UNIVERSIDAD MAYOR DE SAN ANDRES

FACULTAD DE TECNOLOGÍA

Carrera Electrónica y Telecomunicaciones

Nivel Licenciatura

EXAMEN DE GRADO

TRABAJO DE APLICACIÓN

“DISEÑO DE UNA RED VIRTUAL (VLAN) PARA LA SUCURSAL DE TIGO EN EL ALTO”

Postulante: Edwin Lucio Mayta Mamani

La Paz – Bolivia

2012

DEDICATORIA

A DIOS, quien siempre estuvo dándome fortaleza, sabiduría y gracia en todos los caminos que emprendí.

A mi familia, por motivarme a seguir adelante, en especial a mis padres Lucio y Emiliana que siempre me levantaron el ánimo, me orientaron y aconsejaron prudentemente.

GRACIAS.

ÍNDICE

CAPITULO III

CAPITULO IV

RESUMEN DEL TRABAJO.

La Red actual de la empresa de telecomunicaciones TIGO – Telecel es una de las empresas con mayor concurrencia en nuestra ciudad. El trabajo que realizan las áreas de ésta tiene una importancia relevante en el desarrollo de sus funciones. El rendimiento de esta red puede considerarse como un factor importante en la productividad de una organización y su reputación para realizar sus transmisiones en la forma prevista.

En la sucursal de TIGO en la ciudad de El Alto se hizo necesario que cada área de trabajo llegue a independizarse para un mejor orden y cumplimiento de funciones; es por ello que se busca una tecnología que contribuya a dicha necesidad. En este caso la tecnología que ayude al excelente rendimiento de la red es la división de los grandes dominios de broadcast en dominios más pequeños con las VLAN.

Conceptualizando, una Red Virtual o VLAN es la división de grandes dominios de broadcast en dominios más pequeños que pueden estar geográficamente separados.

Con la utilización de la VLAN ya no es necesario que los grupos de trabajo se encuentren físicamente juntos, ya que la red LAN Virtual los considera como si estuvieran en un mismo ambiente de trabajo, de este modo la red funciona con todas las características de una de tipo LAN convencional.

En el caso de la sucursal de TIGO, ubicada en la ciudad de El Alto, se prevé realizar un diseño de las configuraciones para que llegue a enlazarse a la red donde se encuentra el servidor principal con el que se realizan las conexiones de confirmación de contraseña y la utilización de sus respectivos programas.

Para dicho propósito se realizarán los diseños de configuración en los dispositivos de capa 2 y de capa 3, los mismos que permitirán alcanzar los propósitos planteados.

DISEÑO DE UNA RED VIRTUAL (VLAN) PARA LA SUCURSAL DE TIGO EN EL ALTO

CAPITULO I

1.1. INTRODUCCIÓN

El rendimiento de la red puede considerarse como un factor importante en la productividad de una organización y su reputación para realizar sus transmisiones en la forma prevista. Una de las tecnologías que contribuyen al excelente rendimiento de la red es la división de los grandes dominios de broadcast en dominios más pequeños con las VLAN.

Los dominios de broadcast más pequeños limitan el número de dispositivos que participan en los broadcasts, permitiendo así que los dispositivos se separen en agrupaciones funcionales. Éstas podrían encontrarse considerablemente distantes.

Conceptualizando, una Red Virtual o VLAN es la división de grandes dominios de broadcast en dominios más pequeños que pueden estar geográficamente separados.

Con la utilización de la VLAN ya no es necesario que los grupos de trabajo se encuentren físicamente juntos, ya que la red LAN Virtual los toma como si estuvieran en un mismo ambiente de trabajo, de este modo la red funciona con todas las características de una red LAN convencional.

La sucursal de TIGO en la ciudad de El Alto es una de las sucursales más concurridas, por lo que generalmente utiliza bastante los recursos de la red, siendo éste su principal herramienta para el funcionamiento del mismo. Hasta el momento la utilización de los recursos de la Red ha ido incrementando considerablemente, y de acuerdo a las necesidades del mismo se ha considerado

oportuna una reestructuración lógica de dicha red. La utilización de Redes Virtuales es una de las mejores opciones para el mejor desempeño de la Red de dicha sucursal, considerando un desempeño estable en vista de la apertura de otra sucursal en la zona 16 de julio, en cuyo lugar se encuentra gran cantidad de los usuarios de la empresa.

