensajes de actualización de enrutamiento en relación a una ruta específica antes de declarar que está fuera de servicio. Por defecto, en IGRP esta variable es tres veces el lapso de las actualizaciones, es decir 270 segundos.

El temporizador de espera especifica la cantidad de tiempo durante el cual no se toma en cuenta la información sobre rutas menos convenientes. Por defecto, en IGRP esta variable es tres veces el lapso de las actualizaciones, más 10 segundos, es decir 280 segundos. Por último, el temporizador de purga indica cuánto tiempo debe transcurrir antes de que se purgue una ruta de la tabla de enrutamiento. Por defecto, es siete veces el lapso de las actualizaciones de l temporizador de enrutamiento, es decir 630 segundos.

2.2.2 Comandos más importantes.

Para configurar un proceso de enrutamiento IGRP, se emplea el comando de configuración ***router igrp*****,** dentro del modo global. Para desactivar un proceso de enrutamiento IGRP, sencillamente utilice el comando ***no router igrp***, como se lo muestra a continuación:

```
RouterA(config)#router igrp  as-number
RouterA(config)#no router igrp  as-number
```

Donde ***as-number*** identifica el proceso IGRP, es el número del sistema

autónomo, también se lo utiliza para marcar la información de enrutamiento. Para ingresar las redes que participan en los procesos de enrutamiento IGRP, use el comando ***network*** de configuración del router. Para eliminar una entrada, utilice el comando ***no network***, el comando show ip route se lo emplea para verificar una correcta configuración, las rutas aplicadas a IGRP están marcadas con "**I "**.

Los comandos adicionales para verificar la configuración del IGRP son los siguientes:

```
show interface interface
show running-config
show running-config interface interface
show running-config | begin interface interface
show running-config | begin igrp
show ip protocols
```

Los siguientes comandos son útiles en el diagnóstico de fallas en IGRP:

```
show ip protocols
show ip route
debug ip igrp events
debug ip igrp transactions
ping
traceroute
```

Resumen de IGRP

- El número máximo de saltos es 255.
- Su distancia administrativa es 100
- Las actualizaciones son cada 90 segundos.
- Sus métricas son: ancho de banda, retardo, carga y confiabilidad.
- Por defecto están activas: ancho de banda y retardo.
- Publica 3 clases de rutas: interiores, exteriores y de sistema.
- Para el manejo de bucles implementa: lapsos de espera, horizonte dividido y actualizaciones envenenadas.

2.3 RIP V2

2.3.1 Concepto Y funcionamiento.

RIP v2 es una versión mejorada de RIP v1. Abajo se detallan algunas de sus funciones:

1. Es un protocolo de vector-distancia que utiliza el número de saltos como métrica.
2. Utiliza temporizadores de espera para evitar los bucles de enrutamiento – la opción por defecto es 180 segundos.
3. Utiliza horizonte dividido para evitar los bucles de enrutamiento.
4. Utiliza 16 saltos como métrica para representar una distancia infinita

RIP v2 es un protocolo sin clase, en otras palabras soporta VLSM. RIP v2 ofrece autenticación en sus actualizaciones. Se puede utilizar un conjunto de claves en una interfaz como verificación de autenticación. RIP v2 permite elegir el tipo de autenticación que se utilizará en los paquetes RIP v2. Se puede elegir texto no cifrado (texto plano) o cifrado con Message-Digest 5 (MD5). El texto no cifrado es la opción por defecto.

MD5 se puede usar para autenticar el origen de una actualización de enrutamiento. MD5 se utiliza generalmente para cifrar las contraseñas enable secret y no existe forma reconocida de descifrarlo.

RIP v2 envía sus actualizaciones de enrutamiento en multicast con la dirección Clase D 224.0.0.9, lo cual ofrece mejor eficiencia, RIP V1 lo hace a: 255.255.255.255. RIP v2 es un protocolo de enrutamiento dinámico que se configura dando al protocolo de enrutamiento el nombre de RIP Versión 2 y luego asignando números de red IP sin especificar los valores de subred.

2.3.2 Comandos más importantes.

El comando ***router*** inicia el proceso de enrutamiento. El comando ***network*** provoca la implementación de las siguientes tres funciones:

1. Las actualizaciones de enrutamiento se envían por una interfaz en multicast.
2. Se procesan las actualizaciones de enrutamiento si entran por la misma interfaz.
3. Se publica la subred que se conecta directamente a esa interfaz.

El comando ***network*** permite que el proceso de enrutamiento determine cuáles son las interfases que participan en el envío y la recepción de las actualizaciones de enrutamiento.

Los comandos ***show ip protocols*** y ***show ip route*** muestran información Sobre los protocolos de enrutamiento y la tabla de enrutamiento respectivamente.

El comando ***show ip interface brief*** también se puede usar para visualizar un resumen de la información y del estado de la interfaz. Se ejecuta los comandos privilegiados ***show running-config*** o ***show ip protocols*** en el router para verificar la posibilidad de que exista un protocolo de enrutamiento mal configurado. La combinación de los comandos ***router rip*** y ***version 2*** especifica RIP v2 como el protocolo de enrutamiento(véase Bibliografía 16).

El comando ***debug ip rip*** muestra las actualizaciones de enrutamiento RIP a Medida que éstas se envían y reciben. Los comandos ***no debug all*** o ***undebug all*** desactivarán totalmente la depuración.

Resumen de RIP V2

- La única métrica que utiliza es el número de saltos y su máximo es 15.
- Las actualizaciones las envía a una dirección multicast: 224.0.0.9.
- Soporta VLSM y CIDR.
- Para el manejo de bucles utiliza: lapsos de espera, horizonte dividido y rutas envenenadas.
- Es una versión mejorada de RIP V2.

2.4 EIGRP

2.4.1 Concepto Y funcionamiento.

EIGRP es un protocolo de enrutamiento propietario de Cisco, consiste en una

versión avanzada de IGRP, admite CIDR y VLSM, con los que permite que los diseñadores de red maximicen el espacio de direccionamiento, este es un protocolo sin clase, ofrece tiempos de convergencia más rápidos, una mejor escalabilidad y un manejo superior de los bucles de enrutamiento. EIGRP se lo describe como un protocolo de enrutamiento híbrido que ofrece lo mejor de los algoritmos de vector-distancia y del estado de enlace.

EIGRP es un protocolo de enrutamiento avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace. Posee las características de actualizaciones parciales y la detección de vecinos. EIGRP es una opción ideal para las grandes redes multiprotocolos(véase Bibliografía 32).

EIGRP mejora las propiedades de convergencia y eficiencia que IGRP. Esto permite que una red tenga una arquitectura mejorada y pueda mantener las versiones actuales en IGRP, las rutas pueden redistribuirse entre routers IGRP y EIGRP.

En la Tabla IV mostramos las métricas del protocolo EIGRP.

tanto IGRP como EIGRP utilizan el siguiente calculo de metrica:
* metrica = [K1 * ancho de banda + (K2 * ancho de banda) / (256 - carga) + (K3 * retardo)] * [K5 / (confiabilidad + k4)]
los siguientes son los valores por defecto de las constantes:
* K1 = 1 , K2 = 0 , K3 = 1 , K4 = 0 , K5 = 0
* metrica = ancho de banda + retardo
cuando K4 y K5 son 0, la porcion [K5 / (confiabilidad + K4)] de la ecuacion no forman parte del calculo de la metrica. Por tanto, utilizando los valores por defecto de las constantes, la ecuacion de la metrica es:
Ancho de banda + retardo
IGRP y EIGRP utilizan las siguientes ecuaciones para determinar los valores usados en el calculo de la metrica (observe que EIGRP multiplica el valor por 256):
* ancho de banda para IGRP = (10000000 / ancho de banda)
* ancho de banda para EIGRP = (10000000 / ancho de banda) * 256
* retardo para IGRP = retardo / 10
* retardo para EIGRP = retardo / 10 * 256

Tabla IV Fórmula de la métrica de EIGRP.

Algunas de las comparaciones entre EIGRP e IGRP se las detalla a continuación:

- Cálculo de métrica
- Número de saltos
- Etiquetado de rutas
- Modo de compatibilidad
- Redistribución automática de protocolos

EIGRP ofrece compatibilidad multiprotocolo, mientras que IGRP no lo hace. EIGRP e IGRP usan cálculos de métrica diferentes. EIGRP multiplica la métrica de IGRP por un factor de 256. Esto ocurre porque EIGRP usa una métrica que tiene 32 bits de largo, e IGRP usa una métrica de 24 bits. La información EIGRP puede multiplicarse o dividirse por 256 para un intercambio fácil con IGRP. IGRP tiene un número de saltos máximo de 255. El límite máximo para el número de saltos en EIGRP es 224. Esto es más

que suficiente para manejar redes grandes.

Los routers EIGRP mantienen información de ruta y topología a disposición en la RAM, para que puedan reaccionar rápidamente ante los cambios. EIGRP guarda esta información en varias tablas y bases de datos. EIGRP mantiene las siguientes tres tablas:

1. Tabla de vecinos
2. Tabla de topología
3. Tabla de enrutamiento

La tabla de vecinos es la más importante de EIGRP. Cada router EIGRP mantiene una tabla de vecinos que enumera a los routers adyacentes. Existe una tabla de vecinos por cada protocolo que admita EIGRP.

Al conocer nuevos vecinos, se registran la dirección y la interfaz del vecino. Esta información se guarda en la estructura de datos del vecino. Cuando un vecino envía un paquete hello(saludo), publica un tiempo de espera. El tiempo de espera es la cantidad de tiempo durante el cual un router considera que un vecino se puede alcanzar y que funciona.

Cuando vence el tiempo de espera, se informa al Algoritmo de Actualización Difusa (DUAL), que es el algoritmo de vector-distancia de EIGRP, acerca del cambio en la topología para que recalcule la nueva topología.

La tabla de topología se compone de todas las tablas de enrutamiento EIGRP en el sistema autónomo. DUAL toma la información proporcionada en la tabla de vecinos y la tabla de topología y calcula las rutas de menor costo

hacia cada destino. EIGRP rastrea esta información para que los routers EIGRP puedan identificar y conmutar a rutas alternativas rápidamente. La información que el router recibe de DUAL se utiliza para determinar la ruta del sucesor, que es el término utilizado para identificar la ruta principal o la mejor. Esta información también se introduce a la tabla de topología. Los routers EIGRP mantienen una tabla de topología por cada protocolo configurado de red. La tabla de enrutamiento mantiene las rutas que se aprenden de forma dinámica.

A continuación de muestran los campos que conforman la tabla de enrutamiento:

1. **Distancia factible (FD):** Ésta es la métrica más baja calculada hacia cada destino.
2. **Origen de la ruta:** Número de identificación del router que publicó esa ruta en primer lugar. Este campo se llena sólo para las rutas que se aprenden de una fuente externa a la red EIGRP. El rotulado de rutas puede resultar particularmente útil con el enrutamiento basado en políticas.
3. **Distancia informada (RD):** La distancia informada (RD) de la ruta es la distancia informada por un vecino adyacente hacia un destino específico.
4. **Información de interfaz:** La interfaz a través de la cual se puede alcanzar el destino.
5. **Estado de ruta:** El estado de una ruta. Una ruta se puede identificar como pasiva, lo que significa que la ruta es estable y está lista para usar, o activa, lo que significa que la ruta se encuentra en el proceso de recálculo por parte de DUAL.

Puede haber hasta cuatro rutas de sucesor para cada destino en particular. Estas pueden ser de costo igual o desigual y se identifican como las mejores rutas sin bucles hacia un destino determinado.

Un sucesor factible (FS) es una ruta de respaldo. Estas rutas se identifican

al mismo tiempo que los sucesores, pero sólo se mantienen en la tabla de topología. Un sucesor factible debe tener un costo publicado menor que el costo del sucesor actual hacia el destino. Si es imposible identificar un sucesor factible en base a la información actual, el router coloca un estado Activo en una ruta y envía paquetes de consulta a todos los vecinos para recalcular la topología actual. El router puede identificar cualquier nuevo sucesor o sucesor factible a partir de los nuevos datos recibidos de los paquetes de respuesta que responden a los pedidos de consulta.

EIGRP clasifica a las rutas como internas o externas. EIGRP agrega un rótulo de ruta a cada ruta para identificar esta clasificación. Las rutas internas se originan dentro del AS EIGRP(Sistema Autónomo EIGRP).

Las rutas externas se originan fuera del AS EIGRP. Las rutas aprendidas o redistribuidas desde otros protocolos de enrutamiento como RIP, OSPF e IGRP son externas. Las rutas estáticas que se originan fuera del AS EIGRP son externas. El rótulo puede establecerse en un número entre 0-255 para adaptar el rótulo.

EIGRP maneja 5 clases de paquetes:

1. Hello
2. Acuse de recibo
3. Actualización
4. Consulta
5. Respuesta

EIGRP depende de los paquetes hello para detectar, verificar y volver a Detectar los routers vecinos. Los routers EIGRP envían hellos con un intervalo fijo pero configurable que se denomina el intervalo hello. El intervalo hello por defecto depende del ancho de banda de la interfaz. En las redes IP, los routers EIGRP envían hellos a la dirección IP multicast 224.0.0.10. Los routers EIGRP almacenan la información sobre los vecinos en la tabla de vecinos. La tabla de vecinos también incluye un campo de Tiempo de Espera que registra el momento en que se recibió el último paquete. Los paquetes deben recibirse dentro del período correspondiente al intervalo de Tiempo de Espera para mantenerse en el estado Pasivo. El estado Pasivo significa un estado alcanzable y operacional. El tiempo de espera es equivalente al triple del intervalo hello, pero se puede configurar de acuerdo a los requerimientos de la red. Los paquetes hello siempre se envían de forma no confiable. Esto significa que no se transmite un acuse de recibo.

Los routers EIGRP usan paquetes de acuse de recibo para indicar la recepción de cualquier paquete EIGRP durante un intercambio confiable. RTP proporciona comunicación confiable entre hosts EIGRP. El receptor debe enviar acuse de recibo de un mensaje recibido para que sea confiable. Los paquetes de acuse de recibo, que son paquetes hello sin datos, se usan con este fin.

Al contrario de los hellos multicast, los paquetes de acuse de recibo se envían en unicast. Los acuses de recibo pueden adjuntarse a otros tipos de paquetes EIGRP, como los paquetes de respuesta.

Los paquetes de actualización se utilizan cuando un router detecta un nuevo vecino. Los routers EIGRP envían paquetes de actualización en unicast a ese nuevo vecino para que pueda aumentar su tabla de topología. Es posible que se necesite más de un paquete de actualización para transmitir toda la información de topología al vecino recientemente detectado. Los paquetes de actualización también se utilizan cuando un router detecta un cambio en la topología. Todos los paquetes de actualización se envían de forma confiable. Un router EIGRP usa paquetes de consulta siempre que necesite información específica de uno o de todos sus vecinos. Se usa un paquete de respuesta para contestar a una consulta. Si un router EIGRP pierde su sucesor y no puede encontrar un sucesor factible para una ruta, DUAL coloca la ruta en el estado Activo. Entonces se envía una consulta en multicast a todos los vecinos con el fin de ubicar un sucesor para la red destino. Los vecinos deben enviar respuestas que suministren información sobre sucesores o indiquen que no hay información disponible. Las consultas se pueden enviar en multicast o en unicast, mientras que las respuestas siempre se envían en unicast. Ambos tipos de paquetes se envían de forma confiable.

2.4.2 Comandos más importantes.

Se utiliza el siguiente comando para habilitar EIGRP y definir el sistema autónomo:

```
router(config)#router eigrp autonomous-system-number
```

El número de sistema autónomo se usa para identificar todos los routers que pertenecen a la red interna. Este valor debe coincidir para todos los routers dentro de la red interna. Luego se debe de indicar cuales son las redes que pertenecen al sistema autónomo en el router local:

```
router(config-router)#network network-number
```

Network-number es el número de red que determina cuáles son las interfases del router que participan en EIGRP y cuáles son las redes publicadas por el router.

Al configurar los enlaces seriales mediante EIGRP, es importante configurar el valor del ancho de banda en la interfaz. Si el ancho de banda de estas interfases no se modifica, EIGRP maneja el enlace serial con el valor por defecto:

```
router(config-if)#bandwidth kilobits
```

Para habilitar el registro en los cambios de adyacencia de vecinos, permitiendo monitorear la estabilidad del sistema y ayuda a detectar problemas:

```
router(config-router)#eigrp log-neighbor-changes
```

EIGRP resume automáticamente las rutas en el límite con clase. Este es el límite donde termina la dirección de red, de acuerdo con la definición del direccionamiento basado en clase. Sin embargo, es posible que el resumen automático no sea la mejor opción en ciertos casos. Por ejemplo, si existen subredes no contiguas, o se realiza el resumen de forma manual, el resumen automático debe deshabilitarse para que el enrutamiento funcione correctamente, esto se logra con el siguiente comando:

```
router(config-router)#no auto-summary
```

Con EIGRP, una dirección de resumen se puede configurar manualmente al configurar una red prefijo. Las rutas de resumen manuales se configuran por interfaz, de manera que la interfaz que propagará el resumen de ruta se debe seleccionar primero. Entonces, la dirección de resumen se puede definir con el commando ***ip summary-address eigrp***:

```
router(config-if)#ip summary-address eigrp autonomous-system-number ip-address mask administrative-distance
```

Las rutas de resumen EIGRP tienen una distancia administrativa por defecto de 5. De manera opcional, se pueden configurar con un valor entre 1 y 255. En la Tabla V mostramos un resumen de los 4 protocolos revisados. Los siguientes comandos nos sirven para mostrar las configuraciones realizadas:

- **Show ip eigrp interface**. - Muestra las interfases EIGRP.
- **Show ip eigrp topology**. - Muestra los sucesores factibles en la tabla de topología.
- **Show ip eigrp topology all links**. - Muestra toda la tabla de topología.
- **Show ip eigrp traffic**.- Muestra todos los paquetes EIGRP enviados y recibidos.
- **Debug eigrp fsm**.- Muestra la actividad del sucesor factible.
- **Debug eigrp packet**.- Muestra la transmisión y recepción de paquetes EIGRP.
- **Show running-config**.-Muestra la configuración del protocolo EIGRP.
- **Show ip eigrp neighbor**.- Nos muestra la tabla vecino.

Resumen de EIGRP

- Es un protocolo Hibrido.
- Soporta VLSM y CIDR.
- Máximo de saltos es 224.
- Las métricas son ancho de banda, confiabilidad, carga y retardo, por defecto están habilitadas solo: ancho de banda y retardo.
- Es compatible con IGRP.
- La métrica de EIGRP tiene 32 bits de largo, la de IGRP tiene 24.
- Mantiene tres tablas: Topología, Enrutamiento y Vecino.
- Su algoritmo de enrutamiento es DUAL.
- Maneja 5 clases de paquetes: Hello, Acuse de recibo, Actualización, Consulta y Respuesta.

Características	Manejo de VLSM	Soporta Multiprotocolos	tipo de actualizaciones	Admite Autenticación	Admite CIDR	Manejo de bucles	Intervalo por defecto	Número de saltos	Envío de actualizaciones	métricas	multiprotocolo
RIP V1	no	no	broadcast	no	no	Horizonte dividido, temporizador de espera, rutas envenenadas	30 segundos	15	toda la tabla topológica	número de saltos	no
RIP V2	si	no	multicast: 224.0.0.9	si	si	Horizonte dividido, temporizador de espera, rutas envenenadas	30 segundos	15	toda la tabla topológica	número de saltos	no
IGRP	no	no	broadcast	no	no	Horizonte dividido, temporizador de espera, rutas envenenadas	90 segundos	255	toda la tabla topológica	ancho de banda, retardo, carga, confiabilidad	no
EIGRP	si	si	multicast: 224.0.0.10	si	si	Mediante el algoritmo DUAL	paquetes hello cada 5 segundos	224	solo los cambios	ancho de banda, retardo, carga, confiabilidad	si

Tabla V Resumen de los protocolos de las pruebas

CAPITULO 3

DISEÑO Y CONFIGURACION DE LA RED.

En este capítulo detallaremos el procedimiento para asignar las direcciones IP a los usuarios de nuestra red, evitando el desperdicio de las mismas, se aplicará el procedimiento de Subnetting y VLSM para crear las subredes necesarias y tener subredes adicionales para la escalabilidad de la red, en otras palabras tendremos subredes adicionales para así manejar correctamente el crecimiento de la red a futuro, además se tomará una dirección IP de red privada de clase B, porque nos permite tener muchos más usuarios por subred que una clase C, se analizará el direccionamiento de los equipos de Networking que conforman la red, y por último se configurará los equipos para la conectividad Trunking.

