UNAM

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO.

FACULTAD DE ESTUDIOS SUPERIORES.

"ARAGÓN".

"SEGMENTACION DE VLAN'S DENTRO DE LA RED DE LA SHCP".

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN.

P R E S E N T A N:

OSCAR RIVAS HERRERA.
VICTOR MANUEL ARENAS JACOBO.

DIRECTOR DE TESIS:

ING. JUAN GASTALDI PÉREZ.

SAN JUAN DE ARAGÓN, ESTADO DE MÉXICO. 2007.

AGRADECIMIENTOS:

Para poder realizar esta tesis de la mejor manera posible fue necesario el apoyo de muchas personas a las cuales quiero agradecer.

- A mis padres por su comprensión, apoyo y amor.
- A mis hermanos(as) y amigos por su apoyo incondicional.
- A mis profesores y compañeros que sin ellos no hubiera sido posible la realización de este trabajo.

ÍNDICE

CAPITULO IV. CONFIGURACIÓN E IMPLEMENTACIÓN DE LA RED DENTRO DE LA SHCP

INTRODUCCIÓN

Un ordenador solitario, sin conexión con ningún otro, es una isla de información y de recursos que no resulta rentable, especialmente cuando para el trabajo diario se precisa recurrir a diferentes fuentes de datos.

De esto se dieron cuenta muy pronto las empresas, que solicitaron a las compañías de desarrollo de hardware y software un medio compartido de trabajo, en el que diferentes estaciones de trabajo, servidores e impresoras pudieran comunicarse entre ellos y compartir recursos. De este modo surgieron las primeras redes de ordenadores.

Una red está formada por una serie de estaciones de trabajo unidas entre sí por medios de transmisión físicos (cables) o basados en ondas (redes inalámbricas), coordinados por unas máquinas especiales, denominadas servidores, y por una conjunto variable de dispositivos de trabajo, como impresoras, escaners, etc. Además, existen diferentes dispositivos que añaden funcionalidades a las redes, como los routers, switches y hubs.

Uno de los objetivos más ambiciosos de una red virtual es el establecimiento de modelos de grupos de trabajo virtuales. El concepto es que, con una completa implementación de una VLAN a través del entorno de red en el área de trabajo, miembros del mismo departamento o sección puedan aparentar estar en la misma red local, sin ser necesario que la mayoría del tráfico de la red esté en el mismo dominio de *broadcast* de la VLAN. Alguien que se mueva a una nueva localización física pero que permanezca en el mismo departamento se podría mover sin tener que reconfigurar la estación de trabajo.

Esto ofrece un entorno más dinámicamente organizado, permitiendo la tendencia hacia equipos con funciones cruzadas. La lógica del modelo virtual por grupos de trabajo va de la siguiente forma: los equipos pueden estar conectados virtualmente a la misma LAN sin necesidad de mover físicamente a las personas para minimizar el tráfico a través de una red troncal colapsada. Además, estos grupos serán dinámicos: un equipo destinado a un proyecto puede ser configurado mientras dure ese proyecto, y ser eliminado cuando se complete, permitiendo a los usuarios retornar a sus mismas localizaciones físicas.

CAPÍTULO I. VLAN Y TRONCALES

1.1 Definición de VLAN

Las LAN virtuales (VLAN's) son agrupaciones, definidas por software, de estaciones LAN que se comunican entre sí como si estuvieran conectadas al mismo cable, incluso estando situadas en segmentos diferentes de una red de edificio o de área de trabajo. Es decir, la red virtual es la tecnología que permite separar la visión lógica de la red de su estructura física mediante el soporte de comunidades de intereses, con definición lógica, para la colaboración en sistemas informáticos de redes. Este concepto, fácilmente asimilable a grandes trazos implica en la práctica, sin embargo, todo un complejo conjunto de cuestiones tecnológicas. Quizás, por ello, los fabricantes de conmutación LAN se están introduciendo en este nuevo mundo a través de caminos diferentes, complicando aún más su divulgación entre los usuarios.

Además, la red virtual simplifica el problema de administrar los movimientos, adiciones y cambios del usuario dentro de la empresa. Por ejemplo, si un departamento se desplaza a un edificio a través del área de trabajo, este cambio físico será transparente gracias a la visión lógica de la red virtual. Asimismo, se reduce notablemente el tiempo y los datos asociados con los movimientos físicos, permitiendo que la red mantenga su estructura lógica al coste de unas pocas pulsaciones del ratón del administrador de la red. Puesto que todos los cambios se realizan bajo control de software, los centros de cableado permanecen seguros y a salvo de interrupciones.

Según este esquema, la VLAN consiste en una agrupación de puertos físicos que puede tener lugar sobre un switch o también, en algunos casos, sobre varios switches. La asignación de los equipos a la VLAN se hace en base a los puertos a los que están conectados físicamente.

Muchas de las primeras implementaciones de las VLAN's definían la pertenencia a la red virtual por grupos de puertos (por ejemplo, los puertos 1,2, 3, 7 y 8 sobre un switch forman la VLAN A, mientras que los puertos 4,5 y 6 forman la VLAN B). Además, en la mayoría, las VLAN's podían ser construidas sobre un único switch.

La segunda generación de implementaciones de VLAN's basadas en puertos contempla la aparición de múltiples switches (por ejemplo, los puertos 1 y 2 del switch 1 y los puertos 4,5, 6 y 7 del switch 2 forman la VLAN A; mientras que los puertos 3, 4, 5, 6, 7 y 8 del switch 1 combinados con los puertos 1, 2, 3 y 8 del switch 2 configuran la VLAN B). Este esquema es el descrito por la figura 1.

La agrupación por puertos es todavía el método más común de definir la pertenencia a una VLAN, y su configuración es bastante directa. El definir una red virtual completamente basada en puertos no permite a múltiples VLAN's el incluir el mismo segmento físico (o switch).

De todos modos, la principal limitación de definir VLAN's por puertos es que el administrador de la red ha de reconfigurar la VLAN cada vez que un usuario se mueve de un puerto a otro.

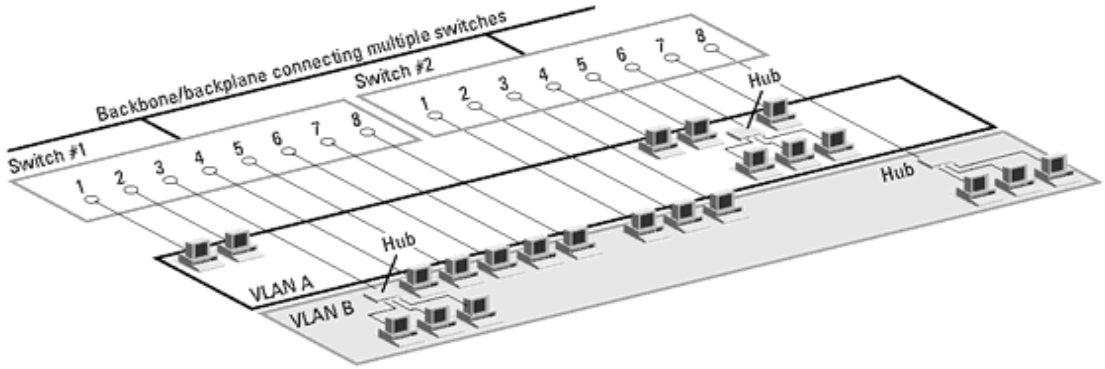
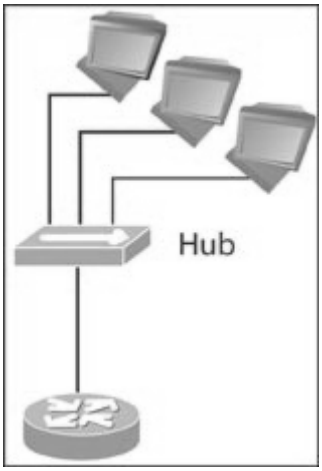


Figura 1.-*VLAN's basadas en puertos.*

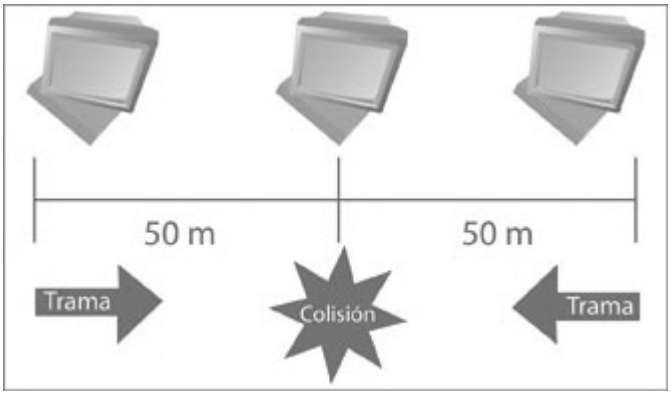
La característica principal de una red de área local es que los dispositivos que la conforman comparten los recursos del medio físico, es decir, el ancho de banda proporcionado por el mismo.

Cuando utilizamos un concentrador o hub dentro de una red, ésta se puede ver como una red de distribución hidráulica, donde las estaciones de trabajo conectadas a la misma toman cierta cantidad de agua, y mientras más máquinas existan en esa LAN, menor será la cantidad de líquido que podrán utilizar. A este segmento de "tubería" se le puede llamar también "dominio de colisiones".



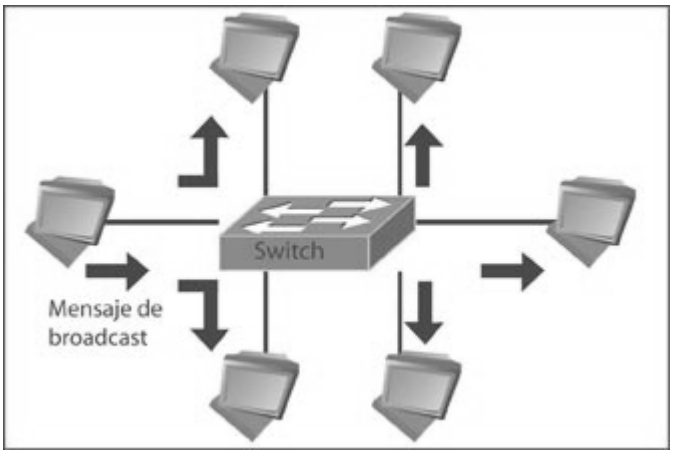
El empleo de un switch mejora el rendimiento de la red debido a que este dispositivo segmenta o divide los "dominios de colisiones", es decir, el comportamiento que se tiene en una LAN al utilizar concentradores o hubs es el de compartir el medio o ancho de banda, por ello puede ocurrir que en algún momento el medio esté ocupado por la transmisión de información por parte de alguna de las computadoras, y si otro quiere enviar información en esa precisa hora, no lo podrá hacer hasta que el medio se encuentre disponible.

Por otro lado, si dos computadoras "escuchan" que el medio está vacío enviarán su información, pero debido a que éste es compartido puede suceder que los datos se encontrarán y "chocarán", por lo que se hablará de una colisión y el material se destruirá; al perderse tendrá que volverse a enviar, lo que llevará a muchas retransmisiones de información.



En una red LAN, cada uno de los puertos es una "tubería" dedicada a cada una de las casas (computadoras) dentro de la red, donde cada computadora dispone de toda la anchura de banda que la red proporciona, en este caso 10 o 100 Mbps, con objeto de evitar las colisiones que pudieran existir en un medio compartido, por ello cada computadora tiene un tubo individual enlazado con el punto central de distribución que es el switch.

Algo que no puede mejorar ni el switch, ni el hub o concentrador, es el envío de mensajes de broadcast dentro de una red LAN; por ejemplo; los que se asemejan a aquellos que escuchamos en una tienda departamental. Estos mensajes los escuchamos todos los que estamos en la tienda (la red LAN), ya sea que estén buscando a alguien o anunciando algún producto, y ninguna de las personas (computadoras) que estamos dentro de la tienda nos encontramos exentos de hacerlo.



En una LAN estos mensajes de broadcast son enviados a través de todos los puertos de un hub o de un switch. Si una computadora quiere comunicarse con otra y no sabe en dónde se encuentra, entonces la "vocea" dentro de la LAN, creando tráfico dentro de ésta, además todas las

computadoras escucharán el mensaje pero sólo podrá contestarlo la que se está buscando, no importando si se encuentra o no conectada dentro del switch o concentrador.

Estos mensajes de broadcast son, en muchas ocasiones, tráfico innecesario como cuando estamos tratando de encontrar una computadora en específico, pero afectamos a todas las que estén dentro del "dominio de broadcast" o LAN.

Para solventar dicha situación se crea el concepto de Redes de Área Local Virtuales (VLAN's), configuradas dentro de los switches, que dividen en diferentes "dominios de broadcast" a un switch, con la finalidad de no afectar a todos los puertos del switch dentro de un solo dominio de broadcast, sino crear dominios más pequeños y aislar los efectos que pudieran tener los mensajes de broadcast a solamente algunos puertos, y afectar a la menor cantidad de máquinas posibles.

Una Red de Área local Virtual (VLAN) puede definirse como una serie de dispositivos conectados en la red que a pesar de estar conectados en diferentes equipos de interconexión (hubs o switches), zonas Geográficas distantes, diferentes pisos de un edificio e, incluso, distintos edificios, pertenecen a una misma Red de Área Local.

Con el switch, el rendimiento de la red mejora en los siguientes aspectos:

• Aísla los "dominios de colisión" por cada uno de los puertos.

• Dedica el ancho de banda a cada uno de los puertos y, por lo tanto, a cada computadora.

• Aísla los "dominios de broadcast", en lugar de uno solo, se puede configurar el switch para que existan más "dominios".

• Proporciona seguridad, ya que si se quiere conectar a otro puerto del switch que no sea el suyo, no va a poder realizarlo, debido a que se configuraron cierta cantidad de puertos para cada VLAN.

• Controla más la administración de las direcciones IP. Por cada VLAN se recomienda asignar un bloque de IP´s, independiente uno de otro, así ya no se podrá configurar por parte del usuario cualquier dirección IP en su máquina y se evitará la repetición de direcciones IP en la LAN.

• No importa en donde nos encontremos conectados dentro del edificio de oficinas, si estamos configurados en una VLAN, nuestros compañeros de área, dirección, sistemas, administrativos, etc., estarán conectados dentro de la misma VLAN, y quienes se encuentren en otro edificio, podrán "vernos" como una Red de Área Local independiente a las demás.

El funcionamiento e implementación de las VLAN's está definido por un organismo internacional llamado IEEE Computer Society y el documento en donde se detalla es el IEEE 802.1Q.

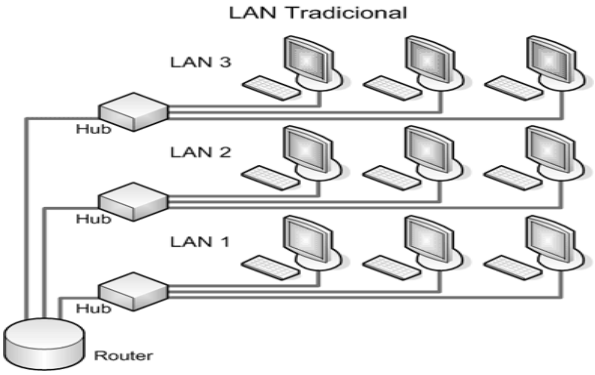
Hasta aquí ya hemos hablado de que se aísla el trafico de colisiones y de broadcast, y que cada VLAN es independiente una de otra, pero todavía falta mencionar cómo es que se comunican entre sí, ya que muchas veces habrá que comunicarse entre computadoras pertenecientes a diferentes VLAN's. Por ejemplo, los de sistemas con los de redes, o los de redes con finanzas, etcétera.

En el estándar 802.1Q se define que para llevar a cabo esta comunicación se requerirá de un dispositivo dentro de la LAN, capaz de entender los formatos de los paquetes con que están formadas las VLAN's. Este dispositivo es un equipo de capa 3, mejor conocido como enrutador o router, que tendrá que ser capaz de entender los formatos de las VLAN's para recibir y dirigir el tráfico hacia la VLAN correspondiente.

Una red de área local (LAN) esta definida como una red de computadoras dentro de un área geográficamente acotada como puede ser una empresa o una corporación. Uno de los problemas que nos encontramos es el de no poder tener una confidencialidad entre usuarios de la LAN como pueden ser los directivos de la misma, también estando todas las estaciones de trabajo en un mismo dominio de colisión el ancho de banda de la misma no era aprovechado correctamente. La solución a este problema era la división de la LAN en segmentos físicos los cuales fueran independientes entre si, dando como desventaja la imposibilidad de comunicación entre las LAN's para algunos de los usuarios de la misma.

La necesidad de confidencialidad como así el mejor aprovechamiento del ancho de banda disponible dentro de la corporación ha llevado a la creación y crecimiento de las VLAN's.

Una VLAN se encuentra conformada por un conjunto de dispositivos de red interconectados (hubs, bridges, switches o estaciones de trabajo) la definimos como una subred definida por software y es considerada como un dominio de Broadcast que pueden estar en el mismo medio físico o bien puede estar sus integrantes ubicados en distintos sectores de la corporación (Figura1).



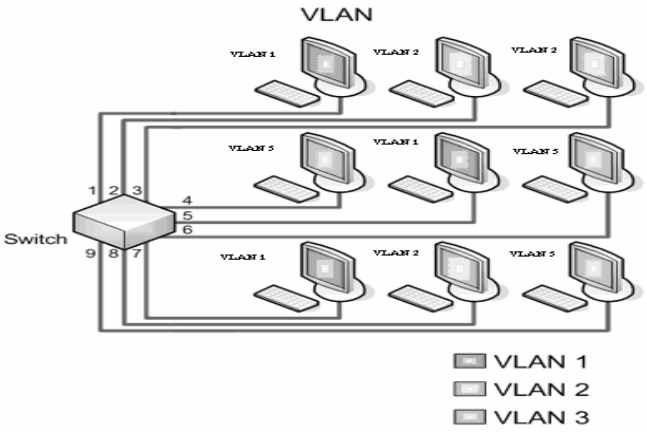


Figura 1

La tecnología de las VLAN's se basa en el empleo de Switches, en lugar de hubs, de tal manera que esto permite un control mas inteligente del tráfico de la red, ya que este dispositivo trabaja a nivel de la capa 2 del modelo OSI y es capaz de aislar el tráfico, para que de esta manera la eficiencia de la red entera se incremente. Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, se logra el incremento del ancho de banda en dicho grupo de usuarios.

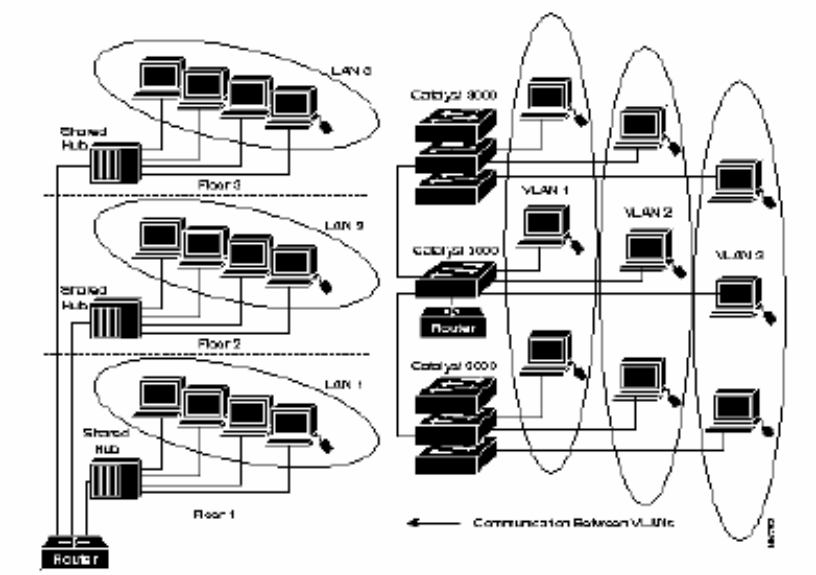
1.1.1 Redes LAN conmutadas (switched LAN's)

Los problemas asociados a las redes compartidas y la emergencia de switches han originado el reemplazo de la configuración tradicional de LAN por la configuración LAN conmutada

Características:

- Switches reemplazan los Hubs principales ubicados en el gabinete o rack de comunicaciones.
- Se generan VLAN para proveer la segmentación tradicionalmente provista por ruteadores.

La figura siguiente muestra la diferencia entre segmentación tradicional y usando VLAN's.



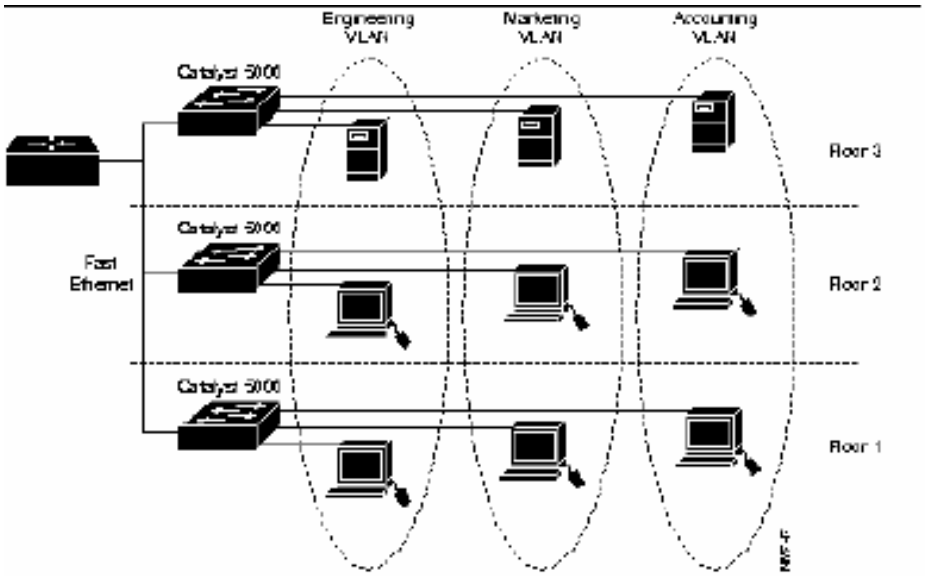
1.1.2. Características de una VLAN

- El núcleo de una VLAN es un Switch.

- Una VLAN es una red conmutada que está lógicamente segmentada en base a funciones (trabajadores de un mismo departamento), grupos de proyectos o usuarios compartiendo la misma aplicación, sin importar la ubicación física de los usuarios. Por ejemplo, cada puerta del switch puede asignarse a una VLAN. Las puertas que no pertenecen a esa VLAN no comparten los broadcast. Esto mejora el comportamiento global de la red.

- La comunicación entre VLAN's es provista a través de ruteo de capa 3.

- Agrupando puertas y usuarios a través de múltiples switches, la VLAN puede cubrir un edificio completo, interconectar edificios, o aun redes WAN (ver Figura)



1.1.3 Switches, el núcleo de las VLAN's

Los switches proveen las siguientes propiedades:

- La inteligencia para realizar filtrado y decisiones de retransmisión de paquetes, basado en métricas de la VLAN definidas por el usuario.

- La habilidad de comunicar información a otros switches o routers en la red.

- En la actualidad, los switches son ubicados entre los segmentos compartidos y los ruteadores ubicados en el backbone. En el futuro, desempeñaran un rol importante en la segmentación de VLAN's y baja latencia de retransmisión.

1.1.4 Control de la actividad de broadcast

El tráfico broadcast ocurre en toda red y depende de los siguientes factores:

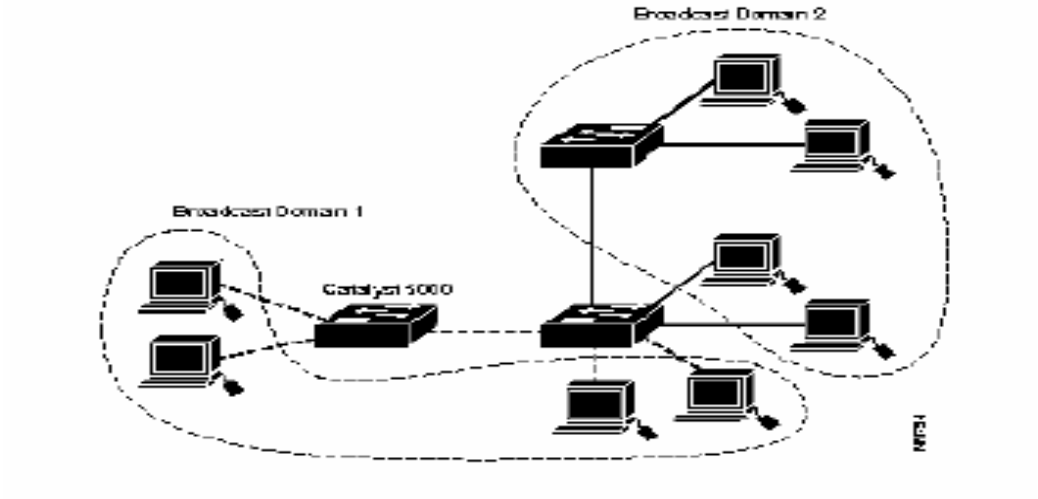
- Tipo de aplicaciones
- Tipo de servidores
- Cantidad de segmentación lógica
- Uso de los recursos de la red

A pesar de que las aplicaciones se hayan optimizado para minimizar el número de broadcast, las aplicaciones multimedia actuales son intensivas en broadcast o multicast.

Los broadcast pueden ser generados también por dispositivos de red o interfaces de red defectuosas.

Si no se administran adecuadamente, pueden degradar seriamente el rendimiento de una red completa o incluso dejarlo no funcional. La medida más efectiva contra este problema es segmentar la red adecuadamente incluyendo firewall de protección, provistos usualmente por un ruteador. Por ello se debe considerar que al segmentar una red mediante switches, se pierde el efecto protector de los ruteadores.

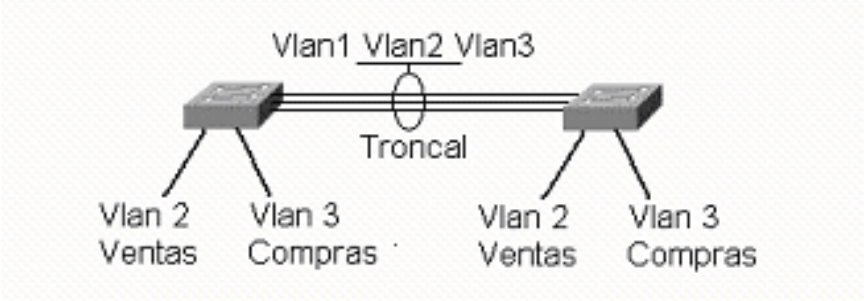
Pero, al igual que los ruteadores, las VLAN permiten establecer firewall. Estos se pueden crear asignando puertas o usuarios a grupos VLAN específicos ubicados en un mismo switch o múltiples switches interconectados. La VLAN no deja salir el tráfico broadcast fuera de su dominio (ver Figura).



1.2 TRONCALES

Muchas veces es necesario agrupar usuarios de la misma Vlan que se encuentran ubicados en diferentes zonas, para conseguir esta comunicación los switches utilizan un enlace troncal. Para que los switches envíen información sobre las vlan que tienen configuradas a través de enlaces troncales es necesaria que las tramas sean identificadas con el propósito de saber a que vlan pertenecen. A medida que las tramas salen del switch son etiquetadas para indicar a que vlan corresponden, esta etiqueta es retirada una vez que entra en el switch de destino para ser enviada al puerto de vlan correspondiente.

Un puerto de switch que pertenece a una vlan determinada es llamado puerto de acceso, mientras que un puerto que transmite información de varias VLAN's a través de un enlace punto a punto es llamado puerto troncal.