1.2. PLANTEAMIENTO DEL PROBLEMA

En la actualidad existen percances en la utilización de la red. Se está haciendo muy común que las áreas de trabajo existentes en la empresa se encuentren aisladas una de la otra, el motivo fundamental es la independencia que tendría que existir en cada área, ya que cada una de ellas realiza labores especificas que al ser realizadas independientemente dan mejor resultado que cuando las aéreas pretenden juntar la información de forma inoportuna.

Al hablar de la independencia nos referimos principalmente a que cada área debe concluir con el desempeño de sus funciones antes de proceder a remitirlo a otro área.

Por dichos motivos se estableció que en todas las sucursales de la empresa de Telecomunicaciones TIGO se debe entregar información completa mediante el correo electrónico institucional, éste se encuentra en el servidor junto al los programas con los que interactúa cada área de trabajo de la sucursal, los cuales serán descritos posteriormente.

En vista de éstas circunstancias se vio conveniente realizar el diseño de la Red de la sucursal de TIGO en la ciudad de El Alto en una Red Virtual (VLAN) que independice cada una de las áreas pero que a la vez pueda acceder a una información en común.

1.3. JUSTIFICACIÓN

Con la utilización de las VLANs o redes virtuales se pretende recurrir a gran parte la misma infraestructura física realizando los enlaces e independencias de cada área de forma lógica, permitiendo así que todos cumplan con el buen desempeño de sus funciones, ya que al utilizar las redes virtual, cada área de trabajo funcionaría como si se encontrase en una red LAN física independiente de otra área.

El presente proyecto presenta una solución a la independencia de cada área de trabajo en la sucursal de TIGO en la ciudad de El Alto y la restructuración lógica de la misma, permitiendo el enlace desde la sucursal hasta el servidor donde se encuentran los programas y los usuarios de cada miembro del personal de trabajo. Para ello se prevé reutilizar todos los dispositivos de capa 2 y capa 3, ya que son precisamente éstos los que posibilitarían el enlace desde la Sucursal hasta el servidor principal.

1.4. OBJETIVOS

1.4.1. OBJETIVO GENERAL

El presente proyecto pretende reestructurar la Red convencional de la sucursal de la empresa de Telecomunicaciones TIGO a una Red Virtual VLAN a través de la configuración de los dispositivos de capa 2 y capa 3, ya que a través de ellos se podrá acceder al enlace necesario para el funcionamiento de dicha sucursal. De este modo se independizaría las aéreas de trabajo sin las limitaciones de la distancia.

1.4.2. OBJETIVOS ESPECÍFICOS

- Realizar una redistribución de la Dirección de Red principal en Subredes más pequeñas, adecuadas a la cantidad de usuarios requeridos para cada área de trabajo.
- Habilitar la seguridad administrativa en los dispositivos de paca 2 y 3, Switchs y Routers por medio de contraseñas de administrador en los tipos de conexión directa y remota.
- Configurar los Routers, Switchs y Host necesarios para demostrar como sería el enlace de las áreas de trabajo con el servidor principal.

CAPITULO II

2.1. FUNDAMENTO TEÓRICO

2.1.1. REDES QUE RESPALDAN LA FORMA EN QUE TRABAJAMOS

En principio, las empresas utilizaban redes de datos para registrar y administrar internamente la información financiera, la información del cliente y los sistemas de nómina de empleados. Las redes comerciales evolucionaron para permitir la transmisión de diferentes tipos de servicios de información, como e□mail, video, mensajería y telefonía.

Las intranets, redes privadas utilizadas sólo por una empresa, les permiten comunicarse y realizar transacciones entre empleados y sucursales globales. Las compañías desarrollan extranets o internetwork extendidas para brindarles a los proveedores, fabricantes y clientes acceso limitado a datos corporativos para verificar estados, inventario y listas de partes.

En la actualidad, las redes ofrecen una mayor integración entre funciones y organizaciones relacionadas que la que era posible en el pasado.