3.1 Análisis VLSM de la red a implementar.

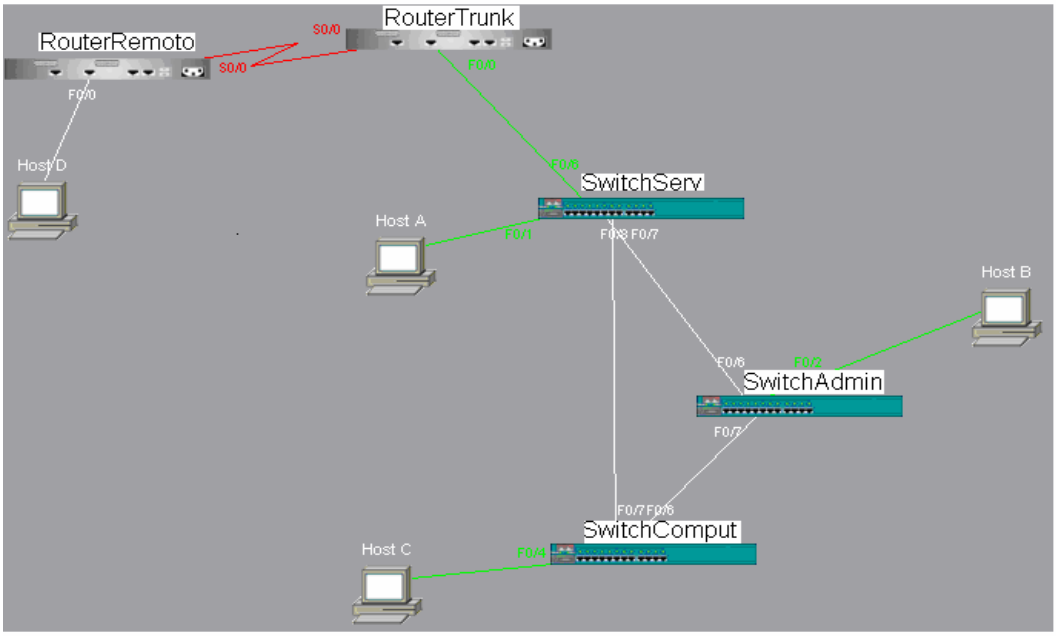

Figura 3.1 Red armada para las pruebas.

A continuación se detalla las partes de la red de prueba:

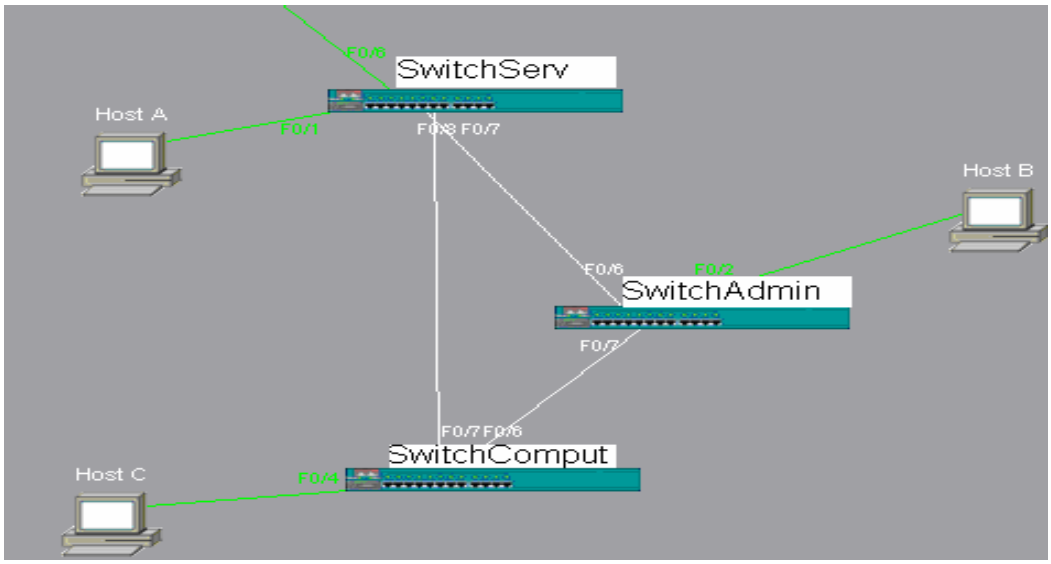

Figura 3.2 Switches Troncalizados que soportan las VLANS.

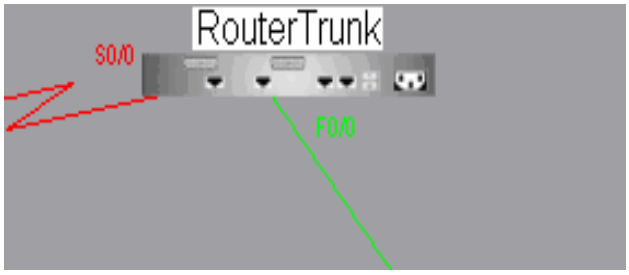

Figura 3.3 Router que permite la conectividad Troncalizada.

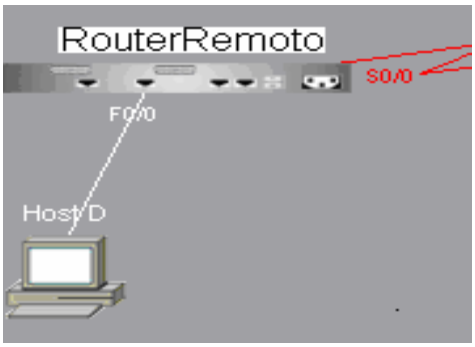

Figura 3.4 Red Remota 172.16.8.0

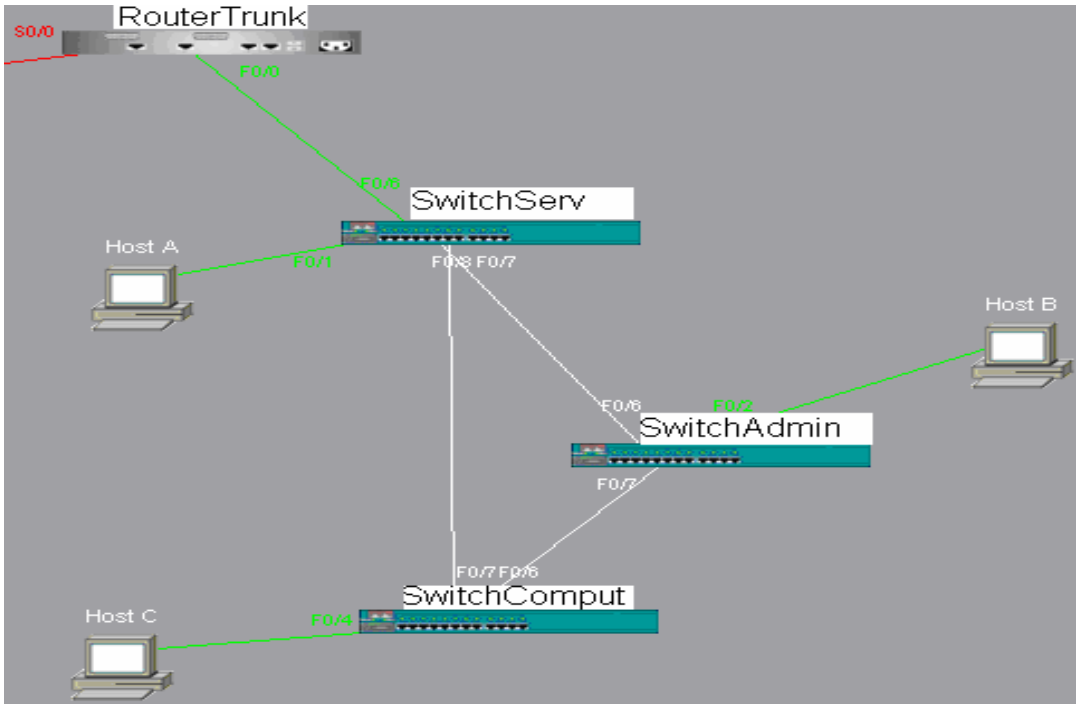

Figura 3.5 Red local con InterVLANS Troncalizada.

Para nuestras pruebas armamos la red mostrada en la figura **3.1**, en la cual vamos a probar la conectividad de los dispositivos con 4 protocolos de enrutamiento: **RIP V1**, **RIP V2**, **IGRP**, e **EIGRP**, y el protocolo **802.1q** para el enlace trunking. En el APENDICE D vamos a realizar pruebas de redundancia, para tener una red segura a prueba de fallas de enlace.

Hemos tomado la red **172.16.0.0** y nuestra máscara será la **255.255.254.0** en las VLANS, recordando que ésta es una red privada de clase B cuya máscara por defecto es **255.255.0.0**, en otras palabras estamos realizando "Subnetting".

Hemos querido diseñar subredes con **510** hosts válidos para asegurar una escalabilidad dentro de las VLANS, esto significa tener direcciones de red disponibles para asignar a futuros usuarios, para este propósito hemos tomado 9 bits para cubrir los 510 hosts, en el método de subnetting mediante la formula: (2 ^ n)– 2, donde n es el numero de bits prestados, para la parte de hosts n sería 9, se resta 2 en la fórmula debido a que no se toman dos direcciones dentro del rango, las cuales son: la primera que es la dirección de red de la subred y la última que es la dirección de broadcast.

Como dentro de una máscara por defecto en clase B tenemos 16 bits

disponibles para realizar subnetting los cuales son los dos últimos octetos, y ya hemos tomado 9, entonces los bits restantes que son 7, los utilizamos para determinar la cantidad de subredes posibles gracias a la misma fórmula con que obtuvimos el número de usuarios: (2 ^ n)– 2, ahora n es 7, esto nos indica que tenemos 126 subredes con 510 hosts disponibles cada una de ellas, así mismo la primera subred no se la toma en cuenta ni la última.

A continuación detallamos en la tabla VI cada subred a utilizar en las pruebas con su rango respectivo de direcciones IP útiles, la tabla completa de las subredes con sus direcciones la podremos hallar en el ANEXO A.

número de subred	dirección de subred	rango de direcciones IP disponibles	dirección de broadcast	hosts	hosts útiles
1	172.16.0.0	172.16.0.1------172.16.1.254	172.16.1.255	512	510
2	172.16.2.0	172.16.2.1------172.16.3.254	172.16.3.255	512	510
3	172.16.4.0	172.16.4.1------172.16.5.254	172.16.5.255	512	510
4	172.16.6.0	172.16.6.1------172.16.7.254	172.16.7.255	512	510
5	172.16.8.0	172.16.8.1------172.16.9.254	172.16.9.255	512	510
6	172.16.10.0	172.16.10.1----172.16.11.254	172.16.11.255	512	510

Tabla VI Direcciones IP de las subredes implementadas.

El escenario que presentamos es de una universidad en proceso de expansión, la cual consta con tres grupos de miembros al inicio: la parte administrativa, la parte docente y los alumnos, es por éste motivo que esta red consta de 3 VLANS, las cuales se detallan a continuación.

VLAN 1: que la hemos denominado la vlan **administrativa**, dentro de esta vlan constan: los departamentos de secretaría de cada facultad, el departamento de Tesorería, los Decanatos y Sub-decanatos y el departamento de Administración de la red.

VLAN 2: que la hemos denominado la vlan **alumnos**, dentro de esta vlan están los alumnos de cada facultad, es decir que las direcciones IP para las computadoras de distintos laboratorios, asociaciones estudiantiles y máquinas que están ubicadas en las distintas bibliotecas son tomadas dentro del rango disponible de esta vlan.

VLAN 3: que la hemos denominado la vlan **profesores,** la conforman las computadoras de los profesores de las distintas facultades.

Hemos tomado la subred **172.16.2.0 /23** para asignarle a la **VLAN 1.**
Hemos tomado la subred **172.16.4.0 /23** para asignarle a la **VLAN 2**.
Hemos tomado la subred **172.16.6.0 /23** para asignarle a la **VLAN 3.**

El **/23** significa que las subredes tienen mascara **255.255.254.0**, esto significa que cada subred tiene la capacidad de **510** usuarios, como anteriormente ya lo explicamos.

El RouterTrunk es el que va a manejar la conectividad trunking entre las VLANS, permitiendo que los usuarios de distintas VLANS se comuniquen entre sí, si dos usuarios de la misma VLAN se requieren comunicar no es necesario el router, porque los paquetes no viajan por las interfases de el router.

A la vez el RouterTrunk gracias a un enlace serial con el RouterRemoto permite conectar a los usuarios de las distintas VLANS con una subred externa, a la cual le hemos asignado la dirección IP **172.16.8.0 /23** , simulando con esto una conexión WAN , el host D pertenece a esta subred externa.

Las demás subredes que sobran mostradas en el ANEXO A pueden servir para una escalabilidad a futuro de la red, puede ser que tengamos VLAN alumnos de mecánica, VLAN para alumnos de eléctrica y así sucesivamente, lo mismo podría ocurrir con el departamento de profesores o con el departamento de administración.

También podríamos tener extensiones de la universidad en distintos sectores del país, o fuera de éste, a largo o mediano plazo, es por esto la razón de tantas subredes disponibles.

Según el estándar **RFC 1918**, dentro de una red privada se pueden asignar direcciones IP desde la clase A a la clase C siendo los rangos, los siguientes:

- **Clase A: 10.0.0.0---10.255.255.255**
- **Clase B: 172.16.0.0---172.31.255.255**
- **Clase C: 192.168.0.0---192.168.255.255**

A los dispositivos dentro de una red privada se les asignan direcciones privadas, y salen hacia el mundo exterior gracias a métodos como NAT(Network Address Translation) o PAT(Port Address Translation). A los dispositivos dentro de una red privada se les asigna las direcciones de manera estática o de manera dinámica, la manera estática es la manera manual, es decir ingresar por nosotros mismos la dirección IP, la máscara de subred, la dirección por defecto, y los DNS(Domain Name System), la manera dinámica es gracias a servidores DHCP(Dynamic Host Configuration Protocol), los cuales asignan de manera dinámica todos los parámetros que el computador necesita para estar en red, esto sucede en el momento que el computador carga el sistema operativo.

3.2 Direccionamiento de los equipos utilizando IPV4.

Cada switch dentro de una red se le debe asignar dirección IP para poder ser monitoreado vía telnet y para que funcione correctamente, por defecto antes de proceder con la creación de vlans, todos los puertos ethernet de un switch pertenecen a una sola vlan, la vlan 1 o también llamada a la vlan administrativa, esto quiere decir que todos los puertos del switch pertenecen al mismo dominio broadcast.

Las direcciones IP para cada switch fueron tomadas de la **VLAN 1** y son las siguientes:

- Dirección IP del SwitchServ: **172.16.2.2 / 23**
- Dirección IP del SwitchAdmin: **172.16.2.3 / 23**
- Dirección IP del SwitchComput: **172.16.2.4 / 23**

Además al switch se le debe de asignar una dirección por defecto, como los Switches están conectados en cascada deben de tener la misma dirección por defecto, la cual es: **172.16.2.1**, que es la dirección IP de la primera subinterfaz del puerto fastethernet 0/0 del RouterTrunk.

Los puertos 2 y 3 en cada switch fueron asignados para la VLAN 2 es decir la VLAN de alumnos. Los puertos 4 y 5 en cada switch fueron asignados para la VLAN 3 es decir la VLAN de profesores.

La verificación de la correcta configuración de los puertos asignados a las VLANS en cada switch, la podemos observar con ***show vlans*** dentro del modo privilegiado, vía consola o Telnet en cada switch.

Los puertos 6,7 y 8 en el SwitchServ fueron asignados para la comunicación Trunking. Los puertos 6 y 7 tanto en el SwitchAdmin como en el SwitchComput fueron asignados para la comunicación trunking.

La verificación de la correcta configuración de los puertos que pertenecen a la conectividad Trunking en cada switch la podemos observar con ***show Start*** dentro del modo privilegiado, vía consola o vía Telnet en cada switch.

Esto significa que si yo conecto una computadora y le asigno una dirección IP dentro del rango de VLAN 2, puedo conectarla en cualquier puerto 2 y 3 de cualquier switch, esta va a pertenecer a la VLAN alumnos, lo mismo sucede con las demás VLANS, esto es lo interesante de crear VLANS, puedes mover una computadora de una VLAN a otra con solo asignarle una

IP dentro de la nueva VLAN sin hacer ningún cambio en la configuración de los switches ni de los routers, y si contáramos con un servidor DHCP, el cambio fuera dinámico, es decir no tendríamos que configurar manualmente el equipo, bastaría con conectar al puerto de la VLAN donde queremos que esté.

Como el puerto 8 del SwitchServ está conectado a la interfase fastethernet 0/0 del RouterTrunk, ambos puertos deben estar en modo full duplex y estar a la misma velocidad.

En la figura **3.2** el host A pertenece a la VLAN 1, el host B pertenece a la VLAN 2 y el host C pertenece a la VLAN 3.

Las direcciones IP para estos hosts (usuarios) fueron las siguientes:

- Host A: **172.16.2.5 /23**
- Host B: **172.16.4.5 /23**
- Host C: **172.16.6.5 /23**

Si nos damos cuenta en la figura **3.2** el cable que une al SwitchAdmin con el SwitchComput es el enlace trunking entre ellos, por ese medio físico van a viajar los paquetes para las distintas VLANS de existir una comunicación entre equipos conectados en estos switches, de la misma manera sucede con el cable que une al SwitchServ con SwitchAdmin, el cable que une al

SwitchServ con SwitchComput es un enlace redundante, el cual no es Tomado en cuenta mientras existan los otros enlaces, esto lo ejecuta el spanning tree, mecanismo del switch que elimina lazos físicos, el SwitchServ es el Switch raíz de este algoritmo.

El RouterTrunk es el router que permite el enrutamiento interVLAN, es decir una comunicación entre las VLANS, para este propósito un cable conecta al SwitchServ con el router, por este medio van a ir los paquetes entre distintas VLANS. Recordemos que la comunicación entre VLANS se logra gracias a un dispositivo de capa de red, el interfase fastethernet 0/0 es el puerto del router que está conectado al SwitchServ, en esta interfase vamos a crear subinterfases, una subinterfase por cada VLAN, es lo correcto y recomendable, un router puede manejar hasta más de 255 VLANS, esto depende del modelo del router, estas subinterfases son Interfases lógicas, al igual que las 3 VLANS creadas en el switch, cada subinterfase debe detener una dirección IP y una máscara de subred, esta dirección IP debe de pertenecer a la VLAN a la cual enruta . A continuación se detallan las direcciones IP que se asignaron a las subinterfases:

- Subinterfase 1 o interfase 0/0.1: **172.16.2.1/23**
- Subinterfase 2 o interfase 0/0.2: **172.16.4.1/23**
- Subinterfase 3 o interfase 0/0.3: **172.16.6.1/23**

El RouterTrunk tiene una conexión serial a través de la interfase serial 0/0 con el RouterRemoto, el RouterTrunk es el DCE en este enlace, es decir que en la interfase serial 0/0 del RouterTrunk se debe de ingresar el comando ***clockrate 56000***, para brindar sincronización, esto se lo hace dentro del modo global, además tanto la interfase serial 0/0 del RouterTrunk y la interfase serial 0/0 del RouterRemoto deben pertenecer a una subred independiente de todas las redes vecinas, a esta subred le hemos designado la IP **172.16.10.0** con máscara **255.255.255.252**, permitiendo sólo dos direcciones útiles como se detalla a continuación:

- Serial 0/0 RouterTrunk:**172.16.10.1/30**
- Serial 0/0 RouterRemoto:**172.16.10.2/30**

El RouterRemoto tiene la red **172.16.8.0/23** conectada a su interfase fastethernet 0/0, además el interfase serial 0/0 actúa como DTE en el enlace WAN o serial con el RouterTrunk, el interfase fastethernet 0/0 tiene la dirección de red **172.16.8.1/23** y el host D que pertenece a la subred ethernet del RouterRemoto tiene la dirección **172.16.8.5/23.**

Todo lo detallado en la página 85 lo podemos visualizar en la Figura **3.6**.