Para evitar que todas las VLAN's viajen por el troncal es necesario quitarla manualmente.

La información de todas la VLAN's creadas viajara por el enlace trocal automáticamente, la vlan 1 que es la vlan por default o nativa lleva la información de estado de los puertos.

El resumen de la información brindada por un show vlan que se muestra a continuación se observa la asociación de las respectivas VLAN, con sus puertos asociados:

switch#show vlan

VLAN	**Name**	**Status**	**Ports**
1	**default**	**active**	**Fa0/1, Fa0/2, Fa0/3, Fa0/4**
2	**VENTAS**	**active**	**Fa0/5, Fa0/6, Fa0/7, Fa0/8,**
			Fa0/10, Fa0/28, Fa0/30
			Fa0/9, Fa0/11, Fa0/12, Fa0/13,
3	**ADMINISTRACION**	**active**	**Fa0/14, Fa0/15, Fa0/16, Fa0/17,**
			Fa0/18, Fa0/19, Fa0/20, Fa0/21,
4	**LOGISTICA**	**active**	**Fa0/22, Fa0/23, Fa0/24, Fa0/25,**
			Fa0/26, Fa0/27, Fa0/29, Fa0/31,
			Fa0/32, Fa0/33, Fa0/34, Fa0/35,
			Fa0/36, Fa0/37, Fa0/38, Fa0/39,
			Fa0/40, Fa0/41, Fa0/42, Fa0/43,
			Fa0/44, Fa0/45, Fa0/46, Fa0/47,
			Fa0/48

1.2.1 IEEE 802.1Q

Las actividades de estandarización de la capa de enlace de datos es donde se encuentran el direccionamiento físico (MAC) que fue diseñado por la ISO/IEC introduciendo el concepto de servicios de filtrado en LAN, con mecanismos de filtrado de direcciones y de bases de datos. Extendieron el concepto de Servicio de Filtrado en Switches LAN adicionando capacidades a los puentes y/o switches:

1. El de facilitar la capacidad de tráfico, para soportar la transmisión de información en tiempo critico en la LAN.

2. El uso de señalamientos de prioridad de información con identificaciones básicos de acuerdo a las clases de tráfico.

3. El servicio de filtrado que pueda soportar la definición dinámica y establecimiento de grupos de trabajo, y el filtrado de tramas por switches de acuerdo a las direcciones de los participantes del grupo y solo estas tendrán acceso a los segmentos de LAN de acuerdo al orden y alcance de los miembros de cada grupo.

4. El uso del Protocolo Genérico de Registro de Atributos (GARP) para soporte de los mecanismos que proveen la capacidad de filtrado de grupos, y solo esta hecho para usar otro atributo de registro en las aplicaciones. Este estándar hace uso de los conceptos y mecanismos de *LAN Switching* que fue introducido por la ISO/IEC, además define los mecanismos que se usan en la implementación de "*Switching LAN Virtual"* o *LAN Virtuales*; y son las siguientes:

5. Servicios Virtuales en LAN Switching;

6. La operación del Proceso de Envió que es requerido para dar soporte a Switching LAN Virtual.

7. La estructura del filtrado de la Base de Datos para soportar LAN Virtuales.

8. La naturaleza de los protocolos y procesos en el orden en que son requeridos para dar soporte a los servicios de VLAN's, incluyendo la definición del formato de tramas para representar la información de identificación de VLAN's, y los procesos usados en orden para insertar y borrar identificadores y encabezados de VLAN's cada vez que son transportados.

9. La habilidad para soportar señalamiento de fin-a-fin con prioridad de información de usuario indiferentemente de la dirección MAC, con los protocolos de señalamiento de prioridad de información.

10. El Protocolo de Registro de VLAN GARP (GVRP) que permite la distribución y registro de información de miembros de la VLAN.

11. La administración y operación de servicios para configurar y administrar Switching LAN Virtual.

El Estándar IEEE 802 referente a Redes de Área Local (LAN) de todos tipos pueden ser conectadas junto con los Switches con Control de Acceso al Medio (MAC), especificada en ISO/IEC. Este estándar define la operación de las Redes de Área Local Virtuales (VLAN's) Puentes que permiten la definición, operación y administración de topologías VLAN con infraestructura Switch LAN.

1.2.2 ISL

Cisco creó ISL después del protocolo 802.1q utilizados para troncales. Porque ISL es propietario de Cisco, sólo puede usarse entre dos switches Cisco. ISL encapsula cada trama Ethernet en la parte frontal y la parte posterior.

1.2.3 Comparando ISL y 802.1Q

Una diferencia importante entre ISL y 802.1Q se relacionan a un rasgo llamado VLAN nativa. 802.1Q definen un VLAN en cada troncal como VLAN nativa; por default, ésta es VLAN 1.

Por la definición, 802.1Q no encapsulan las tramas simplemente en la VLAN nativa al enviar las tramas sobre de la troncal. Cuando el switch en el otro lado del enlace recibe una trama en la VLAN nativa, nota la falta de un 802.1Q en el cabezal y sabe que la trama es la parte del VLAN nativa. VLAN's nativas juegan un papel muy importante de una perspectiva práctica. Imagine que usted tiene muchos PCs conectadas a algunos puertos del switch y esas PCs no entienden 802.1Q. Usted también planea instalar los teléfonos de IP cerca de las PCs. Los teléfonos de IP tienen un switch incorporado para que usted pueda conectar el teléfono al cable de Ethernet del switch y entonces pueda conectar el teléfono a UN PC. El teléfono entiende 802.1Q, para que usted pueda poner el teléfono en un VLAN y la PC en otro. Usted puede configurar todos esos puertos para 802.1Q, mientras poniendo el PC's en el VLAN nativa. Ellos trabajan bien cuando conectas directamente al switch, porque el switch no usa cualquiera encapsulasión para el VLAN nativa. Cuando usted instala un teléfono de IP entre el switch y la PC, el teléfono puede entender el 802.1Q y puede enviar y puede recibir el tráfico de un switch. ISL no usa un concepto como VLAN nativa. Todos idean de todas las VLAN's tiene un cabezal de ISL para la transmisión sobre de una troncal de ISL.

1.3 Configuración de VLAN's

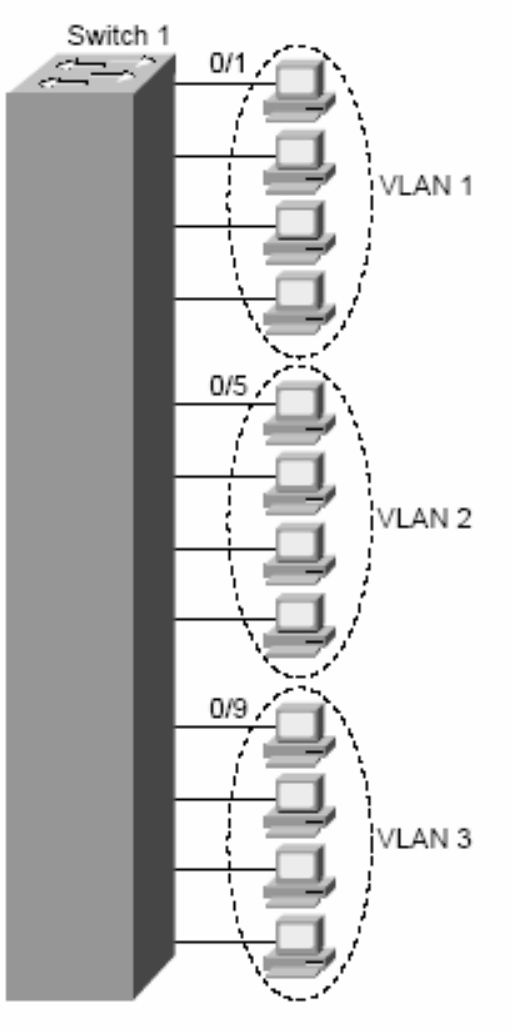
En esta parte veremos como se configuran la parte de VTP (virtual trunk protocol) y además se mostrará como configurarse las Vlan´s. Para ello necesitamos que comando vamos a utilizar dependiendo de cada marca de los switches.

Command	Description
vlan database	EXEC command that puts the user in VLAN configuration mode.
vtp {domain *domain-name* | password *password* | pruning | v2-mode | {server | client | transparent}}	Defines VTP parameters in VLAN configuration mode.
vlan *vlan-id* [name *vlan-name*]	VLAN database configuration command that creates and names a VLAN.
switchport mode {access | dynamic {auto | desirable} | trunk}	Interface subcommand that configures the interface for trunking.
switchport trunk {{allowed vlan *vlan-list*} | {native vlan *vlan-id*} | {pruning vlan *vlan-list*}}	Interface subcommand that refines the list of allowed VLANs, defines the 802.1Q native VLAN, and limits the range of VLANs for which pruning can occur.
switchport access vlan *vlan-id*	Interface subcommand that statically configures the interface into that one VLAN.
show interfaces [*interface-id* | vlan *vlan-id*] [switchport | trunk]	Displays trunk status.
show vlan [brief | id *vlan-id* | name *vlan-name* | *summary*]	EXEC command that lists information about the VLAN.
show vlan [*vlan*]	Displays VLAN information.
show vtp status	Lists VTP configuration and status information.
show spanning-tree vlan *vlan-id*	EXEC command that lists information about the spanning tree for a particular VLAN.

Estos comandos que vemos en la gráfica son de switches marca Cisco que manejaremos en toda la realización de la segmentación de vlan´s.

En la tabla vemos una breve descripción de comandos cubriendo los temas anteriores y un ejemplo explicando lo básico en configuración de Vlan´s, troncales y VTP.

En el siguiente ejemplo se va a configurar en un switch vlan´s donde agregaremos puertos en cada vlan.



En este ejemplo, el usuario empieza creando dos nuevas VLAN's, barney-2 y wilma-3.

El modo de configuración de VLAN se comporta un poco diferentemente del modo de la configuración. Primero, para entrar al modo de configuración de VLAN usamos el comando **vlan databases**, ya que estamos ahí el promt **Switch(vlan)#** cambia para ya poder agregar Vlan´s, usamos los comandos **vlan 2 name barney-2** y **vlan 3 name wilma-3**, es así como se crean las vlan´s con su respectivo nombre, para que estas dos nuevas vlan´s se reflejen o mas bien que se hayan creado tenemos que poner el comando apply o simplemente **exit** para que se creen las vlan´s.

Switch#**vlan database**
Switch(vlan)#**vlan 2 name barney-2**
VLAN 2 added:
Name: barney-2
Switch(vlan)#**vlan 3 name wilma-3**
VLAN 3 added:
Name: wilma-3
Switch(vlan)#?
VLAN database editing buffer manipulation commands:

abort Exit mode without applying the changes
apply Apply current changes and bump revision number
exit Apply changes, bump revision number, and exit mode
no Negate a command or set its defaults
reset Abandon current changes and reread current database
show Show database information
vlan Add, delete, or modify values associated with a single VLAN
vtp Perform VTP administrative functions.
Switch(vlan)#**exit**
APPLY completed.
Exiting....
Switch>enable

Ahora agregaremos puertos del 1 hasta el 4 en VLAN 1, del 5 hasta el 8 en VLAN 2, y del 9 hasta el 12 en VLAN 3, como muestra en la Figura. Sin embargo, la configuración requiere el uso de modo de configuración VLAN así como el modo de la configuración normal.

Para ello con el comando **configure terminal** nos permite el acceso para agregar puertos a las vlan´s que deseemos, para agregar un puerto primero tenemos que nombrar el puerto que se va a cambiar de vlan, el comando es **interface fastEthernet 0/5** y damos enter después el comando **switchport mode access** esto es para decir que el puerto es de acceso ya que también puede hacerse como troncal y damos enter, por ultimo hay que agregarlo a la vlan que le corresponderá con el comando **switchport access vlan 2,** este procedimiento va hacerse con cada uno de los puertos que mencionamos.

Switch#**configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#**interface fastEthernet 0/5**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 2**
Switch(config)#interface fastEthernet 0/6
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config)#interface fastEthernet 0/7
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config)#interface fastEthernet 0/8
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config)#interface range fastEthernet 0/9 - 12
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#^Z

Por ultimo vamos a ver como se agregaron a las vlan los puertos por medio del comando **show vlan brief** el cual nos describe como quedaron las 2 vlan´s creadas con sus respectivos puertos.

Switch#**show vlan brief**
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/18, Fa0/19, Fa0/20, Fa0/21
Fa0/22, Fa0/23, Fa0/24, Gi0/1
Gi0/2
2 barney-2 active Fa0/5, Fa0/6, Fa0/7, Fa0/8
3 wilma-3 active 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

También podemos poner un solo comando para ver solamente una sola vlan con el comando **show vlan id 2** donde nos muestra los puertos que están agregados en la vlan 2 con el nombre barney-2.

Switch#**show vlan id 2**
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
2 barney-2 active Fa0/5, Fa0/6, Fa0/7, Fa0/8
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2 enet 100002 1500 - - - - - 0 0
Remote SPAN VLAN

Disabled
Primary Secondary Type Ports
------- --------- ----------------- --

1.4 Modos de operación VTP

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

VTP opera en estos tres modos:

- **Modo servidor**
- **Modo cliente**
- **Modo transparente**

Modo servidor:

El modo VTP predeterminado es el modo servidor.

En modo servidor pueden crearse, modificar y suprimir VLAN y otros parámetros de configuración que afectan a todo el dominio VTP. En modo servidor, las configuraciones de VLAN se guardan en la memoria de acceso aleatoria no volátil (NVRAM).

En este modo se envían y retransmiten avisos VTP y se sincroniza la información de configuración de VLAN con otros switches. El modo servidor debe elegirse para el switch que se usará para crear, modificar o suprimir VLAN.

Modo cliente:

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

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

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

Modo transparente:

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

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

El modo transparente debe usarse en un switch que necesite para avisos VTP a otros switches, pero que necesitan también capacidad para administrar sus VLAN independientemente.

La pertenencia de los puertos de switch a las VLAN se asigna manualmente puerto a puerto (pertenencia VLAN estática o basada en puertos).

1.4.1 Propagar Vlan Trunking Protocol (VTP)

Por defecto todas las líneas troncales transportan el tráfico de todas las Vlan's configuradas.

Algún tráfico innecesario podría inundar los enlaces perdiendo efectividad. El recorte VTP permite determinar cual es el trafico que inunda el enlace troncal evitando enviarlo a los switches que no tengan configurados puertos de la vlan destino.

La Vlan1 es la vlan de administración y se utiliza para tareas de administración como las publicaciones VTP, no será omitida por el Pruning VTP.

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

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

VTP es un protocolo de mensajería de capa 2 que mantiene la coherencia de la configuración VLAN a través de un dominio de administración común, gestionando las adiciones, supresiones y cambios de nombre de las VLAN a través de las redes.

Un dominio VTP son varios switches interconectados que comparten un mismo entorno VTP. Cada switch se configura para residir en un único dominio VTP.

Copia de un show vtp status

Switch#show vtp status

VTP Version : 2
Configuration Revision : 63
Maximum VLAN's supported locally : 254
Number of existing VLAN's : 20
VTP Operating Mode : Client
VTP Domain Name : damian
VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled
VTP Traps Generation : Enabled
MD5 digest : 0×38 0×3F 0×5F 0xF0 0×58 0xB6 0×74 0×30
Configuration last modified by 104.10.2.3 at 11-4-06 14:49:55

1.4.2 Modo de configuración de VTP (VLAN Trunking Protocol)

Para ver como esta configurado el vtp en nuestro switch tenemos el comando **show vtp status** donde podemos ver la versión del vtp, el máximo de vlan´s soportadas, las 3 formas del vtp y el dominio al que pertenece.

```
Router#sh vtp ?

  counters  VTP statistics
  status    VTP domain status


Router#sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLAN's supported locally : 1005
Number of existing VLAN's       : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xBF 0x86 0x94 0x45 0xFC 0xDF 0xB5 0x70
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 127.0.0.12 on interface EO0/0 (first interface found)
```

Para configurar el vtp entramos igual como hicimos las vlan´s con el comando **vlan database** de ahí nos manda al prompt **Router(vlan)#** ahora si podemos configurar cualquiera de los 3 modos de vtp, en este caso se configurara el cliente con el comando **vtp client,** luego configuramos el vtp domain esto es para la seguridad de la red ya que si un switch no contiene el dominio no podrá tener los mismos servicios que los demás quedándose aislado de los demás, con el comando vtp domain mas agregando el nombre del dominio que uno quiera entonces quedara el comando de la siguiente manera **vtp domain SHCPLV.**

También podemos proteger el vtp con una contraseña para la gente que puede hakear los equipos, este comando seria **vtp password intersys.**

Estas configuraciones que hicimos se hacen igual donde se crean las vlan.

```
Router#vlan database

Router(vlan)# ?
Router(vlan)#vtp ?
  client      Set the device to client mode.
  domain      Set the name of the VTP administrative domain.
  password    Set the password for the VTP administrative domain.
  pruning     Set the administrative domain to permit pruning.
```

```
  server       Set the device to server mode.
  transparent  Set the device to transparent mode.
  v2-mode      Set the administrative domain to V2 mode.
Router(vlan)#vtp client
Setting device to VTP CLIENT mode.
  reset  Abandon current changes and reread current database
  show   Show database information
Router(vlan)#vtp domain
  WORD  The ascii name for the VTP administrative domain.
Router(vlan)#vtp domain SHCPLV
Changing VTP domain name from NULL to SHCPLV
Router(vlan)#vtp password intersys
Setting device VLAN database password to intersys.
Router(vlan)#?
VLAN database editing buffer manipulation commands:
  abort  Exit mode without applying the changes
  apply  Apply current changes and bump revision number
  exit   Apply changes, bump revision number, and exit mode
  no     Negate a command or set its defaults
  reset  Abandon current changes and reread current database
  show   Show database information
  vlan   Add, delete, or modify values associated with a single VLAN
  vtp    Perform VTP administrative functions.

Router(vlan)#exit
In CLIENT state, no apply attempted.
Exiting....
Router#

Router#sh vtp ?
  counters  VTP statistics
  status    VTP domain status
```

Con este ultimo comando **show vtp status** vemos como quedo nuestro vtp y como esta aprendiendo del vtp server por medio de las actualizaciones que hacen los servidores cada 5 minutos.

```
Router#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLAN's supported locally : 1005
Number of existing VLAN's       : 5
VTP Operating Mode              : Client
VTP Domain Name                 : SHCPLV
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x49 0x14 0x92 0xF8 0x68 0x81 0x5F 0xF8
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

CAPÍTULO II. DIRECCIONAMIENTO IP Y SUBREDES

2.1. Concepto del protocolo DHCP

El protocolo DHCP se basa en el conocido modelo Cliente-Servidor. Utiliza un protocolo de comunicaciones muy sencillo, basado en UDP sobre IP. Los clientes de una red que utilicen este protocolo utilizan direcciones IP que les "presta" un servidor (no tiene porqué ser local). Cada vez que un cliente se inicia, pide una dirección IP o una renovación de la que tiene prestada actualmente. El cliente recibe, junto con la dirección, algunos parámetros adicionales: puerta de enlace (gateway) por defecto, servidor WINS, servidor DNS, etc... Lo que DHCP consigue es que la asignación y liberación de las direcciones IP en una red sea dinámica y automática; se evita las duplicidades y se optimiza el consumo de direcciones. La intervención del administrador de redes, aún en grandes configuraciones es mínima.

El protocolo dinámico de configuración de HOST (DHCP) proporciona un mecanismo a través del cual las computadoras que usan el TCP/IP puedan obtener una dirección IP automáticamente cuando ingresan a una red. DHCP es un estándar abierto, desarrollado por el grupo de DHC del Internet Engineering Task Force (IETF).

El parámetro más importante de la configuración asignado por DHCP es la dirección IP. A una computadora se le debe asignar inicialmente una dirección IP específica que es apropiada a la red a la que pertenece esa computadora, y la cual no se asigna a ninguna otra computadora en esa red. Si una computadora se mueve a una nueva red, se le debe asignar una nueva dirección IP. DHCP se puede utilizar para manejar estas asignaciones automáticamente.

DHCP especifica otros parámetros importantes de la configuración, tales como la máscara y el servidor de nombres de dominio (DNS). Usando DHCP, un administrador de la red puede evitar la configuración "manual" de computadoras individuales con aplicaciones complejas y confusas, porque estas computadoras pueden obtener todos los parámetros requeridos de la configuración automáticamente mediante un servidor DHCP.

2.1.2. Simplificando la gestión de direcciones IP DHCP

El protocolo DHCP permite manejar rangos de direcciones IP de forma dinámica y automatizada.

En los años 80's era habitual utilizar un protocolo muy sencillo llamado BOOTP que permitía que algunos sistemas (normalmente máquinas Unix corriendo /etc/bootpd) asignaran direcciones IP a sistemas tales como impresoras o servidores de terminales. El servidor utilizaba un sencillo archivo de texto para buscar la dirección MAC del "cliente" y le asignaba la dirección IP (y algún otro parámetro) según constara en dicho archivo. Actualmente este sistema se usa, por ejemplo, para algunos elementos de electrónica de red

como switches o hubs y en ciertos modelos de impresoras con interfaz de red local.

El protocolo BOOTP utilizaba una estructura de tramas muy sencilla y el tráfico generado era mínimo. Desgraciadamente, no es suficiente para la mayoría de los casos y en redes de tamaño medio, su eficacia es muy baja.

A principios de la década de los 90's, la IETF (Internet Engineering Task Force) desarrolló el protocolo DHCP (Dynamic Host Configuration Protocol). Su objetivo principal era superar las limitaciones de BOOTP, ampliándolo y permitiendo que los administradores de redes se olvidaran, casi por completo, de la asignación de direcciones IP a las decenas o centenares de PC's y otras máquinas de su organización.

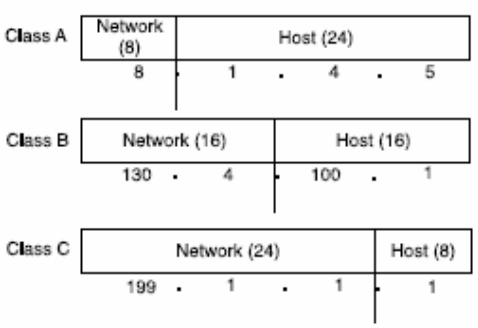
2.2 Revisión de direccionamiento IP

Muchas Clases de redes diferentes existen A, B, y C. La tabla resume los posibles números de redes, el número total de cada tipo, y el número de hosts en cada Clase A, B, y C de la red.

Observa en la tabla, la fila de Números de Red Válidas muestra los números de la red real. Hay algunos casos reservados. Por ejemplo, red 0.0.0.0 (originalmente definido para el uso de direccionamiento de broadcast) y la red 127.0.0.0 (todavía disponible para el uso de direccionamiento de loopback) son reservadas. Redes 128.0.0.0, 191.255.0.0, 192.0.0.0, y 223.255.255.0 también son reservadas.

	Class A	Class B	Class C
First Octet Range	1 to 126	128 to 191	192 to 223
Valid Network Numbers	1.0.0.0 to 126.0.0.0	128.1.0.0 to 191.254.0.0	192.0.1.0 to 223.255.254.0
Number of Networks in This Class	$2^7 - 2$	$2^{14} - 2$	$2^{21} - 2$
Number of Hosts Per Network	$2^{24} - 2$	$2^{16} - 2$	$2^8 - 2$
Size of Network Part of Address (bytes)	1	2	3
Size of Host Part of Address (bytes)	3	2	1

Sin el subneteo, una red de IP diferente debe usarse para cada red física. Por ejemplo, en la figura muestra tres direcciones IP, cada una de diferente red. Una dirección es una Clase A de red, una está en una Clase B red, y una está en una red de clase C.



Por definición, una dirección IP que empieza con 8 en el primer octeto es una red de Clase A, donde la parte de la red de la dirección es el primer byte, o el primer octeto. Una dirección que empieza 130 está en una Clase B de la red. Por definición, la Clase B de direcciones tiene 2-bytes en la parte de red, como vemos. Finalmente, cualquier dirección que empieza con 199 está es una red de clase C la cual tiene 3-bytes en la parte de la red. También por la definición, una Clase A dirección tiene 3-bytes en la parte de host, Clase B tiene 2 -bytes en la parte host, y la clase C tiene 1-byte en la parte de host.

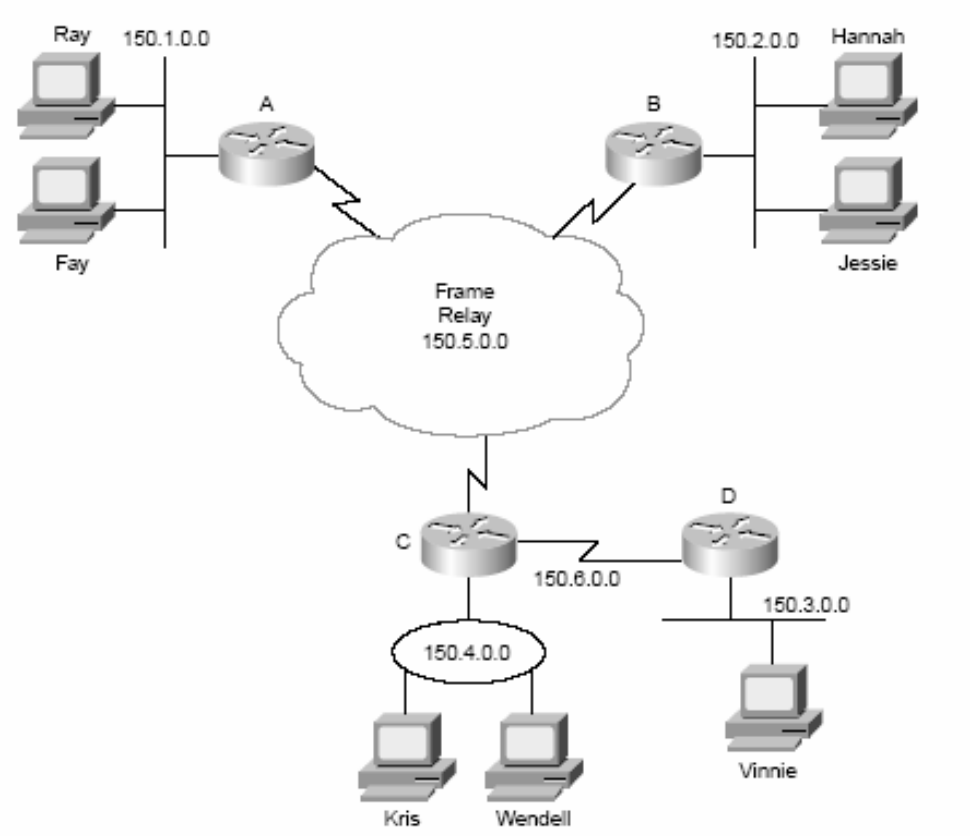
Class A, B, and C Networks: Network and Host Parts and Default Masks

Class of Address	Size of Network Part of Address in Bits	Size of Host Part of Address in Bits	Default Mask for Each Class of Network
A	8	24	255.0.0.0
B	16	16	255.255.0.0
C	24	8	255.255.255.0

2.3. Subneteando IP´s

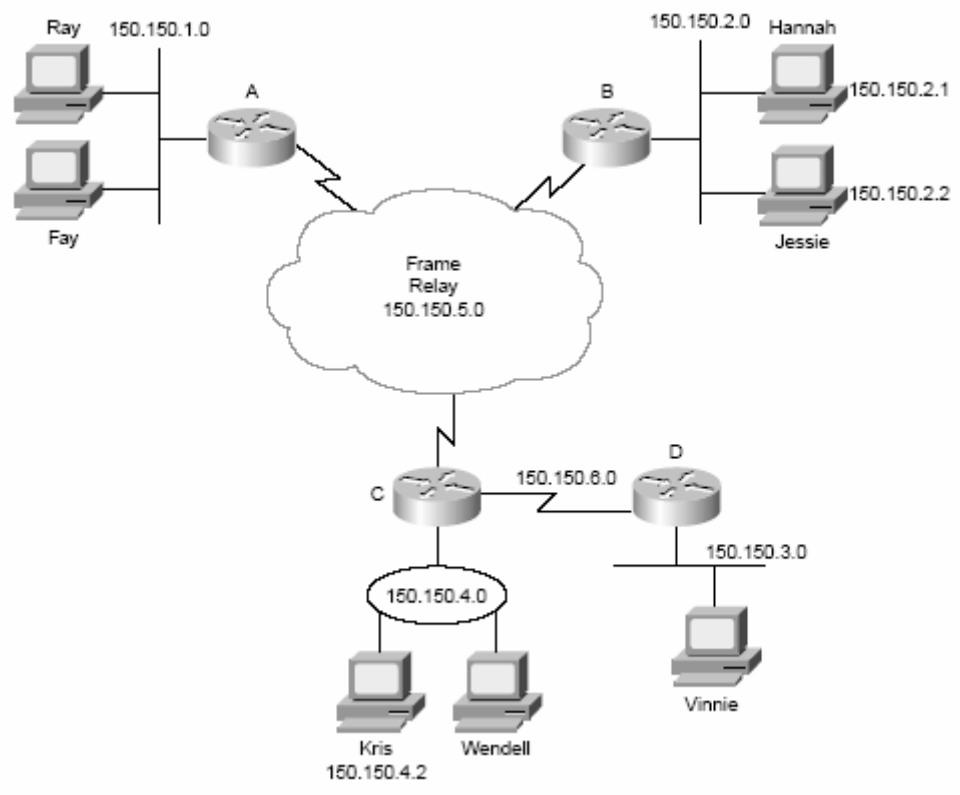
El subneteo de IP crea los números inmensamente más grandes de grupos más pequeños de direcciones de IP comparados utilizando simplemente Clase A, B, y convenciones del C. Las reglas para las redes de Clase A, B, y C todavía existen, pero ahora una sola Clase A, B, o la C de la red puede subdividirse en muchos grupos más pequeños. Subnetéandolos a una subdivisión de una sola Clase A, B, o C de la red como si fuera una red misma. Haciendo así, una sola Clase A, B, o C de la red puede subdividirse en muchas subredes.

Las figuras1 y 2 muestra las diferencias básicas entre una red que no usa subneteo y una que si lo hace. Primero, observemos la primer figura que usa seis redes de IP diferentes.



El diseño mostrado en Figura 1 tiene seis grupos, cada uno de los cuales son de Clase B de la red. En otros términos, las LAN's unidas al router A, B, C, y D son cada una red separada. Adicionalmente, las dos interfaces seriales que comprenden el enlace punto a punto entre el router C y D usan la misma red, porque estas dos interfaces no están separadas por un router. Finalmente, el entorno de la red entre los ruteadores A, B, y C no están separados por una IP del router y comprometería la sexta red.

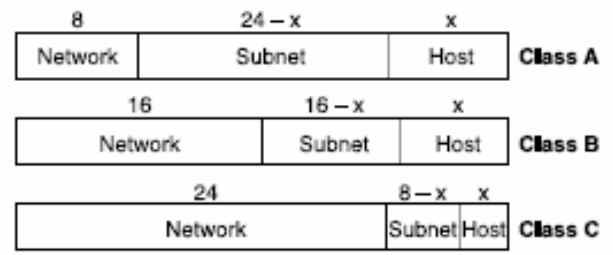
Como en la Figura 1, el plan mostrado en la Figura 2, requiere seis grupos. Al contrario de la Figura 1, la Figura 2 usa seis subredes cada uno de los cuales son una subred de la clase B de red.



Este es un diseño de la subred de Clase B de la red 150.150.0.0. La IP de la red diseñada ha escogido una máscara de 255.255.255.0, el último octeto de que implica 8 bits de hosts. Porque esta es una Clase B de red, hay 16 bits de la red. Hay 8 bits de subred, el cual pasa a ser 17 hasta 24 bits; en otras palabras por consiguiente, el tercer octeto.

Observe que en la red (los primeros dos octetos en este ejemplo) todos empiezan con 150.150, significando que cada uno de las seis subredes es una subred de Clase B conectan una red de computadoras 150.150.0.0.

Con el subneteo, la tercera parte de una dirección IP aparece en la mitad de la dirección. Este campo se crea "robando" o "pidiendo prestado" a los bits de la parte de los hosts de la dirección. El tamaño de la parte de la red de la dirección nunca cambia. En otros términos, las reglas de las redes de las Clases A, B, y C todavía aplican cuando se define el tamaño de la parte de la red de una dirección. Sin embargo, la parte del hosts de la dirección se encoge para hacer lugar a la parte de la subred. La figura muestra el formato de direcciones cuando el subneteo se usa.



2.3.1. Convirtiendo direcciones IP de decimal a binario y viceversa

Las direcciones IP son de 32-bits escritos en números binarios como una serie de números decimales separados por puntos. Es muy importante recordar los siguientes hechos en el proceso de la conversión para las direcciones IP.

- Cuando convertimos de un formato al otro, cada número decimal se representa en 8 bits.
- Cuando convertimos de binario a decimal, el conjunto de 8 bits consecutivos representa un número decimal.

Considerando la conversión de la dirección IP 150.150.2.1 a binario. El número 150, cuando lo conviertes a binario equivale a 10010110. El siguiente byte, otro decimal 150, se convierte a 10010110. El tercer byte, decimal 2, se convierte a 00000010. Finalmente, el cuarto byte, decimal 1, se convierte a 00000001. La serie combinada de la dirección IP en este caso es, 10010110 10010110 00000010 00000001.

Si se empieza con la versión binaria de la dirección IP, podemos separar primero en cuatro juegos de ocho dígitos. Entonces convertimos cada conjunto de ocho dígitos binarios a su equivalente en decimal. Para el ejemplo, escribiendo una dirección IP como sigue es correcto, pero no muy útil:

10010110100101100000001000000001

Para convertir este número a un formulario decimal más conveniente, primero sepárelo en cuatro juegos de ocho dígitos:

10010110 10010110 00000010 00000001

Vemos que los primeros 8 bits convertimos el número a 150 así como el segundo. El tercer juego de 8 bits lo convertimos en 2, y el cuarto juego lo convertimos a 1, quedando 150.150.2.1.

2.3.2. Operación booleana AND

George Boole, un matemático que vivió en los años 80's, creó una rama de matemática llamada "las matemáticas de bolean" debido a su creador. Las matemáticas de Bolean tiene muchas aplicaciones en la teoría computacional. De hecho, nosotros podemos encontrar la subred si se nos proporciona la dirección IP y la mascara de subred utilizando la operación Booleana AND.

La operación Booleana AND es obtener un resultado con un par de números binarios como se muestra en la siguiente lista:

0 AND 0 = **0**
0 AND 1 = **0**
1 AND 0 = **0**
1 AND 1 = **1**

En otros términos, la entrada a la ecuación consiste en dos dígitos binarios, y el resultado de la ecuación es un digito binario. La única vez en que el resultado es 1 binario es cuando ambos números de la entrada también son 1; cualquier otro, el resultado de la operación es un 0.

Podemos realizar la operación AND en los números binarios más largos simplemente realizando un AND en cada par de números. Por ejemplo, si nosotros queremos realizar la operación AND de los siguientes cuatro dígitos, 0110 y 0011, tendríamos que realizar un AND en el primer dígito de cada número y escribir el resultado. Entonces realizamos un AND en el segundo dígito de cada número, y así sucesivamente, para los cuatro dígitos. La tabla muestra este ejemplo.

	Four-Digit Binary Number	First Digit	Second Digit	Third Digit	Fourth Digit
First Number	0110	0	1	1	0
Second Number	0011	0	0	1	1
Boolean AND Result	0010	0	0	1	0

Esta tabla separa los cuatro dígitos del número original para hacer el punto más obvio. El primer dígito del primer número es 0, y el primer dígito del segundo número también es 0; 0 AND 0 es igual a 0. Semejantemente, los segundos dígitos de los dos números originales son 1 y 0, respectivamente, el resultado AND de estos dos dígitos es nuevamente 0. Para el tercer dígito, los dos números originales son 1 y 1, dando como resultado 1. Finalmente, para el cuarto dígito los dos números originales son 0 y 1, dando como resultado 0 para esa columna.

El subneteo de IP en las matemáticas frecuentemente usa el cálculo Booleano AND entre dos números binarios de 32 bits.

En la figura haremos una operación AND con la dirección IP y la mascara para sacar el número de subred.

	Decimal	Binary
Address	150.150.2.1	1001 0110 1001 0110 0000 0010 **0000 0001**
Mask	255.255.255.0	1111 1111 1111 1111 1111 1111 **0000 0000**
Result of AND	150.150.2.0	1001 0110 1001 0110 0000 0010 **0000 0000**

Primero, sólo nos enfocaremos en la tercera columna de la tabla. La conversión binaria de la dirección IP 150.150.2.1 se observa en la primera fila. La próxima fila muestra la conversión binaria de la máscara de la subred de 32-bits (255.255.255.0). La última fila muestra el resultado de la operación AND de los dos primeros números. En otras palabras, el primer bit en cada número es calculado con la operación AND, y entonces el segundo bit de cada número hace la misma operación AND, y el tercero, y así sucesivamente, hasta todos

los 32 bits en el primer número ha sido ANDed con el bit en la misma posición en el segundo número.

El número de 32-bits resultante es número de subred en el cual 150.150.2.1 residen. Todos los que tenemos que hacer regresan al convertir el número de 32-bits al decimal 8 bits en un momento. Los subred numeran en este caso es 150.150.2.0. Si nosotros entendemos la idea básica pero gustaría los ejemplos adicionales para hacerlo más claro. En los próximos ejercicios, usaremos la operación Booleana AND para contestar las preguntas básicas sobre el subneteo IP.

2.3.3. Anotación del prefijo

Entender la anotación del prefijo, es importante saber que todas las máscaras de subred tienen algunos números en binario 1's consecutivo, seguido por los 0's binarios. En otros términos, una máscara de subred no puede tener 1's y 0's esparcidos a lo largo de la máscara. La máscara siempre tiene algún número de binario 1's, seguido solo por 0's binario.

La anotación del prefijo denota el número de binarios 1's simplemente en una máscara, precedió por un /. En otros términos, para el subred de la mascara 255.255.255.0 cuyo equivalente binario es 11111111 11111111 11111111 00000000, la anotación del prefijo equivalente es /24, porque hay 24 binario 1's consecutivo en la máscara. Al hablar sobre subredes, nosotros podemos decir que a las cosas les gusta "Esa subred usa una cuchillada el prefijo 24" o "Ese subred tiene un prefijo del 24-bits" en lugar de decir algo como "Esa subred usa una máscara de 255.255.255.0."

La anotación del prefijo hace hablando un poco más fácil sobre las máscaras de subred, y hace la información también desplegada por el router un poco más breve. Por ejemplo, sólo de la prueba "255.255.255.0" unas veces, e imagina la red está abajo mientras nosotros estamos diciéndolo, y usted oirá el beneficio. Ahora que las herramientas de matemática básicas se han cubierto, el especifico de cómo usarlos encontrar las respuestas correctas a las preguntas de subneteo se cubre luego.

¿Cuántos hosts y Cuántas Subredes?

Nosotros también debemos saber deducir cuántas redes, subredes, y host de bits son utilizados con ese esquema de subneteo. De esos hechos, nosotros podemos deducir a cuántos hosts fácilmente existen en la subred y cuantas subredes que nosotros podamos crear en esa red que usa esa máscara de subred.

Nosotros ya hemos aprendido las Clase A, B, y C de las redes que tienen 8, 16, o 24 bits entre sus campos de la red, respectivamente. Esas reglas no cambian. Nosotros también lo tenemos que hacer sin el subneteo, Clase A, B, y C tienen las direcciones 24, 16, o 8 bits de hosts, respectivamente. Con el subneteo, la parte de la red de la dirección no se encoge o cambia, pero los hosts presentan los encogimientos para hacer el

sitio para el campo de la subred. Así que la clave para contestar estos tipos de preguntas es deducir cuántos bits de los host permanezca después del subneteo. Entonces usted puede decir el tamaño del campo de la subred. El resto de las respuestas sigue de esos dos hechos.

Los hechos siguientes le dicen cómo encontrar los tamaños de la red, la subred, y la parte de hosts de una dirección de IP:

La parte de la red de la dirección siempre se define por las reglas de la clase.

La parte de hosts de la dirección siempre se define por la máscara. Los 0's binarios en la máscara mencionan las direcciones de bits correspondientes que son parte del campo de los hosts.

La parte de la subred de la dirección es lo que falta para completar los 32-bits.

Step	Example	Rules to Remember
Address	8.1.4.5	—
Mask	255.255.0.0	—
Number of Network Bits	8	Always defined by Class A, B, C
Number of Host Bits	16	Always defined as the number of binary 0s in the mask
Number of Subnet Bits	8	32 – (network size + host size)

Este ejemplo tiene 8 bits de la red porque es una red de Clase A, 8.0.0.0. Hay 16 bits de host porque cuando nosotros convertimos 255.255.0.0 al binario, hay 16 0's binarios los últimos 16 bits en la máscara. El tamaño de la parte de la subred de la dirección es lo que sobra, o 8 bits.

Otro ejemplo podría ayudar su comprensión. Considere la dirección 130.4.102.1 con máscara 255.255.255.0. Primero, la dirección 130.4.102.1 está en una Clase B de la red, hay 16 bits de la red así que. Una máscara de subred de 255.255.255.0 tiene sólo 8 0's binarios, mientras que implica 8 bits de hosts que dejan 8 bits de subred en este caso.

Como otro ejemplo, considere la dirección 199.1.1.100 con máscara 255.255.255.0. Este ejemplo no hace ¡uso del subneteo! 199.1.1.100 están en una red de clase C ya que hay 24 bits para la parte de la red. La máscara tiene 8 0's binarios, quedando 8 bits para la parte del hosts y, sin bits para la parte de la subred. De hecho, si nosotros recordáramos que la máscara predefinida para las redes clase C es 255.255.255.0, nosotros ya podríamos haber comprendido que ningún subneteo estaba usándose en este ejemplo.

Nosotros probablemente podemos calcular fácilmente el número de bits de los host a si la máscara sólo usa decimal 255's y 0's, porque es fácil de

recordar ese decimal 255 representa 8 binarios 1's y decimal 0 representan 8 0's binarios. Así, para cada decimal 0 en la máscara, hay 8 bits de hosts. Sin embargo, cuando la máscara usa los valores decimales además del 0 y 255, el número de bits de los hosts es más difícil. Considere las direcciones y máscaras, junto con las versiones binarias de las máscaras, mostradas en la siguiente tabla.

Mask in Decimal	Mask in Binary
130.4.102.1, mask 255.255.252.0	1111 1111 1111 1111 1111 11**00 0000 0000**
199.1.1.100, mask 255.255.255.224	1111 1111 1111 1111 1111 1111 111**0 0000**

La primera máscara, 255.255.252.0, tiene 10 0's binarios, lo cual significa que hay 10 bits para la parte de los hosts. Porque esa máscara se usa con una Clase B (130.4.102.1), implicando 16 bits para la parte de la red, hay 6 bits de la subred restantes. En el segundo ejemplo, la máscara tiene sólo 5 0's binarios, dejando solo 5 bits de hosts. Porque la máscara se usa con una dirección de clase C, hay 24 bits de la red, mientras dejando sólo 3 bits de la subred.

Las reglas de la clase definen la parte de la red.

La máscara en binarios 0's definen la parte de los hosts.

El único problema grande ocurre cuando la máscara es tramposa como se mostró en los últimos dos ejemplos.

Cuando la máscara es difícil, tenemos dos alternativas por conocer cuántos bits de hosts son definidos:

Convertir la máscara a binario con cualquier método de conversión, y cuente el número de 0's.

Convierta la máscara a binario con la ayuda de los nueve valores decimales y binarios mostrado en tabla. Éstos son los únicos nueve valores decimales válidos usados en una subred de la máscara.

La tabla enlista el único decimal válido en una máscara y sus equivalentes binarios. Memorizando estos valores nos ayudarán a convertir las máscaras de su decimal y binario.

Decimal	Binary
0	0000 0000
128	1000 0000
192	1100 0000
224	1110 0000
240	1111 0000
248	1111 1000
252	1111 1100
254	1111 1110
255	1111 1111

¿Dado una dirección y un mascara, cuántos subredes hay? Y cuantos hosts son, ¿Allí en una sola subred?

Dos fórmulas simples proporcionan las respuestas.

$$\text{Número de subredes} = 2^{\textit{No. de subred por bit}} - 2$$
$$\text{Número de hosts por subred} = 2^{\textit{No. de subred por bit}} - 2$$

Estas fórmulas calculan el número de cosas que pueden numerarse usando un número binario y entonces menos 2 para los dos casos especiales. La dirección IP y las combinaciones definen que dos subredes por la red no se usen y que dos hosts por subred no se usen.

La subred que tienen todos los 0's binarios es llamada la subred cero y la subred con todos los binarios 1's es llamada la subred de broadcast y también es reservada. De hecho, se pueden usar ambas subredes en un ruteador de Cisco, pero se recomienda evitar usarlos.

El direccionamiento IP también reserva dos direcciones IP por subred: la primera cuando todos los binarios están en 0's en el campo del hosts de la dirección y la segunda; cuando todos los binarios están en 1's en el campo del hosts de la dirección. No existe forma alguna para utilizar estas dos direcciones.

Cinco Ejemplos de Direcciones/Mascaras, con el Número de Red, Subred, y Hosts Bits.

Address	8.1.4.5/16	130.4.102.1/24	199.1.1.100/24	130.4.102.1/22	199.1.1.100/27
Mask	255.255.0.0	255.255.255.0	255.255.255.0	255.255.252.0	255.255.255.224
Number of Network Bits	8	16	24	16	24
Number of Host Bits	16	8	8	10	5
Number of Subnet Bits	8	8	0	6	3
Number of Hosts Per Subnet	$2^{16} - 2$, or 65,534	$2^8 - 2$, or 254	$2^8 - 2$, or 254	$2^{10} - 2$, or 1022	$2^5 - 2$, or 30
Number of Subnets	$2^8 - 2$, or 254	$2^8 - 2$, or 254	0	$2^6 - 2$, or 62	$2^3 - 2$, or 6

Los detalles del algoritmo que utilizamos respondemos a las preguntas del subneteo sobre el número de hosts y subredes son resumidas en la lista siguiente:

Paso 1 Identificar la estructura de la dirección IP.

Paso 2 Identificar el tamaño de la parte de la red de la dirección basado en las reglas de Clase A, B, y C.

Paso 3 Identificar el tamaño de la parte del hosts de la dirección basado en el número de 0's binarios en la máscara. Si la máscara es difícil.

Paso 4 El tamaño de la parte de la subred que esta a la izquierda, matemáticamente, esto es 32 -(el número de red + los bits de host).

Paso 5 Declaran el número de subredes que es $2^{\text{número-de-subred-bits}}-2$.

Paso 6 Declaran el número de host por subred que es $2^{\text{número-de-host-bits}}-2$.

¿Cuál es el número de Subred, y cuales son las Direcciones IP en el Subred?

Una de las situaciones más comunes que tenemos que afrontar después de que conocemos la dirección IP y la mascara de subred debemos responder las preguntas sobre ellas. La pregunta puede ser directa ¿cual es el número de subred?, o podría ser más sutil, como ¿Cuales son las direcciones IP siguientes que están en la misma subred como la dirección indicada?

2.3.4. Encontrando el número de subred

En las tablas siguientes mostraremos el proceso de 5 ejercicios usando la operación Booleana AND.

Cálculo de la Subred con la Dirección 8.1.4.5, Máscara 255.255.0.0

Address	8.1.4.5	0000 1000 0000 0001 0000 0100 0000 0101
Mask	255.255.0.0	1111 1111 1111 1111 **0000 0000 0000 0000**
AND Result	8.1.0.0	0000 1000 0000 0001 0000 0000 0000 0000

Cálculo para la Subred con la Dirección 130.4.102.1, Máscara 255.255.255.0

Address	130.4.102.1	1000 0010 0000 0100 0110 0110 0000 0001
Mask	255.255.255.0	1111 1111 1111 1111 1111 1111 **0000 0000**
AND Result	130.4.102.0	1000 0010 0000 0100 0110 0110 0000 0000

Cálculo para la Subred con la Dirección 199.1.1.100, Máscara 255.255.255.0

Address	199.1.1.100	1100 0111 0000 0001 0000 0001 0110 0100
Mask	255.255.255.0	1111 1111 1111 1111 1111 1111 **0000 0000**
AND Result	199.1.1.0	1100 0111 0000 0001 0000 0001 0000 0000

Cálculo para la Subred con la Dirección 130.4.102.1, Máscara 255.255.252.0

Address	130.4.102.1	1000 0010 0000 0100 0110 0110 0000 0001
Mask	255.255.252.0	1111 1111 1111 1111 1111 11**00 0000 0000**
AND Result	130.4.100.0	1000 0010 0000 0100 0110 0100 0000 0000

Cálculo para la Subred con la Dirección 199.1.1.100, Máscara 255.255.255.224

Address	199.1.1.100	1100 0111 0000 0001 0000 0001 0110 0100
Mask	255.255.255.224	1111 1111 1111 1111 1111 1111 111**0 0000**
AND Result	199.1.1.96	1100 0111 0000 0001 0000 0001 0110 0000

Estas tablas muestran las respuestas, pero no muestran el procedimiento. Los pasos tomados para completar las tablas son los siguientes:

Paso 1 Empezamos colocando la dirección decimal y la máscara

Paso 2 Convertimos los dos números a binario, como se muestra en los cinco ejemplos.

Paso 3 Con cada bit se realiza la operación Booleana AND entre la dirección y la mascara en la misma posición con el otro número.

Paso 4 Debemos convertir el resultado de la operación Booleana AND a decimal.

El último paso en este proceso, es convertir el número binario de regreso a decimal. En algunos casos, la conversión es simple. Por ejemplo, la máscara de subred es 255.255.0.0. Porque la máscara tiene sólo 255's, o 0's en el decimal, el límite entre la subred y los campos del hosts también están en un byte el límite entre el segundo y tercer byte en este caso. Así la conversión del binario a decimal para el resultado de la operación Booleana AND es:

0000 1000 0000 0001 0000 0000 0000 0000.

La confusión surge típicamente cuando el límite entre la subred y parte del host de la dirección está en mitad de un byte que ocurre cuando la máscara de la subred tiene un valor diferente de 0 o 255 decimal. Por ejemplo, con 130.4.102.1, la mascara 255.255.252.0, los primeros 6 bits del tercer octeto comprenden el campo de la subred, y los últimos 2 bits del tercer octeto, más el cuarto octeto entero, comprenden el campo de los hosts. El problema puede surgir cuando la poca experiencia de las personas al convertir la subred de 6-bits de la parte de la subred de binario a decimal y los 10-bits de la parte del hosts a decimal. Sin embargo, al convertir el binario a decimal, al encontrar el punto decimal de la dirección IP siempre se convierte el octeto entero aun cuando la parte del octeto está en la parte de la subred de la dirección y parte está en la parte del hosts de la dirección.

Así que, en este ejemplo, el número de subred (130.4.100.0) en binario es 1000 0010 0000 0100 **0110 0100** 0000 0000. El tercer octeto entero se muestra en negrita en que convierte a 100 en decimal. Cuando convertimos el número en entero, cada uno de 8 bits se convierte al decimal, dando como resultado 130.4.100.0.

2.3.5. Encontrando la dirección de subred y la de broadcast

La dirección de subred de broadcast, a veces llamada comúnmente dirección de broadcast, puede usarse para enviar un paquete a cada dispositivo en una subred. Sin embargo, algunas herramientas y protocolos usan la dirección de subred de broadcast. Sin embargo, calculando la dirección de subred de broadcast, podemos calcular fácilmente las IP válidas para la subred que es una parte importante de contestar las preguntas de subneteo.

Hay una operación binaria para calcular la dirección de subred de broadcast. Hay un proceso más fácil sin embargo, sobre todo si ya tenemos el número de subred en binario:

Cambiar todos los valores de bits de hosts en el número de subred a 1´s binarios.

Podemos analizar las operaciones de una forma más sencilla a través de las siguientes tablas para calcular la dirección de subred de broadcasts. La

parte de hosts de las direcciones, las máscaras, el número de subred, y la dirección de broadcast están en negritas.

Calculando la Dirección de broadcast: Dirección 8.1.4.5, Máscara 255.255.0.0

Address	8.1.4.5	0000 1000 0000 0001 **0000 0100 0000 0101**
Mask	255.255.0.0	1111 1111 1111 1111 **0000 0000 0000 0000**
AND Result	8.1.0.0	0000 1000 0000 0001 **0000 0000 0000 0000**
Broadcast	8.1.255.255	0000 1000 0000 0001 **1111 1111 1111 1111**

Calculando la Dirección de broadcast: Dirección 130.4.102.1, Máscara 255.255.255.0

Address	130.4.102.1	1000 0010 0000 0100 0110 0110 **0000 0001**
Mask	255.255.255.0	1111 1111 1111 1111 1111 1111 **0000 0000**
AND Result	130.4.102.0	1000 0010 0000 0100 0110 0110 **0000 0000**
Broadcast	130.4.102.255	1000 0010 0000 0100 0110 0110 **1111 1111**

Calculando la Dirección de broadcast: Dirección 199.1.1.100, Máscara 255.255.255.0

Address	199.1.1.100	1100 0111 0000 0001 0000 0001 **0110 0100**
Mask	255.255.255.0	1111 1111 1111 1111 1111 1111 **0000 0000**
AND Result	199.1.1.0	1100 0111 0000 0001 0000 0001 **0000 0000**
Broadcast	199.1.1.255	1100 0111 0000 0001 0000 0001 **1111 1111**

Calculando la Dirección de broadcast: Dirección 130.4.102.1, Máscara 255.255.252.0

Address	130.4.102.1	1000 0010 0000 0100 0110 01**10 0000 0001**
Mask	255.255.252.0	1111 1111 1111 1111 1111 11**00 0000 0000**
AND Result	130.4.100.0	1000 0010 0000 0100 0110 01**00 0000 0000**
Broadcast	130.4.103.255	1000 0010 0000 0100 0110 01**11 1111 1111**

Calculando la Dirección de broadcast: Dirección 199.1.1.100, Máscara 255.255.255.224

Address	199.1.1.100	1100 0111 0000 0001 0000 0001 011**0 0100**
Mask	255.255.255.224	1111 1111 1111 1111 1111 1111 111**0 0000**
AND Result	199.1.1.96	1100 0111 0000 0001 0000 0001 011**0 0000**
Broadcast	199.1.1.127	1100 0111 0000 0001 0000 0001 011**1 1111**

Examinando la dirección de subred de broadcast en binario, podemos ver que estos son idénticos a los números de la subred, sólo que todos los bits de hosts tienen un valor binario 1 en lugar de binario 0.

2.3.6. Encontrando el rango de válidas direcciones IP en una subred

Sabemos que en cualquier subred, dos números son reservados. Los dos números reservados son el número de subred y la dirección de subred de broadcast. El número de subred es el numéricamente el número más pequeño en la subred, y la dirección de broadcast es el numéricamente el número más grande. Así el rango de direcciones IP válidas comienzan con 1 más que el número de subred y terminan con 1 menos de la dirección de broadcasts.

Aquí es una definición formal del "algoritmo" para encontrar las primeras y últimas direcciones IP en una subred cuando sabemos el número de subred y dirección de broadcast:

Para la primera dirección IP válida, copia el número de subred, pero súmale 1 al cuarto octeto.

Para la última dirección IP válida, copia la dirección de subred de broadcast, pero réstale 1 al cuarto octeto.

El rango de direcciones IP validas empiezan con el primer número y termina con el último.

En las tablas siguientes veremos las respuestas para los cinco ejemplos usados en este tema.

Subred: 8.1.4.5 / 255.255.0.0

Octet	1	2	3	4
Address	8	1	4	5
Mask	255	255	0	0
Subnet Number	8	1	0	0
First Address	8	1	0	1
Broadcast	8	1	255	255
Last Address	8	1	255	254

Subred: 130.4.102.1/255.255.255.0

Octet	1	2	3	4
Address	130	4	102	1
Mask	255	255	255	0
Subnet Number	130	4	102	0
First Address	130	4	102	1
Broadcast	130	4	102	255
Last Address	130	4	102	254

Subred: 199.1.1.100/255.255.255.0

Octet	1	2	3	4
Address	199	1	1	100
Mask	255	255	255	0
Subnet Number	199	1	1	0
First Address	199	1	1	1
Broadcast	199	1	1	255
Last Address	199	1	1	254

Subred: 130.4.102.1/255.255.252.0

Octet	1	2	3	4
Address	130	4	102	1
Mask	255	255	252	0
Subnet Number	130	4	100	0
First Address	130	4	100	1
Broadcast	130	4	103	255
Last Address	130	4	103	254

Subred: 199.1.1.100/255.255.255.224

Octet	1	2	3	4
Address	199	1	1	100
Mask	255	255	255	224
Subnet Number	199	1	1	96
First Address	199	1	1	97
Broadcast	199	1	1	127
Last Address	199	1	1	126

2.3.7. Encontrando las respuestas sin usar el binario

Podemos derivar el número de subred y direcciones de broadcast sin convertir a binario o realizando el calculo Booleano. Usando las operaciones binarias exigiendo encontrar el número de subred y la dirección de broadcast realmente nos ayuda a entender el subneteo hasta cierto punto. Para conseguir las respuestas correctas más rápidamente, podríamos evitar todas las conversiones y las operaciones binarias.

Si puedes encontrar el número de subred y dirección de broadcast, podemos encontrar el rango de direcciones válidas fácilmente en la subred. Las operaciones descritas en esta sección son enfocadas en ayudarnos a encontrar el número de subred y dirección de broadcast.

2.3.8. Calculo sencillo con mascaras fáciles

De todas las posibles mascaras de subred, solo tres mascaras usan solo 255´s y 0´s, 255.0.0.0, 255.255.0.0, y 255.255.255.0. A esto se le llama mascaras "fáciles" porque podemos encontrar el número de la subred y la dirección de broadcast mas fácilmente.

De estas tres máscaras fáciles, 255.0.0.0 no causa ningún subneteo. Por consiguiente, en este tema sólo nos preocupa cómo usar las dos máscaras fáciles que pueden usarse para el subneteo 255.255.0.0 y 255.255.255.0.

El proceso es simple. Encontrar el número de subred cuando dan una dirección IP y una máscara de 255.255.0.0 o 255.255.255.0, hacer lo siguiente:

Paso 1 Copia los primeros dos octetos (máscara 255.255.0.0) o los primeros tres octetos (máscara 255.255.255.0) de la dirección de IP original.

Paso 2 Apunta 0´s en los últimos dos octetos (máscara 255.255.0.0) o el último octetos (máscara 255.255.255.0).

¡Si, eso es fácil! Encontrando la dirección de subred de broadcast es así de sencillo:

Hacer la misma cosa como lo hicimos para encontrar la subred, pero en lugar de apuntar los 0´s en los 2 últimos octetos, escribir 255's.

En cuanto sepamos que el número de subred y dirección de broadcast, podemos encontrar las primeras y últimas direcciones IP fácilmente en la subred que usa la misma lógica vista anteriormente:

Para encontrar las primeras direcciones IP válidas en la subred, copia el número de subred, pero agrega 1 al cuarto octeto.

Para encontrar las últimas direcciones IP válidas en la subred, copia la dirección de broadcast, pero réstale 1 del cuarto octeto.

Cuando la máscara de subred no es 255.255.0.0 o 255.255.255.0, se considera que la máscara es difícil. ¿Por qué es difícil? sólo es difícil en la mayoría de las personas que no puede derivar fácilmente el número de subred y la dirección de broadcast sin usar las operaciones binarias. Podemos usar los mismos procesos binarios y exactamente la misma manera si la máscara es fácil o difícil. Sin embargo, estos procesos binarios toman tiempo para hacer cuando no podemos usar una calculadora. Así que un método más rápido de encontrar las mismas respuestas puede ayudar.

El proceso siguiente nos ayuda a encontrar el número de subred y dirección de broadcast sin las matemáticas binarias cuando la máscara es difícil.

Simplemente apunta la dirección IP y la mascara como se muestra la tabla más adelante, mientras ponemos cada octeto en una columna diferente.

La parte inusual de este método empieza cuando dibujamos un cuadro alrededor del octeto "interesante" en la tabla. Ya que el octeto de la máscara no es 255 o 0. El cuadro atrae la atención a la parte difícil de la lógica usada en este método.

Por ejemplo, la dirección 130.4.102.1, con máscara 255.255.252.0. Porque el tercer octeto de la máscara no es 0 o 255, el tercer octeto es donde la parte interesante del método tiene lugar.

Creamos un cuadro de la subred, rellena la parte de la dirección y la mascara, y dibuja un cuadro alrededor del tercer octeto, como se muestra en la tabla.

Subred: 130.4.102.1/255.255.252.0 después de Dibujar un cuadro alrededor del Interesante octeto

Octet	1	2	3	4
Address	130	4	102	1
Mask	255	255	252	0
Subnet Number				
First Address				
Broadcast				
Last Address				

Para completar el cuadro, observa la dirección IP original del octeto y copia la parte izquierda de la dirección hasta antes del recuadro del octeto interesante y colócalo dentro del número de subred, primera dirección, broadcast, y última dirección.

Observa que esta completamente lleno la parte izquierda del cuadro. El octeto interesante que está dentro del cuadro no debe copiarse.

En la tabla muestra el mismo ejemplo después de este paso.

Subred: 130.4.102.1/255.255.252.0 después de Copiar los Octetos a la Izquierda

Octet	1	2	3	4
Address	130	4	102	1
Mask	255	255	252	0
Subnet Number	130	4		
First Address	130	4		
Broadcast	130	4		
Last Address	130	4		

Para encontrar el número de subred, tenemos un par de pasos. El primer paso es fácil. En la parte derecha del recuadro del octeto interesante en el número de subred inserte 0.

Luego viene la parte tramposa del método que le da el valor del número de la subred en el octeto interesante. Primero encontrar a lo que se llama "número mágico", 256 menos la máscara del octeto interesante. En este caso, tenemos 256 - 252, o un número mágico de 4. Encontramos el múltiplo del número mágico que es el más cercano a la dirección del octeto más interesante pero este debe ser menos ó igual a este. En este ejemplo, 100 es un múltiplo del número mágico (4 * 25), y este múltiplo es menor o igual a 102. El próximo múltiplo supera el número mágico que es 104, que es mayor a 102, por lo tanto no es el correcto. El múltiplo del número mágico es el más cercano, pero no más grande, la dirección del octeto interesante es el valor de la subred del octeto interesante. Esto se resume en los siguientes pasos:

Paso 1 Hallar el número mágico que es 256 menos el valor de la máscara del octeto interesante.

Paso 2 Hallar el múltiplo del número mágico que es el más cercano, pero no mayor que el octeto interesante de la dirección.

Paso 3 Escribe abajo ese múltiplo del número mágico como el valor del el número de la subred del octeto más interesante.

En este ejemplo, simplemente colocamos el 100 para el tercer octeto del número de la subred en la tabla.

En cuanto sepamos que el número de subred, podemos encontrar fácilmente la primera dirección IP válida en la subred:

Encontrar la primera válida dirección IP de la subred, copia el número de subred, pero súmale 1 al cuarto octeto.

¡Eso es todo! Las tablas muestran el mismo ejemplo, pero con el número de la subred y primera válida dirección IP.
Subred: 130.4.102.1/255.255.252.0 con Subred y Primera dirección IP

Octet	1	2	3	4	Comments
Address	130	4	102	1	
Mask	255	255	252	0	
Subnet Number	130	4	100	0	Magic number = 256 – 252 = 4. 4 * 25 = 100, the closest multiple <= 102.
First Address	130	4	100	1	Add 1 to the subnet's last octet.
Broadcast	130	4			
Last Address	130	4			

Para encontrar el valor del octeto interesante, compare el octeto interesante de la dirección IP para encontrar el múltiplo más cercano del número mágico que no es más grande, el cual es 100 en este caso. Para conseguir la primera dirección válida, simplemente súmale 1 al último octeto del número de la subred, dándonos 130.4.100.1.

El paso final en este método encuentra la dirección de broadcast del el cual podemos encontrar la última dirección válida de la subred. Primero, en la dirección de broadcast, apunta un decimal 255 para todos los octetos a la derecha del recuadro. No apunte un 255 en el octeto dentro del recuadro. Recuerde, los octetos a la izquierda del recuadro de la subred ya deben estar rellenados, mientras dejando un solo octeto sin ningún valor a la derecha del octeto interesante. Para llenar el octeto interesante de la dirección de broadcast, usamos el número mágico de nuevo. El número mágico es 256 menos la máscara interesante del octeto. En este caso, tenemos 256 - 252, o un número mágico de 4. Entonces agregamos el número mágico al valor del octeto interesante del número de la subred y restarle 1.

El resultado es el valor de la dirección de broadcast en el octeto interesante. En este caso, el valor es:

100 + 4 (el número mágico) -1 = 103.

En cuanto sepamos la dirección de broadcast, podemos encontrar fácilmente la última dirección IP válida de la subred:

Para encontrar la última dirección IP válida en la subred, copia la dirección de broadcast, pero réstale 1 del cuarto octeto.

Resumido la parte tramposa de este algoritmo:

Encontrar el valor del octeto interesante de la dirección de broadcast, toma el valor del octeto interesante del número de la subred, súmale el número mágico, y réstale 1.

En la tabla nos muestra las respuestas completas, con las anotaciones.

Subred: 130.4.102.1/255.255.252.0 completados

Octet	1	2	3	4	Comments
Address	130	4	102	1	
Mask	255	255	252	0	
Subnet Number	130	4	100	0	Magic number = 256 – 252 = 100. 4 * 25 = 100, the closest multiple <= 102.
First Address	130	4	100	1	Add 1 to the subnet's last octet.
Broadcast	130	4	103	255	Subnet-interesting-octet, plus the magic number, minus 1 (100 + 4 – 1).
Last Address	130	4	103	254	Subtract 1 from the fourth octet.

¿Qué mascara de subred conoce los requisitos del diseño?

Hasta ahora se ha explicado cómo responder a preguntas que proporcionan el número de subred.

Sin embargo, algunas preguntas no proporcionan el número de subred, pero en cambio se le puede pedir que escoja la mascara de subred correcta proporcionando un par de requisitos. Las preguntas mas frecuentes pueden decir algo así:

Estamos utilizando una red X de Clase B, y se necesitan 200 subredes, con al menos 200 host por subred. ¿Cual de las máscaras de subred siguientes podemos utilizar? Esto es seguido por algunas máscaras de subred y tendremos que elegir la respuesta correcta.

Para encontrar las respuestas correctas a estos tipos de preguntas, primero necesitamos decidir cuántos bits de subred y bits de hosts necesitamos para reunir los requisitos. Básicamente, el número de hosts por subred es "2^x – 2", dónde x es el número de bits por hosts en la dirección. Igualmente, el número de subredes en una red, asumiendo que la misma máscara de subred se usa en toda la red, también es 2^x - 2, pero donde x es el número de bits de la subred. En cuanto conozcamos cuantos bits de subred y bits de hosts son requeridos, se podrá deducir que mascara será requerida para conseguir este objetivo.

Ejemplo:

Se tiene una red 130.1.0.0 de clase B. ¿Qué mascara de subred se requiere para tener al menos 200 hosts por subred?

Primero necesitamos conocer cuántos hosts por subred nos permite 200 subredes. Utilizamos la fórmula 2^X -2 y se le da valores a x hasta que uno de los resultados nos de por lo menos 200. En este caso, x resulta ser 8. En otros términos, se necesitan por lo menos 8 hosts por subred para permitir 200 subredes.

A continuación se muestra una tabla con los resultados de la formula.

El Número máximo de Subredes/Hosts

Number of Bits in the Host or Subnet Field	Maximum Number of Hosts or Subnets ($2^x - 2$)
1	0
2	2
3	6
4	14
5	30
6	62
7	126
8	254
9	510
10	1022
11	2046
12	4094
13	8190
14	16,382

En cuanto a la pregunta que se realizo anteriormente, 7 bits de la subred no son suficientes, porque esto solo permitiría 126 subredes. Se Necesitarían 8 bits para la subred.

Finalmente, se necesita decidir qué máscara(s) utilizar, conociendo que se tiene una red de clase B y que se deben tener por lo menos 8 bits de la subred y 8 bits para los hosts. Usando la letra N para representar los bits de la red, la letra S para representar los bits de la subred, y la letra H para representar los bits de hosts, lo siguiente muestra el tamaño de estos campos.

NNNNNNNN NNNNNNNN SSSSSSSS HHHHHHHH

Esto nos muestra que necesitamos 8 bits para la subred y 8 para los hosts y debido a que tenemos una red de clase B se necesitan 16 bits para la red, por consiguiente solo una mascara es posible para cumplir con este requerimiento.

"Por definición los bits de la red y la subred en una mascara de subred son todos binarios 1's. Semejantemente, los bits del hosts en una máscara de subred son, por definición, todos 0's binarios".

Así que, solo la única mascara de subred valida, en binario es la siguiente:

11111111 11111111 11111111 00000000

Cuando se convierte al decimal este binario quedaría así, 255.255.255.0.

Otro ejemplo donde se muestra múltiples posibles mascaras de subred es mostrado a continuación:

"Se tiene la red de clase B con dirección 130.1.0.0. ¿Qué máscara de subred se requiere para permitir al menos 50 subredes, con al menos 200 hosts por subred?"

Para este diseño, se necesita por lo menos 8 bits de hosts, pero ahora sólo se requieren por lo menos 6 bits de subred. 6 bits de subred permiten 2^6 - 2, o 62 subredes. Siguiendo el ejemplo anterior, pero usando una letra X para los bits que pueden ser utilizados para la subred o para los hosts, el formato para esta estructura quedaría de la siguiente forma:

NNNNNNNN NNNNNNNN SSSSSSXX HHHHHHHH

En otras palabras, la dirección de la mascara de subred quedaría algo así, tendría 16 bits de red, por lo menos 6 bits de subred, y por lo menos 8 bits de hosts. Este ejemplo permite tres mascaras de subred validas, cuya estructura es la siguiente:

NNNNNNNN NNNNNNNN **SSSSSSSS HHHHHHHH** - ***8 subred, 8 host***

NNNNNNNN NNNNNNNN **SSSSSSSH HHHHHHHH** -***7 subred, 9 host***

NNNNNNNN NNNNNNNN **SSSSSSHH HHHHHHHH** - ***6 subred, 10 host***

Así que, basado en los requerimientos de la pregunta, las tres mascaras de subred validas que cumplen con estos requisitos serían las siguientes:

11111111 11111111 11111111 00000000 - ***255.255.255.0***
11111111 11111111 11111110 00000000 - ***255.255.254.0***
11111111 11111111 11111100 00000000 - ***255.255.252.0***

CAPÍTULO III. RUTEADORES

3.1 Definición de Ruteador

Los dispositivos que generalmente se usan en la actualidad para realizar la interconexión de redes se denominan Routers.

Un ruteador es un dispositivo de propósito general diseñado para segmentar la red, con la idea de limitar tráfico de brodcast y proporcionar seguridad, control y redundancia entre dominios individuales de brodcast, también puede dar servicio de firewall. El ruteador cuenta normalmente con una o más interfaces LAN, una o más interfaces WAN y una conexión para una consola de control.

El ruteador opera en la capa 3 del modelo OSI y tiene más facilidades de software que un switch. Al funcionar en una capa mayor que la del switch, el ruteador distingue entre los diferentes protocolos de red, tales como IP, IPX, AppleTalk o DECnet. Esto le permite hacer una decisión más inteligente que al switch, al momento de reenviar los paquetes.

Un router opera mediante un sistema operativo (generalmente propietario) denominado IOS (Internetworking Operating System), el cual posee una serie de comandos mediante los cuales se realiza la configuración del mismo.

El ruteador realiza las siguientes funciones básicas:

- El rol de ruteador cambia desde el rol tradicional de proveer firewall y supresión de broadcast a un control basado en políticas, administración de broadcast y procesamiento/distribución de rutas.

- El ruteador es responsable de crear y mantener tablas de ruteo para cada capa de protocolo de red, estas tablas son creadas ya sea estáticamente o dinámicamente. De esta manera el ruteador extrae de la capa de red la dirección destino y realiza una decisión de envío basado sobre el contenido de la especificación del protocolo en la tabla de ruteo.

- La inteligencia de un ruteador permite seleccionar la mejor ruta, basándose sobre diversos factores, más que por la dirección MAC destino. Estos factores pueden incluir la cuenta de saltos, velocidad de la línea, costo de transmisión, retrazo y condiciones de tráfico. La desventaja es que el proceso adicional de procesado de frames por un ruteador puede incrementar el tiempo de espera o reducir el desempeño del ruteador cuando se compara con una simple arquitectura de switch.

- Segmentar la red dentro de dominios individuales de brodcast.

- Suministrar un envío inteligente de paquetes. Y

- Soportar rutas redundantes en la red.

Aislar el tráfico de la red ayuda a diagnosticar problemas, puesto que cada puerto del ruteador es una subred separada, el tráfico de los brodcast no pasara a través del ruteador.

Otros importantes beneficios del ruteador son:

- Los ruteadores siguen siendo vitales para las arquitecturas conmutadas configuradas como VLAN´s ya que ellos proveen la comunicación entre grupos de trabajo definidos lógicamente.

- Los ruteadores proveen acceso de la VLAN a recursos compartidos tales como servidores o computadoras centrales.

- Ellos también proveen la conectividad a otras partes de la red que están lógicamente segmentadas con el esquema más convencional de subredes o permiten el acceso a sitios remotos a través de enlaces WAN.

- Los ruteadores externos se pueden integrar en la arquitectura conmutada con una o múltiples conexiones backbone de alta velocidad (FDDI, Fast Ethernet o ATM). Estas conexiones proveen las siguientes ventajas:

  - Una mayor comunicación entre switches y ruteadores

  - Consolidación de un mayor número total de puertas físicas de ruteo para comunicación entre VLAN´s

- Proporcionar seguridad a través de sotisficados filtros de paquetes, en ambiente LAN y WAN.

- Permitir diseñar redes jerárquicas, que deleguen autoridad y puedan forzar el manejo local de regiones separadas de redes internas.

La comunicación de los ruteadores con otros (y el mantenimiento de sus tablas de ruteo) se ejecuta a través de la transmisión de una variedad de mensajes. El mensaje *routing update* es uno de tales mensajes. Este consiste generalmente de toda o una porción de una tabla de ruteo. Analizando los routings updates de otros ruteadores, un ruteador puede construir una imagen detallada de la topología de la red.

Un *link-state-advertisement* es otro ejemplo de los mensajes enviados entre ruteadores. Este informa a otros ruteadores del estado del vínculo del remitente. La información de enlace puede también ser usada para construir una imagen

completa de la topología de red. Una vez que la topología de red es entendida, los ruteadores pueden determinar las rutas óptimas para los destinos de la red.

3.2 Configuración del ruteador

Los algoritmos de conmutación son relativamente simples, y son básicamente los mismos para la mayoría de los protocolos de ruteo. En la mayoría de los casos, un host determina que debe enviar un paquete a otro host. Teniendo la dirección de un ruteador de alguna manera, el host fuente envía un paquete direccionado específicamente a una dirección física de un ruteador (MAC layer), pero con la dirección de protocolo (Network layer) del host destino. Examinando la dirección de destino de protocolo del paquete, el ruteador determina o no como enviar el paquete al siguiente salto. Si el ruteador no conoce como enviar el paquete, típicamente lo descarta. En caso contrario cambia la dirección física del destino para el siguiente salto y transmite el paquete. El siguiente salto puede o no ser el host destinatario final. Si no lo es, será generalmente otro ruteador, el cual ejecuta nuevamente el proceso de decisión de conmutación. Mientras el paquete se mueve a través de la red, sus direcciones físicas cambian, pero su dirección de protocolo permanece constante.

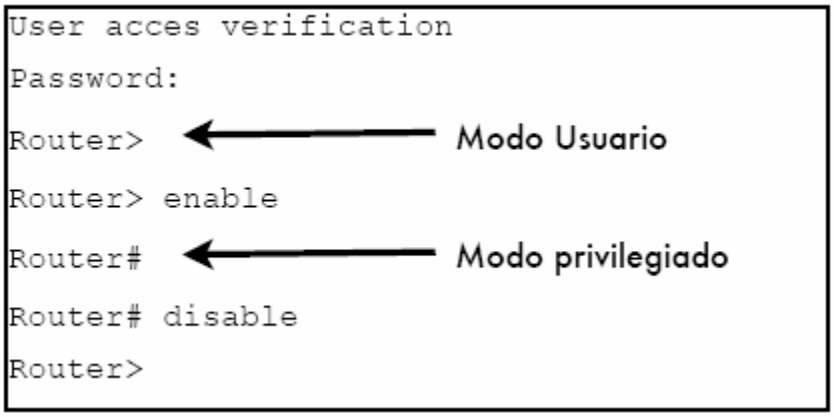
La configuración de un ruteador se realiza mediante una línea de comandos similar a un sistema UNIX. Dicha configuración puede ser realizada de forma local o remota. Para ello, el ruteador cuenta con un puerto de consola, que es el que se utiliza para realizar la configuración de manera local, y también un puerto auxiliar, el cual se utiliza para configurarlo de manera remota.

Para configurar el ruteador localmente se utiliza un conector serial del tipo DB-9 en un extremo, y RJ-45 en el otro.

Cable de conexion para configuracion local

Una vez realizada la conexión entre el ruteador y la PC, debemos configurar Hyperterminal para acceder a la línea de comandos. Una vez terminada la configuración de Hyperterminal (la cual es muy sencilla), se nos presentara en pantalla la línea de comandos del ruteador.

El ruteador presenta dos modos de trabajo, para una mayor seguridad. Estos se denominan "Modo usuario" y "Modo privilegiado". El modo usuario presenta una cantidad reducida de comandos del ruteador, y se utiliza únicamente para ver el estado del ruteador. En este modo no se permite realizar cambios en la configuración del ruteador. En el modo privilegiado, a diferencia del modo usuario, se presenta todo el set de comandos de configuración del ruteador, y es justamente este modo quien nos permite realizar cambios en dicha configuración. Para diferenciar entre los dos modos de trabajos, debemos poner atención al prompt que tenemos en pantalla.



Si estamos trabajando en modo usuario, entonces deberemos tener un signo ">" (sin comillas) seguido del nombre del ruteador. En cambio, si estamos trabajando en modo privilegiado, deberemos ver un "#" seguido del nombre del ruteador. Si nos queremos desconectar por completo del ruteador, se utiliza el comando "exit", tanto desde el modo usuario como también desde el modo privilegiado.

Si nos queremos desconectar por completo del ruteador, se utiliza el comando "exit", tanto desde el modo usuario como también desde el modo privilegiado.

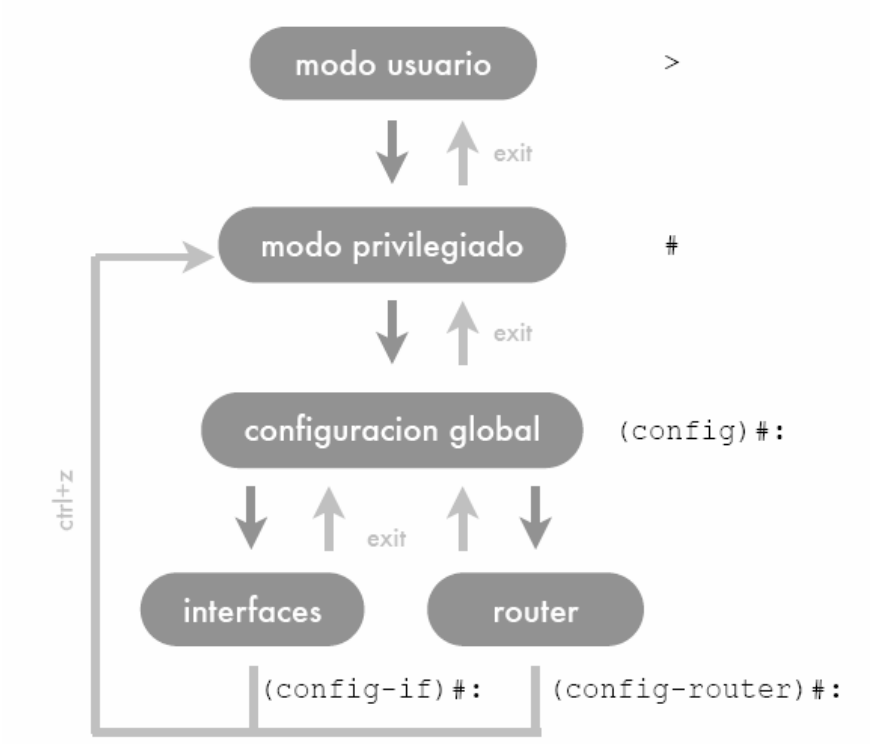
Cuando ingresamos al ruteador, inicialmente se nos sitúa en el modo usuario. Como dijimos, desde este modo solo es posible verificar el estado del ruteador, sin poder realizar cambios en la configuración del mismo. Para ello, debemos ingresar en el modo privilegiado. Para realizar esto, utilizamos el comando *enable* desde el modo usuario. Ahora, si queremos volver al modo usuario, se utiliza el comando "*disable*". Desde el modo privilegiado podemos

acceder a diferentes modos de configuración del ruteador, los cuales se listan en la siguiente tabla.

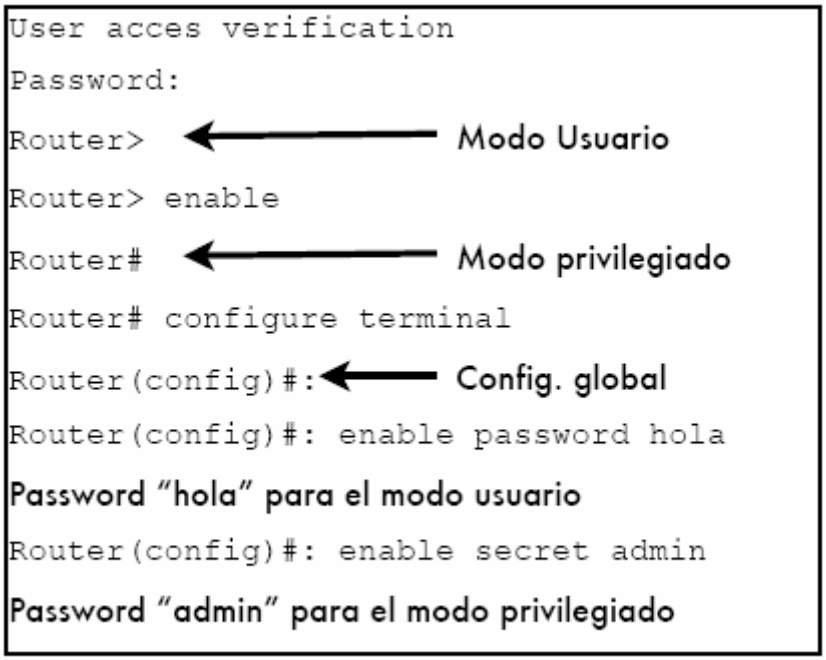
Modo	Comando/Prompt	Descripcion
Configuracion global	`Router#: configure terminal` ↓ `Router(config)#:`	A partir de este modo, podemos acceder a los que se describen a continuacion en la tabla, como asi tambien configurar algunos parametros del router.
Configuracion de interfaces	`Router(config)#: interface ethernet 0` ↓ `Router(config-if)#:`	En este modo es posible configurar las diferentes interfaces que contenga el router, como por ejemplo, asignar direcciones ip, direcciones de red, etc.
Configuracion de protocolos de enrutamiento	`Router(config)#: router protocolo` ↓ `Router(config-router)#:`	En este modo configuramos el protocolo de enrutamiento a usar, el cual es especificado como parametro del comando "router"

La tabla muestra los modos de configuración mas importantes, no todos.

3.2.1 Modo de configuración global

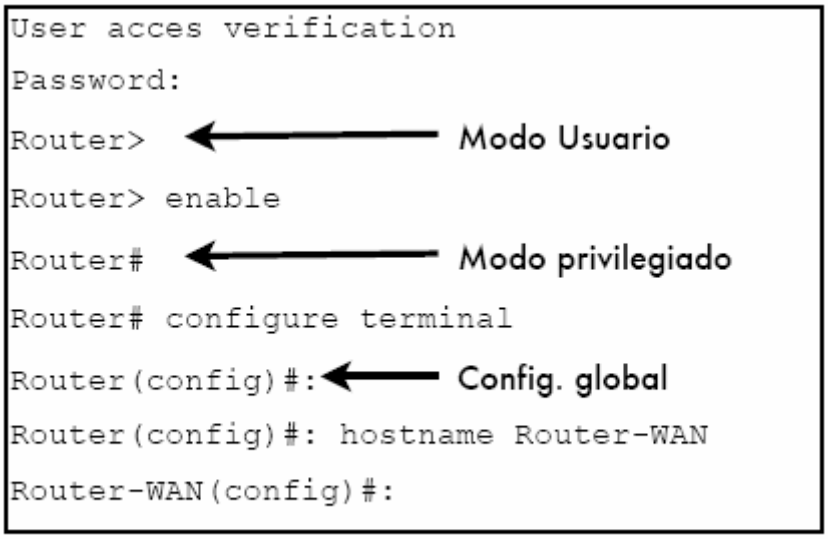


Dentro de este modo podemos definir parámetros como ser el nombre del ruteador, contraseñas para los modos usuarios y privilegiado, mensajes de bienvenida, etc. Para dar seguridad al ruteador mediante contraseñas, tanto para el modo usuario como para el modo privilegiado, debemos utilizar el comando "*enable password*" (para la contraseña del modo usuario) y "*enable secret*" (para la contraseña del modo privilegiado) seguidos de la contraseña a utilizar. Cabe aclarar que la contraseña utilizada para el modo usuario no se encuentra encriptada. Esto no ocurre con la contraseña del modo privilegiado, la cual si esta encriptada. A continuación vemos un ejemplo de protección de ambos modos mediante passwords.



Proteccion de un router con passwords

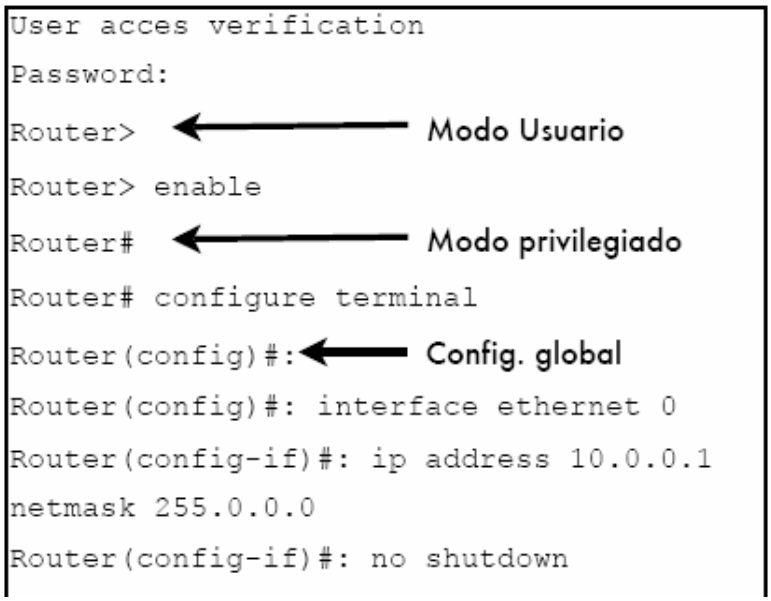
Otro parámetro que podemos configurar dentro de este modo es el nombre del ruteador. Esto es útil para diferenciar un ruteador del otro, colocando un nombre de acuerdo a la ubicación geográfica del mismo, departamento dentro de una organización al que pertenece, etc. Para configurar el nombre del ruteador, se utiliza el comando "hostname" seguido del nombre que queremos ponerle. A continuación se muestra un ejemplo en donde se le asigna el nombre Router-WAN al dispositivo.



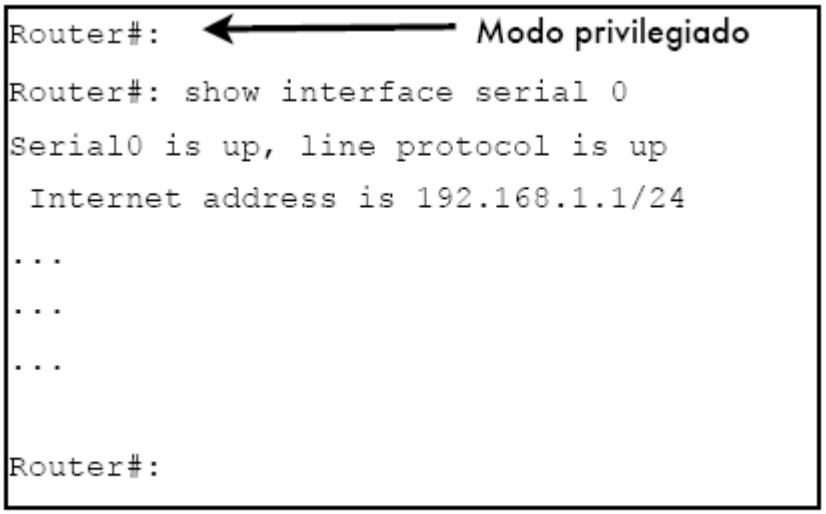
Configuracion del nombre

3.2.2. Configuración de interfaces

Dentro de este modo lo que se hace es configurar las interfaces del ruteador, asignándoles una dirección, levantándolas, etc. Como vimos anteriormente, para ingresar a este modo, debemos hacerlo desde el modo de configuración global. Una vez en el, utilizamos el comando "*interface*" seguido del tipo de interfaz y el numero en el caso de poseer mas de una interfaz del mismo tipo. Por ejemplo, en un ruteador que cuenta con dos interfaces Ethernet, para configurar una de ellas el comando seria '*interface ethernet 0*'dentro del modo de configuración global, lo cual luego nos introducirá en el modo de configuración de dicha interfaz, dentro del cual aparece una nueva serie de comandos disponibles.



Si queremos asignar una dirección ip a la interfaz en la que nos encontramos, utilizamos el comando "*ip address*" seguido de la dirección ip y la mascara de subred. Una vez hecho esto, la interfaz queda configurada con dicha dirección y mascara, pero no esta activada. Para ello, debemos utilizar el comando "*no shutdown*" para levantarla y dejarla funcional. Finalizada la configuración de la interfaz, podemos ver los parámetros que configuramos mediante el comando "*show interface*" *interfaz* del modo privilegiado, donde interfaz se refiere al nombre de la interfaz que acabamos de configurar (serial0, ethernet0, etc.). A continuación vemos un resumen de lo que obtenemos como salida de dicho comando:



Resumen de la configuracion de una interfaaz serial

De la salida del comando, lo que más nos interesan son las dos primeras líneas. La primera (*Serial0 is up, line protocol is up*) nos permite saber si la interfaz se encuentra configurada correctamente o no, y además permite saber de que tipo de problema se trata en el caso de que tengamos uno. A continuación vemos las diferentes posibilidades respecto al estado de una interfaz.

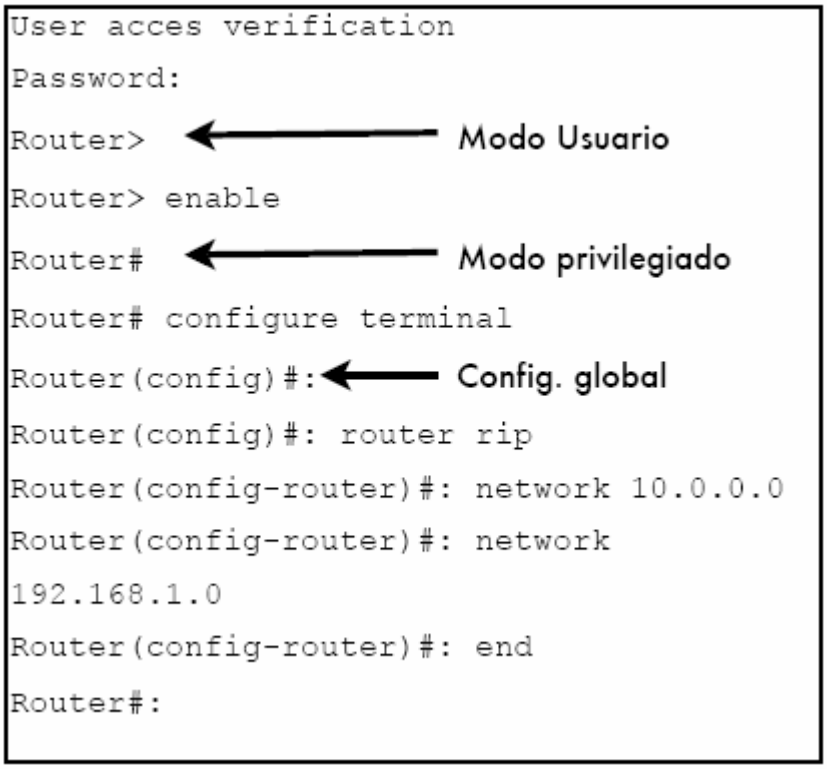
La segunda línea nos indica la dirección ip de la interfaz junto con la mascara de subred (el /24 hace referencia a la mascara e indica que dicha mascara es de 24 bits, es decir, 255.255.255.0).

Por ultimo, si la interfaz que estamos configurando actúa como DCE, debemos especificar un clock rate para la sincronización entre los ruteadores. A esto lo hacemos con el comando "*clock rate*" seguido de un numero entre 300 bps y 4000000 bps dentro del modo de configuración de interfaz.

Interface# is	line protocol is	Descripcion
down	down	Problema de interfaz
up	up	Interfaz op-eracional
up	down	Problema de conexion (cable)
admin down	down	Deshabilitada (levantar mediante no shutdown)

3.2.3. Configuración del protocolo de ruteo

Para la configuración del protocolo de enrutamiento a utilizar, debemos ingresar al modo de configuración global, desde el cual luego ingresaremos al modo de configuración de dicho protocolo mediante el comando "*router*" seguido del nombre del protocolo que quieramos utilizar (RIP, IGRP, etc.). Luego, dentro del modo de configuración del protocolo, debemos especificar las redes a las que el ruteador se encuentra directamente conectado. A esto lo hacemos mediante el comando "*network*" seguido de la dirección de dicha(s) red(es). Veamos un ejemplo donde utilizamos RIP como protocolo de enrutamiento y el ruteador se encuentra conectado a las redes 192.168.1.0 y 10.0.0.0:

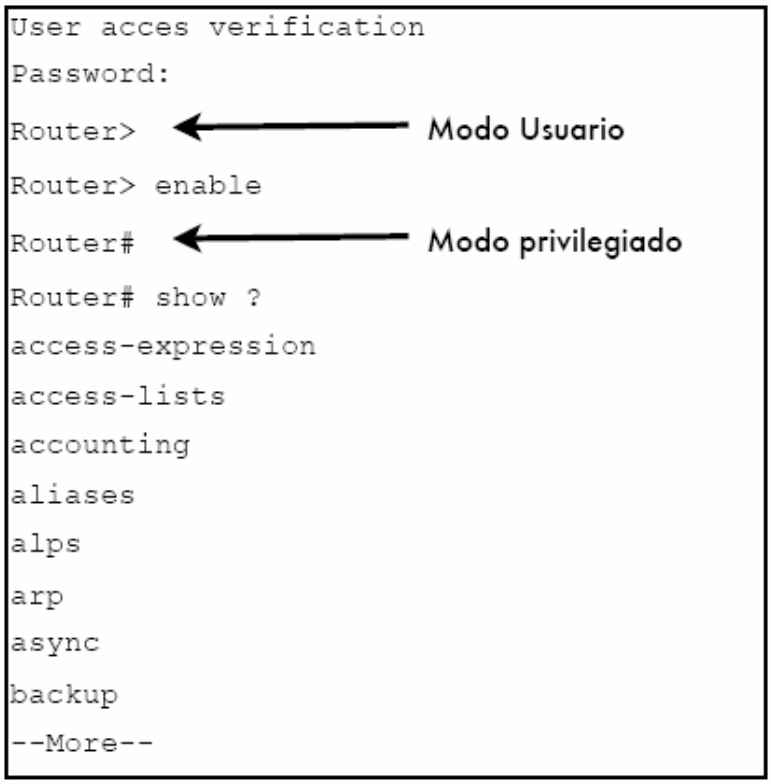


Vemos que debemos escribir una entrada por cada red a la que el ruteador se encuentra conectado. En el caso de utilizar IGRP como protocolo de ruteo, el mecanismo es el mismo, salvo que al especificar el nombre del protocolo, también debemos asignar un número de sistema autónomo.

3.2.4. Algunos comandos del ruteador

Los comandos "*show*" permiten monitorear el ruteador y de esa manera verificar el estado del mismo como así también detectar fallas. Existe una gran variedad de estos comandos, por lo que es recomendable escribir parte del comando y utilizar el signo de pregunta para ver las opciones posibles. Esto se puede realizar con todos los comandos disponibles, y resulta de gran utilidad cuando no nos acordamos de todos los parámetros que debemos pasar a determinados comandos.

Por ejemplo, para el caso del comando *show*, escribimos *show ?* y nos aparecerá una lista con todas las opciones disponibles. Lógicamente, la lista será diferente para el modo usuario que para el modo privilegiado, siendo la de este último la más extensa. A esto lo podemos ver en el ejemplo de la derecha. Como vemos, la palabra "*More*" al final de la lista indica que todavía tenemos más opciones para el comando. Nosotros solo analizaremos las que mas útiles nos resultaran a la hora de verificar el estado del ruteador. A continuación se muestra una tabla con los comandos "*show*" mas utilizados, con una descripción de cada uno.



Comando	Descripcion
show running-config	Muestra informacion sobre el archivo de configuracion actualmente en uso por el router.
show startup-config	Muestra informacion sobre el archivo de configuracion guardado en el router, es decir, con el que se inicio el router antes de haber realizado cambios al mismo.
show version	Muestra informacion general del router, como ser, la configuracion de hardware, version del sistema operativo, la imagen de arranque, etc.
show interfaces	Muestra las interfaces del router, como asi tambien el estado de las mismas.
show ip route	Muestra informacion sobre las tablas de ruteo.
show protocols	Muestra informacion sobre los protocolos de ruteo configurados en el router.
show flash	Muestra informacion acerca de la memoria flash del router, que es donde se encuentra almacenada la imagen del IOS.

3.3 Protocolos de ruteo

Los protocolos de ruteo determinan la ruta óptima a través de la red usando algoritmos de ruteo e información de transporte sobre estas rutas. Los protocolos de ruteo funcionan en la capa de red del modelo de referencia OSI. Ellos usan información específica de la capa de red, incluyendo direcciones de red, para mover unidades de información a través de la red.

Los algoritmos de los protocolos de ruteo actúan en dos funciones primarias:

Determinación de la ruta: la determinación de la ruta permite a un ruteador seleccionar la interfaz más apropiada para enviar un paquete.

Conmutación de la ruta: la conmutación de la ruta permite a un ruteador a aceptar un paquete en una interfaz y mandarlo por una segunda interfaz.

3.3.1. Protocolo de información de ruteo RIP

La Internet se compone de una gran cantidad de sistemas autónomos (AS). Cada AS es operado por una organización diferente y puede usar internamente su propio algoritmo de enrutamiento. El algoritmo de enrutamiento interno de un AS se llama protocolo de pasarela interior; al algoritmo de enrutamiento entre varias AS se le llama protocolo de pasarela exterior. El protocolo RIP, al igual que sus antecesores propietarios, es un protocolo de ruteo que fue diseñado para funcionar como protocolo "*vector distancia*". Se debe que tener en cuenta las siguientes tres limitaciones:

1) El protocolo no permite más de quince saltos;

2) El problema del "*conteo a infinito*", que puede surgir en situaciones atípicas en las cuales se puedan producir bucles;

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

Tabla de ruteo del RIP

La base de datos de ruteo de cada uno de los hosts de la red que utilizan el protocolo de ruteo RIP tiene los siguientes campos: dirección de destino, siguiente salto, interfaz de salida del enrutador, métrica y temporizador.

3.3.2. Protocolo de enrutamiento de pasarela interior: OSPF

El protocolo de pasarela interior original de Internet fue un protocolo de vector de distancia (RIP) basado en el algoritmo Bellman-Ford. En 1988, la Internet Engineering Task Force (Grupo de Trabajo de Ingeniería de Internet) comenzó a trabajar en su sucesor. Ese sucesor llamado OSPF (Open Shortest Path First, abrir primero la trayectoria más corta), se convirtió en estándar en 1990.

3.3.3. Protocolo IGRP

IGRP es un protocolo Distancia Vector desarrollado por Cisco que tiene varias características que lo diferencian de otros protocolos Distancia Vector, como RIP.

Características:

Mayor escalabilidad – IGRP ha sido desarrollado para el ruteo de redes más grandes comparadas con las que utilizan RIP.

Métrica mas sofisticada – IGRP utiliza una métrica compuesta que provee más flexibilidad en la selección de rutas. *Delay y Bandwidth* por defecto y opcionalmente *load, reliability y MTU* son considerados en las decisiones de ruteo. Además se mejora el límite de 15 saltos de RIP pudiendo llegar hasta 100 saltos por defecto y hasta 255 saltos configurado el límite máximo.

Múltiples rutas – IGRP puede mantener hasta seis rutas desiguales entre una red de origen y otra de destino; las rutas no necesitan tener igual costo como en el caso de RIP. Se puede utilizar varias rutas para incrementar el ancho de banda disponible o para redundancia de rutas.

La métrica de IGRP incluye los siguientes componentes:

Bandwith*: el valor de ancho de banda en la ruta.
Delay*: retraso acumulativo de las interfaces a lo largo de la ruta.
Reliability: la confiabilidad entre origen y destino sobre la base de los keepalives.
Loading: la carga en una conexión entre origen y destino en base a bits por segundo
MTU: el valor de MTU de la ruta

- Usados por default

La métrica compuesta de IGRP soporta múltiples rutas entre un origen y un destino. Además múltiples rutas pueden ser utilizadas aun cuando no tengan la misma métrica. El balanceo de carga sobre rutas con métricas diferentes puede ser extendido hasta seis rutas lo que posibilita una mejor confiabilidad y un ancho de banda extendido.

Ruteo IGRP – Configuración

Para habilitar el protocolo de ruteo IGRP, se deben configurar de la siguiente manera:

Router(config)#router igrp autonomous-system
Router(config-router)#network número de la red

El comando *router igrp* selecciona IGRP como protocolo de ruteo. Si bien IGRP requiere un número de sistema autónomo, este no necesita estar registrado en el IANA, pero todos los ruteadores dentro del sistema autónomo deben tener el mismo número para poder intercambiar información de ruteo.

El comando *network* indica los números de red a las cuales el router esta directamente conectado.

Verificando el Protocolo IGRP

Una vez conectados los ruteadores, para saber de que manera esta corriendo el protocolo ejecutaremos los siguientes comandos:

Router#show ip protocols

Este comando muestra parámetros, filtros e información de red correspondiente al ruteador. Esta información incluye el sistema autónomo, los timers de ruteo, redes y distancia administrativa.

Routing protocol: el protocolo de ruteo y el sistema autónomo.
Update: Periodo de tiempo en el que se envían los updates.
Invalid: Número de segundos luego que una ruta es declarada inválida.
Holddown: número de segundos durante el cual no se acepta información de ruteo con métricas peores.
Flush: número de segundos que deben pasar antes que la ruta sea removida de la tabla de ruteo.

Visualizando la tabla de ruteo

Router#show ip route

Este comando muestra el contenido de la tabla de ruteo ip. La tabla contiene una lista de todas las redes y subredes aprendidas.

Configurando la interface serial

Como vamos a conectar un cable DCE en la interface de uno de los ruteadores (con esto lograremos realizar la conexión back to back al otro ruteador) y será esta la que suministre la señal de clock. Usaremos el comando:

Router(config-if)#clock rate 64000

En este ejemplo 64000 corresponde a una velocidad de 64000 bits por Segundo. Estas velocidades pueden ser de 1200, 2400, 4800, 9600, 19200, 38400, 56000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000 y 4000000.

10.0.1.0 Red
10.0.1.1 /255.255.255.252
10.0.1.2 /255.255.255.252
10.0.1.3 Broadcast
10.0.1.4 Red
10.0.1.5 /255.255.255.252
10.0.1.6 /255.255.255.252
10.0.1.7 Broadcast

3.3.4. Protocolo EIGRP

EIGRP: Enhanced IGRP, protocolo de enrutamiento óptimo basado en el algoritmo DUAL (Diffussing Update Algorithm) diseñado por el Dr. García-Luna Aceves. El EIGRP consume mucho menos ancho de banda que el IGRP, porque éste es capaz de limitar el intercambio de información de ruteo para incluir solamente la información que ha cambiado.

Además, es capaz de manipular información de ruteo de AppleTalk e IPX, además de IP.

En las instalaciones que sólo utilizan equipo de Cisco Systems, el implementar el protocolo EIGRP, creación de ese fabricante, ofrece ciertas ventajas importantes. Por principio de cuentas, EIGRP –el sucesor de IGRP-- propaga rápidamente los cambios en el estado de los enlaces, como hace OSPF, pero con menos overhead. La principal desventaja de este protocolo radica en que no es un estándar de la industria; es decir, sólo pueden utilizarlo aquellas compañías que únicamente tienen productos de Cisco.

Al igual que OSPF, los ruteadores EIGRP descubren a sus vecinos e intercambian paquetes de saludo. Este protocolo envía paquetes de saludo cada cinco segundos. Si no llegan tres, se da por hecho que el ruteador vecino está muerto y se utilizan rutas alternativas. EIGRP también envía actualizaciones incrementales acerca de cambios en la topología (cuando son necesarias) y, a

diferencia de RIP, no gasta ancho de banda en anunciar actualizaciones regulares.

EIGRP llama "sucesor" al siguiente ruteador que está en su camino hacia un destino de red. El protocolo también se mantiene al tanto de los ruteadores de siguiente salto, denominados "sucesores factibles", los cuales pueden ofrecer rutas de respaldo carentes de ciclos.

Esta información queda registrada en la tabla de topología. Si una ruta deja de estar disponible, se puede consultar rápidamente dicha tabla para encontrar "sucesores factibles". Si se encuentra uno, la convergencia es instantánea. Si no hay ninguno, el ruteador comenzará a indagar entre sus vecinos locales para tratar de descubrir otra ruta, y correspondientemente actualizará la tabla de topología y la tabla de ruteadores.

Cuando el estado de un enlace en un ruteador local cambia, el dispositivo recalcula su tabla de topología con base en la nueva información. Mientras que OSPF de inmediato propagaría el cambio en el estado del enlace a todos los ruteadores de la red, EIGRP sólo se dirige a los equipos afectados directamente por las modificaciones. Esto permite un uso más eficiente del ancho de banda y de los recursos de CPU del ruteador. Además, EIGRP nunca utiliza más del 50% del ancho de banda, lo que es una gran ventaja en los enlaces WAN de bajo ancho de banda.

Otra ventaja del protocolo de Cisco Systems: reconoce los ambientes Novell/IPX y AppleTalk, lo que podría significar menos capacitación de trabajadores en entornos multiprotocolo. Si su compañía ya está ejecutando IGRP, le será mucho más fácil efectuar la transición a EIGRP que hacia OSPF.

EIGRP tiene 4 componentes básicos:

*Vecino discovery/discovery

*Protocolo Confiable del transporte

*Automata finito DUAL

*Módulos dependientes del protocolo

Cada ruteador guarda el estado sobre vecinos adyacentes. Cuando se insertan nuevos ruteadores el direccionamiento y la interfaz del nuevo vecino se registra. Esta información se guarda en la estructura de datos vecina

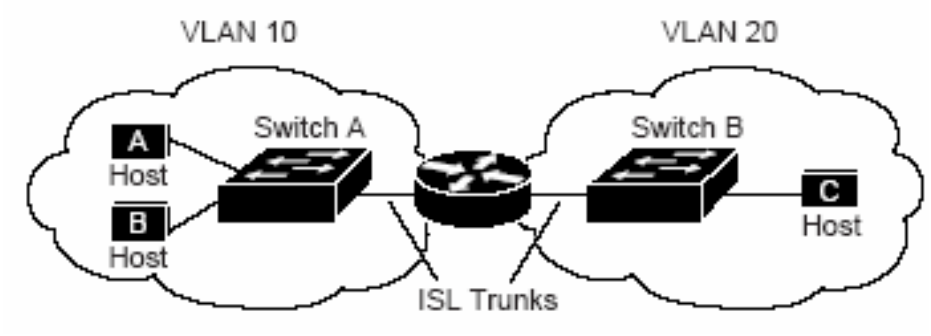
3.4 Entendiendo cómo las VLAN´s trabajan en el ruteador

Los dispositivos de la red en VLAN´s diferentes no pueden comunicarse entre si, sin un router para enviar tráfico entre las VLAN´s. En el entorno de la red, las VLAN´s son asociadas como redes individuales o subredes.

Por ejemplo, en una red con determinada IP, en donde cada subred se conforma en una VLAN individual.

Configurando VLAN´s ayuda no solo a controlar el tamaño del dominio de broadcast sino también el tráfico local. Cuando una estación de trabajo que pertenece a una vlan quiere comunicarse con otra estación de trabajo de vlan´s distintas, se requiere de un router para hacer posible la comunicación. Esta comunicación se proporciona por la asignación de ruta de vlan´s. Para eso se configura uno o más routers para dirigir el tráfico al destino apropiado de VLAN´s.

La figura muestra una configuración de vlan´s básica. El switch 1 está en la VLAN 10 y el switch B está en la VLAN 20. El ruteador tiene una interfaz en cada VLAN.

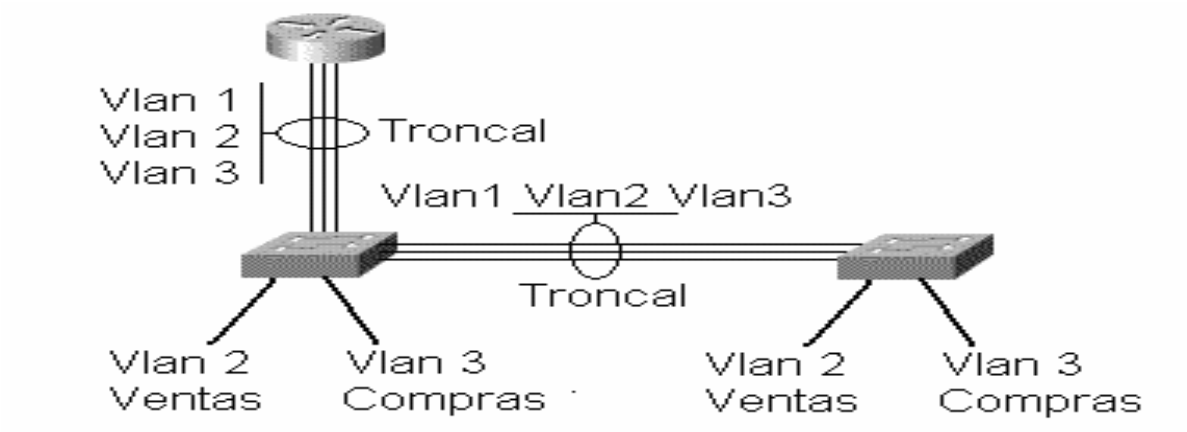


Cuando el host A en la VLAN 10 necesita comunicarse con el host B en la VLAN 10, envía un paquete a la dirección ese host. El switch A envía el paquete directamente al host B, sin enviarlo al ruteador.

Cuando el host A envía un paquete al host C en la VLAN 20, El switch envía el paquete al ruteador que recibe el tráfico por la interfaz de la VLAN 10. El ruteador verifica la tabla de la asignación de ruta, determina la interfaz saliente correcta, y envía el paquete fuera de la interfaz VLAN 20 para la interface del switch B. El switch B recibe el paquete y lo envía al host C.

3.5 Enrutamiento entre VLAN´s

Para que las Vlan´s puedan establecer comunicación entre ellas deben ser necesarios los servicios de un router. Para esto se deben establecer Subinterfaces FastEthernet, encapsulasión y dirección IP correspondiente de manera que cada una de estas pertenezca a una VLAN determinada.



Los pasos que siguen establecen las configuraciones de una Subinterfaz FastEthernet:

Router(config)#interface fastethernet Nºde slot/Nºde interfaz.Nºde Subinterfaz
Router(config-subif)#encapsulation [dot1q|ISL] Nºde vlan
Router(config-subif)#ip address direction IP+mascara
Router(config-subif)#exit
Router(config)#interface fastethernet Nºde slot/Nºde interfaz
Router(config-if)#no shutdown

Para que la subinterfaz este no shutdown se debe ejecutar este comando directamente desde la interfaz física.

Ejemplo de configuración de un enlace troncal sobre dos subinterfaces:

Router(config)#interface fastethernet 0/0.1
Router(config-subif)#encapsulation dot1q 3
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fastethernet 0/0.2
Router(config-subif)#encapsulation dot1q 3
Router(config-subif)#ip address 200.200.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fastethernet 0/0
Router(config-if)#no shutdown

Ejemplo: Configurar un solo switch con dos diferentes VLAN's (con los comandos de arriba). Conmutar el tráfico entre las dos VLAN's con un router.

Una troncal del switch se conectará a una interface FastEthernet del router, la cual se subdivide en dos sub-interfaces (una para cada VLAN).

Comandos para el switch:

vtp mode transparent
o también: vtp mode server
(El default es "server", que sirve para este ejercicio.)

interface F0/5
switchport mode trunk
(comandos para encapsulación)
switchport trunk allow vlan all

El switch 2950 sólo soporta un encapsulamiento, y no soporta comandos para cambiar el encapsulamiento. Sin embargo, es importante recordar que en otros switches posiblemente se tenga que seleccionar el encapsulamiento correcto (dot1q, o isl).

Comandos para el router:

interface F0 (o: F0/0)
no shutdown
interface F0.2 (o: F0/0.2) (selecciona una sub-interface)
encapsulation dot1q 2
ip address ...
interface F0.3
encapsulation dot1q 3
ip address ...
(Repetir para cada VLAN.)

Comandos para los hosts:

Obviamente, aparte de configurar el router y el switch, también se deben configurar los hosts conectados. Específicamente, se tiene que asignar:

- La dirección IP. Se debe recordar que; la dirección IP debe estar en la misma subred que la sub-interfaz correspondiente del router; y, para la configuración de VLAN´s en general, diferentes VLAN´s corresponden a diferentes subredes.
- La máscara de subred.
- La puerta de enlace, que debe apuntar a la sub-interfaz correspondiente de router.

3.6. Switches

Los problemas asociados con las LAN compartidas y la consolidación de los switches están haciendo que las configuraciones LAN tradicionales sean sustituidas por configuraciones de red de VLAN conmutada. Las configuraciones VLAN conmutadas se diferencian de las configuraciones LAN tradicionales en lo siguiente:

- Los switches eliminan las restricciones físicas impuestas por una arquitectura de hub compartido, ya que los usuarios y puertos de la empresa se agrupan lógicamente. Los switches sustituyen a los hubs en el recinto de cableado. Los switches se instalan fácilmente sin haber prácticamente ningún cambio en el cableado, y pueden sustituir completamente a un hub compartido con servicio de puerto para cada usuario.

- Los switches pueden ser utilizados para crear VLAN con el fin de proporcionar servicios de segmentación (que suelen ser proporcionados por los routers en las configuraciones LAN). Los switches constituyen uno de los componentes centrales de las comunicaciones VLAN. Llevan a cabo funciones VLAN críticas, actuando como punto de entrada para los dispositivos finales en el tejido conmutado y para las comunicaciones de la empresa.

Todo switch tiene la inteligencia necesaria para filtrar y reenviar las decisiones por trama, en base a la métrica VLAN definida por los administradores de la red. El switch también puede comunicar esta información a los demás switches y routers de la red.

Las soluciones más habituales para el agrupamiento lógico de los usuarios en VLAN distintas son el filtrado de trama y la identificación de trama. Ambas técnicas examinan la trama cuando se recibe o reenvía por el switch. En base al conjunto de reglas que defina el administrador, estas técnicas determinan donde va a ser enviada, filtrada o difundida la trama. Estos mecanismos de control pueden administrarse centralmente (por medio de software de administración de redes) y se implementan fácilmente en la red.

El filtrado de trama examina la información concreta de cada trama. En cada switch se desarrolla una tabla de filtrado; esto proporciona un alto nivel de control administrativo, ya que se pueden examinar muchos atributos de cada trama. En función de la sofisticación del switch LAN, es posible agrupar a los usuarios en base a las direcciones MAC o el tipo de protocolo de la capa de red. El switch compara las tramas que filtra con las entradas de la tabla, y toma la acción oportuna en base a las entradas. En sus primeros días, las VLAN estaban basadas en filtros y agrupaban a los usuarios en base a una tabla de filtrado. Este modelo no escalaba bien, ya que había que hacer referencia a cada trama con arreglo a una tabla de filtrado.

El etiquetado de trama asigna un ID de VLAN a cada trama. Los ID de VLAN son asignados a cada VLAN en la configuración del switch por el administrador del switch. Esta técnica fue la elegida por los el IEEE (Instituto de ingenieros eléctricos y electrónicos), debido a su escalabilidad. El etiquetado de trama esta ganando aceptación como mecanismo normal de trunking (enlace troncal); en comparación con el filtrado de trama, puede proporcionar una solución más escalable al despliegue VLAN que puede implementarse en todo el campus. La IEEE 802.1q establece que el etiquetado de trama es la forma de implementar las VLAN.

El etiquetado de trama VLAN es una solución que ha sido desarrollada específicamente para las comunicaciones conmutadas. El etiquetado de trama coloca un identificador único en la cabecera de cada trama cuando es reenviada por el backbone de red. El identificador es entendido y examinado por cada switch, con antelación a las difusiones o transmisiones a otros switches, routers o dispositivos finales. Cuando la trama sale del backbone de red, el switch elimina el identificador antes de que se transmita la trama a la estación final de destino. La identificación de trama de Capa 2 requiere algo de procesamiento o estructura administrativa.

El procesamiento de paquetes en un switch sigue 3 pasos principales:

- Recepción del paquete desde la puerta de entrada y almacenamiento en la cola de entrada de la puerta.

- Transferencia del paquete a la memoria de procesamiento del switch y su correspondiente inspección, para determinar la puerta de salida. La inspección se realiza en base a su dirección física de destino o alguna otra marca (como veremos más adelante).

- Inserción en la cola de salida de la puerta que se usará para despachar.

Los switches pueden dividirse en ciertas categorías, lo cual define además el precio que podrán tener. Definiremos las siguientes clases:

- Expansibles
- Configurables
- Administrables

Expansibles

- Incluyen en su configuración física la posibilidad de incluir módulos con más puertas de diferentes tipos.

- También provee la posibilidad de actualizar sus capacidades mediante actualizaciones del S.O que ejecutan.

- Configurables.

- Generalmente asociado a los equipos expansibles, se puede definir la configuración del equipo mediante diferentes métodos: CLI (Command Line Interface) o GUI (Graphic User Interface).

- Se puede definir funciones para las puertas, activarlas o desactivarlas, etc.

- Administrables.

- Generalmente asociado a la posibilidad de configurarse, los switches administrables mantienen información interna acerca del tráfico recibido y despachado, entre otros datos.

- Esto es de especial utilidad en la administración de redes, para determinar la capacidad en uso de la red y planificar ampliaciones (o considerar rediseños).

CAPÍTULO IV. CONFIGURACIÓN E IMPLEMENTACIÓN DE LA RED DENTRO DE LA SHCP.

ESQUEMA DE DIRECCIONAMIENTO IP UTILIZADO PARA LA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

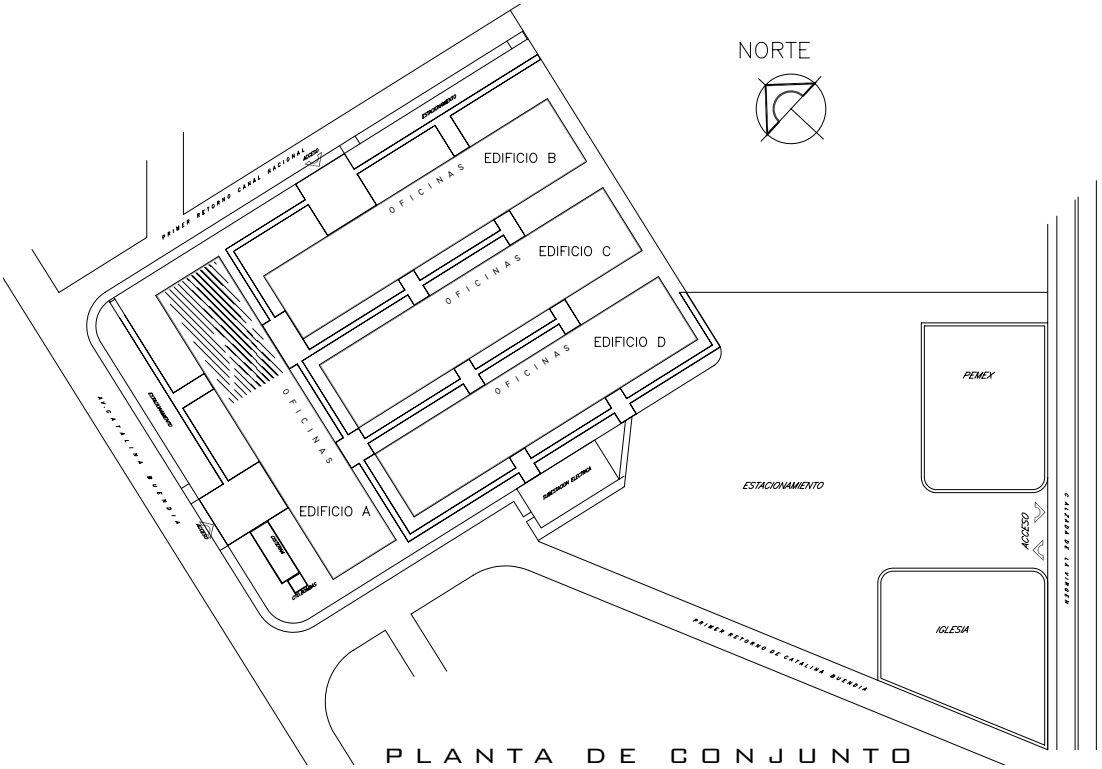
4.1. Antecedentes.

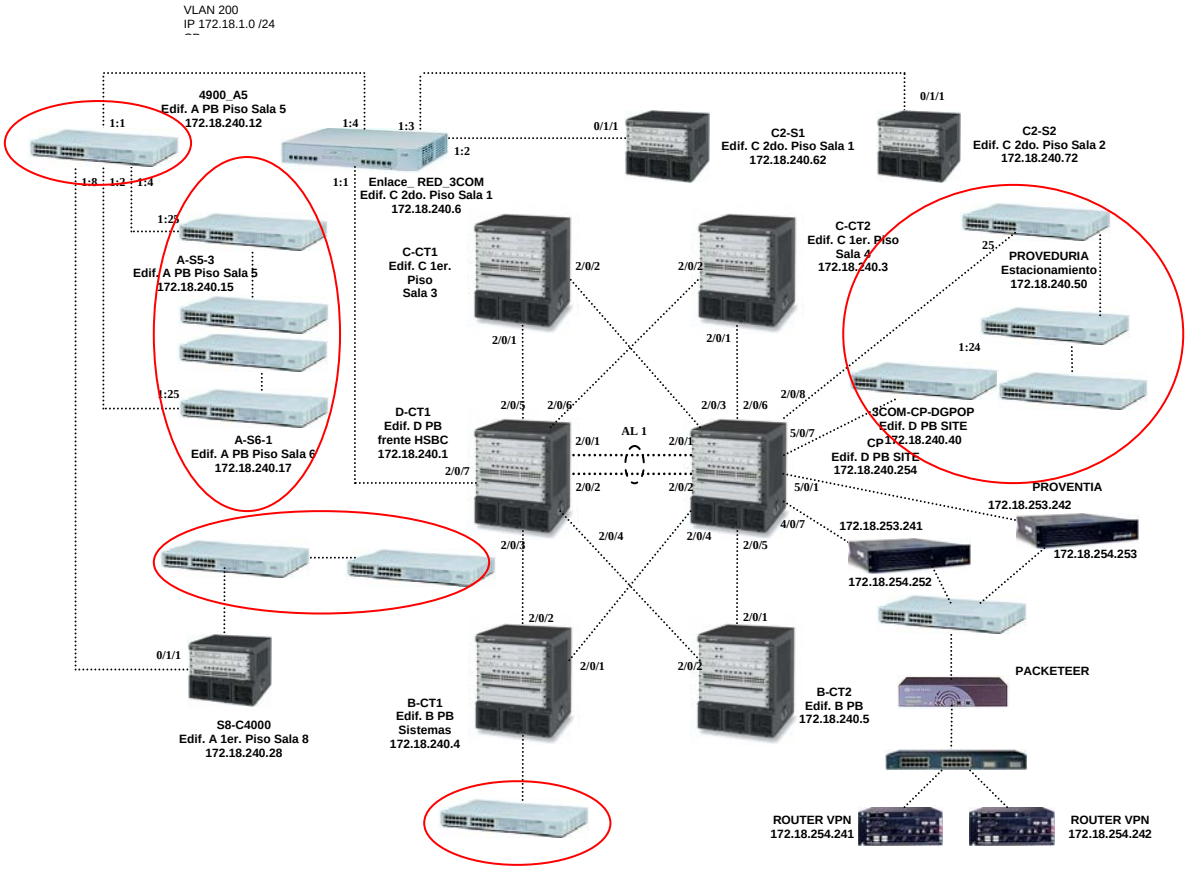
Dentro de la SHCP se cuenta con 3 edificios de los cuales existen las siguientes áreas de trabajo:

- Recursos Financieros
- Informática
- Recursos Materiales
- Recursos Humanos
- Presupuesto

El diagrama siguiente proporcionado por la SHCP se observa la distribución de los equipos de comunicaciones en el inmueble, que a primera vista vemos el cascareo de varios hubs en todos los equipos, lo que ocasionan demasiadas colisiones de dominio provocando que la red se sature de información llegando a un punto donde se puede bloquear la red por el consumo de ancho de banda.

A continuación se muestra el croquis geográfico de la ubicación física del inmueble de la SHCP:





Al conectarnos a cada uno de los equipos de comunicaciones encontramos el exceso de propagación de VLAN´s de todas las áreas de trabajo mas aparte habilitados puertos de red sin tener un usuario final conectado.

En el siguiente recuadro vemos todas las VLAN´s que existen en un equipo de comunicación.