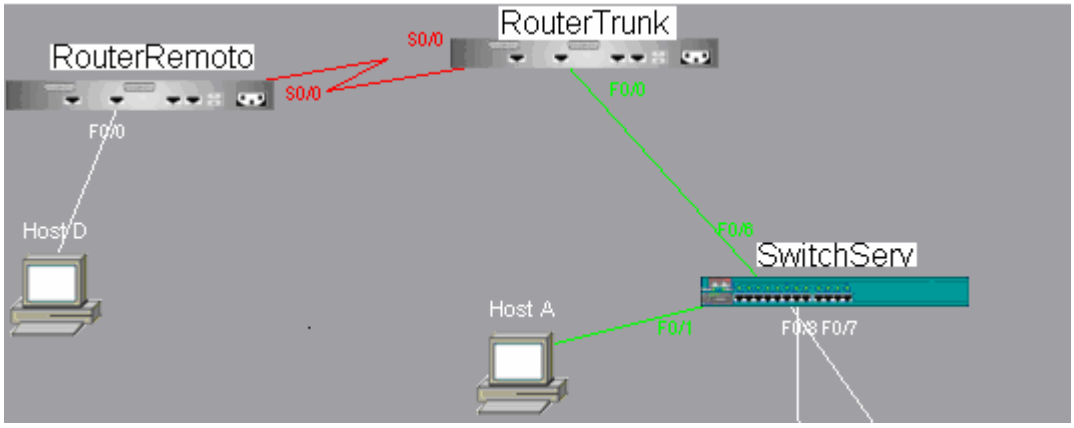

Figura 3.6 Parte de la red Armada

3.3 Análisis y Configuración de la conectividad interVLAN Troncalizada.

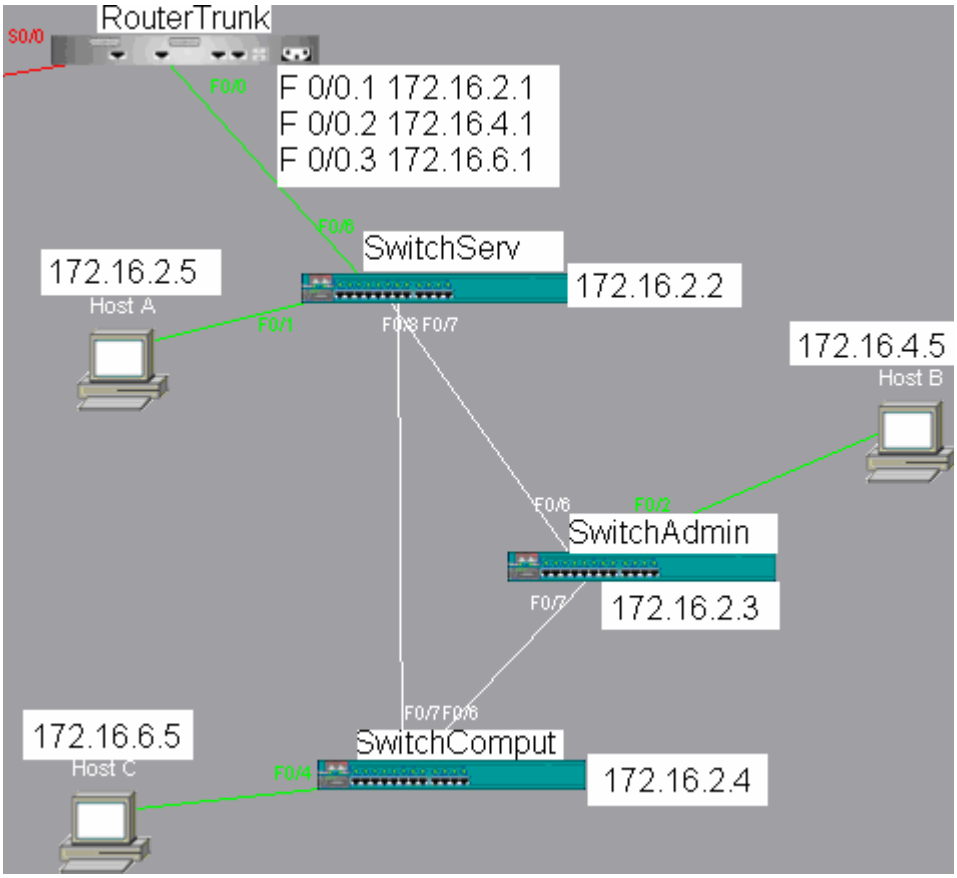

Figura 3.7 InterVLANS Troncalizada con direcciones IP.

Cabe señalar que las configuraciones son los datos que ingresamos al switch, en su momento indicaremos las salidas que brindan los switches y routers debido a la configuración ingresada y al esquema de la red.

Configuración de SwitchServ:

Por lo general el switch arranca en modo usuario:

Switch>

Entramos al modo privilegiado, gracias al comando enable.

```
Switch>enable
Switch#
```

Esta es la salida del switch en el momento que entramos al modo privilegiado:

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

Creamos las VLAN:

```
switch#vlan database
switch(vlan)#vlan 2 name alumnos
VLAN 2 added:
Name: alumnos
```

```
switch(vlan)#vlan 3 name profesores
VLAN 3 added:
Name: profesores
switch(vlan)#exit
APPLY completed.
Exiting....
```

Entramos al modo de configuración global, y le asignamos nombre al switch.

```
switch#conf t
switch(config)#hostname SwitchServ
SwitchServ(config)#
```

Asignamos los puertos 2 y 3 del switch a la VLAN 2:

```
SwitchServ(config)#int fast 0/2
SwitchServ(config-if)#switchport mode access
SwitchServ(config-if)#switchport access vlan 2
SwitchServ(config-if)#no shut
SwitchServ(config-if)#exit
SwitchServ(config)#in fas 0/3
SwitchServ(config-if)#switchport mode access
SwitchServ(config-if)#switchport access vlan 2
SwitchServ(config-if)#no shut
SwitchServ(config-if)#exit
```

Asignamos los puertos 4 y 5 a la VLAN 3:

```
SwitchServ(config)#int fast 0/4
SwitchServ(config-if)#switchport mode access
SwitchServ(config-if)#switchport access vlan 3
SwitchServ(config-if)#no shut
SwitchServ(config-if)#exit
SwitchServ(config)#int fast 0/5
SwitchServ(config-if)#switchport mode access
SwitchServ(config-if)#switchport access vlan 3
SwitchServ(config-if)#no shut
SwitchServ(config-if)#exit
```

Asignamos los puertos 6,7 y 8 al modo trunking:

```
SwitchServ(config)#int fast 0/6
SwitchServ(config-if)#switchport mode trunk
SwitchServ(config-if)#no shut
SwitchServ(config-if)#exit
SwitchServ(config)#int fast 0/7
SwitchServ(config-if)#switchport mode trunk
SwitchServ(config-if)#no shut
SwitchServ(config-if)#exit
SwitchServ(config)#int fast 0/8
SwitchServ(config-if)#switchport mode trunk
SwitchServ(config-if)#no shut
```

Como la interfaz 8 es la que está conectada al router debe de manejar comunicación full duplex, la configuramos para ese propósito:

```
SwitchServ(config)#int fast 0/8
SwitchServ(config-if)#duplex full
SwitchServ(config-if)#speed 100
SwitchServ(config-if)#exit
```

Configuramos la dirección IP en el switch y el default gateway:

```
SwitchServ(config)#int vlan 1
SwitchServ(config-if)#ip address 172.16.2.2 255.255.254.0
SwitchServ(config-if)#no shut
SwitchServ(config-if)#exit
SwitchServ(config)#ip default-gateway 172.16.2.1
```

Configuramos las claves de consola y la de acceso vía telnet:

```
SwitchServ(config)#line con 0
SwitchServ(config-line)#pass cisco
SwitchServ(config-line)#login

SwitchServ(config-line)#exit

SwitchServ(config)#line vty 0 15
SwitchServ(config-line)#pass cisco
SwitchServ(config-line)#login
SwitchServ(config-line)#exit
SwitchServ(config)#exit
```

Por defecto en los switches catalyst 2950 una vez configuradas las VLAN se activa el modo VTP, que es el que propaga las VLAN creadas en un switch para que otros las aprendan:

```
SwitchServ#vlan database
```

Luego configuramos el modo VTP:

```
SwitchServ(vlan)#vtp server
Device mode already VTP SERVER.
SwitchServ(vlan)#exit
APPLY completed.
Exiting....
```

Copiamos la configuración realizada que esta corriendo en la RAM del switch a la NVRAM del switch, la RAM es una memoria volátil, los datos se pierden una vez apagado el equipo, situación que no sucede con la NVRAM:

```
SwitchServ#copy run s
Destination filename [startup-config]?
Building configuration...
[OK]
```

Configuración de SwitchAdmin y SwitchComput.

Como los tres switches están en un dominio VTP, protocolo propietario de CISCO explicado en el APENDICE A de la tesis, las VLAN creadas en SwitchServ se propagan tanto a SwitchAdmin como a SwitchComput.

Los puertos 2 y 3 de SwitchAdmin se configuran de la misma manera que los puertos 2 y 3 de SwitchServ. Los puertos 4 y 5 de manera similar son configurados como los puertos 4 y 5 de SwitchServ.

De igual manera los puertos 6 y 7 se configuran de manera idéntica a los puertos 6 y 7 de SwitchServ.

Las claves de consola y Telnet son configuradas de igual manera como en SwitchServ, al igual que la dirección IP del SwitchAdmin (172.16.2.3), todos los switches deben de tener la misma salida por defecto.

Todos los pasos detallados para SwitchAdmin se deben de seguir para SwitchComput, la única diferencia es la dirección IP de la VLAN 1 que para SwitchComput es 172.16.2.4.

Configuración del RouterTrunk

El RouterTrunk a través de sus subinterfases en la fastethernet 0/0, permite la conectividad InterVLAN, gracias al protocolo de la IEEE que es de estándar abierto, el 802.1q, a continuación la configuración del RouterTrunk:, utilizamos este protocolo por la disponibilidad de equipos, el switch CISCO CATALYST 2950 solo maneja el protocolo 802.1q.

Entramos al modo privilegiado:

```
Router>enable
Router#conf ter
```

Ingresamos al interfaz fastethernet 0/0:

```
Router(config)#inter fastEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#
```

Ingresamos a cada subinterfase las habilitamos para el enrutamiento trunking con encapsulamiento dot1q (el estándar de la IEEE, el 8021q), y les asignamos su respectiva dirección IP, y máscara de red:

```
Router(config-if)#inter fa 0/0.1
Router(config-subif)#encapsulation dot1q 1
Router(config-subif)#ip add 172.16.2.1 255.255.254.0
Router(config-if)#inter fa 0/0.2
Router(config-subif)#encapsulation dot1q 2
Router(config-subif)#ip add 172.16.4.1 255.255.254.0
Router(config-subif)#int fast 0/0.3
Router(config-subif)#encapsulation dot1q 3
Router(config-subif)#ip add 172.16.6.1 255.255.254.0
```

Habilitamos la interfase fastethernet para que maneje comunicación full duplex:

```
Router(config)#int fast 0/0
Router(config-if)#duplex full
Router(config-if)#speed 100
```

```
Router(config-if)#no shut
Router(config-if)#exit
```

Habilitamos la clave de consola y la de Telnet:

```
Router(config)#line con 0
Router(config-line)#pass cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#line vty 0 4
Router(config-line)#pass cisco
Router(config-line)#login
Router(config-line)#exit
```

Asignamos la dirección IP para la interfase serial 0/0, y la habilitamos para que trabaje como DCE, además le asignamos el nombre:

```
Router(config)#int s 0/0
Router(config-if)#ip add 172.16.10.1 255.255.255.252
Router(config-if)#clockrate 56000
Router(config-if)#no shu
Router(config-if)#exit
Router(config)#host RouterTrunk
RouterTrunk(config)#
RouterTrunk(config)#
```

Y no nos olvidemos de grabar esta configuración en la NVRAM.

CAPITULO 4

PRUEBAS DE DESEMPEÑO DE LA RED.

4.1 Capa de RED.

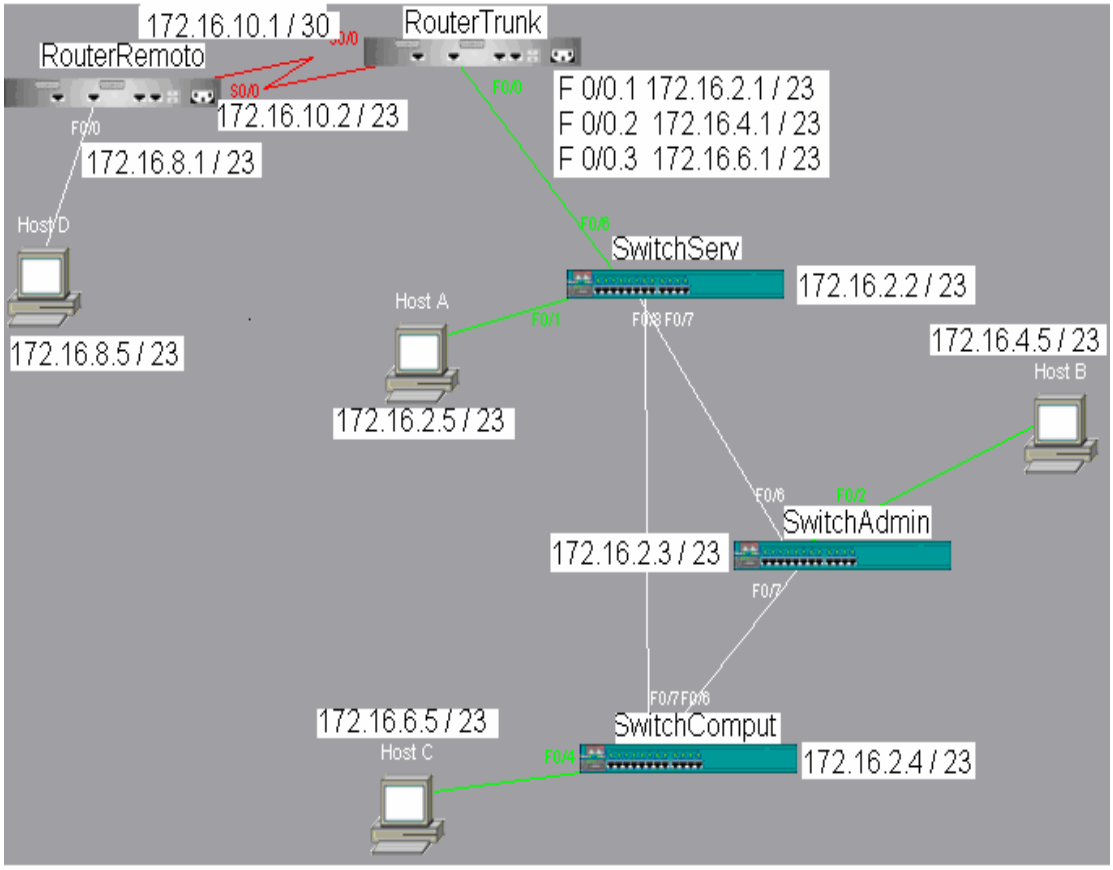

Figura 4.1 Red con direcciones IP respectivas.

En este capítulo se van a realizar pruebas de conectividad sobre la red mostrada en la figura **4.1** con los protocolos **RIP V1**, **IGRP**, **RIP V2** y **EIGRP**. Los equipos de la red se deben de conectar siguiendo las normas de cableado estructurado indicadas en el apéndice E, con las conclusiones que se saque de las pruebas con cada uno de los protocolos, se va a escoger el más idóneo, el que nos permita tener una red más segura; Sobre ese protocolo se va a implementar las ACLS en las interfases de los routers.

Introducción.

Recordemos las asignaciones de direcciones IP que se hicieron dentro de la Red en el capítulo 3:

SwitchServ……...172.16.2.2
SwitchAdmin……...172.16.2.3
SwitchComput……....….172.16.2.4
Default Gateway de switches y equipos dentro de VLANS…….172.16.2.1
Host A que pertenece a VLAN 1……..…172.16.2.5
Host B que pertenece a VLAN 2…….172.16.4.5
Host C que pertenece a VLAN 3…….172.16.6.5
Host D que pertenece red externa……172.16.8.5
Subinterfaz 1 de fastethernet de RouterTrunk….172.16.2.1
Subinterfaz 1 de fastethernet de RouterTrunk….172.16.4.1
Subinterfaz 1 de fastethernet de RouterTrunk….172.16.6.1
Interfaz serial 0/0 de RouterTrunk……...……172.16.10.1
Interfaz serial 0/0 de RouterRemoto…….……...172.16.10.2
Interfaz Fastethernet 0/0 de RouterRemoto…….172.16.8.1
Dirección de red VLAN 1……172.16.2.0 / 23
Dirección de red VLAN 2……172.16.4.0 / 23
Dirección de red VLAN 3……172.16.6.0 / 23
Dirección de red WAN entre RouterTrunk y Router Remoto….172.16.10.0 / 23
Dirección de red remota en RouterRemoto……..172.16.8.0 / 23

Las pruebas que se llevarán a cabo con distintos protocolos de enrutamiento sobre la misma red, no afectarán en ningún aspecto a la configuración de los switches mostrada en el capítulo 3, porque éstos son dispositivos de capa de enlace y no manejan direcciones IP; Los que van a tener cambios leves tanto en su configuración como en la tabla de enrutamiento son los routers, las pruebas que se realizaron se detallan a continuación:

1. Ping desde usuario de una VLAN a usuario de la misma VLAN.
2. Ping desde usuario de una VLAN a usuario de otra VLAN.
3. Ping desde usuario de una VLAN a los routers de la red.
4. Ping desde usuario de una VLAN a red remota.
5. Ping desde consola de cada switch a distintos puntos de la red.
6. Ping desde consola de los routers a distintos puntos de la red.
7. Ping desde red remota a usuarios de las distintas VLAN.
8. Telnet desde usuarios de las distintas VLAN hacia los routers.
9. Telnet desde usuario de red remota hacia routers de la red.

Las salidas mostradas por los equipos activos en todas las pruebas de este capítulo, se las puede apreciar en el APENDICE C.

4.1.1 Pruebas con RIP V1.

Configuración del RouterTrunk para enrutamiento con RIP V1.

Se debe de ingresar al modo de configuración global, luego ingresar el comando ***router rip*** e ingresar mediante el comando ***network*** cada una de las subredes directamente conectadas a las interfases del router, como se muestra a continuación:

- Donde **172.16.10.0** es la subred del enlace serial.
- Donde **172.16.2.0** es la subred de la VLAN 1.
- Donde **172.16.4.0** es la subred de la VLAN 2.
- Donde **172.16.6.0** es la subred de la VLAN 3.

```
RouterTrunk(config)#router rip

RouterTrunk(config-router)#network 172.16.10.0

RouterTrunk(config-router)#network 172.16.2.0
```

```
RouterTrunk(config-router)#network 172.16.4.0
RouterTrunk(config-router)#network 172.16.6.0
RouterTrunk(config-router)#exit
RouterTrunk(config)#exit
RouterTrunk#
```

Y finalmente se graban los cambios hechos a la NVRAM:

```
RouterTrunk#copy run s
```

A continuación se presenta la configuración del RouterRemoto:

Ingresamos al modo de configuración global:

```
Router#conf t
Router(config)# host RouterRemoto
```

Configuramos la clave de consola y la de Telnet:

```
RouterRemoto(config)#line con 0
RouterRemoto(config-line)#pass cisco
RouterRemoto(config-line)#login
RouterRemoto(config-line)#exit
RouterRemoto(config)#line vty 0 4
RouterRemoto(config-line)#pass cisco
RouterRemoto(config-line)#login
RouterRemoto(config-line)#exit
```

Configuramos la interfase fastethernet 0/0:

```
RouterRemoto(config)#int fast 0/0
RouterRemoto(config-if)#ip add 172.16.8.1 255.255.254.0
RouterRemoto(config-if)#no shut
RouterRemoto(config-if)#exit
RouterRemoto(config)#
```

Configuramos la interfase serial 0/0:

```
RouterRemoto(config)#int s 0/0
RouterRemoto(config-if)#ip add 172.16.10.2 255.255.255.252
RouterRemoto(config-if)#no shut
RouterRemoto(config-if)#exit
RouterRemoto(config)#
```

Configuramos al RouterRemoto para que trabaje con el protocolo de enrutamiento RIP V1 e ingresamos las subredes directamente conectadas a las interfases del router:

```
RouterRemoto(config)#router rip
RouterRemoto(config-router)#network 172.16.10.0
RouterRemoto(config-router)#network 172.16.8.0
RouterRemoto(config-router)#exit
RouterRemoto(config)#exit
```

Por ultimo grabamos la configuración a la NVRAM:

```
RouterRemoto#copy run s
```

Las salidas mostradas por los equipos activos de la red usted las podrá apreciar en el APENDICE C, gracias a esas salidas obtenemos el resumen con cada uno de los protocolos de enrutamiento.

Resumen de pruebas con RIP V1.

- Es un protocolo diseñado para redes pequeñas y no tan complejas.
- Es un protocolo que no soporta VLSM.
- Si un interfaz tiene máscara distinta al resto de redes, las actualizaciones no son enviadas por ese interfaz.
- Tener en cuenta la versión del protocolo RIP tanto de envío como de recepción de paquetes.
- Envía actualizaciones broadcast a 255.255.25.255
- Los comandos shows nos ayudan a verificar la correcta configuración de los equipos.
- Los comandos debugs nos ayudan a resolver problemas de conectividad.

4.1.2 Pruebas con IGRP.

Configuración en el RouterRemoto para enrutamiento con IGRP.

```
RouterRemoto(config)#router igrp 101
RouterRemoto(config-router)#network 172.16.10.0
RouterRemoto(config-router)#network 172.16.8.0
RouterRemoto(config-router)#exit
RouterRemoto(config)#exit
RouterRemoto# copy run start
```

Configuración en el RouterTrunk para enrutamiento con IGRP.

```
RouterTrunk# config t
RouterTrunk(config)#router igrp 101
RouterTrunk(config-router)#network 172.16.10.0

RouterTrunk(config-router)#network 172.16.2.0
RouterTrunk(config-router)#network 172.16.4.0
RouterTrunk(config-router)#network 172.16.6.0
RouterTrunk(config-router)#exit
RouterTrunk(config)#exit
RouterTrunk#copy run start
```

Resumen de pruebas con IGRP.

- No propaga rutas con distintas máscaras de subred.
- No soporta VLSM
- Es compatible con el protocolo EIGRP.
- Las métricas por defecto son: ancho de banda y retardo, aunque no se las toman en cuenta, la carga y la confiabilidad son métricas de IGRP.
- Se maneja por sistemas autónomos.
- Las actualizaciones las envía mediante broadcast(255.255.255.255)
- Las métricas por defecto son: ancho de banda y retardo.
- El número de saltos por defecto son de 100.