```
Router#sh vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------
------
1    default                             active
2    DGRMSG                              active
4    DGRH                                active
10   DGPOP10                             active
20   DGPOP20                             active
30   DGPOP30                             active
60   DGRMSG60                            active
70   DGRMSG70                            active
80   DGRMSG80                            active
110  DGRH110                             active
120  DGRH120                             active
130  DGRH130                             active
200  SEGURIDAD                           active
```

```
201  SEGURIDAD-DMZ                     active
202  VLAN0202                          active
230  VLAN0230                          active
235  USUARIOSCAT                       active
240  VLAN0240                          active
250  VLAN0250                          active
251  VLAN0251                          active
300  FIDELIQ                           active
500  VLAN-DEL-SAT                      active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1
Trans2
1    enet  100001     1500  -      -      -        -    -        1002
1003
2    enet  100002     1500  -      -      -        -    -        0      0
4    enet  100004     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
60   enet  100060     1500  -      -      -        -    -        0      0
70   enet  100070     1500  -      -      -        -    -        0      0
80   enet  100080     1500  -      -      -        -    -        0      0
110  enet  100110     1500  -      -      -        -    -        0      0
120  enet  100120     1500  -      -      -        -    -        0      0
130  enet  100130     1500  -      -      -        -    -        0      0
           100200     1500  -      -      -        -    -        0      0
201  enet  100201     1500  -      -      -        -    -        0      0
     enet  100202     1500  -      -      -        -    -        0      0
  230  enet  100230     1500  -      -      -        -    -        0
0
  235  enet  100235     1500  -      -      -        -    -        0
0
  240  enet  100240     1500  -      -      -        -    -        0
0
  250  enet  100250     1500  -      -      -        -    -        0
0
  251  enet  100251     1500  -      -      -        -    -        0
0
  300  enet  100300     1500  -      -      -        -    -        0
0
```

B-CT2#sh vlan

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
------
1    default                          active    Fa2/5, Fa2/6, Fa2/7,Fa2/8
2    DGRMSG                           active    Fa2/25, Fa2/26, Fa2/27,
Fa2/13, Fa2/14
4    DGRH                             active    Fa3/1, Fa2/21, Fa2/22,
Fa2/23, Fa2/24
10   DGPOP10                          active    Fa2/33, Fa2/34, Fa2/35,
Fa2/36
```

```
20   DGPOP20                          active    Fa2/9, Fa2/10, Fa2/11,
Fa2/12
30   DGPOP30                          active    Fa2/29, Fa2/30, Fa2/31,
Fa2/32
60   DGRMSG60                         active    Fa2/37, Fa2/38, Fa2/39,
Fa2/40
70   DGRMSG70                         active    Fa2/17, Fa2/18
80   DGRMSG80                         active    Fa2/19, Fa2/20Fa2/4
110  DGRH110                          active    Fa2/15, Fa2/16, Fa2/28
120  DGRH120                          active    Fa2/1, Fa2/2, Fa2/3
                                                Fa2/41, Fa2/42, Fa2/43,
                                                Fa2/44, Fa2/45, Fa2/46,
                                                Fa2/47, Fa2/48, Fa3/2,
                                                Fa3/3, Fa3/4, Fa3/5
                                                Fa3/6, Fa3/7, Fa3/8,
                                                Fa3/9, Fa3/10, Fa3/11,
                                                Fa3/12, Fa3/13, Fa3/14,
                                                Fa3/15, Fa3/16, Fa3/17
                                                Fa3/18, Fa3/19, Fa3/20,
                                                Fa3/21, Fa3/22, Fa3/23,
                                                Fa3/24, Fa3/25, Fa3/26,
                                                Fa3/27, Fa3/28, Fa3/29,
                                                Fa3/30, Fa3/31, Fa3/32,
                                                Fa3/33, Fa3/34, Fa3/35,
                                                Fa3/36, Fa3/37, Fa3/38,
                                                Fa3/39, Fa3/40, Fa3/41,
                                                Fa3/42, Fa3/43, Fa3/44,
                                                Fa3/45, Fa3/46, Fa3/47,
                                                Fa3/48, Fa4/1, Fa4/2,
                                                Fa4/3, Fa4/4, Fa4/5,
                                                Fa4/6, Fa4/7, Fa4/8,
                                                Fa4/9, Fa4/10, Fa4/11,
                                                Fa4/12, Fa4/13, Fa4/14,
                                                Fa4/15, Fa4/16, Fa4/17,
                                                Fa4/18, Fa4/19, Fa4/20,
                                                Fa4/21, Fa4/22, Fa4/23,
                                                Fa4/24, Fa4/25, Fa4/26,
                                                Fa4/27, Fa4/28, Fa4/29,
                                                Fa4/30, Fa4/31, Fa4/32,
                                                Fa4/33, Fa4/34, Fa4/35,
                                                Fa4/36, Fa4/37, Fa4/38,
                                                Fa4/39, Fa4/40, Fa4/41,
                                                Fa4/42, Fa4/43, Fa4/44,
                                                Fa4/45, Fa4/46, Fa4/47,
                                                Fa4/48, Fa5/1, Fa5/2,
                                                Fa5/3, Fa5/4, Fa5/5,
                                                Fa5/6, Fa5/7, Fa5/8,
                                                Fa5/9, Fa5/10, Fa5/11,
                                                Fa5/12, Fa5/13, Fa5/14,
                                                Fa5/15, Fa5/17, Fa5/19,
                                                Fa5/20, Fa5/21, Fa5/22,
                                                Fa5/23, Fa5/24, Fa5/25,
                                                Fa5/26, Fa5/27, Fa5/28,
                                                Fa5/29, Fa5/30, Fa5/31,
                                                Fa5/32, Fa5/33, Fa5/34,
                                                Fa5/35, Fa5/36, Fa5/37,
```

```
                                                  Fa5/38, Fa5/39, Fa5/40,
                                                  Fa5/41, Fa5/42, Fa5/43,
                                                  Fa5/44, Fa5/45, Fa5/46,
                                                  Fa5/47, Fa5/48
130  DGRH130                          active    Fa5/16, Fa5/18
200  SEGURIDAD                        active
201  SEGURIDAD-DMZ                    active
202  VLAN0202                         active
230  VLAN0230                         active
235  USUARIOSCAT                      active
240  VLAN0240                         active
250  VLAN0250                         active
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
------
251  VLAN0251                         active
300  FIDELIQ                          active
500  VLAN-DEL-SAT                     active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1
Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ -
-----
1    enet  100001     1500  -      -      -        -    -        1002
1003
2    enet  100002     1500  -      -      -        -    -        0      0
4    enet  100004     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
60   enet  100060     1500  -      -      -        -    -        0      0
70   enet  100070     1500  -      -      -        -    -        0      0
80   enet  100080     1500  -      -      -        -    -        0      0
110  enet  100110     1500  -      -      -        -    -        0      0
120  enet  100120     1500  -      -      -        -    -        0      0
130  enet  100130     1500  -      -      -        -    -        0      0
200  enet  100200     1500  -      -      -        -    -        0      0
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1
Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ -
-----
201  enet  100201     1500  -      -      -        -    -        0      0
202  enet  100202     1500  -      -      -        -    -        0      0
230  enet  100230     1500  -      -      -        -    -        0      0
235  enet  100235     1500  -      -      -        -    -        0      0
240  enet  100240     1500  -      -      -        -    -        0      0
250  enet  100250     1500  -      -      -        -    -        0      0
251  enet  100251     1500  -      -      -        -    -        0      0
300  enet  100300     1500  -      -      -        -    -        0      0
500  enet  100500     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      0      -        -    -        1
1003
```

```
1003 tr    101003     1500  1005   0      -        -    srb      1
1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
B-CT2#
```