4.1.3 Pruebas con RIP V2.

Configuración en el RouterTrunk para que trabaje con el protocolo RIP V2:

```
RouterRemoto#conf
RouterRemoto(config)#router  rip
```

Basta con poner el comando ***version 2*** luego de ejecutar ***router rip*** para que los paquetes sean enrutados mediante **RIP V2**, antes de esto el router debe de estar configurado con RIP V1 tal como en 4.1.1

```
RouterRemoto(config-router)#version 2
RouterRemoto(config-router)#exit
RouterRemoto(config)#exit
RouterRemoto#
```

Se guarda la nueva configuración en la NVRAM:

```
RouterRemoto#copy run start
```

Configuración de RouterRemoto para que maneje RIP V2.

```
RouterRemoto# conf t
RouterTrunk(config)#router rip
RouterTrunk(config-router)#version 2
RouterTrunk(config-router)#exit
RouterTrunk(config)#exit
RouterTrunk# copy run start
```

Resumen de pruebas con RIP V2

- Es un protocolo que propaga rutas con distintas máscaras de subred.
- Soporta VLSM.
- Verificar si tanto en el envío como en la recepción esta correcta la versión del protocolo.
- Tiene las mismas características que RIP V1.
- Es la versión mejorada de RIP V1.
- Envía las actualizaciones a una dirección multicast (224.0.0.9).

4.1.4 Pruebas con EIGRP.

Configuración del RouterRemoto para trabajar con el protocolo EIGRP.

```
RouterRemoto(config)#no router rip
RouterRemoto(config)#router eigrp 101
RouterRemoto(config-router)#network 172.16.8.0
RouterRemoto(config-router)#network 172.16.10.0
RouterRemoto(config-router)#exit
RouterRemoto(config)#exit
```

En el enlace serial debemos configurar el ancho de banda que debe de ser igual al ***clockrate*** del enlace WAN, ingresado en el RouterTrunk, además el comando ***eigrp log-neighbor-changes*** permite habilitar el registro de cambios en adyacencias de vecinos EIGRP.

```
RouterRemoto(config)#int s 0/0
RouterRemoto(config-if)#bandwidth 56000
RouterRemoto(config-if)#exit
RouterRemoto(config)#router eigrp 101
RouterRemoto(config-router)#eigrp log-neighbor-changes
```

Debemos ingresar este comando si el router maneja redes no continuas:

```
RouterRemoto(config-router)#no auto-summary
```

Resumen de pruebas con EIGRP

- Es el protocolo más completo de todos los analizados en esta tesis.
- Es un protocolo que mantiene 3 tablas para una convergencia automática, ante cualquier cambio topológico.
- Es un protocolo sin clase el cual soporta VLSM y CIDR, por lo tanto se propagan todas las rutas conocidas por más máscaras variables que estén presentes en la red.
- Las actualizaciones se realizan ante un cambio topológico y solo se propagan los cambios.
- La comunicación entre routers se efectúa mediante el paquete HELLO que es un paquete sin datos así no satura el ancho de banda del enlace, y éste es enviado por defecto cada 5 segundos.
- Las actualizaciones son enviadas a una dirección multicast(224.0.0.10)
- EIGRP maneja 5 tipos distintos de paquetes para mantener las tablas que maneja EIGRP actualizadas, haciendo a este protocolo el mejor de todos lo analizados en esta tesis.

4.1.5 Resultados totales de las pruebas.

- Los protocolos de estado de enlace permiten una convergencia más rápida de los equipos ante un cambio topológico inesperado.

- Los protocolos sin clase permiten tener máscaras de subred variables dentro de una red, permitiendo así el ahorro de direcciones IP.

- Todo el conjunto de métricas que maneja EIGRP (ancho de banda, retardo, carga, confiabilidad), hacen de EIGRP el protocolo más confiable y seguro de todos.

- Gracias a las 3 tablas que maneja EIGRP (tabla vecino, tabla topología y tabla de enrutamiento), permite tener un conocimiento total de toda la red y tener presente rutas de respaldo, que se activan de manera automática ante algún cambio topológico.

- Los 5 tipos de paquetes que maneja EIGRP y su algoritmo de enrutamiento DUAL permiten mantener las rutas de menor costo hacia todos los puntos de la red y una comunicación constante entre equipos para actuar de manera inteligente y rápida ante la falla de algún enlace.

- Por todo esto hace que EIGRP sea el protocolo más completo y por ende el más confiable.

- En el siguiente capitulo vamos a hablar de la implementación en la red de listas de acceso para la seguridad de la misma, y las pruebas se realizaran sobre la red con el protocolo de enrutamiento EIGRP soportado por los equipos, que es el protocolo más práctico, seguro, confiable y rápido para el manejo de la red.

4.2 Seguridades de Acceso aplicados a la red.

4.2.1 Implementación de ACLS a la red.

Hay muchas maneras de proteger la información y restringir el acceso de personas no autorizadas a una red, en esta tesis nos enfocamos a la implementación de Listas de Control de Acceso (ACLS).

A continuación presentamos la configuración de los routers que son los dispositivos que van a aceptar o rechazar un paquete de acuerdo a la condición de sentencia que implementemos en las ACLS, para motivo de práctica, vamos a implementar ACLS estándares, las cuales pueden bloquear todo paquete entrante o saliente en las interfases del router.

Nosotros vamos a bloquear todo paquete entrante en la subinterfaz del router RouterTrunk que permite la comunicación de la VLAN 1 (administración) con las demás subredes de la red, y además vamos a bloquear todo paquete entrante por la subinterfaz que permite que la VLAN 3 (profesores) se comunique con las demás subredes, a parte vamos a restringir el acceso a los terminales virtuales de los routers, y sólo miembros de la VLAN 1 van a poder acceder a estos terminales, dicho en otras palabras, solo los miembros de la VLAN 1 van a estar permitidos de acceder a los routers vía Telnet, esto es muy necesario, en el caso de que los routers fallen y no se puedan acceder localmente a ellos(vía Consola), y también es muy importante

prevenir que usuarios no autorizados realicen cambios en los equipos que pueden afectar el correcto desempeño de la red.

A continuación presentamos las configuraciones de RouterTrunk y RouterRemoto.

Configuración del RouterTrunk para restringir el acceso Telnet (virtual) de cualquier computadora que no pertenezca a la VLAN administrador, incluso restringir el acceso de algún host remoto de la subred **172.16.8.0**, dicho en otras palabras, solo usuarios de la VLAN 1 que es la VLAN administrador van a poder realizar TELNET hacia el router RouterTrunk.

```
RouterTrunk# config t
RouterTrunk(config)#access-list 2 permit 172.16.2.1 0.0.0.255
RouterTrunk(config)#access-list 2 deny any
RouterTrunk(config)#line vty 0 4
RouterTrunk(config-line)#pass cisco

RouterTrunk(config-line)#login
RouterTrunk(config-line)#access-class 2 in
RouterTrunk(config-line)#exit
```

La verificación de que los equipos están correctamente configurados, se las Puede apreciar en el APENDICE C.

No se va a permitir ningún paquete entrante por la subinterfaz 172.16.2.1 que es la subinterfaz 1 de la interfaz fastethernet 0/0 del RouterTrunk, que permite la conectividad de la VLAN administrador con las redes externas, así evitamos que alguna persona tenga acceso hacia la parte de tesorería, secretaría o a algún decanato o rectorado.

```
RouterTrunk(config)#access-list 3 permit 172.16.2.0 0.0.1.255
RouterTrunk(config)#access-list 3 deny any
RouterTrunk(config)#int fast 0/0
RouterTrunk(config-if)#int fast 0/0.1
RouterTrunk(config-subif)#ip access-group 3 in
RouterTrunk(config-subif)#no shut
RouterTrunk(config-subif)#exit
```

No se va a permitir ningún paquete entrante por la subinterfaz 172.16.6.1 que es la subinterfaz 3 de la interfaz fastethernet 0/0 del RouterTrunk que permite la conectividad de la VLAN profesores con las redes externas, así evitamos que alguna persona no autorizada tenga acceso hacia la parte de los docentes.

```
RouterTrunk(config)#access-list 4 permit 172.16.6.0 0.0.1.255
RouterTrunk(config)#access-list 4 deny any
RouterTrunk(config)#int fast 0/0
RouterTrunk(config-if)#int fast 0/0.3
```

```
RouterTrunk(config-subif)#ip access-group 4 in
RouterTrunk(config-subif)#no shut
RouterTrunk(config-subif)#exit
RouterTrunk(config)#exit
```

En el RouterRemoto no manejamos las VLAN pero si queremos evitar que alguien entre vía Telnet, a cambiar la configuración del router, solo la VLAN administrador es la única autorizada para este efecto, esto lo logramos con las siguientes sentencias.

```
RouterRemoto> en
RouterRemoto# conf t
RouterRemoto(config)#access-list 1 permit 172.16.2.1 0.0.0.255
RouterRemoto(config)#access-list 1 deny any
RouterRemoto(config)#line vty 0 4
RouterRemoto(config-line)#pass cisco
RouterRemoto(config-line)#login
RouterRemoto(config-line)#access-class 1 in
RouterRemoto(config-line)#exit
RouterRemoto# copy run start
```

A continuación se presentan fotos tomadas de los equipos en que se realizaron las pruebas de esta tesis, cabe destacar que todos los switches y routers fueron equipos marca **CISCO**, y que todas las configuraciones y comandos utilizadas en esta tesis son de equipos **CISCO**. Se utilizaron **Routers CISCO 2620** y **Switches CATALYST 2950**.

Figura 4.2 Red armada

Figura 4.3 Switch CISCO CATALYST 2950.

CAPITULO 5

ANALISIS DE COSTO DEL PROYECTO

5.1 Costo de implementación.

Los costos de implementación, es el gasto más fuertes que una empresa realiza debido que estos incluyen: los gastos en la adquisión de equipos, los honorarios por las horas que se tomaría una persona experta en Networking en configurar los equipos, los gastos en el cableado estructurado (ver APENDICE E), para el tendido de los puntos de acceso, con el fin de conectar en red a todas las computadoras, impresoras, servidores, y equipos activos.

Vamos a revisar a continuación los costos en lo que respecta a la adquisición de equipos para la implementación de nuestra red, cabe recalcar que en nuestro estudio no tomamos en cuenta los equipos pasivos de la red, hemos asumido que el tendido de los puntos de acceso ya están implementados, las proformas en su integridad constan en el Anexo B.

LA Compañía MAINT nos brinda dos soluciones, ambas con equipos NORTEL.

La primera solución es con un switch de capa 3 NORTEL 3510-24T con 24 Puertos 10/100/1000 Mbps, cuyo costo es de 1745,88 dólares sin incluir IVA, Además la configuración del equipo tiene un costo de 600 dólares.

En la solución alternativa, MAINT nos presenta un switch router marca NORTEL 1424T CON 24 PUERTO 10/100 TX a un costo de 3893,32, la configuración del equipo no varía, sigue siendo en esta propuesta el valor de 600 dólares.

La compañía COMWARE nos presenta en su proforma el switch Matriz E1 de la marca Enterasys con 24 puertos 10/100 Mbps a un valor de 1890 dólares, y el costo de la instalación y configuración del equipo es de 100 dólares la hora, estos valores no incluyen IVA.

La compañía ANDEANTRADE de Quito, nos presenta en su propuesta económica el switch marca CISCO modelo WS-C3560-24TS-S Catalyst 3560 con 24 puertos 10/100 tiene un costo de 1600 dólares, el costo por la configuración y la instalación de este equipo tiene un costo total de 300 dólares, estos valores son sin incluir el precio del IVA.

Si nos damos cuenta, todos los modelos de switches presentados en las propuestas son multicapas, es decir trabajan tanto en capa 2 como en capa 3, no necesitamos un router externo para la comunicación InterVLAN, en cambio en las pruebas empleamos equipos por separado debido a la disponibilidad que teníamos, pero hoy en día para abaratar costos, tanto el switch de capa 2 y el router vienen integrados en un switch de capa 3, el cual maneja direcciones MAC y direcciones IP.

Revisando las propuestas, la proforma de ANDEANTRADE, es la más Económica, por el precio y por la marca que nos ofrecen CISCO, recordemos que sólo en equipos CISCO el protocolo EIGRP está presente, EIGRP resultó ser el mejor protocolo de enrutamiento, por todos los beneficios que nos brindó en las pruebas realizadas en el capítulo 4.

Además podemos obtener el Smartnet (8*5*4) que nos brinda CISCO, por solo 250 dólares al año, Smartnet es una garantía de fabrica, que funciona de la siguiente manera: CISCO nos devuelve el equipo nuevo si es que resulta defectuoso, en el menor tiempo posible.

5.2 Costo de mantenimiento.

El mantenimiento anual brindado por MAINT en su proforma consta de dos mantenimientos preventivos y dos mantenimientos correctivos y tiene el costo total de 300 dólares anuales en la opción 1 y en la opción 2 tiene el costo de 600 dólares anuales.

COMWARE en su proforma nos detalla un costo por hora de 100 dólares, para realizar el mantenimiento, cada vez que la red lo necesite, ellos no poseen una infraestructura como lo ofrece MAINT. MAINT es una empresa que está dedicada a brindar soporte a las redes por niveles, siendo los niveles más altos, los más críticos.

ANDEANTRADE, en su proforma nos presenta un rubro de 200 dólares por mantenimiento y nos sugiere que éste sea realizado cada 6 meses.

Otra vez ANDEANTRADE nos presenta la propuesta más económica en lo que respecta gastos por mantenimiento.

5.3 Resultados del análisis de costo.

En esta tesis, las pruebas fueron realizadas en equipos CISCO, por la disponibilidad que tuvimos en practicar en ellos la red que diseñamos, cabe recalcar que ellos manejan protocolos de enrutamiento como RIP V1, RIP V2 y OSPF que son de estándar abierto, por lo tanto están presentes en otras marcas, pero al final de las pruebas por todas las bondades que nos brinda EIGRP nos quedamos con él, y como este protocolo es propietario de CISCO Escogemos esta marca para que sea la encargada de brindar conectividad a nuestra red.

Además CISCO es una marca reconocida a nivel mundial, es la más Confiable y sus equipos son los más robustos del mercado, años de garantía es su mejor carta de presentación.

ANDEANTRADE es distribuidor directo de equipos CISCO, y vende equipos al por mayor y menor, con sede en Quito distribuye a nivel nacional esta marca, existen otros distribuidores de equipos CISCO, pero la propuesta más económica es la que nos presenta ANDEANTRADE.

Además la garantía que nos brinda el Smartnet de CISCO, es única, ya que podemos contar con un soporte constante y efectivo.

Además debemos tener un administrador permanente, que brinde soporte a Los usuarios internos de las VLAN, se ha considerado revisando los salarios de las distintas empresas de telecomunicaciones, que el valor de 600 dólares al mes por salario estaría correcto cancelarle por sus servicios, además esta persona se podría encargar de los mantenimientos tanto de los equipos activos como pasivos de la red y la empresa se ahorraría este rubro.

A continuación se presenta un resumen de todas las propuestas recibidas para el desarrollo del capítulo 5.

Cuadro comparativo entre las diferentes ofertas.				
Configuración	**opción 1 MAINT** 600 USD	**opción 2 MAINT** 600 USD	**COMWARE** 100 USD la hora	**ANDEANTRADE** 300 USD
Equipo	1745,88 USD	3893,32 USD	1890 USD	1600 USD
Mantenimiento	300 USD	600 USD	100 USD la hora	400 USD
Garantía	1 año	1 año	1 año	1 año
Adicionalmente por 250 dólares se puede contar con el servico de Smartnet en equipos CISCO, ANDEANTRADE nos ofrece equipos CISCO. MAINT en sus dos propuestas nos presenta equipos NORTEL. COMWARE en su propuesta nos ofrece equipo Enterasys.				

Tabla VII Cuadro comparativo de las propuestas.

Se presenta un cuadro detallando los gastos en que incurrirá la empresa para la implementación de la red, no constan los costos de cables, e infraestructura para la colocación de los puntos de acceso, hemos asumido que esa parte ya está instalada.

Se escoge la oferta de ANDEANTRADE y se muestran los gastos que haremos para implementar la red.	
Gastos de configuración	300 USD
Costo de equipo	1600 USD
Mantenimiento	400 USD al año
Garantía	250 USD al año
Sueldo del administrador de la red	600 USD mensual

Tabla VIII Gastos para implementar la red.

CONCLUSIONES
Y
RECOMENDACIONES

Conclusiones

1. Se escogió al protocolo EIGRP propietario de **CISCO** como el más indicado para trabajar en una red de este tipo, debido, que al ser un protocolo híbrido, combina lo mejor de los protocolos de estado de enlace y de los protocolos vector distancia, permite a cada router conocer la topología de toda la red, las actualizaciones no inundan la red ya que al ser tipo multicast y solo enviar los cambios no consume todo el ancho de banda de la red, está en constante comunicación con los routers que son partes de la red a través de paquetes que no consumen mucho ancho de banda del enlace y ante cualquier cambio topológico repentino, la red converge rápidamente, debido que las tablas que permiten escoger la mejor ruta están almacenada en la RAM, además EIGRP es multiprotocolo, y puede redistribuir rutas con routers que manejan IGRP.

2. Se escogió trabajar con una red de clase **B** porque nos permite tener subredes con mayor cantidad de usuarios que nos brinda la clase C, adicional a esto nos permite tener gran cantidad disponible de subredes adicionales para una futura ampliación del instituto.

3. Etherchannel propietario de **CISCO** es un método que permite tener varios puertos asociados como uno solo y si uno de ellos falla, pues la comunicación del enlace no se corta, ya que tenemos a los otros de respaldo, este es un método de redundancia muy utilizado, cuando se tiene varios switches en cascada. Por ejemplo si por cada puerto estuviésemos transmitiendo a 100 Mbps, y creáramos un etherchannel con dos puertos, lograríamos transmitir a 200 Mbps.

4. Se escogió trabajar con ACLS, porque son muy útiles para restringir el tráfico hacia recursos y aplicaciones dentro de la red a personas no autorizadas, para que no saturen el ancho de banda de la red, además prohíbe el acceso hacia una red o subred a personas externas y/o ajenas a la organización. Cuando se trabajan con ACLS extendidas, se hacen sentencias más selectivas, en lo que respecta a la aceptación o negación de tráfico. Se debe siempre tener presente si queremos bloquear el tráfico entrante o saliente de un interfaz.

5. El trafico Broadcast dentro de una Vlan es independiente del trafico Broadcast dentro de otra VLAN, ya que son segmentos lógicamente separados.

6. Los equipos deben de manejar los mismos protocolos para poder comunicarse.

7. No se debe de tener duplicados ni de direcciones ip, ni direcciones de subred dentro de una red.

8. La configuración de los equipos debe de estar almacenada como información de respaldo en un servidor TFTP, para contar con los comandos y configuraciones ante una falla de funcionamiento de los equipos como reseteos repentinos ocasionados por fallas eléctricas u otros factores ajenos a la organización.

9. Una comunicación troncalizada, es más eficiente, tanto en el ahorro de puertos en los equipos activos como en el manejo de tráfico de la red.

10. En las pruebas, el router fue externo, y el switch fue de capa 2 debido a la disponibilidad de equipos, pero en la actualidad ya existen switches de capa 3, que al tener módulo de enrutamiento, hacen el papel de ambos: de un switch de capa 2 y de un router.

11. Siempre tener equipos con el sistema operativo actualizado, para que soporten y manejen las tecnologías de punta, y a la vez nos permitan un mejor manejo de la red.

12. Se hicieron las pruebas en el enlace troncalizado con el protocolo 802.1Q estándar de la IEEE debido que los switches CISCO CATALYST 2950 solo manejan ese protocolo.

Recomendaciones

1. Se debe de cumplir las normas de cableado estructurado como se lo indica en el APENDICE A de la presente tesis.

2. Se recomienda que los equipos de Networking dentro de la red sean del mismo fabricante, para que haya compatibilidad en todos los protocolos de comunicación.

3. Los equipos activos de cualquier marca deben de tener un sistema operativo actualizado para que soporten todas las características actuales de transmisión, por ejemplo en los Switches CISCO CATALYST 2950, estos deben de tener un sistema operativo superior a la versión **12.0.**

4. El router fue externo en las pruebas, debido a la disponibilidad de equipos activos, además es recomendable, si una empresa no cuenta con el dinero suficiente, primero armen las VLAN y luego implementen la comunicación InterVLAN a través de un router, además esto permite no tener todo concentrado en un solo equipo, y tener un solo punto de falla, en la actualidad ya existen switches de capa 3 que tienen modulo de enrutamiento, esto permite abaratar costos.

5. Seguir un orden en la asignación de direcciones IP a los dispositivos dentro de una VLAN.

6. Seguir un orden en la asignación de Subredes dentro de la red.

7. Tener un enlace redundante entre switches, y entre el switch que está directamente conectado al router que permite la comunicación InterVLAN, para que permita la continuidad de la conectividad dentro de la red, ante una falla en el enlace principal.

8. Tener el mismo encapsulamiento InterVLAN en todos los dispositivos de la red.

9. Si el router no está manejando redes contiguas, deshabilitar la propiedad de autosumarización, en el caso que se implemente EIGRP.

10. Si se están manejando subredes con máscaras distintas dentro de la red, verificar si el protocolo de enrutamiento soporta esta característica.

11. Si se están manejando distintos protocolos enrutados, verificar si el protocolo de enrutamiento soporta esta característica.

12. Si se van a tener varias VLAN, realizar pruebas para verificar la conectividad y si no hay saturación en la red debido a las distintas aplicaciones que se manejará.

13. Preferible tener al switch y al router trabajando separadamente, aunque en la actualidad por abaratar costos se está implementando switches de capa 3.

14. Es preferible implementar ACLS extendidas para ser más selectivos en el tipo de tráfico que queremos restringir.

15. Se recomienda grabar la configuración de los dispositivos en un servidor TFTP o aplicar la captura de la misma mediante el programa HyperTerminal, para así ante el reseteo del equipo, o mal funcionamiento del mismo, se pueda cargar la configuración al equipo que va a funcionar por el dañado.

16. Se recomienda VLAN geográficas, para el eficiente uso de los recursos de la red.

17. Tener cuidado con cada sentencia cuando se esta implementando las ACLS en las interfases del router.

18. Se recomienda verificar que se haya realizado una correcta configuración con los comandos de ayuda como lo son todos los comandos de ***show***.

19. Si algo en la red no está funcionando como debería de ser, es muy útil saber que contamos con los comandos de ***debug***.

20. Si se está utilizando algunos protocolos de enrutamiento dentro de la red, preferible utilizar aquellos que permitan una redistribución de las rutas entre ellos, por ejemplo: IGRP Y EIGRP.

21. Trate de darle a los dispositivos de networking de la red nombres de acuerdo a su función dentro de la red, para que así se le haga más fácil alguna configuración o el monitoreo de los equipos.

22. Evite el desperdicio de direcciones de red, puede que las necesite a largo o corto plazo.

APENDICE A

Concepto de VTP

VTP(protocolo de enlace troncal virtual) fue diseñado para reducir el trabajo en la administración de una red conmutada, cuando se configura una nueva VLAN en un servidor VTP, la nueva VLAN se distribuye a través de todos los switches dentro del dominio, esto reduce el trabajo de configurar la misma VLAN en todas partes, este protocolo es propietario de **CISCO**, los paquetes VTP son enviados sea en tramas ISL, o en tramas 802.1q, estos paquetes son enviados a la dirección MAC multicast destino: 01-00-0c-cc-cc-cc con un código de enlace lógico de control (LLC) del protocolo de acceso de subred (SNAP) (AAAA) y un tipo de 2003(en la cabecera SNAP), abajo se muestra el formato de paquete VTP encapsulado en tramas ISL.

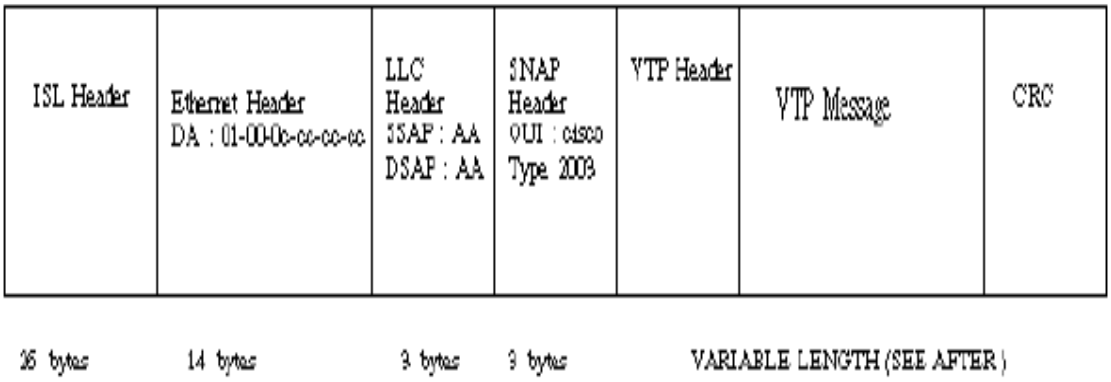

Figura A.1 Formato de la trama del protocolo VTP.

También se puede tener paquetes VTP dentro de tramas 8021q, en este caso la cabecera ISL y el chequeo de redundancia cíclica (CRC) deben ser remplazados por el etiquetado dot1q.

El formato de la cabecera VTP puede variar dependiendo del tipo de mensaje VTP, cualquiera que este sea todos deben de tener los siguientes campos: Versión, Tipo de mensaje (puede ser: Indicación global, indicación parcial, indicación de consulta, y mensaje de unión VTP), manejo de longitud de dominio, y manejo de nombre de dominio. El número de revisión de configuración es de 32 bits, e indica el nivel de revisión de paquetes VTP, cada dispositivo almacena este número, el paquete contiene el número del transmisor, esta información es utilizada para determinar si la información recibida es más reciente que la información actual, cada vez que se realiza algún cambio en algún dispositivo dentro del dominio VTP, este número aumenta en uno, para resetear este número basta con cambiar el nombre al dominio VTP y luego volver al nombre original.

Las indicaciones globales suceden cada 5 minutos, e informan a switches adyacentes, el nombre del dominio VTP y el número de revisión de configuración, el dispositivo al recibir este paquete compara el nombre actual del dominio con el que contiene el paquete si son diferentes, simplemente lo ignora, si son iguales, revisa el número de revisión de configuración, si es mayor al guardado, el switch sobrescribe la información guardada con la información actual.

Si se ha añadido VLAN, o se ha hecho algún cambio con las existentes, el servidor VTP, donde los cambios se han realizado aumenta el número de revisión de configuración y se envía indicaciones globales y parciales (las cuales contienen información de las VLAN).

VTP V2 brinda soporte para VLAN en Token Ring, para configurar una clave VTP, se necesita configurar en todos los switches del dominio VTP, y debe de ser la misma, y se utiliza un algoritmo en una palabra de 16 bytes (con valor MD5), y es transportada en paquetes de indicación global, Por defecto, los dominios de administración se establecen en modo no seguro.

característica	servidor	cliente	transparente
mensajes VTP origen	SI	SI	NO
escuchar mensajes VTP	SI	SI	NO
crear las VLAN	SI	NO	SI(local)
recordar las VLAN	SI	NO	SI(local)

Figura A.2 Característica de switches dentro de dominio VTP.

Clasificación

Los **servidores VTP** pueden crear, modificar y eliminar la VLAN y los parámetros de configuración de VLAN de todo un dominio. Los servidores VTP guardan la información de la configuración VLAN en la NVRAM del switch. Los servidores VTP envían mensajes VTP a través de todos los puertos de enlace troncal.

Los **clientes VTP** no pueden crear, modificar ni eliminar la información de VLAN. Este modo es útil para los switches que carecen de memoria suficiente como para guardar grandes tablas de información de VLAN. El único rol de los clientes VTP es procesar los cambios de VLAN y enviar mensajes VTP desde todos los puertos troncales.

Los switches en modo **VTP transparente** envían publicaciones VTP pero ignoran la información que contiene el mensaje. Un switch transparente no modifica su base de datos cuando se reciben actualizaciones o envían una actualización que indica que se ha producido un cambio en el estado de la VLAN. Salvo en el caso de envío de publicaciones VTP, VTP se desactiva en un switch transparente.

Comandos

Para acceder a la configuración del protocolo VTP se debe entrar donde se configuran la VLAN:

```
switch # vlan database
```

Luego se escoge la versión del VTP a implementar con:

```
Vtp version [ 1 / 2 ]
```

Basta con poner la palabra **no** delante del anterior comando para deshabilitar la acción del mismo.
Luego se escoge el modo que va a trabajar el switch, hay tres modos, como ya los detallamos anteriormente.

```
Vtp mode [ server / client / transparent ]
```

Para monitorear la operación y estado de VTP se emplean los comandos:

```
Show vtp status

Show vtp counters
```

Concepto de Spanning – Tree

Spanning-tree (protocolo de la IEEE 802.1D) se encarga de detectar el puerto raíz, bloquear puertos, y que los puertos reciban BPDUS (Bridge Protocol Data Unit), los paquetes BPDUs contienen información acerca de puertos, direcciones, prioridades y costos, los puentes no siguen a los BPDUs, es más esta información genera nuevos BPDUs, los BPDUs contienen la siguiente información:

- BID de la raíz: el BID (Bridge ID) del puente que el puente transmisor cree es el puente raíz.
- Costo del camino: El costo del camino para alcanzar al puente raíz, si el segmento es juntado al puente raíz, tiene el costo de 0.
- BID del transmisor: el BID del puente que envía este BPDU.
- ID del puerto: el ID del puerto en el puente que envía este BPDU.

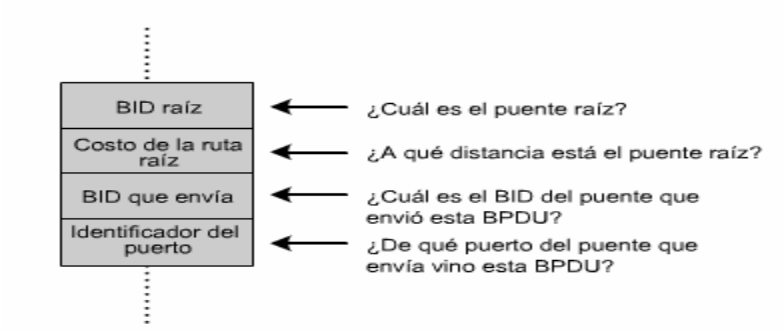

Figura A.3 Estructura del BPDU

STP(Spanning-Tree Protocol) es un protocolo de capa 2 que provee caminos con redundancia, mientras previene lazos indeseables en la red, para que una red ethernet funcione correctamente, debe de existir solamente un camino entre dos estaciones. Se debe de establecer una topología libre de lazos llamada spanning-tree, la operación de spanning-tree es transparente para los usuarios, los cuales no detectan si están conectados a un solo segmento o varios segmentos.

Cuando se diseña redes tolerantes a fallas, se debe de tener un camino libre de lazos a través de una red conmutada, múltiples caminos activos causan lazos en la red, si existiesen lazos, los usuarios recibirían tramas duplicadas y las interfases de los switches tendrían repetidas direcciones MAC. Spanning-tree define un árbol con un switch como raíz y un camino libre de lazos desde la raíz a todos los switches de la red, este protocolo forza a caminos redundantes a pasar a estados bloqueados, si un segmento de red falla y un camino redundante existe, el spanning-tree recalcula la topología y activa el camino que estaba bloqueado, cuando dos puertos en el mismo switch son partes de un lazo, la prioridad del puerto establecida por spanning-tree y el costo del camino establecen cual pasa a estado de bloqueado, en otras palabras cual no transmite, el valor de prioridad representa la ubicación del puerto dentro de la topología y que tanto tráfico pasa por éste, el costo del camino es representado por la velocidad del medio.
Todos los switches participan dando información acerca de otros switches en la red, por el intercambio de BPDUs, provocando:

- La elección de un único switch raíz para todo momento del spanning-tree
- La elección de un switch designado para cada segmento de LAN
- La eliminación de lazos en redes conmutadas, bloqueando puerto conectados a enlaces redundantes.

Los estados de los puertos en una topología STP son:

- Bloqueado
- Escuchando
- Aprendizaje
- Envío
- Deshabilitado

Estado Bloqueado: no participa en el envío de paquetes, descarta todo paquete, cuando un switch es encendido todos los puertos están en este estado

Estado Escuchando: Es el primer estado transiente, después del estado de bloqueo, los puertos entran en este estado cuando STP determina que puertos deben de participar en el envío de tramas.

Estado de Aprendizaje: En este estado se prepara para el envío de tramas.

Estado de Envío: Participa en el envío de tramas.

Estado Deshabilitado: No participa en el método STP, los puertos no hacen nada.

APENDICE B

Salidas de los equipos configurados en el capítulo 3.

Salidas del SwitchServ:

A continuación mostramos las salidas que brindan los comandos ***show*** en el SwitchServ, estos sirven para verificar la correcta configuración de los equipos:

SwitchServ#show vlan.- muestra las vlan creadas, e indica los puertos que hemos asignado a estas VLAN (ver negrillas)

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/8, Fa0/9, Fa0/10
Fa0/11, Fa0/12, Fa0/13, Fa0/14
Fa0/15, Fa0/16, Fa0/17, Fa0/18
Fa0/19, Fa0/20, Fa0/21, Fa0/22
Fa0/23, Fa0/24
2    alumnos                           active    Fa0/2, Fa0/3
3    administracion                    active    Fa0/4, Fa0/5
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1
Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    srb      0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1
Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type           Ports
------- --------- ---------------- ------------------------------------------
```

SwitchServ#show spanning-tree.- Nos muestra los costos de los puertos y el switch raíz del protocolo Spanning-Tree, hay que recordar que esto nos ayuda para eliminar lazos físicos.

```
VLAN0001
Spanning tree enabled protocol ieee
Root ID    Priority    32769
Address     000b.4638.5b00
Cost        19
Port        7 (FastEthernet0/7)
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
Address     000b.46f0.f4c0
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time 300
Interface        Role Sts Cost      Prio.Nbr Type
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/7            Root FWD 19        128.7    P2p
VLAN0002
Spanning tree enabled protocol ieee
Root ID    Priority    32770
Address     000b.4638.5b00
Cost        19
Port        7 (FastEthernet0/7)
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID  Priority    32770  (priority 32768 sys-id-ext 2)
Address     000b.46f0.f4c0
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time 300
Interface        Role Sts Cost      Prio.Nbr Type
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/7            Root FWD 19        128.7    P2p
VLAN0003
Spanning tree enabled protocol ieee
Root ID    Priority    32771
Address     000b.4638.5b00
Cost        19
Port        7 (FastEthernet0/7)
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID  Priority    32771  (priority 32768 sys-id-
ext 3)
Address     000b.46f0.f4c0
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time 300
Interface        Role Sts Cost      Prio.Nbr Type
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/7            Root FWD 19        128.7    P2p
```

El comando ***show start-config*** nos muestra la configuración almacenada en la NVRAM, también podemos ver los puertos asignados al Trunking, y las características de todos los puerto del switch, este comando también es válido en routers.

```
interface FastEthernet0/2
switchport access vlan 2
switchport mode access
interface FastEthernet0/3
switchport access vlan 2
switchport mode access
interface FastEthernet0/4
switchport access vlan 3
switchport mode access
interface FastEthernet0/5
switchport access vlan 3
switchport mode access
interface FastEthernet0/6
switchport mode trunk
interface FastEthernet0/7
switchport mode trunk
interface FastEthernet0/8
switchport mode trunk
speed 100
duplex full
```

```
interface Vlan1
ip address 172.16.2.2 255.255.254.0
no ip route-cache
ip default-gateway 172.16.2.1
ip http server
line con 0
password cisco
login
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
```

Salidas de SwitchAdmin:
A continuación mostramos la configuración del SwitchAdmin gracias a la ayuda de los comandos ***show***.
SwitchAdmin#show interface vlan 1.- Nos muestra la dirección IP asignada al SwitchAdmin.

```
Vlan1 is up, line protocol is up
Hardware is CPU Interface, address is 000f.f71d.5e80 (bia 000f.f71d.5e80)
Internet address is 172.16.2.3/23
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:35:12, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
```

```
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 2000 bits/sec, 4 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
93036 packets input, 6196031 bytes, 0 no buffer
Received 1171 broadcasts (0 IP multicast)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 575 ignored
8187 packets output, 3389004 bytes, 0 underruns
0 output errors, 4 interface resets
0 output buffer failures, 0 output buffers swapped out
```

Salidas del SwitchComput:

A continuación mostramos la configuración del SwitchComput gracias a la ayuda de los comandos ***show***:

SwitchComput#show int vlan 1. - Podemos visualizar la dirección IP asignada al switch.

```
Vlan1 is up, line protocol is up
Hardware is CPU Interface, address is 000b.4638.5b00 (bia 000b.4638.5b00)
Internet address is 172.16.2.4/23
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:52:04, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 4000 bits/sec, 5 packets/sec
3376 packets input, 512429 bytes, 0 no buffer
Received 570 broadcasts (0 IP multicast)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
105997 packets output, 6553350 bytes, 0 underruns
0 output errors, 4 interface resets
0 output buffer failures, 0 output buffers swapped out
```

APENDICE C

Salidas mostradas por los equipos configurados en el capítulo 4.

Pruebas de conectividad dentro de la red con RIP V1.

Show ip protocols nos muestra el protocolo de enrutamiento que en estos momentos esta soportando el router, a continuación mostramos las salidas en el RouterTrunk, el que nos permite la conectividad InterVLAN, tanto en el envío como recepción de paquetes la versión del protocolo es RIP V1.

```
RouterTrunk#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 26 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
 Default version control: send version 1, receive version 1
    Interface          Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/0.1  1     1 2
    FastEthernet0/0.2  1     1 2
    FastEthernet0/0.3  1     1 2
    Serial0/0          1     1 2
  Automatic network summarization is in
effect
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.10.2          120      00:03:03
  Distance: (default is 120)
```

Show interface nos muestra direcciones IP asignadas a las interfases, modos de transmisión de ellas, paquetes transmitidos, perdidos, paquetes en el buffer de espera, y otras características más.

```
RouterTrunk#show int
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 000c.ceba.b300 (bia 000c.ceba.b300)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
```

```
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     9403 packets input, 697203 bytes
     Received 7620 broadcasts, 0 runts, 0 giants, 0
throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     2927 packets output, 254564 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     0 babbles, 0 late collision, 0 deferred
     10 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
FastEthernet0/0.1 is up, line protocol is up
  Hardware is AmdFE, address is 000c.ceba.b300 (bia 000c.ceba.b300)
  Internet address is 172.16.2.1/23
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1.
  ARP type: ARPA, ARP Timeout 04:00:00
  Last clearing of "show interface" counters never
FastEthernet0/0.2 is up, line protocol is up
  Hardware is AmdFE, address is 000c.ceba.b300 (bia 000c.ceba.b300)
  Internet address is 172.16.4.1/23
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  2.
  ARP type: ARPA, ARP Timeout 04:00:00
  Last clearing of "show interface" counters never
FastEthernet0/0.3 is up, line protocol is up
  Hardware is AmdFE, address is 000c.ceba.b300 (bia 000c.ceba.b300)
  Internet address is 172.16.6.1/23
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  3.
  ARP type: ARPA, ARP Timeout 04:00:00
  Last clearing of "show interface" counters never
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 172.16.10.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
```

```
  Last input 00:00:00, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/2/32 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 96 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     847 packets input, 58128 bytes, 0 no buffer
     Received 473 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     849 packets output, 59691 bytes, 0 underruns
     0 output errors, 0 collisions, 21 interface resets
     0 output buffer failures, 0 output buffers swapped out
     5 carrier transitions   DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Al activar el comando ***debug ip rip events*** nos damos cuenta que las actualizaciones en el enlace serial no se están efectuando, esto es debido que RIP V1 no soporta **VLSM**, **suppressing null update** nos indica que no se están dando las actualizaciones**,** por la interfaz serial que tiene IP **172.16.10.1.**

```
RouterTrunk#debug ip rip events
RIP event debugging is on
*Mar  1 07:05:01.043: RIP: sending v1 update to 255.255.255.255
via Serial0/0 (172.16.10.1) - suppressing null update
*Mar  1 07:05:02.971: RIP: sending v1 update to 255.255.255.255
via FastEthernet 0/0.1 (172.16.2.1)
*Mar  1 07:05:02.971: RIP: Update contains 2 routes
*Mar  1 07:05:02.971: RIP: Update queued
*Mar  1 07:05:02.971: RIP: Update sent via
FastEthernet0/0.1
*Mar  1 07:05:16.515: RIP: sending v1 update to 255.255.255.255
via FastEthernet 0/0.2 (172.16.4.1)
*Mar  1 07:05:16.515: RIP: Update contains 2 routes
*Mar  1 07:05:16.515: RIP: Update queued
*Mar  1 07:05:16.515: RIP: Update sent via
FastEthernet0/0.2
*Mar  1 07:05:21.991: RIP: sending v1 update to 255.255.255.255
via FastEthernet 0/0.3 (172.16.6.1)
*Mar  1 07:05:21.991: RIP: Update contains 2 routes
*Mar  1 07:05:21.991: RIP: Update queued
*Mar  1 07:05:21.991: RIP: Update sent via
FastEthernet0/0.3
*Mar  1 07:05:29.783: RIP: sending v1 update to 255.255.255.255
via Serial 0/0 (172.16.10.1) - suppressing null update
```

Distintos Ping desde la consola del SwitchComput a varios puntos de la red.
(**!!!!!!** Significa que obtenemos respuesta del ping, y **U.U.U** significa que no logramos llegar)

Ping a SwitchAdmin
SwitchComput#ping 172.16.2.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
Ping a si mismo
SwitchComput#ping 172.16.2.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
Ping a SwitchServ
SwitchComput#ping 172.16.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Ping a subinterface 1 de fastethernet 0/0 de RouterTrunk
SwitchComput#ping 172.16.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1000 ms
Ping a interface serial 0/0 de RouterTrunk
SwitchComput#ping 172.16.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Ping a interface serial 0/0 de RouterRemoto y falla
Esto sucede porque RIP V1 no soporta VLSM y no propaga rutas aprendidas
SwitchComput#ping 172.16.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Ping a interface fastethernet 0/0 de RouterRemoto y falla
Esto sucede porque RIP V1 no soporta VLSM y no propaga rutas aprendidas
SwitchComput#ping 172.16.8.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.8.1, timeout is 2 seconds:
U.U.U

Pruebas de conectividad dentro de la red con IGRP

Con el comando ***show ip protocols*** podemos verificar que el comando de enrutamiento validos es **igrp**, y que el sistema autónomo es **101**, como también el número de saltos por defecto y que las métricas validas por defecto son: Ancho de banda y retardo.

```
RouterTrunk#show ip protocols
Routing Protocol is igrp 101
  Sending updates every 90 seconds, next due in 55 seconds
  Invalid after 270 seconds, hold down 280, flushed after 360
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
 Default networks accepted from incoming updates
IGRP metric weight  k1=1,k2=0,k3=1,k4=0,k5=0
IGRP maximum hopcount 100
IGRP maximum metric variance 1
Redistributing igrp 300
Routing for Networks:
172.16.0.0
Routing information sources
Gateway         Distance          Last Update
172.16.2.1          100               0:0:52
Distance: (default is 100 )
```

Si existiese problemas de conectividad los, comandos ***Debug***, son muy útiles y se puede apreciar que se envían las actualizaciones vía Fastethernet tipo broadcast (255.255.255.25) y que a través del enlace serial no se están efectuando las actualizaciones, y esto es debido que IGRP no soporta VLSM.

```
RouterRemoto# debug ip igrp events
IGRP event debugging is on
00:21:38: IGRP: sending update to 255.255.255.255
via Fastethernet 0/0 (172.16.8.1)
00:21:38: IGRP:Update contains 0 interior, 2 system, and 0
exterior routes
00:21:38:IGRP: Total routes in update:
2
00:21:38:IGRP: sending update to 255.255.255.255
via Serial0/0 (172.16.10.2)
00:21:38:IGRP:Update contains 0 interior, 1 system, and 0
exterior routes
00:21:38:IGRP: Total routes in
update: 0
```

Pruebas de conectividad dentro de la red con RIP V2

Ahora desde la consola del RouterTrunk le hacemos ***ping*** a un host de la red remota **172.16.8.0**, y obtenemos resultados positivos, esto es debido que **RIP V2** si propaga rutas con distintas mascaras, es decir si soporta **VLSM**, permitiendo conocer al RouterTrunk dé de la existencia de la red **172.16.8.0** conectada en la interfaz fastethernet 0/0 del RouterRemoto y permitiendo conocer al RouterRemoto la existencia de las VLANS troncalizadas:

```
RouterTrunk#ping 172.16.8.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.8.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32
ms
```

Observemos el contenido del comando ***show ip route*** en los routers, y nos damos cuenta de una nueva ruta aprendida, esta ruta no se la aprendió ni con **RIP V1** ni con **IGRP**, esto es debido que ellos al no soportar VLSM, no había actualizaciones en el enlace serial, por ende las rutas aprendidas no se propagaban entre los routers. En el RouterTrunk la ruta con **"R"** nos indica que la aprendió mediante el protocolo de enrutamiento RIP V2 a través de la IP **172.16.10.2** que es la serial 0/0 del RouterRemoto que esta conectada al serial 0/0 del RouterTrunk.

```
RouterTrunk#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
    172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
R      172.16.8.0/23 [120/1] via 172.16.10.2, 00:00:06, Serial0/0
C      172.16.10.0/30 is directly connected, Serial0/0
C      172.16.4.0/23 is directly connected, FastEthernet0/0.2
C      172.16.6.0/23 is directly connected, FastEthernet0/0.3
C      172.16.2.0/23 is directly connected, FastEthernet0/0.1
```

Podemos ver como se ejecutan las actualizaciones periódicas del protocolo **RIP V2** mediante el comando ***Debug***, viendo un resultado positivo en las actualizaciones de la interfase serial 0/0, es decir las actualizaciones si son propagadas a través del interfaz serial, las actualizaciones son enviadas a una

dirección multicast **224.0.0.9**, el enlace serial si se actualiza esto ocurre porque **RIPV2** si soporta **VLSM**.