Revisando en los equipos de comunicaciones las troncales configuradas se observa que no hay seguridad en cuanto a que todas las VLAN´s, están permitidas pasar por toda la red por lo cual aparte de consumir recursos de la red no hay delimitación de comunicación entre los equipos de VLAN´s distintas. Como se muestra en la siguiente configuración de un equipo de la SHCP:

```
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet1/0/1
#
interface GigabitEthernet1/0/2
#
interface GigabitEthernet2/0/1
 port access vlan all
 port link-aggregation group 1
#
interface GigabitEthernet2/0/2
 port access vlan all
 port link-aggregation group 1
#
interface GigabitEthernet2/0/3
 port access vlan all
 port link-aggregation group 1
#
interface GigabitEthernet2/0/4
 port access vlan all
 port link-aggregation group 1
#
interface GigabitEthernet2/0/5
 port access vlan all
 port link-aggregation group 1
#
interface GigabitEthernet2/0/6
 port access vlan all
 port link-aggregation group 1
#
interface GigabitEthernet2/0/7
 port access vlan all
 port link-aggregation group 1
#
interface GigabitEthernet2/0/8
 port access vlan all
 port link-aggregation group 1
#
interface GigabitEthernet2/0/9
 port link-type trunk
 port trunk permit vlan all
```

```
 port link-aggregation group 2
#
interface GigabitEthernet2/0/10
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 2
#
interface GigabitEthernet2/0/11
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 2
#
interface GigabitEthernet2/0/12
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 2
#
interface GigabitEthernet2/0/13
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 2
#
interface GigabitEthernet2/0/14
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 2
#
interface GigabitEthernet2/0/15
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 2
#
interface GigabitEthernet2/0/16
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 2
#
interface GigabitEthernet2/0/17
 description Plano_1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan all
#
interface GigabitEthernet2/0/18
 description Plano_2
 port link-type trunk
 port trunk permit vlan all
#
interface GigabitEthernet2/0/19
 description Plano_3
 port link-type trunk
 port trunk permit vlan all
#
interface GigabitEthernet2/0/20
 description Plano_4
 port link-type trunk
```

```
 port trunk permit vlan all
#
interface GigabitEthernet3/0/1
 stp instance 0 cost 45000
 port access vlan all
 port link-aggregation group 3
#
interface GigabitEthernet3/0/2
 stp instance 0 cost 45000
 port access vlan all
 port link-aggregation group 3
#
interface GigabitEthernet3/0/3
 stp instance 0 cost 45000
 port access vlan all
 port link-aggregation group 3
#
interface GigabitEthernet3/0/4
 stp instance 0 cost 45000
 port access vlan all
 port link-aggregation group 3
#
interface GigabitEthernet3/0/5
 stp instance 0 cost 45000
 port access vlan all
 port link-aggregation group 3
#
interface GigabitEthernet3/0/6
 stp instance 0 cost 45000
 port access vlan all
 port link-aggregation group 3
#
interface GigabitEthernet3/0/7
 stp instance 0 cost 45000
 port access vlan all
 port link-aggregation group 3
#
interface GigabitEthernet3/0/8
 stp instance 0 cost 45000
 port access vlan all
 port link-aggregation group 3
#
interface GigabitEthernet4/0/1
 description Plano_5
 port link-type trunk
 port trunk permit vlan all
#
interface GigabitEthernet4/0/2
 description Plano_6
 port link-type trunk
 port trunk permit vlan all
#
interface GigabitEthernet4/0/3
#
interface GigabitEthernet4/0/4
#
```

```
interface GigabitEthernet4/0/5
#
interface GigabitEthernet4/0/6
#
interface GigabitEthernet4/0/7
#
interface GigabitEthernet4/0/8
#
```

4.2 Premisas del rediseño

EL CENTRO DE ADMINISTRACIÓN TECNOLÓGICA, CUYO OBJETIVO SEA PROVEER A LOS USUARIOS DE LA SHCP DE CAPACIDAD DE CÓMPUTO Y CONECTIVIDAD CON ALTOS NIVELES DE SERVICIO" se contempla la homologación del direccionamiento IP que operarían en el inmueble de la SHCP y que permita llevar a cabo el objetivo de ésta.