RIP event debugging is on
***Mar 1 07:24:11.099: RIP: sending v2 update to 224.0.0.9 via Serial0/0 (172.16.10.1)**
*Mar 1 07:24:11.099: RIP: Update contains 3 routes
*Mar 1 07:24:11.099: RIP: Update queued
*Mar 1 07:24:11.099: RIP: **Update sent via Serial0/0**
*Mar 1 07:24:13.127: RIP: sending v2 update to 224.0.0.9 via FastEthernet0/0.3 (172.16.6.1)
*Mar 1 07:24:13.127: RIP: Update contains 4 routes
*Mar 1 07:24:13.127: RIP: Update queued
*Mar 1 07:24:13.127: RIP: Update sent via FastEthernet0/0.3
*Mar 1 07:24:19.119: RIP: sending v2 update to 224.0.0.9 via FastEthernet0/0.2 (172.16.4.1)
*Mar 1 07:24:19.119: RIP: Update contains 4 routes
*Mar 1 07:24:19.119: RIP: Update queued
*Mar 1 07:24:19.119: RIP: Update sent via FastEthernet0/0.2
***Mar 1 07:24:32.635: RIP: received v2 update from 172.16.10.2 on Serial0/0**
*Mar 1 07:24:32.635: RIP: Update contains 1 routes
*Mar 1 07:24:34.471: RIP: sending v2 update to 224.0.0.9 via FastEthernet0/0.1 (172.16.2.1)
*Mar 1 07:24:34.471: RIP: Update contains 4 routes
*Mar 1 07:24:34.471: RIP: Update queued
*Mar 1 07:24:34.471: RIP: Update sent via FastEthernet0/0.1
***Mar 1 07:24:37.571: RIP: sending v2 update to 224.0.0.9 via Serial0/0 (172.16.10.1)**

Pruebas de conectividad dentro de la red con EIGRP.

Podemos apreciar que el protocolo que está soportando el router RouterRemoto es **EIGRP**, y el sistema autónomo es **101**, y que las métricas por defecto son ancho de banda y Retardo, también podemos ver el costo de la distancia interna (**90**), Y la externa (**170**), todo esto por medio del comando ***show ip protocol.***

```
RouterRemoto#sh  ip prot
Routing Protocol is "eigrp 101"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 101
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.10.1           90      00:00:24
  Distance: internal 90 external 170
```

show ip eigrp topology, podemos ver que RouterRemoto tiene como Feasible sucesor al RouterTrunk.

```
RouterRemoto#sh ip eigrp topology
IP-EIGRP Topology Table for AS(101)/ID(172.16.10.2)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 172.16.8.0/23, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 172.16.10.0/30, 1 successors, FD is 557568
         via Connected, Serial0/0
P 172.16.4.0/23, 1 successors, FD is 560128
         via 172.16.10.1 (560128/28160), Serial0/0
P 172.16.6.0/23, 1 successors, FD is 560128
         via 172.16.10.1 (560128/28160), Serial0/0
P 172.16.2.0/23, 1 successors, FD is 560128
         via 172.16.10.1 (560128/28160), Serial0/0
```

Distintos Ping desde la consola del SwitchComput a varios puntos de la red.

Esto sucede porque EIGRP soporta VLSM y propaga las rutas aprendidas.
SwitchComput#ping 172.16.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Ping a interface fastethernet 0/0 de RouterRemoto y llegamos con éxito.
Esto sucede porque EIGRP soporta VLSM y propaga las rutas aprendidas.
SwitchComput#ping 172.16.8.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.8.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Por medio de los distintos comandos que se derivan de ***debug***, nos permite entender como la red se esta comportando, podemos ver que **EIGRP** envía paquetes **HELLO (**como lo vimos en el **capitulo 2** de esta tesis en la parte teórica de **EIGRP)** para mantener un contacto permanente con los routers vecinos y también apreciamos el listado de todos los paquetes que EIGRP maneja para mantener sus tablas actualizadas para una rápida convergencia ante cualquier cambio topológico súbito.

RouterRemoto#debug eigrp pack
EIGRP Packets debugging is on
(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK,
STUB, SIAQUERY, SIAREPLY)
01:50:11: EIGRP: Sending HELLO on Serial0/0
01:50:11: AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
01:50:13: EIGRP: Received HELLO on Serial0/0 nbr 172.16.10.1
01:50:13: AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely
01:50:13: EIGRP: Sending HELLO on FastEthernet0/0
01:50:13: AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
01:50:15: EIGRP: Sending HELLO on Serial0/0
01:50:15: AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
01:50:18: EIGRP: Received HELLO on Serial0/0 nbr 172.16.10.1
01:50:18: AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely
01:50:18: EIGRP: Sending HELLO on FastEthernet0/0
01:50:18: AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
01:50:20: EIGRP: Sending HELLO on Serial0/0
01:50:20: AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
01:50:22: EIGRP: Received HELLO on Serial0/0 nbr 172.16.10.1
01:50:22: AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely

Salidas con la implementación de ACLS (con el protocolo EIGRP).

Salidas mostradas desde RouterTrunk.

Con la ayuda del comando ***show access-lists***, podemos apreciar cuantas listas de acceso han sido creadas, y el tipo de listas presentes.

```
RouterTrunk#sh access-lists
Standard IP access list 2
    10 permit 172.16.2.0, wildcard bits 0.0.0.255
    20 deny   any
Standard IP access list 3
    10 permit 172.16.2.0, wildcard bits 0.0.1.255
    20 deny   any
Standard IP access list 4
    10 permit 172.16.6.0, wildcard bits 0.0.1.255
    20 deny   any
```

Gracias al comando ***show running-config,*** podemos ver en que interfases están siendo aplicadas las ACLS, podemos apreciar que en las subinterfases 1 y 3 del router RouterTrunk y en la Terminal virtual también las estamos aplicando.

```
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 172.16.2.1 255.255.254.0
 ip access-group 3 in
 no snmp trap link-status
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 172.16.4.1 255.255.254.0
 no snmp trap link-status
interface FastEthernet0/0.3
 encapsulation dot1Q 3
ip address 172.16.6.1 255.255.254.0
 ip access-group 4 in
 no snmp trap link-status
interface Serial0/0
 ip address 172.16.10.1 255.255.255.252
 clockrate 56000
interface Serial0/1
 no ip address
 shutdown
router rip
 network 172.16.0.0
ip classless
ip http server
```

```
no ip http secure-server
access-list 2 permit 172.16.2.0 0.0.0.255
access-list 2 deny   any
access-list 3 permit 172.16.2.0 0.0.1.255
access-list 3 deny   any
access-list 4 permit 172.16.6.0 0.0.1.255
access-list 4 deny   any
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 access-class 2 in
 password cisco
 login
!
end
```

Como en las sentencias de las ACLS, indicamos que solo los usuarios de la VLAN 1 pueden acceder virtualmente a cualquiera de los dos routers, eso es lo que comprobamos en la figura **4.8** donde mostramos el éxito de acceder remotamente a RouterRemoto, y en la figura **4.9** mostramos el éxito de acceder al Terminal virtual del RouterTrunk.

```
User Access Verification

Password:
RouterRemoto>
RouterRemoto>
RouterRemoto>
RouterRemoto>enable
Password:
RouterRemoto#
RouterRemoto#
```

Figura C.7 Sesión Telnet positiva desde VLAN 1

```
User Access Verification
Password:
RouterTrunk>
RouterTrunk>
RouterTrunk>enable
Password:
RouterTrunk#
RouterTrunk#
```

Figura C.8 Telnet desde VLAN 1 al RouterTrunk

APENDICE D

Pruebas de redundancia

Pruebas en la red con EIGRP y Etherchannel

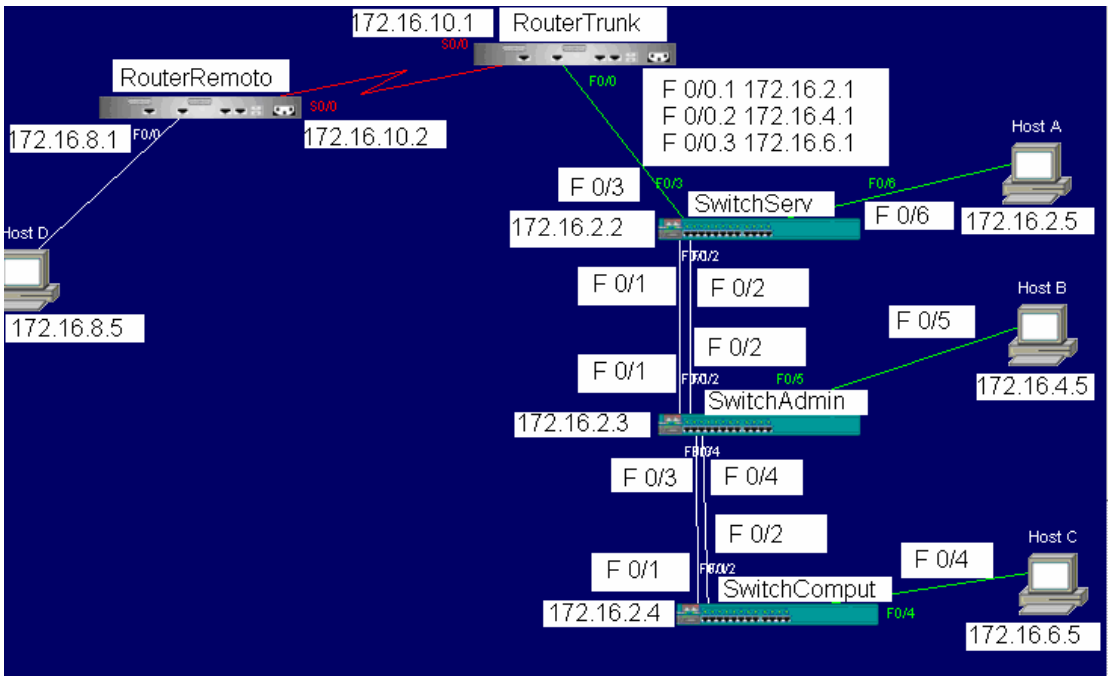

Figura D.1 Red para las pruebas con Etherchannel.

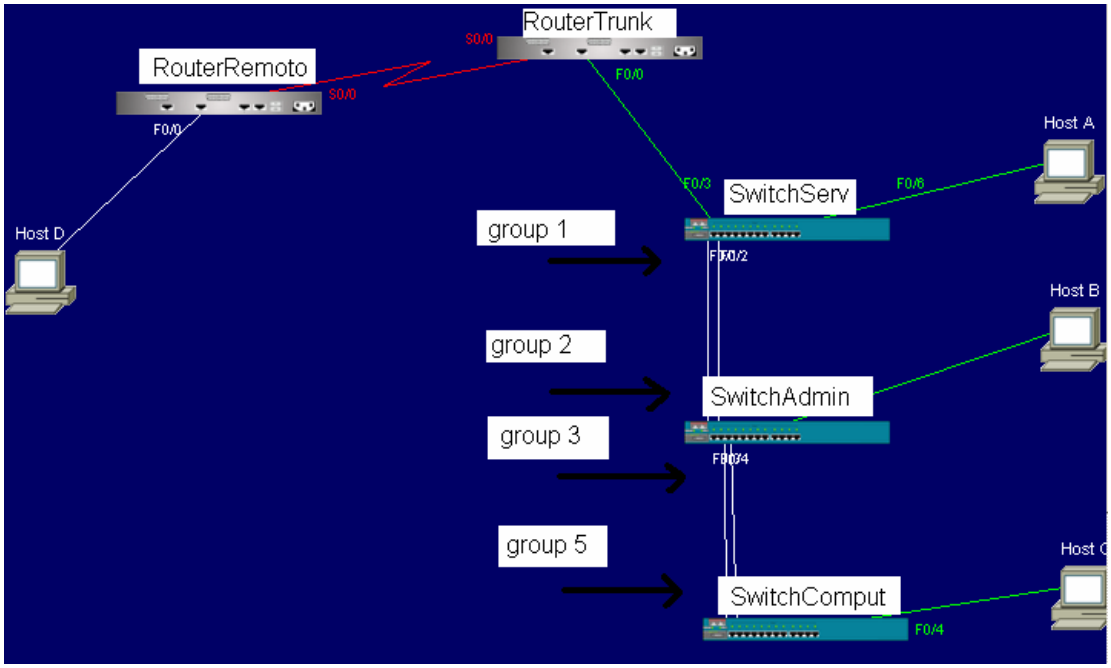

Figura D.2 Puertos que forman parte de los grupos.

El protocolo de enrutamiento en los routers es EIGRP, la configuración en los routers con EIGRP la vimos en la parte 4.1.4 del capitulo 4, la dirección de red y l as direcciones IP en el enlace serial son las mismas, la red remota tiene la misma dirección, al igual que los hosts A, B, C y D como lo vimos en el capítulo 3, las subinterfases de RouterTrunk tienen la misma dirección y maneja las mismas VLAN, por último las direcciones IP en los switches no ha cambiado. Solo se probó en los switches, porque los routers no soportan Etherchannel.

Etherchannel consiste en unir enlaces individuales en un solo enlace lógico, se puede crear un Etherchannel para interfases de capa 2 como también para interfases de capa 3, existen dos protocolos para implementar esta característica tanto en switches como en routers: **PApG**(Port Aggregation Protocol), que es el que implementamos en nuestra red, usando **PApG**, el switch aprende a identificar a sus vecinos, que puedan soportar **PApG**, éste luego agrupa dinámicamente interfases similarmente configuradas en un sólo enlace lógico, éstas interfases son agrupadas basadas en parámetros administrativos y de hardware como: misma velocidad, mismo protocolo de Trunking, misma VLAN, etc. Luego de agrupar a las interfases en un sólo enlace lógico añade al grupo al protocolo Spanning-Tree, como un sólo puerto de switch. El otro protocolo es **LAcP**(Link Aggregation Control Protocolo), ambos son definidos en el estándar IEEE 802.3ad.

A la red se le realizaron los siguientes cambios:

Configuración de SwitchServ para que soporte Etherchannel.

Los puertos 1,2, y 3 fueron configurados para que soporten comunicación Trunking, adicional los puertos 1 y 2 soportan Etherchannel, el puerto 4 se le asignó a VLAN 2, el puerto 5 se le asignó a VLAN 3, y el resto de puertos por defecto pertenecen a VLAN 1, de no asignársele a ninguna VLAN. Los puertos 1 y 2 se conectan a SwitchAdmin y pertenecen a channel-group 1, y el puerto 3 se conecta a la Fastethernet 0/0 de RouterTrunk.

Configuración de los puertos 1, 2 y 3 para comunicación Trunking, los puertos 1 y 2 pertenecen a channel-group 1.

```
SwitchServ(config)#int fast 0/1
SwitchServ(config-if)#switchport mode trunk
SwitchServ(config-if)#channel-group 1 mode desirable

SwitchServ(config-if)#no shut
SwitchServ(config-if)#exit
SwitchServ(config)#int fast 0/2
SwitchServ(config-if)#switchport mode trunk
SwitchServ(config-if)#channel-group 1 mode desirable


SwitchServ(config-if)#no shut
SwitchServ(config-if)#exit
SwitchServ(config)#int fast 0/3
SwitchServ(config-if)#switchport mode trunk
SwitchServ(config-if)#no shut
SwitchServ(config-if)#exit
```

Configuración del Puerto 4 para VLAN 2.

```
SwitchTrunk(config)#int fast 0/4
SwitchTrunk(config-if)#switchport mode access
SwitchTrunk(config-if)#switchport access vlan 2
SwitchTrunk(config-if)#no shut
SwitchTrunk(config-if)#exit
```

Configuración del Puerto 5 para VLAN 3

```
SwitchTrunk(config)#int fast 0/5
SwitchTrunk(config-if)#switchport mode access
SwitchTrunk(config-if)#switchport access vlan 3
SwitchTrunk(config-if)#no shut
SwitchTrunk(config-if)#exit
```

Configuración de SwitchAdmin para que soporte Etherchannel.

Los puertos 1 y 2 están conectados con SwitchServ y pertenecen a channel-group 2, los puertos 3 y 4 están conectados a SwitchComput y pertenecen a channel-group 3. El puerto 5 se le asignó a VLAN 2, el puerto 6 se le asignó a VLAN 3, el resto de puertos al no ser asignados a una VLAN, por defecto pertenecen a VLAN 1. Los comandos para los puertos 1 y 2 son los mismos que se aplicaron para SwitchServ (puertos 1 y 2), y sólo difieren en el número de channel-group, lo mismo ocurre con los puerto 3 y 4, los comandos para el puerto 5 son los mismos que se configuraron en SwitchServ (puerto 4), y en el puerto 6 son los mismos comandos que se configuraron en SwitchServ (puerto 5).

Configuración de SwitchComput para que soporte Etherchannel.

Los puertos 1 y 2 están directamente conectados a SwitchAdmin y pertenecen a channel-group 5, el puerto 3 se le asignó a VLAN 2, el puerto 4 se le asignó a VLAN 3, y el resto de puertos pertenecen a VLAN 1, al no ser asignados a ninguna VLAN.
La configuración en los puertos 1 y 2 es la misma que en SwitchServ con respecto a los puertos 1 y 2, sólo difieren del channel-group, el puerto 3 tiene la misma configuración que el puerto de VLAN 2 en el SwitchServ, y el puerto 4 tiene la misma configuración que el puerto de VLAN 2 en SwitchServ.

Salidas de los switches

Salida de SwitchServ.

Con el comando ***Show cdp neighbor*** aplicado a SwitchServ podemos apreciar que se conecta a RouterTrunk por el puerto **3**, y que se conecta a SwitchAdmin por dos puertos: **1** y **2**. El comando CDP que lo vimos en el capítulo 1 es propietario de **CISCO**, y podemos ver los dispositivos **CISCO** conectados a las interfases.

```
SwitchServ#show cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
RouterTrunk      Fas 0/3           142        R S         2621XM    Fas 0/0.1
SwitchAdmin      Fas 0/2           139        S I         WS-C2950-2Fas 0/2
SwitchAdmin      Fas 0/1           139        S I         WS-C2950-2Fas 0/1
```

Con el comando ***show etherchannel port-channel***, vemos el estado en que se encuentran los puertos que forman parte de algún grupo de Etherchannel, y el tipo de protocolo Etherchannel que está soportando SwitchServ, el cual es **PAgP.**

```
switchServ#show etherchannel port-channel
 Channel-group listing:
Group: 1
            Port-channels in the group:
Port-channel: Po1
Age of the Port-channel   = 0d:00h:47m:13s
Logical slot/port   = 1/0         Number of ports = 2
GC                  = 0x00010001      HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =  PAgP
Ports in the Port-channel:
Index   Load   Port     EC state        No of bits
  0     00     Fa0/1    Desirable-Sl      0
  0     00     Fa0/2    Desirable-Sl      0
Time since last port bundled:    0d:00h:45m:28s    Fa0/2
```

Si el cable conectado al Puerto 1 que enlaza a SwitchServ con SwitchAdmin sufre algún desperfecto y el enlace se cae, por consola se muestra:

```
01:04:12: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, chang
ed state to down
01:04:13: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
```

Con el comando ***show etherchannel 1 port-channel***, vemos que sólo el

Puerto **2,** pertenece a channel-group 1, como era de esperarse, debido que el enlace en el puerto **1** falló.

```
SwitchServ#sh etherchannel 1 port-channel
            Port-channels in the group:
            ---------------------------
Port-channel: Po1
Age of the Port-channel   = 0d:01h:09m:01s
Logical slot/port   = 1/0         Number of ports = 1
GC                = 0x00010001      HotStandBy port = null
Port state         = Port-channel Ag-Inuse
Protocol           =   PAgP
Ports in the Port-channel:
Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
 0     00     Fa0/2    Desirable-Sl      0
Time since last port bundled:    0d:01h:07m:16s    Fa0/2
Time since last port Un-bundled: 0d:00h:14m:28s    Fa0/1
```

Salida de SwitchAdmin

Con el comando ***Show etherchannel port-channel***, vemos que en SwitchAdmin se han creado dos Channel-Group (2 y 3) y vemos los puertos miembros de cada grupo.

```
show etherchannel port-channel
  Channel-group listing:
Group: 2
            Port-channels in the group:
Port-channel: Po2
Age of the Port-channel   = 0d:01h:41m:06s
Logical slot/port   = 1/0         Number of ports = 2
GC                = 0x00020001      HotStandBy port = null
Port state         = Port-channel Ag-Inuse
Protocol           =   PAgP
Ports in the Port-channel:
Index   Load   Port     EC state        No of bits
 0     00     Fa0/1    Desirable-Sl      0
 0     00     Fa0/2    Desirable-Sl      0
Time since last port bundled:    0d:00h:05m:51s    Fa0/1
Time since last port Un-bundled: 0d:00h:22m:29s    Fa0/1
```

```
Group 3
Age of the Port-channel   = 0d:01h:33m:48s
Logical slot/port   = 1/1         Number of ports = 2
```

```
GC              = 0x00030001      HotStandBy port = null
Port state      = Port-channel Ag-Inuse
Protocol        =  PAgP
Ports in the Port-channel:
 0    00    Fa0/3    Desirable-Sl      0
 0    00    Fa0/4    Desirable-Sl      0
Time since last port bundled:    0d:01h:32m:12s    Fa0/4
```

Con los comandos ***Show run int port-channel 2*** y ***Show run int port-channel 3***, verificamos que están creados los channel-group 2 y 3 respectivamente en SwitchAdmin.

```
SwitchAdmin#show run int port-channel 2
Building configuration...
Current configuration : 76 bytes
interface Port-channel2
 switchport mode trunk
 flowcontrol send off
end
SwitchAdmin#show run int port-channel 3
Building configuration...
Current configuration : 76 bytes
interface Port-channel3
 switchport mode trunk
 flowcontrol send off
end
```

Salida de SwitchComput.

El comando ***show int port-channel 5 etherchannel***, nos muestra todos los puertos que pertenecen a channel-group 5.

```
SwitchComput#sh int port-channel 5 etherchannel
Age of the Port-channel   = 00d:02h:24m:56s
Logical slot/port   = 1/0         Number of ports = 2
GC              = 0x00050001      HotStandBy port = null
Port state      = Port-channel Ag-Inuse
Protocol        =  PAgP
Ports in the Port-channel:
Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
 0    00    Fa0/1    Desirable-Sl    0
 0    00    Fa0/2    Desirable-Sl    0
Time since last port bundled:    00d:00h:05m:16s    Fa0/1
Time since last port Un-bundled: 00d:00h:13m:42s    Fa0/1
```

APENDICE E

Concepto de cableado estructurado.

Un cableado Estructurado es un medio de comunicación físico-pasivo para las redes LAN de cualquier empresa o edificio de oficinas. Con él se busca un medio de transmisión independiente de la aplicación, es decir que no dependa del tipo de red, formato o protocolo de transmisión que se utilice sino que sea flexible a todas estas posibilidades.
El cableado estructurado utiliza topología física estrella con el fin de que todos los puntos de red se concentren y de esta forma poder disponer de un Hub como bus activo y repetidor. Esta topología introduce bastantes ventajas entre las más importantes la administración y el mantenimiento. Aunque la topología física sea estrella, la topología lógica sigue siendo la que indique el protocolo de nivel de enlace, o sea bus para Ethernet y anillo para Token ring. El hub se encarga de definir la topología.

Cables
UTP

Es el cable más utilizado, su nombre se deriva de las iniciales en inglés Unshielded Twisted Pair o sea par trenzado sin pantalla o blindaje De este tipo de cable existen dos presentaciones de acuerdo a la utilización. El UTP rígido o sólido, es el que posee un solo conductor por hilo y se utiliza para el cableado horizontal. El UTP Flexible, se utiliza para los patch cord y presenta más perdidas que el sólido. Está conformado de 4 pares trenzados diferenciados por el código de colores para cables de telefonía así:

Numero del Par	Color
1	Blanco - Azul
2	Blanco - Naranja
3	Blanco - Verde
4	Blanco - Marrón (café)

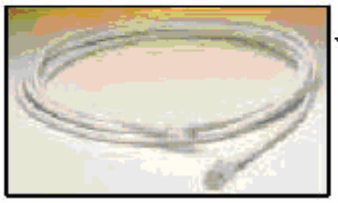

Figura E.1 Gráfico de UTP y código de colores.

STP

Es un cable que a diferencia del UTP posee blindaje (Shielded Twisted Pair) y es de sólo dos pares, su utilización era principalmente para voz, Ethernet 10 baseT y Token Ring, pero con el advenimiento de nuevas aplicaciones que demandaban más velocidad como Ethernet 100 baseT, la cantidad de cables se convirtió en un problema para seguir siendo utilizado, Su blindaje aunque protege los datos de interferencia, cosa que no hace el UTP, presenta mayores pérdidas por las capacitancias parásitas.

ScTP

Este cable poco conocido, es la versión del STP pero de cuatro pares, o sea un UTP con blindaje. El comportamiento eléctrico es el mismo que presenta el STP también se le conoce con el nombre de STP-A. Los cables UTP, STP y ScTP hacen parte de la norma

americana 568-A-5 para cableado estructurado, el siguiente cable FTP hace parte de la norma Europea ISO/IEC 11801.

FTP

Es un cable a cuatro pares blindado, más rígido que el ScTP por la malla que lo recubre parecida al coaxial. Su utilización en América es más bien poca, pero en Europa goza de muy buena aceptación. Posee menor impedancia característica que el cable americano. Su nombre se deriva de las iniciales en inglés Foiled Twisted Pair.

Categoría de cables.

Categoría 5e

Especificada sólo a 100MHz igual que la categoría 5. Especifica los nuevos requisitos de desempeño para cables, conectores canales y enlaces.

NEXT	Mejor NEXT que la categoría 5.
PSNEXT	Nuevo requisito para la categoría 5e
ELFEXT	Nuevo requisito para la categoría 5e
PSELFEXT	Nuevo requisito para la categoría 5e
Pérdida de retorno	Nuevo requisito para la categoría 5e
Atenuación	Igual que la categoría 5.

Figura E.2 Características de categoría 5e.

Diferencias entre categoría 5e y 5.

La Categoría 5e tiene parámetros recientemente especificados de FEXT y pérdida de retorno. De igual manera, tiene mejor NEXT que la categoría 5.El beneficio principal de la categoría 5e es un mejor margen de operación para señales 1000 Base-T.

Diferencias entre categoría 6 y 5e.

La categoría 6 se distingue de la categoría 5e en todos los parámetros especificados en el recuadro siguiente:

Atenuación	Mejor que la categoría 5e
NEXT y PSNEXT	Mejor que la categoría 5e
FEXT, ELFEXT y PSELFEXT	Mejor que la categoría 5e
Pérdida de retorno	Mejor que la categoría 5e

Figura E.3 Diferencias entre categoría 6 y 5e.

Otros elementos:

Jack.

Son los conectores que se utilizan en la salida de telecomunicaciones, en el patch panel y en los equipos activos. Es el conector hembra (DCE) del sistema de cableado. Está compuesto por ocho contactos de tipo deslizante dispuestos en fila y recubiertos por una capa fina de oro de aproximadamente 50um para dar una menor pérdida por reflexión estructural a la hora de operar con el conector macho.

Plug.

Es el conector macho del sistema de cableado estructurado. Su utilización está orientada principalmente hacia los patch cord (cables que une los equipos activos a los patch panel). Posee también ocho contactos y un recubrimiento en oro. Al igual que al jack, el plug se le exige una muy buena calidad en los contactos y en la instalación, ya que es en estos dos elementos donde más problemas se presenta en la puesta en marcha y durante la operación normal de transmisión.

Rack de comunicaciones.

Es un gabinete necesario y recomendado para instalar el path panel y los equipos activos proveedores de servicios. Posee unos soportes para conectar los equipos con una separación estándar de 19". Debe estar provisto de ventiladores y extractores de aire, además de conexiones adecuadas de energía.

Patch panel

Es un arreglo de conectores hembra RJ 45 que se utiliza para realizar conexiones cruzadas (diferente a cable cruzado) entre los equipos activos y el cableado horizontal. Permite un gran manejo y administración de los servicios de la red, ya que cada punto de conexión del patch panel maneja el servicio de una salida de telecomunicaciones.

Path Cord

Son los cables que se arman para interconectar los patch panel con los equipos activos con el equipo del Usuario. Son cables directos (uno a uno) con plug en ambos extremos y hechos con cable UTP flexible por facilidad de manejo. En estos patch cord es donde se presentan la mayoría de fallas de un cableado estructurado. Para todo punto de red se necesitan dos patch cord, uno para el patch panel y otro para el área de trabajo.

NORMA TIA/EIA 569-A

Estándar sobre las prácticas de diseños y construcción específicos los cuales darán soporte a los medios de transmisión y al equipo de telecomunicaciones.

Alcance

Se limita a los aspectos de teIecomunicaciones en el diseño y construcción de edificios comerciales. El estándar no cubre los aspectos de seguridad en el diseño del edificio. Incluye:

- Rutas de cableado Horizontal
- Rutas de cableado Vertical
- Area de Trabajo
- Closet de Telecomunicaciones
- Cuarto de equipos
- Entrada de servicios

Rutas de Cableado horizontal

Facilidades para la instalación del cable desde el closet de telecomunicaciones hasta el área de trabajo, incluye conceptos como: ductos bajo el piso, piso falso, escalerilla para cable, entre otros.

Rutas de cableado Vertical

Conecta la entrada de servicios a los closet de telecomunicaciones, no debe de colocarse en los cubos de los elevadores, y deben estar apropiadamente equipados con bloqueos contra el fuego.

ANSI/TIA/EIA-568-A

Siglas de “Alambrado de Telecomunicaciones para Edificios Comerciales”. Este estándar define un sistema genérico de alambrado de telecomunicaciones para edificios comerciales que puedan soportar un ambiente de productos y proveedores múltiples.

El propósito de este estándar es permitir el diseño e instalación del cableado de telecomunicaciones contando con poca información acerca de los productos de telecomunicaciones que posteriormente se instalarán. La instalación de los sistemas de cableado durante el proceso de instalación y/o remodelación son significativamente más baratos e implican menos interrupciones que después de ocupado el edificio.

La norma ANSI/TIA/EIA-568-A publicada en Octubre de 1995 amplio el uso de UTP y elementos de conexión para aplicaciones LAN de alto rendimiento. La edición de la ANSI/TIA/EIA-568-A integra los Boletines Técnicos de Servicio TSB 36 y TSB 40A los cuales prolongan el uso del UTP en un ancho de banda de hasta 100 MHz. Esto

permite el uso de Modo de Transferencia Asíncrona (ATM), Medio Físico Dependiente del Par Trenzado (TP-PMD), 100Base-Tx y otras 100 Mbps o transmisiones superiores sobre UTP.

Esta norma guía la selección de sistemas de cableado al especificar los requisitos mínimos de sistemas y componentes, y describe los métodos de pruebas de campo necesarios para satisfacer las normas.

Propósito de Estándar EIA/TIA 568-A:

- Establecer un cableado estándar genérico de telecomunicaciones que respaldará un ambiente multiproveedor.
- Permitir la planeación e instalación de un sistema de cableado estructurado para construcciones comerciales.
- Establecer un criterio de ejecución y técnico para varias configuraciones de sistemas de cableado.

TIA/EIA 568-B.2

Detalla las especificaciones de cable categoría 5e.

TIA/EIA 568-B.2-1

Detalla las especificaciones de cable categoría 6.

Test	Cat 5E Spec	Cat 6 Spec	
	100 Mhz	100 Mhz	250 Mhz
Insertion Loss	22.0	19.8	32.8
NEXT	35.3	44.3	38.3
PS-NEXT	32.3	42.3	36.3
EL-FEXT	23.8	27.8	19.8
PS EL-FEXT	20.8	24.8	16.8
Return Loss	20.1	20.1	17.3

Figura E.4 Especificaciones de pruebas realizadas a categorías 5e y 6.

ANEXO A

Tabla completa de direcciones de subred con el rango disponible en cada una de ellas.

número de subred	dirección de subred	rango de direcciones IP disponibles	dirección de broadcast	hosts	hosts útiles
1	172.16.0.0	172.16.0.1------172.16.1.254	172.16.1.255	512	510
2	172.16.2.0	172.16.2.1------172.16.3.254	172.16.3.255	512	510
3	172.16.4.0	172.16.4.1------172.16.5.254	172.16.5.255	512	510
4	172.16.6.0	172.16.6.1------172.16.7.254	172.16.7.255	512	510
5	172.16.8.0	172.16.8.1------172.16.9.254	172.16.9.255	512	510
6	172.16.10.0	172.16.10.1----172.16.11.254	172.16.11.255	512	510
7	172.16.12.0	172.16.12.1----172.16.13.254	172.16.13.255	512	510
8	172.16.14.0	172.16.14.1----172.16.15.254	172.16.15.255	512	510
9	172.16.16.0	172.16.16.1----172.16.17.254	172.16.17.255	512	510
10	172.16.18.0	172.16.18.1----172.16.19.254	172.16.19.255	512	510
11	172.16.20.0	172.16.20.1----172.16.21.254	172.16.21.255	512	510
12	172.16.22.0	172.16.22.1----172.16.23.254	172.16.23.255	512	510
13	172.16.24.0	172.16.24.1----172.16.25.254	172.16.25.255	512	510
14	172.16.26.0	172.16.26.1----172.16.27.254	172.16.27.255	512	510
15	172.16.28.0	172.16.28.1----172.16.28.254	172.16.28.255	512	510
16	172.16.30.0	172.16.30.1----172.16.31.254	172.16.31.255	512	510
17	172.16.32.0	172.16.32.1----172.16.33.254	172.16.33.255	512	510
18	172.16.34.0	172.16.34.1----172.16.35.254	172.16.35.255	512	510
19	172.16.36.0	172.16.36.1----172.16.37.254	172.16.37.255	512	510
20	172.16.38.0	172.16.38.1----172.16.39.254	172.16.39.255	512	510
21	172.16.40.0	172.16.40.1----172.16.41.254	172.16.41.255	512	510
22	172.16.42.0	172.16.42.1----172.16.43.254	172.16.43.255	512	510
23	172.16.44.0	172.16.44.1----172.16.45.254	172.16.45.255	512	510
24	172.16.46.0	172.16.46.1----172.16.47.254	172.16.47.255	512	510
25	172.16.48.0	172.16.48.1----172.16.49.254	172.16.49.255	512	510
26	172.16.50.0	172.16.50.1----172.16.51.254	172.16.51.255	512	510
27	172.16.52.0	172.16.52.1----172.16.53.254	172.16.53.255	512	510
28	172.16.54.0	172.16.54.1----172.16.55.254	172.16.55.255	512	510
29	172.16.56.0	172.16.56.1----172.16.57.254	172.16.57.255	512	510
30	172.16.58.0	172.16.58.1----172.16.59.254	172.16.59.255	512	510
31	172.16.60.0	172.16.60.1----172.16.61.254	172.16.61.255	512	510
32	172.16.62.0	172.16.62.1----172.16.63.254	172.16.63.255	512	510
33	172.16.64.0	172.16.64.1----172.16.65.254	172.16.65.255	512	510
34	172.16.66.0	172.16.66.1----172.16.67.254	172.16.67.255	512	510
35	172.16.68.0	172.16.68.1----172.16.69.254	172.16.69.255	512	510
36	172.16.70.0	172.16.70.1----172.16.71.254	172.16.71.255	512	510
37	172.16.72.0	172.16.72.1----172.16.73.254	172.16.73.255	512	510
38	172.16.74.0	172.16.74.1----172.16.75.254	172.16.75.255	512	510
39	172.16.76.0	172.16.76.1----172.16.77.254	172.16.77.255	512	510
40	172.16.78.0	172.16.78.1----172.16.79.254	172.16.79.255	512	510
41	172.16.80.0	172.16.80.1----172.16.81.254	172.16.81.255	512	510
42	172.16.82.0	172.16.82.1----172.16.83.254	172.16.83.255	512	510
43	172.16.84.0	172.16.84.1----172.16.85.254	172.16.85.255	512	510
44	172.16.86.0	172.16.86.1----172.16.87.254	172.16.87.255	512	510
45	172.16.88.0	172.16.88.1----172.16.89.254	172.16.89.255	512	510
46	172.16.90.0	172.16.90.1----172.16.91.254	172.16.91.255	512	510
47	172.16.92.0	172.16.92.1----172.16.93.254	172.16.93.255	512	510

número de subred	dirección de subred	rango de direcciones IP disponibles	dirección de broadcast	hosts	hosts útiles
48	172.16.94.0	172.16.94.1----172.16.95.254	172.16.95.255	512	510
49	172.16.96.0	172.16.96.1----172.16.97.254	172.16.97.255	512	510
50	172.16.98.0	172.16.98.1----172.16.99.254	172.16.99.255	512	510
51	172.16.100.0	172.16.100.1--172.16.101.254	172.16.101.255	512	510
52	172.16.102.0	172.16.102.1--172.16.103.254	172.16.103.255	512	510
53	172.16.104.0	172.16.104.1--172.16.105.254	172.16.105.255	512	510
54	172.16.106.0	172.16.106.1--172.16.107.254	172.16.107.255	512	510
55	172.16.108.0	172.16.108.1--172.16.109.254	172.16.109.255	512	510
56	172.16.110.0	172.16.110.1--172.16.111.254	172.16.111.255	512	510
57	172.16.112.0	172.16.112.1--172.16.113.254	172.16.113.255	512	510
58	172.16.114.0	172.16.114.1--172.16.115.254	172.16.115.255	512	510
59	172.16.116.0	172.16.116.1--172.16.117.254	172.16.117.255	512	510
60	172.16.118.0	172.16.118.1--172.16.119.254	172.16.119.255	512	510
61	172.16.120.0	172.16.120.1--172.16.121.254	172.16.121.255	512	510
62	172.16.122.0	172.16.122.1--172.16.123.254	172.16.123.255	512	510
63	172.16.124.0	172.16.124.1--172.16.125.254	172.16.125.255	512	510
64	172.16.126.0	172.16.126.1--172.16.127.254	172.16.127.255	512	510
65	172.16.128.0	172.16.128.1--172.16.129.254	172.16.129.255	512	510
66	172.16.130.0	172.16.130.1--172.16.131.254	172.16.131.255	512	510
67	172.16.132.0	172.16.132.1--172.16.133.254	172.16.133.255	512	510
68	172.16.134.0	172.16.134.1--172.16.135.254	172.16.135.255	512	510
69	172.16.136.0	172.16.136.1--172.16.137.254	172.16.137.255	512	510
70	172.16.138.0	172.16.138.1--172.16.139.254	172.16.139.255	512	510
71	172.16.140.0	172.16.140.1--172.16.141.254	172.16.141.255	512	510
72	172.16.142.0	172.16.142.1--172.16.143.254	172.16.143.255	512	510
73	172.16.144.0	172.16.144.1--172.16.145.254	172.16.145.255	512	510
74	172.16.146.0	172.16.146.1--172.16.147.254	172.16.147.255	512	510
75	172.16.148.0	172.16.148.1--172.16.149.254	172.16.149.255	512	510
76	172.16.150.0	172.16.150.1--172.16.151.254	172.16.151.255	512	510
77	172.16.152.0	172.16.152.1--172.16.153.254	172.16.153.255	512	510
78	172.16.154.0	172.16.154.1--172.16.155.254	172.16.155.255	512	510
79	172.16.156.0	172.16.156.1--172.16.157.254	172.16.157.255	512	510
80	172.16.158.0	172.16.158.1--172.16.159.254	172.16.159.255	512	510
81	172.16.160.0	172.16.160.1--172.16.161.254	172.16.161.255	512	510
82	172.16.162.0	172.16.162.1--172.16.163.254	172.16.163.255	512	510
83	172.16.164.0	172.16.164.1--172.16.165.254	172.16.165.255	512	510
84	172.16.166.0	172.16.166.1--172.16.167.254	172.16.167.255	512	510
85	172.16.168.0	172.16.168.1--172.16.169.254	172.16.169.255	512	510
86	172.16.170.0	172.16.170.1--172.16.171.254	172.16.171.255	512	510
87	172.16.172.0	172.16.172.1--172.16.173.254	172.16.173.255	512	510
88	172.16.174.0	172.16.174.1--172.16.175.254	172.16.175.255	512	510
89	172.16.176.0	172.16.176.1--172.16.177.254	172.16.177.255	512	510
90	172.16.178.0	172.16.178.1--172.16.179.254	172.16.179.255	512	510
91	172.16.180.0	172.16.180.1--172.16.181.254	172.16.181.255	512	510
92	172.16.182.0	172.16.182.1--172.16.183.254	172.16.183.255	512	510
93	172.16.184.0	172.16.184.1--172.16.185.254	172.16.185.255	512	510
94	172.16.186.0	172.16.186.1--172.16.187.254	172.16.187.255	512	510
95	172.16.188.0	172.16.188.1--172.16.189.254	172.16.189.255	512	510
96	172.16.190.0	172.16.190.1--172.16.191.254	172.16.191.255	512	510