Dentro de las consideraciones de diseño global se contempla el uso del rango válido para Intranet de acuerdo al RFC 1918, que corresponde a las redes de 172.16.0.0 a 172.31.0.0, debido a que se piensa implementar en otros inmuebles de la SHCP. Se opta por poner el direccionamiento de clase B con la utilización de una máscara de red de 24 bits lo cual nos permite 254 direcciones de host por subred ya que la utilización de una máscara menor no era justificable por la cantidad de usuarios por red, además de que amplía el rango de broadcast existente en las redes el cual genera tráfico innecesario; se determinó empezar la numeración a partir de la red 172.16.0.0 como punto de partida.

Con la finalidad de contar con un nuevo esquema de direccionamiento mas fácilmente administrable se contempló la creación de nuevas VLAN's que estuvieran ligadas a las nuevas redes.

En base a esa misma información se hizo una distribución de los segmentos para poder ubicar el tipo de equipo en base a su rango de IP, estos rangos se describen a detalle posteriormente.

Depurar el cableado estructurado para ver si se están utilizando todos los nodos de red y si no para liberar puertos del equipo para eliminar hubs.

Se homologó la utilización de la última dirección de cada segmento (.254) como Gateway de la red correspondiente.

Se determinó la eliminación de la VLAN 1 para tráfico de usuarios.

Se generó una VLAN específica para la administración de los equipos de comunicaciones.

Se generó una VLAN dedicada para los servidores de Directorio Activo y otros destinados a proveer de servicios de Centro de Administración Tecnológico (CAT).

Se consideró la homologación de las direcciones IP para la VPN.

Se generó una VLAN para la colocación de servidores de la Secretaría que contaran con usuarios tanto locales como remotos.
Detalle de los Rangos de Direccionamiento.

La distribución de IP´s se considera de la siguiente manera:

Los servidores de aplicaciones de uso local o equipos que requieran IP fijas se consideran dentro de las primeras 20 direcciones IP de cada red, quedando como sigue:

172.16. X.1 a 172.16.X.20

Las impresoras en red se considerarán dentro del rango de las direcciones IP 21 a la 30 de cada red, quedando como sigue:

172.16. X.21 a 172.16.X.30

Las PC´s de usuario final se considerarán dinámicamente asignadas por el servidor de DHCP y estarán dentro del rango de las direcciones 31 a 239 de cada red, quedando a disposición de dicho servidor:

172.16. X.31 DHCP

……

172.16. X.239 DHCP

Las últimas direcciones de cada red (172.17.X.240 a 172.17.X.254) serán de uso reservado para la administración de la red, por ejemplo para las direcciones asignadas a los gateways o algún servidor de monitoreo que sea necesario ya sea temporal o permanente.

Redundancia en ruteo: IP activa e IP de standby: 172.16.X.252 y 172.16.X.253

Gateway 172.16.X.254

4.3 Segmentos utilizados

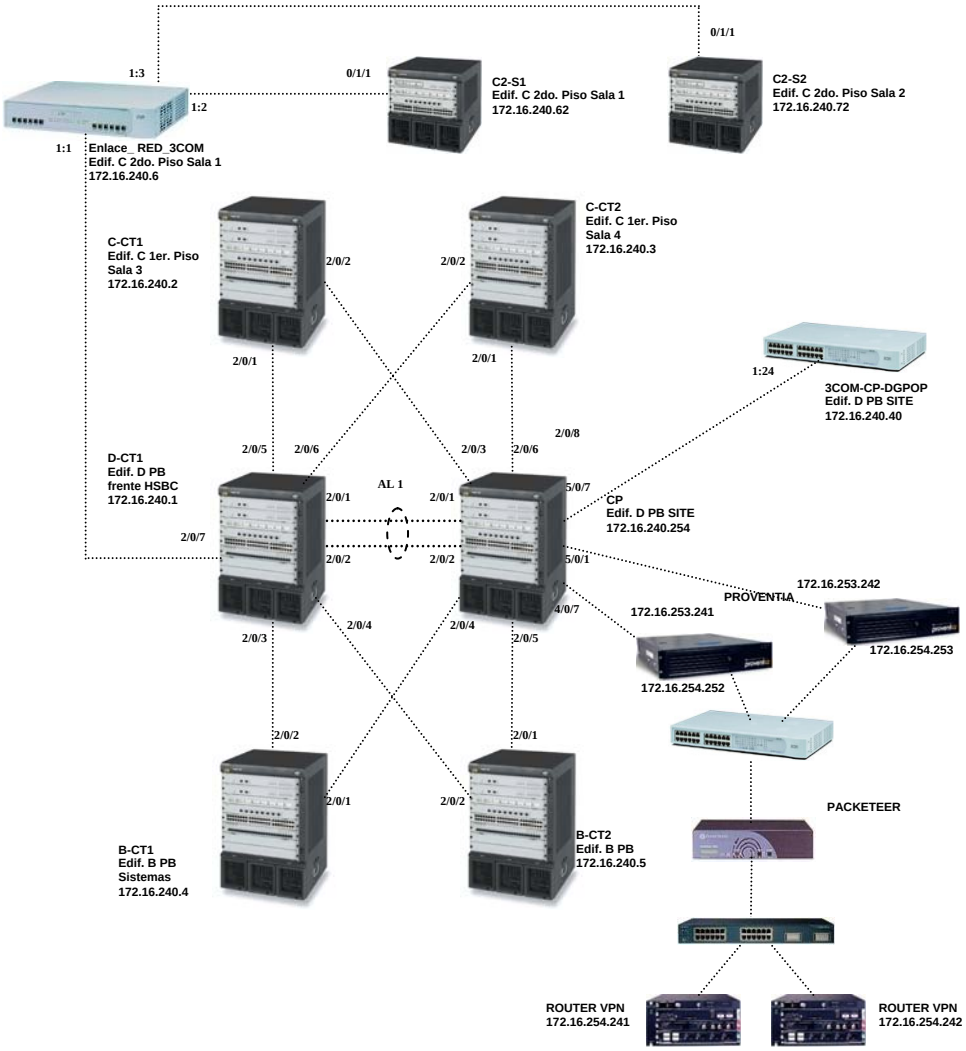
Debido a los requerimientos de la S.H.C.P se decidió planear la segmentación por áreas para poder identificar rápidamente en los equipos de comunicación y determinar más fácilmente problemas ocasionados por terminales de los usuarios ó exceso de tráfico en la red. Dando un mejor control y orden de las áreas.

LA VIRGEN

NOMBRE SWITCH	AREAS	SERVICIOS	VLAN ID	Dirección de red
INFORMATICA	CGTIC		10	172.16.10.0
		IMPRESORAS	235	172.16.235.0
		COMUNICACIONES	240	172.16.240.0
		SERVIDORES	250	172.16.250.0
FINANCIEROS	DGRF		20	172.16.20.0
		IMPRESORAS	235	172.16.235.0
		COMUNICACIONES	240	172.16.240.0
		SERVIDORES	250	172.16.250.0
HUMANOS	DGRH		30	172.16.30.0
		IMPRESORAS	235	172.16.235.0
		COMUNICACIONES	240	172.16.240.0
		SERVIDORES	250	172.16.250.0
PRESUPUESTO	DGPOP		40	172.16.40.0
		IMPRESORAS	235	172.16.235.0
		COMUNICACIONES	240	172.16.240.0
		SERVIDORES	250	172.16.250.0
MATERIALES	DGRMSG		50	172.16.50.0
		IMPRESORAS	235	172.16.235.0
		COMUNICACIONES	240	172.16.240.0
		MESA DE AYUDA	245	172.18.16.0
		SERVIDORES	250	172.16.250.0

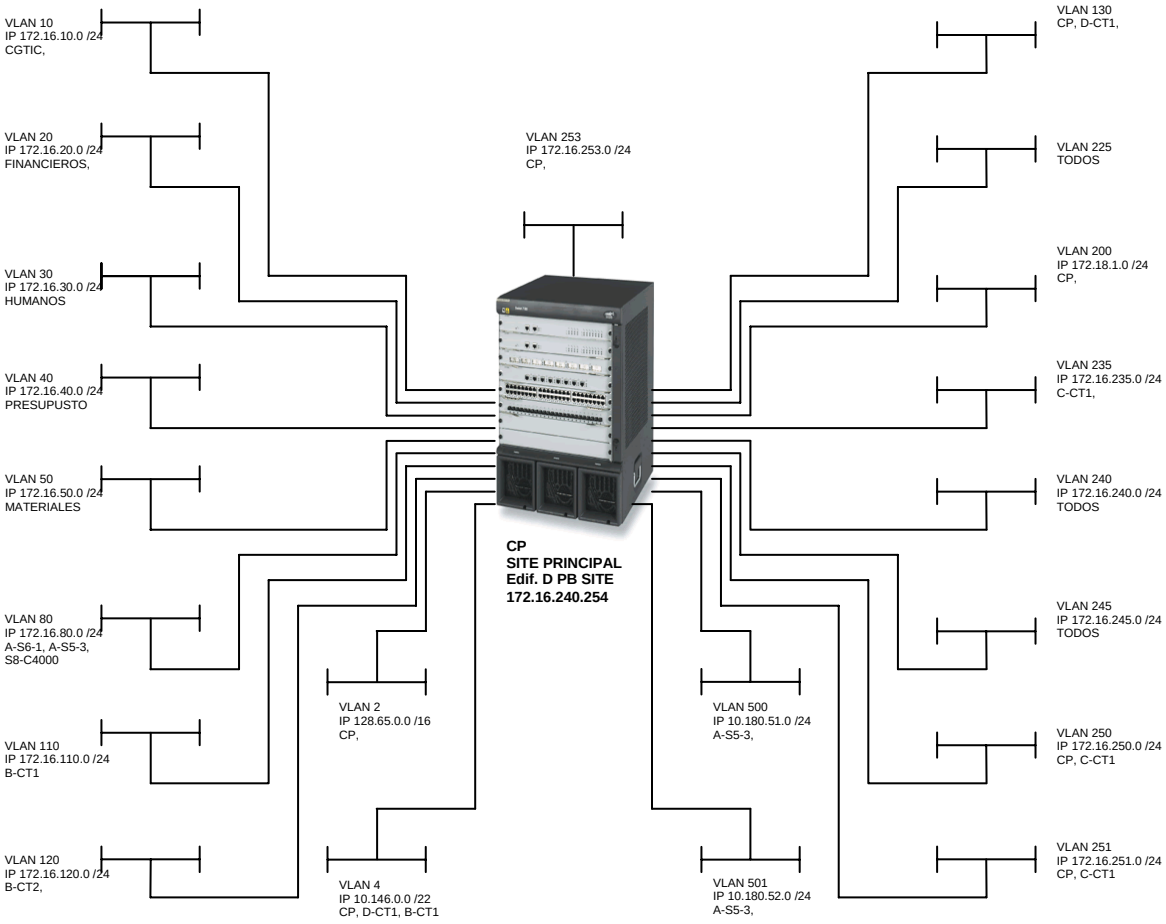
4.4 TOPOLOGÍA FISICA DE LA RED DENTRO DE LA SHCP

En el diagrama observamos que se eliminaron todos los hubs que ocasionaban colisiones de dominio, para esto se tuvo que reubicar y en algunos casos cablear al site correspondiente. Los switches tienen la capacidad para agregar más tarjetas de puertos de red.



4.5 TOPOLOGÍA LOGICA DE LA RED DENTRO DE LA SHCP

La topología lógica siguiente se muestra todas las vlan´s que se alojan dentro del equipo de ruteo, acaba destacar que no solo las vlan´s del inmueble están configuradas, se puede observar otras vlan´s externas o locales que no tienen direccionamiento IP de ruteo que solo sirven para formar equipos locales para que trabajen en pequeños grupos.



En la siguiente tabla mostramos con más detalle simplificado cada equipo de telecomunicaciones y sus especificaciones dándonos una visión general de los cambios que se realizaron para eliminar problemas de la red que no permitía el rendimiento adecuado.

4.6 ESPECIFICACIONES TÉCNICAS DE LOS EQUIPOS DE COMUNICACIONES

LA VIRGEN											
Switch			Imagen de Software		VLAN Pricipal	Ubicación	Tarjetas				
Nombre	Modelo	IP	Versión	Nombre			Tipo	Slot	Velocidad	Ptos Totales	Ptos Disponibles
FINANCIEROS	CISCO 6000	172.16.240.1	V3.00Rp09	77803_00rp09.APP	172.16.20.0 172.16.235.0 172.16.240.0 172.16.250.0	EDIFICIO D PB ALA NORTE FRENTE AL BITAL	3C16857R	0	-	-	-
							3C16857	1	-	-	-
							3C16862	2	1 GB	20	10
							3C16860	3	10/100 MB	48	10
							3C16860	4	10/100 MB	48	0
							3C16860	5	10/100 MB	48	0
							3C16860	6	10/100 MB	48	13
							3C16860	7	10/100 MB	48	35
							No. DE SLOTS DISPONIBLES	0	-	240 RJ45 20 F.O.	58 RJ45 8 F.O.
PRESUPUESTO	CISCO 6000	172.16.240.2	V3.00R	77803_00r.APP	172.16.40.0 172.16.235.0 172.16.240.0 172.16.250.0	EDIFICIO C 1er PISO ALA NORTE SALA 3	3C16857	0	-	-	-
							LIBRE	1	-	-	-
							3C16858	2	1 GB	8	6
							3C16860	3	10/100 MB	48	0
							3C16860	4	10/100 MB	48	0
							3C16860	5	10/100 MB	48	0
							3C16860	6	10/100 MB	48	0
							3C16860	7	10/100 MB	48	2
							No. DE SLOTS DISPONIBLES	1	-	240 RJ45 8 F.O.	2 RJ45 6 F.O.

Switch			Imagen de Software		VLAN Pricipal	Ubicación	Tarjetas				
Nombre	Modelo	IP	Versión	Nombre			Tipo	Slot	Velocidad	Ptos Totales	Ptos Disponibles
PRESUPUESTO	CISCO 6000	172.16.240.3	V3.00R	77803_00r.APP	172.16.40.0 172.16.235.0 172.16.240.0 172.16.250.0	EDIFICIOC 1er PISO ALA SUR SALA 4, DGRMSG	3C16857	0	-	-	-
							LIBRE	1	-	-	-
							3C16858	2	1 GB	8	6
							3C16860	3	10/100 MB	48	1
							3C16860	4	10/100 MB	48	2
							3C16860	5	10/100 MB	48	4
							3C16860	6	10/100 MB	48	0
							3C16860	7	10/100 MB	48	14
							No. DE SLOTS DISPONIBLES	1	-	240 RJ45 8 F.O.	21 RJ45 6 F.O.
HUMANOS	CISCO 6000	172.16.240.4	V3.00R	77803_00r.APP	172.16.30.0 172.16.235.0 172.16.240.0 172.16.250.0	EDIFICIO B PB ALA NORTE, CENTRO DE COMPUTO	3C16857	0	-	-	-
							LIBRE	1	-	-	-
							3C16858	2	1 GB	8	6
							3C16860	3	10/100 MB	48	12
							3C16860	4	10/100 MB	48	1
							3C16860	5	10/100 MB	48	0
							3C16860	6	10/100 MB	48	20
							3C16860	7	10/100 MB	48	7
							No. DE SLOTS DISPONIBLES	1	-	240 RJ45 8 F.O.	40 RJ45 6 F.O.

Switch			Imagen de Software		VLAN Pricipal	Ubicación	Tarjetas				
Nombre	Modelo	IP	Versión	Nombre			Tipo	Slot	Velocidad	Ptos Totales	Ptos Disponibles
HUMANOS	CISCO 6000	172.16.240.5	V3.00R	77803_00r.APP	172.16.30.0 172.16.235.0 172.16.240.0 172.16.250.0	EDIFICIO B PB ALA SUR, RH	3C16857	0	-	-	-
							LIBRE	1	-	-	-
							3C16858	2	1 GB	8	6
							LIBRE	3	-	-	-
							3C16860	4	10/100 MB	48	0
							3C16860	5	10/100 MB	48	0
							3C16860	6	10/100 MB	48	0
							3C16860	7	10/100 MB	48	0
							No. DE SLOTS DISPONIBLES	1	-	192 RJ45 8 F.O.	0 RJ45 6 F.O.
Enlace_Red	SW 4900 SX	172.16.240.6	4	'	-	EDIFICIO C 2do PISO ALA NORTE, SALA 1	3C17702	-	1 GB	12	8
							No. DE SLOTS DISPONIBLES	-	-	12 F.O.	8 F.O.
INFORMATICA	CISCO 6000	172.16.240.40	5		172.16.10.0	EDIFICIO D PB ALA SUR, CUARTO PRINCIPAL	3C17206	-	10/100 MB	24	0
							No. DE SLOTS DISPONIBLES	-	-	24 RJ45 1 F.O.	0 RJ45 1 F.O.

Switch			Imagen de Software		VLAN Pricipal	Ubicación	Tarjetas				
Nombre	Modelo	IP	Versión	Nombre			Tipo	Slot	Velocidad	Ptos Totales	Ptos Disponibles
MATERIALES	CISCO 6000	172.16.240.62	V3.00	77403_00C12.APP	172.16.50.0 172.16.235.0 172.16.240.0 172.16.250.0	EDIFICIO C 2do PISO ALA NORTE, SALA 1	3C16872	0	1 GB	4	3
							3C16860	1	10/100 MB	48	4
							3C16860	2	10/100 MB	48	3
							LIBRE	3	-	-	-
										4 F.O.	3 F.O.
MATERIALES	CISCO 6000	172.16.240.72	V3.00	77403_00C12.APP	172.16.50.0 172.16.235.0 172.16.240.0 172.16.250.0	EDIFICIO C 2do PISO ALA SUR, SALA 2, DGRMSG	3C16872	0	1 GB	4	3
							3C16860	1	10/100 MB	48	0
							3C16860	2	10/100 MB	48	1
							3C16860	3	10/100 MB	48	24
							No. DE SLOTS DISPONIBLES	0	-	144 RJ45 4 F.O.	25 RJ45 3 F.O.
INFORMÁTICA	CISCO 6500	172.16.240.254	V3.00R	77803_00r.APP	172.16.10.0 172.16.20.0 172.16.30.0 172.16.40.0 172.16.50.0 172.16.235.0 172.16.240.0 172.16.245.0 172.16.250.0	EDIFICIO D PB ALA SUR, CUARTO PRINCIPAL	3C16857	0	-	-	-
							3C16857	1	-	-	-
							3C16862	2	1 GB	20	12
							3C16860	3	10/100 MB	48	4
							3C16860	4	10/100 MB	48	0
							3C16860	5	10/100 MB	48	3
							3C16860	6	10/100 MB	48	2
							3C16860	7	10/100 MB	48	1
							No. DE SLOTS DISPONIBLES	0	-	240 RJ45 20 F.O.	10 RJ45 12 F.O.

CONCLUSIONES

Como podemos observar en el desglose del direccionamiento se hicieron las modificaciones necesarias para una mejor administración que nos permite identificar y aislar con mayor rapidez cualquier problema que se pueda presentar en la red, adicionalmente, se cumple con el objetivo de tener una numeración IP específica para cada entidad que cumpla con estándares y cuya distribución facilite la sumarización y por ende, mejore el desempeño de la red y la eficiencia de la misma se incremente.

Se completó la eliminación de los segmentos que se encontraban operando en la Secretaría con la finalidad de lograr en un 100% la homologación de las redes.

Se aisló la parte de troncales dejando solo las VLAN´s para dar servicio solo al área que pertenece cada equipo de comunicación logrando así una mejor administración de la red y seguridad de la misma.

Se reviso y se depuro todo a lo que concierne el cableado estructurado para liberar espacio en las tarjetas de los equipos de comunicación a lo que se refiere a puertos de red (RJ-45) para poder eliminar todos los hubs que ocasionaban colisiones de dominio disminuyendo los niveles de servicio de la red.

En general los cambios realizados en la SHCP optimizaron la productividad y disponibilidad de los servicios de red llegando a un porcentaje casi del 100% que no se obtenía antes de realizar los cambios.

En cuestión de seguridad es más fácil detectar una terminal con cierta dirección IP, ya que podemos determinar en que equipo de comunicación esta conectado con la distribución de VLAN´s; con esta información se pueden tomar medidas de seguridad pertinentes; como bloquear el puerto que este afectando la red, bloquear la VLAN conflictiva y en un caso extremo desconectar el equipo de comunicación de la red sin afectar a los demás terminales (ya sea usuarios, impresoras, servidores, etc.).

Los equipos de comunicaciones que realicen las funciones de ruteo nos proporcionan la facilidad de elegir que VLAN´s son las autorizadas para convivir con otras y cuales serían las VLAN´s que estarían aisladas de todas las demás.

Estos cambios realizados en la SHCP se podrán reflejar también a los demás inmuebles para optimizar la convivencia con las demás redes existentes y mejorar la calidad de servicio. Esto se implemento en un inmueble para ver el impacto que se obtendría y comparar el impacto sobre los demás inmuebles.

GLOSARIO

10BASE-T
Norma de conexión de redes del IEEE sobre el cableado Ethernet de par trenzado a 10 Mbps.

100BASE-TX
Norma de conexión de redes del IEEE sobre el cableado Ethernet de par trenzado a 100 Mbps; llamada también Fast Ethernet.

100BASE-FX
Norma de conexión de redes del IEEE para Ethernet por cableado de fibra óptica multimodo a 100 Mbps. Una de las versiones de Fast Ethernet.

1000BASE-SX
Norma de conexión de redes del IEEE para un tipo de Gigabit Ethernet por cableado de fibra óptica multimodo con una longitud de onda de 850 nm.

1000BASE-LX
Norma de conexión de redes del IEEE para un tipo de Gigabit Ethernet por cableado de fibra óptica multimodo y monomodo con una longitud de onda de 1330 nm.

1000BASE-T
Norma de conexión de redes del IEEE para un tipo de Gigabit Ethernet por cable de par trenzado sin blindar.

Agregación de enlaces
Agrupamiento de múltiples enlaces de red en un enlace lógico de ancho de banda elevado. Al agrupar cuatro conexiones Ethernet de 100 Mbps en un enlace lógico, se puede obtener un caudal bidireccional de hasta 800 Mbps entre el servidor y el conmutador.

Almacenar y enviar
Función de conmutación en la que el puerto receptor recibe todo el marco de entrada y almacena las memorias intermedias antes de enciarla al puerto de destino.

Alojamiento Web
Consiste en colocar la página web del cliente en un servidor web comercial. Un solo servidor puede albergar cientos e incluso miles de pequeños sitios web, mientras que otros sitios web de mayor tamaño usan un servidor dedicado o varios servidores.

Ancho de banda
Cantidad máxima de datos que se pueden transmitir en un período de tiempo determinado. Normalmente se expresa en bits por segundo o bytes por segundo.

Anfitrión
Cualquier entidad de la red que puede dar inicio a una transmisión. Un enrutador, servidor o equipo.

Árbol de expansión
Proceso empleado para eliminar rutas de datos redundantes e incrementar la eficiencia de la red.

ASIC
Del inglés, Application-Specific Integrated Circuit (Circuito Integrado Específico para Aplicaciones). Chip diseñado para una aplicación en particular. Estos circuitos se utilizan en los dispositivos de conexión de redes para maximizar el rendimiento a un costo mínimo.

ASP
Del inglés Application Service Provider (Proveedor de Servicios de Aplicaciones). Empresa que hospeda aplicaciones de software en los servidores de sus instalaciones. Los clientes pueden acceder a estas aplicaciones por líneas privadas o Internet.

ATM
Del inglés, Asynchronous Transfer Mode (Modo de Transferencia Asíncrona). Tecnología de redes basada en celdas que transmite datos, voz, vídeo y tráfico de retransmisión de tramas.

Autonegociación
Proceso de dos etapas en que un dispositivo de red capta automáticamente la velocidad y la capacidad de dúplex de otro dispositivo.

Autodetección
Proceso en que un dispositivo de red capta automáticamente la velocidad de otro dispositivo.

Banda ancha
Infraestructura de comunicaciones con un ancho de banda elevado (conductos grandes de transmisión) que acelera la transmisión de datos y garantiza el uso de aplicaciones futuras para la economía basada en Internet.

BGP
Del inglés Border Gateway Protocol (Protocolo de Pasarelas de Borde). Protocolo de Internet que permite que grupos de enrutadores (denominados sistemas autónomos) compartan información de enrutamiento para establecer rutas eficientes y sin bucles. Los proveedores de servicios de Internet (ISP) utilizan con frecuencia el BGP, dentro de su red o entre las distintas redes. El protocolo está definido en RFC 1771.

BGP4
Del inglés Border Gateway Protocol (Protocolo de Pasarelas de Borde). Extensión de este protocolo de Internet que permite que grupos de enrutadores (denominados sistemas autónomos) compartan información de enrutamiento

para establecer rutas eficientes y sin bucles. Los proveedores de servicios de Internet (ISP) utilizan con frecuencia el BGP, dentro de su red o entre las distintas redes.

BLEC
Del inglés Building Local Exchange Carrier (Portadora Local para Inmuebles). Tipo de proveedor de servicios que ofrece acceso a Internet y servicios de redes de datos para los edificios con múltiples inquilinos que son propiedad de inmobiliarias comerciales o residenciales.

Cable de fibra monomodo
Fibra con un diámetro relativamente estrecho, a través del cual solo se puede propagar un modo. Transporta un mayor ancho de banda que la fibra multimodo, pero requiere una fuente de luz con poco ancho de espectro.

Cable de Fibra Multimodo
Cable de fibra con un núcleo extenso. La luz se refleja a lo largo del núcleo en varios ángulos y se propaga por múltiples caminos. Cada ruta tiene una longitud diferente y por consiguiente, un tiempo para recorrer la fibra diferente. Esos ángulos o modos múltiples hacen que los elementos de la señal se dispersen con el tiempo, de manera que las distorsiones producidas se limitan a la distancia a la que se puede mantener la integridad de la señal. La fibra multimodo es el principal tipo de fibra LAN que se instala en los edificios y es menos costosa que la fibra de modo único.

Calidad de servicio basada en directivas (Qos)
Servicio de red que permite establecer la prioridad entre los diferentes tipos de tráfico y manejar ancho de banda en una red.

Cableado con capacidad para transmitir voz
Término que se refiere generalmente a líneas análogas con el ancho de banda requerido para transmitir voz humana, normalmente, cerca de cuatro mil Hertz (4KHz).

Capa 1
La primera capa (física) del modelo abierto de interconexión de sistemas (OSI). Transmite datos por un enlace de red. Esta capa debe regular la señal y mantener su intensidad. Los concentradores y repetidores trabajan en la capa 1. Todos los paquetes recibidos se repiten hacia el cableado.

Capa 2
La segunda capa (enlace de datos) del modelo abierto de interconexión de sistemas (OSI). Es la capa de control de acceso a soportes (MAC). Transmite los paquetes a un enlace físico de la capa 1 leyendo las direcciones MAC de origen y destino de cada paquete. La conmutación trabaja en la capa 2. Los conmutadores tienen una tabla de reenvío con las direcciones de hardware de los dispositivos que están conectados. Cuando llegan los paquetes, el conmutador lee la dirección de capa 2 y si corresponde con una dirección de la tabla, reenvía el paquete a ese puerto. En caso contrario, reenvía o "desborda" el paquete a todos los puertos.

Capa 3
La tercera capa (red) del modelo abierto de interconexión de sistemas (OSI). La capa de red enruta los datos hacia las diferentes LAN y WAN basándose en la dirección de red.

Capa 4
La cuarta capa (transporte) del modelo abierto de interconexión de sistemas (OSI). Incluye los servicios de red para la administración punta-a-punta de una sesión de comunicaciones.

Capa 7
La séptima capa (aplicación) del modelo abierto de interconexión de sistemas (OSI). Define los servicios que sirven de apoyo directo a las aplicaciones como los software de administración de redes, correo electrónico o transferencia de archivos.

Capa de enlace de datos.
Categoría 5 (CAT5)
Norma de conexión de redes que certifica que un cable de cobre puede transmitir datos hasta 100 Mbps. Véase UTP.

Chipset
Conjuntos de circuitos de hardware integrados, como los ASIC (circuitos integrados específicos para aplicaciones), que cumplen una función determinada. Estos circuitos se utilizan en los dispositivos de conexión de redes para maximizar el rendimiento a un costo mínimo. Los conmutadores se basan en el poderoso chipset de la serie "i". Véase ASIC.

CLI
Del inglés Command Line Interface (Interfaz de la Línea de Comando). Interfaz que permite al usuario interactuar con el sistema operativo introduciendo comandos y argumentos opcionales.

Cliente/Servidor
Modelo de comunicación en que los equipos de escritorio "clientes" pueden acceder a la información de múltiples "servidores" y compartir estos datos.

Colisión
Transmisiones Ethernet que se originan en dos o más dispositivos y confluyen en el mismo segmento.

Conformación bidireccional de la velocidad
Tecnología de hardware que aplica las directivas de tráfico y uso de las rutas, y al mismo tiempo administra el tráfico dirigiendo los paquetes de datos a la cola de ingreso lógico y procesando las directivas de manera bidireccional. Se denomina también ancho de banda por segmentos.

Conmutación de aplicación
Dispositivo de conexión de redes de centros de datos que trabaja en las capas 4-7 y realiza funciones inteligentes para detectar las distintas aplicaciones y asignarle a cada una los recursos y servicios de red solicitados en función de la facturación del cliente. El conmutador de aplicación SummitPx1 de Extreme hace todo esto a la velocidad de la línea de Gigabit Ethernet. Las funciones de red, como el análisis, finalización, origen e incluso modificación de la sesión TCP a la velocidad del cable, se realizan totalmente en el hardware.

Conmutador
Dispositivo de red que filtra y transmite paquetes entre segmentos LAN y escritorios.

Conmutador Enterprise Desktop
El conmutador Enterprise Desktop (escritorio empresarial) combina el bajo costo y la simplicidad de un dispositivo de extremo apilable con las funciones para empresas de los conmutadores en bastidor de mayor costo.

Concentrador
Dispositivo usado en una red LAN para combinar las transmisiones de un conglomerado de clientes y/o servidores.

COPS
Del inglés Common Open Policy Service (Servicio de Directiva Abierta Común). Protocolo que se utiliza con RSVP y las conexiones de redes basadas en directivas para establecer la comunicación entre un dispositivo de red y la autoridad de administración de directivas. Esta última es, por lo general, un servidor de directivas o un servidor de control de admisión de llamadas. El protocolo define el transporte y el formato de los datos que se usan en la comunicación.

Densidad de puerto
Número de puertos, físicos o lógicos por dispositivo de red.

DHCP
Del inglés Dynamic Host Control Protocol (Protocolo de Control Dinámico de Anfitrión). Es un mecanismo eficaz para asignar y reutilizar de manera dinámica un número fijo de direcciones IP cuando la cantidad de dispositivos en la red sobrepasa las direcciones disponibles. Un servidor DHCP asigna de manera dinámica direcciones IP a los dispositivos que las solicitan. Estas direcciones asignadas se vencen en determinado lapso que establece el administrador de la red. Después de la fecha de vencimiento, el servidor DHCP reasigna estas direcciones a otros dispositivos según las necesidades. El DHCP es una extensión del protocolo BOOTP en que la asignación de direcciones es estática.

Difusión
Mensaje reenviado a todos los dispositivos de una red. La difusión está presente en la capa 2.

DiffServ
Del inglés Servicios Diferenciados. Estándar del IETF que fue creado para resolver problemas de calidad del IP. DiffServ se implementa en la capa 3 y permite la negociación fuera de banda. El protocolo se basa en los controladores del tráfico que se encuentran en el extremo de la red para así indicar los requisitos de cada paquete.

Dirección
Conjunto de caracteres que identifica un nodo de red individual.

Dirección de destino
La dirección IP o MAC del nodo que va a recibir el paquete.

Dirección de subred
Método que un administrador puede usar para conectar múltiples redes físicas con una sola dirección de red IP. Los enrutadores locales y conmutadores inteligentes usan extensiones de las direcciones de red IP para identificar y enrutar el tráfico a segmentos locales, físicos.

Dirección del hardware
Dirección física o de control de acceso a medios (MAC) de un dispositivo.

Dirección fuente
La dirección de IP o de control de acceso a soportes (MAC) del nodo que emite el paquete.

Dorsal
Interconexión de subredes y grupos de trabajo en una red LAN o WAN. Designa también la conexión de alta velocidad a las subredes de menor velocidad. Por ejemplo, una dorsal de red Gigabit Ethernet conectada a subredes Fast Ethernet.

Dúplex
Modo de comunicación en que un dispositivo puede enviar y recibir datos por el mismo enlace. El dispositivo puede funcionar en "full-duplex" y "half-duplex".

Duplicación de puerto
Función de conmutación que permite duplicar datos en la capa control de acceso a soportes (MAC) de un puerto a otro puerto para ser supervisado por un analizador de redes.

DVMRP
Del inglés, Distance Vector Multicast Routing Protocol (Protocolo de Enrutamiento de Multidifusión por Vector de Distancia) se utiliza para comunicar y distribuir la información de la tabla de enrutamiento de multidifusión. Se basa en el protocolo RIP utilizado para el enrutamiento de unidifusión. Véase IETF document draft-ietf-dvmrp-v3-07.

Encabezamiento
Información especial que aparece al principio de una trama.

Enlace ascendente
Conexión de un dispositivo inferior a uno superior. Concentrador a conmutador, conmutador a enrutador, enrutador a servidor.

Enrutador
Dispositivo de redes que envía paquetes a destinos basado en direcciones IP capa 3. Un enrutador implementa diferentes protocolos para mantener información en el sitio sobre otros enrutadores. Un enrutador lee la información de la dirección de la red capa 3 en cada paquete que recibe y determina si se debe enviarla o no. Si debe enviarla, el enrutador mira la tabla de enrutamiento para determinar cuál es la mejor ruta entre un emisor y un receptor.

Enrutamiento
Proceso de entrega de un mensaje a través de la red o redes.

Enrutamiento por múltiples trayectos de igual costo (ECMP)
Distribuye el tráfico de red por muchos enlaces de gran ancho de banda para aumentar el desempeño. Extreme usa OSPF, lo que permite tener múltiples trayectos de igual costo entre los puntos y distribuir el tráfico equitativamente entre los trayectos disponibles. Puede existir un máximo de cuatro enlaces en un enlace de ECMP y el tráfico se divide según las sesiones abiertas por las direcciones IP origen/destino.

ERP
Del inglés, Enterprise Resource Planning (Planificación de Recursos Empresariales). Sistema de administración empresarial que integra todas las facetas de la actividad comercial de la empresa, como la planificación, fabricación, venta y mercadeo. Como la metodología del ERP es cada vez más popular, se han desarrollado aplicaciones de software para ayudar a los gerentes de negocios a poner en práctica el ERP.

ESRP
Del inglés, Extreme Standby Router Protocol (Protocolo de Enrutamiento de Respaldo de Extreme). Este protocolo permite que los dispositivos de servidor sigan comunicándose si falla un enrutador físico.

Ethernet
Norma de conexión de redes del IEEE, que fue desarrollada por Xerox, para transmitir datos a 10 Mbps.

Extranet
Sitio web seguro destinado a los consumidores y proveedores y no al público general. Puede otorgar acceso a investigaciones subvencionadas, existencias actuales y bases de datos internas, es decir, todo tipo de información privada que no se publica para todo el mundo. La extranet usa la Internet pública como sistema de transmisión, pero se necesita una contraseña para poder tener acceso a esta zona restringida.

Fast Ethernet
Norma de conexión de redes del IEEE para transmitir datos a 100 Mbps. Véase 100BASE-TX.

FDDI
Del inglés, Fiber Distributed Data Interface (Interfaz de Datos Distribuidos por Fibra). Norma de conexión de redes del ANSI diseñada para las redes LAN por fibra óptica a 100 Mbps. Este estándar se utiliza a gran escala como tecnología de dorsal de red para interconectar varias redes Ethernet o en anillo.

Filtro
Acción que realiza el conmutador para descartar ciertos tipos de paquetes de datos.

Firmware
Rutinas de software que se escriben de forma permanente en la memoria de sólo lectura.

Fisgoneo
Búsqueda de paquetes para obtener información.

Fisgoneo IGMP
Método que permite reenviar de manera inteligente los paquetes de multidifusión en un dominio de difusión amplia de capa 2. El protocolo extrae la información de registro del IGMP y crea una lista de distribución de equipos para saber cuáles estaciones finales recibirán la información con una dirección de multidifusión específica.

Full-duplex
Modo de comunicación en que un dispositivo puede enviar y recibir datos simultáneamente por el mismo enlace, con lo que duplica el ancho de banda. Una conexión full-duplex de 100 Mbps tiene 200Mbps de ancho de banda. Una conexión full-duplex de 1000 Mbps tiene 2000Mbps de ancho de banda.

GBIC
Del inglés Gigabit Interface Connector (Conector de Interfaz Gigabit). Conexión física a los dispositivos Gigabit Ethernet.

Gbps
Gigabits por segundo.

Gigabit Ethernet
Norma de conexión de redes para transmitir datos a 1000 Mbps.

Grupo de trabajo
Serie de equipos que están agrupados para compartir recursos como datos y dispositivos periféricos.

Half-Duplex
Modo de comunicación en que un dispositivo puede enviar o recibir datos, pero no simultáneamente.

HTTP
Del inglés Hypertext Transfer Protocol (Protocolo de Transferencia Hipertexto) Define la forma en que el servidor web y el navegador cliente manejan las solicitudes de archivos HTML y gráficos que componen una página web.

Hub
Dispositivo de red no inteligente que envía una señal a todas las estaciones que están conectadas a él.

ICMP
Del inglés Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet) Parte del protocolo IP que maneja los mensajes de error y control. El conmutador emite mensajes ICMP para notificar los problemas de datagramas IP a su fuente.

IEEE 802
Conjunto de normas del Instituto de Ingenieros Electrónicos y Eléctricos que definen los métodos de acceso y control de las redes LAN.

IGMP
Del inglés Internet Group Management Protocol (Protocolo de Administración de Grupos en Internet). Protocolo que usan los servidores y anfitriones para informar a los enrutadores locales sobre su afiliación a grupos de multidifusión. Cuando todos los anfitriones se salen del grupo, el enrutador deja de enviar los datagramas que le llegan para ese grupo.

Internet
La Internet está formada por más de 65 millones de computadoras en más de 100 países y cubre los rubros comercial, académico y gubernamental.

Intranet
Sitio web interno que presta servicios a los empleados de la empresa. Si bien las páginas de la red interna pueden estar enlazadas con la Internet, el público en general no tiene acceso a la intranet.

IP
Protocolo de capa 3 (capa de red) que contiene la información de direccionamiento y control para el enrutamiento de los paquetes.

IPX
Del inglés Internetwork Packet Exchange (Intercambio de Paquetes en Redes Interconectadas). Protocolo de redes utilizado por los sistemas operativos Novell® NetWare®. Como el UDP/IP, IPX es un protocolo de datagramas que se usa para las comunicaciones sin conexión.

ISO
Del inglés International Standards Organization (Organización Internacional de Normalización).

LAN
Redes de área local Red en la que los equipos conectados están cerca, como en el mismo edificio u oficina; un sistema de red LAN con equipos conectados a distancia se denomina red de área amplia (WAN).

Latencia
Todo retraso que se produce en la red e impide que se envíen los paquetes a la velocidad del cable.

Listas de control de acceso
Base de datos que describe el acceso que tiene cada usuario a un servicio.

Localización compartida
Designa el hecho de colocar el equipo de un cliente en las instalaciones seguras de otra compañía. Estas instalaciones brindan espacio para los equipos, seguridad y otros servicios, así como interconexiones y acceso a Internet a los equipos instalados.

MAC
Del inglés Media Access Control (Control de acceso a soportes). Capa 2 del modelo de interconexión abierta de sistemas (OSI). La capa de enlaces de datos es responsable de la programación, transmisión y recepción de datos en una red de área local.

Dirección MAC
Dirección de control de acceso a soportes. Dirección física específica para cada tarjeta de interfaz de la red.

MAN
Del inglés Metropolitan Area Network (Red de Área Metropolitana). Red de datos diseñada para un pueblo o ciudad. En términos de amplitud geográfica, las MAN son de mayor tamaño que las redes de área local (LAN), pero más pequeñas que las redes de área amplia (WAN). Las MAN se caracterizan por permitir conexiones de gran velocidad con cables de fibra óptica o cualquier otro medio.

Máscara de subred
Cifra que el administrador entra para decirle al conmutador cómo filtrar los paquetes que entran. Por ejemplo, una máscara de subred 255.255.0.0 par la dirección 192.3.1.254 le dice al conmutador que solo acepte el tráfico destinado a la dirección IP que empieza por 192.3. Los demás paquetes los abandona.

Mbps
Megabits por segundo.

MIB
Del inglés Management Information Base (Base de Información de Administración) Base de datos de información que el conmutador pone a disposición de los sistemas de administración de información. Por ejemplo, estadísticas sobre el tráfico y configuración de puerto.

MPLS
Del inglés Multiprotocol Label Switching (Conmutación de etiquetas multiprotocolo). Un protocolo de conmutación que integra la información de la capa 2 sobre los enlaces de la red en la capa 3 para simplificar y mejorar el intercambio de paquete IP.

Multidifusión
Un paquete o transmisión destinado a muchos clientes.

NIC
Del inglés Network Interface Card (Tarjeta de interfaz de la red). Tarjeta de expansión que va en una estación de trabajo o servidor y permite la conexión a la red.

OC
Del inglés Opticar Carrier. Portadora óptica empleada para especificar la velocidad de las redes de fibra óptica según las normas SONET. OC-1 = 51,85 Mbps, OC-3 = 155,52 Mbps, OC-12 = 622,08 Mbps, OC-24 = 1,244 Gbps, OC-48 = 2,488 Gbps, OC-96 = 4,976 Gbps, OC-192 = 9,6 Gbps and OC-255 = 13,21 Gbps

OSPF
Del inglés Open Shortest Path First (Primer trayecto más corto abierto). Se trata de un protocolo de enrutamiento que mantiene un mapa de todos los demás enrutadores y redes con las que se conecta. Envía mensajes cortos en los que pregunta si un vecino está activado y al alcance. Es más eficiente y escalable que los protocolos de enrutamiento por vector de distancia que mantienen tablas de todos los destinos conocidos y números de saltos para llegar hasta ellos.

Paquete sobre SONET
Tecnología de transporte de red de área metropolitana (MAN) o red de área amplia (WAN) que transporta paquetes IP directamente sobre la transmisión SONET sin ninguna instalación de enlace de datos como ATM de por medio. Paquete sobre SONET transmite datos a la velocidad más elevada posible porque SONET tiene una sobrecarga de los encabezamientos de paquete menor que ATM (28 bytes de una trama de 810 bytes comparado con 5 de una celda ATM de 53 bytes).

Perfiles de acceso
Los perfiles de acceso controlan todos los aspectos de la administración remota de los conmutadores de Extreme Networks. Un perfil de acceso puede contener una lista de direcciones IP y máscaras de red. Cada método de administración remota puede ser asignado independientemente a un perfil de

acceso. Los métodos de administración remota que están controlados por los perfiles de acceso incluyen SNMP Lectura, SNMP Lectura/Escritura, Web/ExtremeWare Vista, Telnet y acceso SSH2.

PIM DM
Del inglés Protocol Independent Multicast, Dense Mode (Protocolo Independiente de Multidifusión Modo Denso). Un protocolo de multidifusión similar a DVMRP en el sentido que utiliza reenvío por ruta inversa pero no requiere ningún protocolo unidifusión en particular.

PIM SM
Del inglés Protocol Independent Multicast Sparse Mode. Protocolo de multidifusión cuyo trabajo consiste en definir un punto de encuentro común tanto para el emisor como para el receptor. El emisor y el receptor inician la comunicación en el punto de encuentro y cuando empieza el flujo, se produce en una ruta optimizada.

Plano posterior
Bus o matriz de conmutación que se encuentra dentro de un conmutador o el bastidor de un concentrador; todo el tráfico atraviesa este plano posterior por lo menos una vez.

POP
Del inglés Point of presence (Punto de presencia). Punto en el que una portadora de larga distancia se conecta con una empresa telefónica local o con un usuario si la empresa local no está involucrada. Para los servicios en línea y proveedores de servicio Internet, el POP es el marcado de los usuarios de intercambio local a través del módem.

PHY Redundante
Una de las maneras más eficaces, económicas y simples de lograr una redundancia de enlaces con una recuperación sub secundaria es a través de conexiones físicas redundantes, también conocidas como PHY Redundante (se pronuncia 'fî'). Con este tipo de redundancia hay normalmente un enlace primario activo y un enlace secundario de respaldo. Por ejemplo, un solo puerto gigabit puede incorporar dos conexiones físicas. Si el enlace primario falla, el enlace secundario remplazará el primero.

RADIUS
Servicio al usuario a través del marcado telefónico para la autenticación remota, un sistema de autenticación y contabilidad empleado por numerosos provedores de servicio de Internet (ISP). Cuando se marca para tener acceso al ISP se debe colocar el nombre de usuario y la contraseña. Esta información pasa al servidor RADIUS, el cual verifica que la información sea correcta y luego autoriza el acceso al sistema ISP.

RAN
Del inglés Regional area network (Red de Área Regional). Red de datos que interconecta negocios, residencias y gobiernos en una región geográfica específica. Las RAN son de mayor tamaño que las redes de área local (LAN) y

las redes de área metropolitana (MAN), pero más pequeñas que las redes de área amplia (WAN). Las RAN se caracterizan por permitir conexiones de gran velocidad con cables de fibra óptica o cualquier otro medio.

Red de conmutadores
Término empleado para especificar el ancho de banda máximo de un conmutador en la tarjeta madre de plano posterior.

Red dorsal concentrada
Arquitectura de red LAN en la que la interconexión de la subred está concentrada en un conmutador o enrutador de capa 3.

Red Privada Virtual (VPN)
Red privada que se configura dentro de una red pública.

Redirección transparente del caché web
Capacidad inherente de los conmutadores de la serie "i" de Extreme Networks para redireccionar el tráfico web según el criterio capa 4, como HTTP Puerto 80, a la velocidad del cable a uno o más puertos de carga compartida a lo largo de diferentes servidores caché web sin reconfigurar las aplicaciones del navegador.

Resistencia a fallos
Capacidad que tiene un dispositivo de protegerse o recuperarse de los fallos internos y de la red. Los elementos clave de la resistencia a fallos son los módulos intercambiables en caliente, las fuentes de alimentación redundantes con repartición de cargas, los planos posteriores pasivos y sistemas de refrigeración redundantes.

RIP
Del inglés Routing Información Protocol (Protocolo de Información de Enrutamiento). Protocolo definido por RFC 1058 que especifica la manera en que los enrutadores intercambian la información de la tabla de enrutamiento. Con RIP, los enrutadores intercambian periódicamente tablas completas.

RMON
Del inglés Remote Monitoring (Monitoreo Remoto). Protocolo de manejo de redes que permite reunir información sobre la red en una sola estación de trabajo.

RSVP
Del inglés Resource Reservation Protocol (Protocolo de Reservación de Recursos). Norma IETF empleada para suministrar calidad de servicio al reservar ancho de banda antes de la transferencia de paquetes para garantizar su disponibilidad.

Servicio de LAN transparentes (TLS)
Servicio de comunicaciones de una empresa telefónica local o portadora común que enlaza las LAN remotas.

Shell Seguro (SSH)
Shell seguro es un programa que permite conectarse con otro equipo a través de una red, para ejecutar comandos en una máquina remota y desplazar archivos de una máquina a otra. Suministra una buena autenticación y comunicaciones seguras en canales inseguros. SSH protege la red de ataques como IP spoofing, enrutamiento de la fuente IP y DNS spoofing. Para penetrar una red, el atacante solo puede forzar la desconexión del SSH. Dicho atacante no puede reproducir el tráfico o secuestrar las conexiones cuando el cifrado está activado.

Sin bloqueos
Capacidad de un conmutador de transmitir y recibir paquetes en todos los puertos simultáneamente a la velocidad del cable.

Sistema de Contexto de Enlace Dinámico
El Sistema de Contexto de Enlace Dinámico permite establecer directivas basadas en los nombres de usuarios o dispositivos de escritorio, y automáticamente crea correspondencias entre estas directivas y las direcciones de las capas más bajas.

Segmento
Sección de una red delimitada por puentes o conectores. El hecho de dividir Ethernet en múltiples segmentos es una manera común de incrementar en ancho de banda en una LAN.

SNMP
Del inglés Simple Network Management Protocol (Protocolo de Administración de Red Simple) Norma para reunir datos estadísticos sobre el tráfico y el comportamiento de los componente de la red; SNMP utiliza bases de datos de información de administración (MIB), que definen qué información está disponible en cualquier dispositivo de la red que puede ser manejado.

Sobresuscripción
La sobresuscripción o relación de sobresuscripción maneja específicamente los puntos de la red en los que se producen cuellos de botella. El resultado de las relaciones de sobresuscripción es la congestión, la cual provoca la pérdida de paquetes. Las relaciones de sobresuscripción se calculan sumando los requerimientos potenciales de ancho de banda de una ruta en particular y dividiendo el total por el ancho de banda real de la ruta. Aunque una relación superior a 1:0 se considera como sobresuscrita, esto no significa necesariamente que habrá congestión.

SONET
Redes ópticas síncronas, norma para la conexión de sistemas de transmisión de fibra óptica. SONET define las normas de interfaz en la capa física del modelo OSI. La norma define una jerarquía de velocidades de interfaz que permiten multiplexar a los flujos continuos de datos a diferentes velocidades. SONET establece niveles de portadora óptica (OC) de 51,8 Mbps (semejante a la línea T-3) a 9,2 Gbps. Con la implementación de SONET, las empresas de telecomunicación en el mundo pueden interconectar sus sitemas de portadora

digital existente y de fibra óptica. El equivalente internacional de SONET, normalizado por el ITU, se denomina SDH.

T1/E1
Conexión digital dedicada punto a punto configurada para transportar tráfico de voz o datos, ampliamente utilizada en redes privadas así como en interconexiones entre el PBX o LAN de una organización y el telco.

Tabla de direcciones
Base de datos que mantiene el conmutador con todas las direcciones aprendidas y los puertos de conmutación por los que se puede acceder a estas direcciones. El conmutador usa esta base de datos para reenviar paquetes y tomar decisiones de filtrado.

TCP/IP
Del inglés Transmission Control Protocol/Internet Protocol (Protocolo de Control de Transmisión/Protocolo Internet). Serie de protocolos de comunicaciones para conectar anfitriones a Internet.

Telnet
Protocolo dentro de la serie protocolo TCP/IP que suministra una función de emulación de terminal.

Topología
Disposición física o lógica o configuración de una red.

Topología entretejida
Red construida con una mezcla de diferentes topologías de redes. Por ejemplo, una red con una dorsal de gran ancho de banda que se conecte con una serie de segmentos más lentos.

UDP
Del inglés User Datagram Protocol (Protocolo de Datagramas de Usuario). Protocolo sin conexión que, como el TCP, funciona por encima de las redes IP.

Unidifusión
Paquete destinado a una sola dirección.

UTP
Del inglés Unshielded Twisted Pair (Par trenzado sin blindaje). Cableado con cables que están trenzados unos con otros; los cables individuales no están aislados. Véase Categoría 5.

VDSL
Del inglés Very High Speed Digital Subscriber Line (Línea suscriptora digital a muy alta velocidad). Esta línea transmite datos a 10 Mbps-55Mbps en distancias cortas, normalmente, entre 1000 y 6000 pies, en cables con capacidad para transmitir voz.

Velocidad del cable
Velocidad teórica máxima a la que los paquetes pueden ser transmitidos y recibidos en una interfaz de redes.

VID
Identificador VLAN. Número que identifica un VLAN específico.

VLAN
LAN virtuales. Grupo de dispositivos lógicos y no físicos, definidos por software. Las VLAN le permiten a los administradores de la red resegmentar sus redes sin reconfigurar físicamente los dispositivos o conexiones de las redes.

WAN
Del inglés Wide Area Network (Red de Área Amplia). Red que usa tecnología de telecomunicaciones para conectar equipos o redes en largas distancias.

WDM
Del inglés Wavelength Division Multiplexing (Multiplexado por División de Longitud de Onda). Tipo de multiplexado creado para ser utilzado con fibra óptica. WDM modula cada uno de los diferentes flujos de datos a una parte diferente del espectro de luz.

WINS
Del inglés Windows Internet Naming Service (Servicio de nombrado Internet Windows). Sistema que determina la dirección IP asociada a un equipo de la red particular.

BIBLIOGRAFÍA

⇒ "Comunicaciones World nº 93 - Septiembre 1995".

⇒ "Comunicaciones World nº 100 - Abril 1996".

⇒ "Comunicaciones World nº 109 - Febrero 1997".

⇒ David Passmore y John Freeman, "The Virtual LAN Technological Report", http://www.3com.com/nsc/200374.html

⇒ "3com Transcend VLAN's", http://www.3com.com/nsc/200375.html

⇒ "Cisco VLAN Readmap", http://www.cisco.com/warp/public/538/7.html

⇒ http://www.cisco.com/warp/public/793/lan_switching/3.html

⇒ http://www.cisco.com/en/US/tech/tk389/tk390/technologies_configuration_example09186a00800949fd.shtml

⇒ "Internetworking with TCP/IP. Volume I: Principles, Protocols and Architecture", D. E. Comer. 3rd ed., Prentice-Hall, 1995

⇒ "TCP/IP Illustrated, Volume 1. The Protocols", W. Richard Stevens, Addison Wesley, 1994.

⇒ "Configuración de un Router CISCO". Disponible en: http://www.lab.dit.upm.es/~labrst/config/config-ciscos.htm

⇒ "Manuales de Configuración de CISCO". Disponibles en: http://www.lab.dit.upm.es/~labrst/config/manuales-cisco

⇒ "Referencia sobre comandos de CISCO". Disponible en: http://www.lab.dit.upm.es/~labrst/config/ciscopedia/

⇒ CCNA ICND Exam Certification Guide, Wendell Odom, Published by: Cisco Press, 201 West, 103rd Street Indianapolis, IN 46290 USA, 641 pages.