número de subred	dirección de subred	rango de direcciones IP disponibles	dirección de broadcast	hosts	hosts útiles
97	172.16.192.0	172.16.192.1--172.16.193.254	172.16.193.255	512	510
98	172.16.194.0	172.16.194.1--172.16.195.254	172.16.195.255	512	510
99	172.16.196.0	172.16.196.1--172.16.197.254	172.16.197.255	512	510
100	172.16.198.0	172.16.198.1--172.16.199.254	172.16.199.255	512	510
101	172.16.200.0	172.16.200.1--172.16.201.254	172.16.201.255	512	510
102	172.16.202.0	172.16.202.1--172.16.203.254	172.16.203.255	512	510
103	172.16.204.0	172.16.204.1--172.16.205.254	172.16.205.255	512	510
104	172.16.206.0	172.16.206.1--172.16.207.254	172.16.207.255	512	510
105	172.16.208.0	172.16.208.1--172.16.209.254	172.16.209.255	512	510
106	172.16.210.0	172.16.210.1--172.16.211.254	172.16.211.255	512	510
107	172.16.212.0	172.16.212.1--172.16.213.254	172.16.213.255	512	510
108	172.16.214.0	172.16.214.1--172.16.215.254	172.16.215.255	512	510
109	172.16.216.0	172.16.216.1--172.16.217.254	172.16.217.255	512	510
110	172.16.218.0	172.16.218.1--172.16.219.254	172.16.219.255	512	510
111	172.16.220.0	172.16.220.1--172.16.221.254	172.16.221.255	512	510
112	172.16.222.0	172.16.222.1--172.16.223.254	172.16.223.255	512	510
113	172.16.224.0	172.16.224.1--172.16.225.254	172.16.225.255	512	510
114	172.16.226.0	172.16.226.1--172.16.227.254	172.16.227.255	512	510
115	172.16.228.0	172.16.228.1--172.16.229.254	172.16.229.255	512	510
116	172.16.230.0	172.16.230.1--172.16.231.254	172.16.231.255	512	510
117	172.16.232.0	172.16.232.1--172.16.233.254	172.16.233.255	512	510
118	172.16.234.0	172.16.234.1--172.16.235.254	172.16.235.255	512	510
119	172.16.236.0	172.16.236.1--172.16.237.254	172.16.237.255	512	510
120	172.16.238.0	172.16.238.1--172.16.239.254	172.16.239.255	512	510
121	172.16.240.0	172.16.240.1--172.16.241.254	172.16.241.255	512	510
122	172.16.242.0	172.16.242.1--172.16.243.254	172.16.243.255	512	510
123	172.16.244.0	172.16.244.1--172.16.245.254	172.16.245.255	512	510
124	172.16.246.0	172.16.246.1--172.16.247.254	172.16.247.255	512	510
125	172.16.248.0	172.16.248.1--172.16.249.254	172.16.249.255	512	510
126	172.16.250.0	172.16.250.1--172.16.251.254	172.16.251.255	512	510
127	172.16.252.0	172.16.252.1--172.16.253.254	172.16.253.255	512	510
128	172.16.254.0	172.16.254.1--172.16.255.254	172.16.255.255	512	510

ANEXO B

Proforma presentada por la compañía COMWARE, para la adquisición de equipos de Networking.

Propuesta: *Equipos de redes Enterasys*
Fecha: *28-Oct-05*
Atención: *Mariuxi Desiderio Rodrigo*
Email: mdesider@ceibo.fiec.espol.edu.ec

equipo Enterasys Matrix E1 con 24 puertos 10/100
un slot de expansión……1890 dólares

costo de módulo con 16 puertos 10/100 adicionales……1320 dólares

Costo de instalación y configuración del equipo……...100 dólares la hora

Saludos cordiales
--

FABIÁN ALBA ABAD
DIRECTOR DE PROYECTOS TELECOMUNICACIONES
Telf: (593) 4 2690170
Cel: (593) 9 6172493

En las dos páginas siguientes se muestran la proformas enviadas por la compañía MAINT, la primera es la opción 1, la siguiente es la opción 2.

MAINT

NORTEL

Cliente: *NIELSI*
Propuesta: *Equipos de redes NORTEL*
Fecha: *28-Oct-05*
Atención: *Ing. Narcisa Cardoso*
Email: pedro_solis_sanchez@hotmail.com

DESCRIPCIÓN	PRODUCTO	CANT.	PRECIO UNITARIO	PRECIO TOTAL
HARDWARE				
ERS 3510-24T with 24 10/100/1000 ports plus 4 fiber mini-GBIC ports.	AL1001E08	1	1745.88	$ 1.745,88
			SUBTOTAL1	$ 1.745,88
SERVICIO DE INSTALACION Instalación física de equipos. Configuración de vlans. Configuración de interfases IP. Configuración de enrutamiento básico RIP.	MAINT1	1	$ 600,00	$ 600,00
			SUBTOTAL2	$ 600,00
SERVICIO DE MANTENIMIENTO ANUAL Mantenimientos Preventivos en el año 2 Mantenimientos Correctivos: 2 Cobertura de repuestos. Equipo de contingencia de similares o superiores características	MAINT1	1	$ 300,00	$ 300,00
			SUBTOTAL3	$ 300,00
			Subtotal	**$ 2.645,88**
			Iva (12%)	***$317,51***
			Total	**$ 2.963,39**

Condiciones de la Propuesta

Tiempo Máximo de Entrega:	45 dias
Garantía:	1 año
Validez de Oferta :	15 dias
Terminos de pago:	70% a la orden-30% contra entrega

Atentamente

Javier Pactong
Ingeniero de Preventa
Maint Cia. Ltda.

MAINT

NORTEL

Cliente: *NIELSI*
Propuesta: *Equipos de redes NORTEL*
Fecha: *28-Oct-05*
Atención: *Ing. Narcisa Cardoso*
Email: pedro_solis_sanchez@hotmail.com

DESCRIPCIÓN	PRODUCTO	CANT.	PRECIO UNITARIO	PRECIO TOTAL
HARDWARE				
Passport 1424T Routing Switch with 24 10/100TX ports and 2 GBIC slots.	DI141.2E05	1	3893.32	$ 3.893,32
			SUBTOTAL1	$ 3.893,32
SERVICIO DE INSTALACION	MAINT1	1	$ 600,00	$ 600,00
Instalación física de equipos. Configuración de vlans. Configuración de interfases IP. Configuración de enrutamiento básico RIP.				
			SUBTOTAL2	$ 600,00
SERVICIO DE MANTENIMIENTO ANUAL	MAINT1	1	$ 600,00	$ 600,00
Mantenimientos Preventivos en el año 2 Mantenimientos Correctivos: 2 Cobertura de repuestos. Equipo de contingencia de similares o superiores caracteristicas				
			SUBTOTAL3	$ 600,00

Subtotal	$	5.093,32
Iva (12%)		$611,20
Total	**$**	5.704,52

Condiciones de la Propuesta

Tiempo Máximo de Entrega:	45 dias
Garantía:	1 año
Validez de Oferta :	15 días
Terminos de pago:	70% a la orden-30% contra entrega

Atentamente

Javier Pactong
Ingeniero de Preventa
Maint Cia. Ltda.

Proforma presentada por ANDEANTRADE.

WS-C3560-24TS-S Catalyst 3560 24 10/100 2 SFP Standard Image adicionales	1.600 USD
WS-C3560-24TS-S Catalyst 3560 24 10/100 2 SFP Standard Image OPEN BOX adicionales	1.450 USD
CON-SNTE-PKG3 SMARTNET 8X5X4 PKG CAT3	250 USD
Configuración e instalación del equipo	300 USD
Mantenimiento cada seis meses	200 USD

Álvaro Prado
Gerente de Cuenta
ANDEANTRADE
PASAJE ROSSEAN E8-20 y AV. DE LOS SHYRIS
PBX: (593-2) 2443-868
Fax: Ext. 102
Base Celular1: (593-9) 6204-905
Móvil1: (593-9) 9734-749
Móvil2: (593-9) 6019-861
Casilla: 17-22-20254
Quito. Ecuador

GLOSARIO

GLOSARIO

Actualizaciones activadas: Obligan al router a que envíe una difusión inmediatamente al recibir "malas noticias", en lugar de esperar el próximo período de difusión.

Actualizaciones generadas por evento: Inmediatamente sucede un cambio topológico en la red, el router envía actualizaciones de este cambio a los routers conectados directamente a él.

Algoritmo de Dijkstra: Algoritmo utilizado por los protocolos de enrutamiento de estado de enlace, que permite escoger la ruta de menor costo primero.

Apple Talk: Es un protocolo enrutado.

Backbone: Estructura central de una red.

BPDU: Siglas de Bridge Protocol Data Unit, son los paquetes que envía Spanning-Tree a los dispositivos para tener una red libre de lazos físicos.

Broadcast: Envío de paquetes a todos los dispositivos de la red.

CDP: Protocolo propietario de **CISCO**, que significa protocolo de descubrimiento de CISCO, nos brinda información acerca de los dispositivos que están directamente conectados a los dispositivos de red.

CIDR: "Enrutamiento entre dominios sin clase", esto permite que un router Sumarice rutas y tenga menos de ellas en la tabla de enrutamiento, permitiendo así una rápida convergencia ante cualquier cambio topológico.

Consola: Por medio de este medio se configura localmente a los equipos, se utiliza el hyperterminal, programa de la maquina y mediante un cable DB9 a RJ45 conectamos la computadora al equipo que deseamos configurar.

Cuenta al infinito: Característica de los protocolos de enrutamiento que permite tener un número máximo de saltos, luego de eso la ruta se la considera inalcanzable y es borrada de la tabla de enrutamiento.

DCE: Equipo que provee la sincronización en un enlace WAN.

DHCP: Siglas de “Dynamic Host Configuration Protocol”, este protocolo permite la asignación dinámica de los parámetros necesarios para que un dispositivos formen parte de la red.

Direcciones ip útiles: Direcciones disponible para asignarles a los dispositivos de una red.

Direcciones lógicas: Son las direcciones IP o direcciones de capa 3 que se asignan a los dispositivos que forman parte de una red.

Direcciones privadas: Direcciones que se asignan a dispositivos que forman parte de una red privada.

Direcciones públicas: Direcciones que se asignan a dispositivos que viajan a través del Internet.

DNS: Siglas de “Domain Name System”, parámetro para poder navegar por Internet para los dispositivos.

DTE: Equipo Terminal de datos, generalmente este papel, lo ejecuta un router del lado del usuario.

DUAL: Algoritmo utilizado solamente por EIGRP, para encontrar la mejor ruta hacia todos los puntos de la red en un router, y así mismo tener la mejor ruta de respaldo, por si acaso la ruta activa falla.

Duplex: Se realiza la transmisión y la recepción al mismo tiempo.

Enable secret: Clave secreta, codificada.

Encabezado: Campo al inicio de una trama en particular.

Equipos activos: Son los equipos que brindan conectividad en la red como: switches y routers, también llamados dispositivos de Networking.

Enrutamiento: Procedimiento que realiza el router en el envío de paquetes a su destino correcto.

FS: Siglas en inglés de sucesor factible, es el router que está listo a remplazar al que esta funcionando correctamente en la conectividad de una red, debido a alguna falla que se presente en la red.

Gateway: Se llama así a la ruta de último recurso donde los paquetes son direccionados de no haber otra ruta presente en la tabla de enrutamiento.

Horizonte dividido: Característica de los protocolos de enrutamiento, que permite a un router registrar la interfaz por la que ha recibido una ruta particular y no difunde la información acerca de la ruta de regreso sobre la misma interfaz.

Hub Dispositivo de capa física que sirve para repartir el ancho de banda que maneja entre todos los usuarios que se conectan en sus interfases, es un multi-repetidor.

HyperTerminal: Programa utilizado por la computadora para la configuración por medio del interfaz de consola de los equipos que van a manejar la red.

IDF: Intermediate Distribution Frame, parte de la red telefónica pública.

IGP: Siglas de Interior Gateway Protocol, protocolo que enruta tráfico dentro de un sistema autónomo.

InterVLAN: Conectividad entre VLANS, esto es logrado mediante el enrutamiento de los paquetes que van de una VLAN a otra.

Ios: Imagen del Sistema operativo de switches y routers.

IPV4: Internet versión 4, es la tecnología que se utiliza actualmente, ya en el mundo se la está empezando a remplazar por IPV6.

LAN: Red de área local, cubre pequeños sectores, como máquinas en una misma oficina o edificio

LED: Indicador lumínico de cada Puerto del switch, éste nos indica en que estado se encuentra el puerto.

MAC: Dirección de control de acceso al medio, es la dirección de los dispositivos en la capa de control de enlace, consta de doce dígitos

hexadecimales, los primeros 6 identifican al fabricante, los restantes 6 son la serie de la interfaz.

Máscara de red: Parámetro utilizado para que un equipo entre en red, todos los equipos de la misma red deben de tener la misma máscara de subred.

MD5: "Message Digest 5", tipo de cifrado que se utiliza cuando se aplica seguridad.

MDF: Main Distribution Frame, parte de la red telefónica pública.

Modo de configuración global: Modo de configuración dentro del modo privilegiado, que nos permite realizar cambios más avanzados en el equipo.

Modo privilegiado: Modo en los dispositivos de Networking, que nos permite realizar cambios en la configuración del equipo.

Modo usuario: Modo de los dispositivos de Networking, en el cual no se puede realizar ningún cambio en la configuración del equipo.

Multicast: Envío de paquetes de un dispositivo a una parte de la red.

NAT: Siglas de "Network Address Translation", es un protocolo que permite asociar direcciones privadas con públicas.

NVRAM: Es memoria no volátil, significa que los datos no se pierden si es que el equipo se lo apaga.

PAT: Siglas de "Port Address Translation", es un protocolo que permite asociar muchas más direcciones privadas con direcciones publicas.

Ping: Es un programa básico que verifica que una dirección IP en particular existe y puede aceptar solicitudes. El comando **ping** funciona enviando paquetes IP especiales, llamados datagramas de petición de eco ICMP (Internet Control Message Protocol/Protocolo de mensajes de control de Internet) a un destino específico.

Poison reverse: Una vez que una conexión desaparece, el router anuncia la conexión conservando la entrada de información por varios períodos de actualización e incluye un costo infinito en la difusión.

RAM: Memoria de acceso aleatorio, la información almacenada se pierde cuando se apaga el equipo.

Router: Dispositivo de capa 3 y 4 del modelo OSI que envía la información analizando las direcciones lógicas que contienen los paquetes.

RTP: Siglas en inglés de "Protocolo de Transporte Confiable", es un protocolo de capa de transporte que garantiza la entrega ordenada de paquetes EIGRP a todos los vecinos.

Spanning-Tree: Protocolo utilizado en los switches para evitar tener lazos lógicos, aunque estos existan físicamente.

SPF: Siglas en inglés de "short path first", algoritmo utilizado por los protocolos de estado de enlace, en especial **OSPF**.

SPT: Siglas de Spanning-Tree Protocol.

Subinterfase: Son interfases lógicas que se crean dentro de una interfase física.

Subnetting: Procedimiento que se utiliza para la creación de subredes, a partir de una red.

Switch raíz: Switch principal en el método del Spanning-Tree.

Telnet: Protocolo que permite al usuario conectarse a un host de Internet y ejecute comandos. El cliente de Telnet recibe el nombre de host local. El servidor de Telnet recibe el nombre de host remoto.

Temporizadores de espera: Los protocolos tienen algunos, que ayudan a una mejor convergencia ante cualquier cambio topológico, y se lo puede configurar para el ahorro del ancho de banda.

Texto cifrado: Mensaje codificado, para seguridad de la transmisión.

Texto plano: Mensaje sin codificar, que se lo puede leer sin ningún problema.

TFTP: Siglas de "Trivial File Transfer Protocol", utiliza paquetes UDP.

Servidores TFTP, son utilizados para almacenar las configuraciones de los equipos, si por algún motivo, los equipos se resetean, se descarga el archivo desde el servidor TFTP, y nos ahorramos el tiempo de volver a configurar el equipo. Los Routers utilizan el TFTP para transferir los archivos de configuración e imágenes IOS de Cisco y para transferir archivos entre los sistemas que admiten TFTP.

Traceroute: Protocolo que permite visualizar todas las rutas que un paquete recorre hasta alcanzar el destino final, este protocolo es bien útil, con lo que respecta a resolución de problemas de conectividad, nos ayuda a encontrar posibles conexiones de red interrumpidas.

Trunking: Tecnología de comunicación que permite que por un mismo medio viajen distintas señales.

Unicast: Envío de paquetes a un solo dispositivo de la red.

VLAN: Segmento de red conmutado que está lógicamente segmentado por función, proyecto o aplicación sin importar la ubicación física de los usuarios.

VLAN 1: VLAN administrativa del switch, por defecto todos los switches pertenecen a la VLAN 1, a esta VLAN se le asigna una dirección IP, para poder monitorear a los switches desde cualquier punto de la red.

VLSM: permite tener subredes con distintas capacidades de usuarios, por ende varias máscaras de subred, esto fue creado para evitar el desperdicio de direcciones IP.

VTP: permite el cruce de información desde switches servidores a los demás switches que conforman la red, respecto a configuraciones de VLAN pertenecientes a la red.

BIBLIOGRAFIA

Bibliografía

1. Huidrovo José y Roldán David **Integración de voz y datos** Mc Graw-Hill 2003.

2. Tanenbaum Andrew **Redes de computadoras** Pearson 4ta edición 2003.

3. Keagy Scout **Integración de redes de voz y datos** CISCO Systems 2001.

4. **Guía del primer año CCNA 1 y 2** CISCO Systems tercera edición 2004.

5. Sackett George **Manual de routers CISCO** Osborne Mc Graw-Hill 2002.

6. www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

7. www.cisco.com/warp/public/537/6.html

8. www.cisco.com/univercd/cc/td/ doc/product/lan/cat5000/rel_5_2/config/vtp.htm

9. www.itlp.edu.mx/publica/ revistas/revista_isc/actual/**vlan**.htm
10. es.wikipedia.org/wiki/Trunking_(red)

11. www.cisco.com/warp/public/473/21.html

12. www.cisco.com/univercd/ cc/td/doc/cisintwk/ito_doc/**rip**.htm

13. www.cisco.com/univercd/ cc/td/doc/cisintwk/ito_doc/**igrp**.htm

14. www.cisco.com/univercd/cc/ td/doc/cisintwk/ito_doc/en_igrp.htm

15. www.ciscopress.com/articles/article.asp?p=27839

16. www.cisco.com/univercd/cc/td/doc/
product/software/ios122/122cgcr/fiprrp_r/1rf**rip**.htm

17. www.cisco.com/univercd/cc/td/doc/product/
rtrmgmt/sw_ntman/cwsimain/cwsi2/cwsiug2/vlan2/stpapp.htm

18. www.cisco.com/univercd/cc/td/doc/ product/lan/cat5000/rel_5_2/config/spantree.htm

19. www.cisco.com/univercd/cc/td/doc/ product/lan/cat5000/rel_5_2/config/channel.htm

20. www.**cisco**.com/warp/public/cc/pd/rt/**2600**/index.shtml

21. www.**cisco**.demos.su/routers/**2600**.html

22. nfo.**cisco**.de/global/DE/solutions/ smb/produkte/**cisco_2950**_catalyst.pdf

23. www.ciscopress.com/articles/ article.asp?p=29803&seqNum=3 - 35k

24. www.cisco.com/en/US/products/hw/switches/
ps663/products_security_notice09186a0080264647.html - 21k –

25. www.ciscopress.com/articles/article.asp?p=29803 - 33k

26. www.itlp.edu.mx/publica/ revistas/revista_isc/actual/**vlan**.htm

27. www.ieee802.org/1/pages/802.1v.html

28. www.3com.com/nsc/200374.html

29. en.wikipedia.org/wiki/Virtual_LAN

30. es.wikipedia.org/wiki/RIP_(protocolo)

31. www.webopedia.com/TERM/I/ Interior_Gateway_Routing_Protocol.html

32. es.wikipedia.org/wiki/EIGRP - 20k