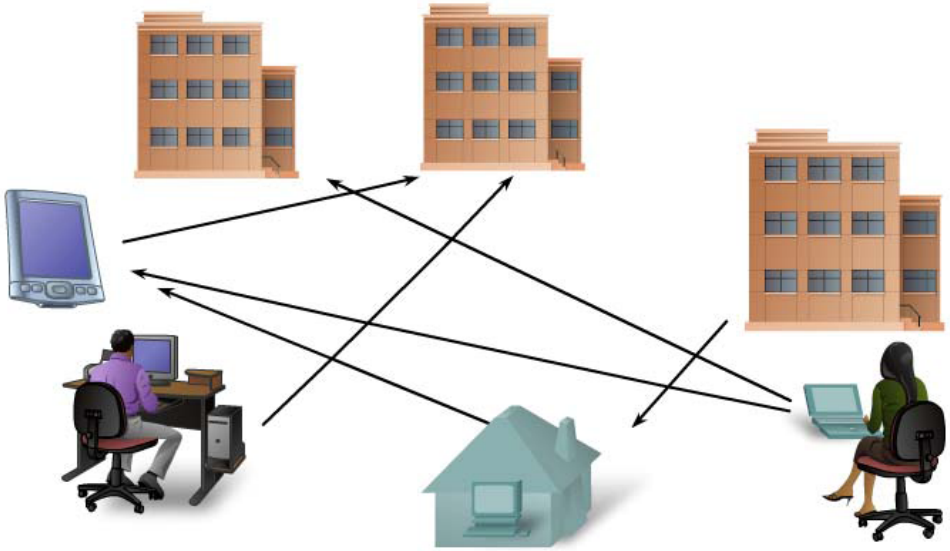


Figura 1
Trabajos que se encuentran en donde estemos
Fuente: http://cisco.netacad.net

2.1.2. COMUNICACIÓN A TRAVÉS DE REDES

Poder comunicarse en forma confiable con todos en todas partes es de vital importancia para nuestra vida personal y comercial. Para respaldar el envío inmediato de los millones de mensajes que se intercambian entre las personas de todo el mundo, confiamos en una Web de redes interconectadas. Estas redes de información o datos varían en tamaño y capacidad, pero todas las redes tienen cuatro elementos básicos en común:

- Reglas y acuerdos para regular cómo se envían, redireccionan, reciben e interpretan los mensajes.
- Los mensajes o unidades de información viajan de un dispositivo a otro.
- Una forma de interconectar esos dispositivos, un medio que puede transportar los mensajes de un dispositivo a otro.
- Y los dispositivos de la red que cambian mensajes entre sí.

La estandarización de los distintos elementos de la red permite el funcionamiento conjunto de equipos y dispositivos creados por diferentes compañías. Los expertos en diversas tecnologías pueden contribuir con las mejores ideas para desarrollar una red eficiente sin tener en cuenta la marca o el fabricante del equipo.

2.2. PROTOCOLOS DE RED

A nivel humano, algunas reglas de comunicación son formales y otras simplemente sobreentendidas o implícitas, basadas en los usos y costumbres. Para que los dispositivos se puedan comunicar en forma exitosa, una nueva suite de protocolos debe describir los requerimientos e interacciones precisos.
Las suite de protocolos de networking describen procesos como los siguientes:

- El formato o estructura del mensaje.
- El método por el cual los dispositivos de networking comparten información sobre rutas con otras redes.
- Cómo y cuando se pasan los mensajes de error y del sistema entre dispositivos.
- O el inicio y terminación de las sesiones de transferencia de datos.

Los protocolos individuales de una suite de protocolos pueden ser específicos de un fabricante o de propiedad exclusiva.

Propietario, en este contexto, significa que una compañía o proveedor controla la definición del protocolo y cómo funciona. Algunos protocolos propietarios pueden ser utilizados por distintas organizaciones con permiso del propietario. Otros, sólo se pueden implementar en equipos fabricados por el proveedor propietario.

Figura 2
El rol de los Protocolos
Fuente: http://cisco.netacad.net

2.3. ARQUITECTURA DE UNA RED

Las redes deben admitir una amplia variedad de aplicaciones y servicios, y también funcionar con diferentes tipos de infraestructuras físicas. El término arquitectura de red, en este marco, se refiere a las tecnologías que admiten la infraestructura, los servicios y protocolos programados que pueden trasladar los mensajes en toda esa infraestructura. Debido a que Internet evoluciona, al igual que las redes en general, descubrimos que existen cuatro características básicas que la arquitectura subyacente necesita para cumplir con las expectativas de los usuarios: tolerancia a fallas, escalabilidad, calidad del servicio y seguridad.

2.3.1. MODELOS DE PROTOCOLO Y REFERENCIA

Existen dos tipos básicos de modelos de networking: modelos de protocolo y modelos de referencia.

Un modelo de protocolo proporciona un modelo que coincide fielmente con la estructura de una suite de protocolo en particular. El conjunto jerárquico de

protocolos relacionados en una suite representa típicamente toda la funcionalidad requerida para interconectar la red humana con la red de datos. El modelo TCP/IP es un modelo de protocolo porque describe las funciones que se producen en cada capa de los protocolos dentro del conjunto TCP/IP.

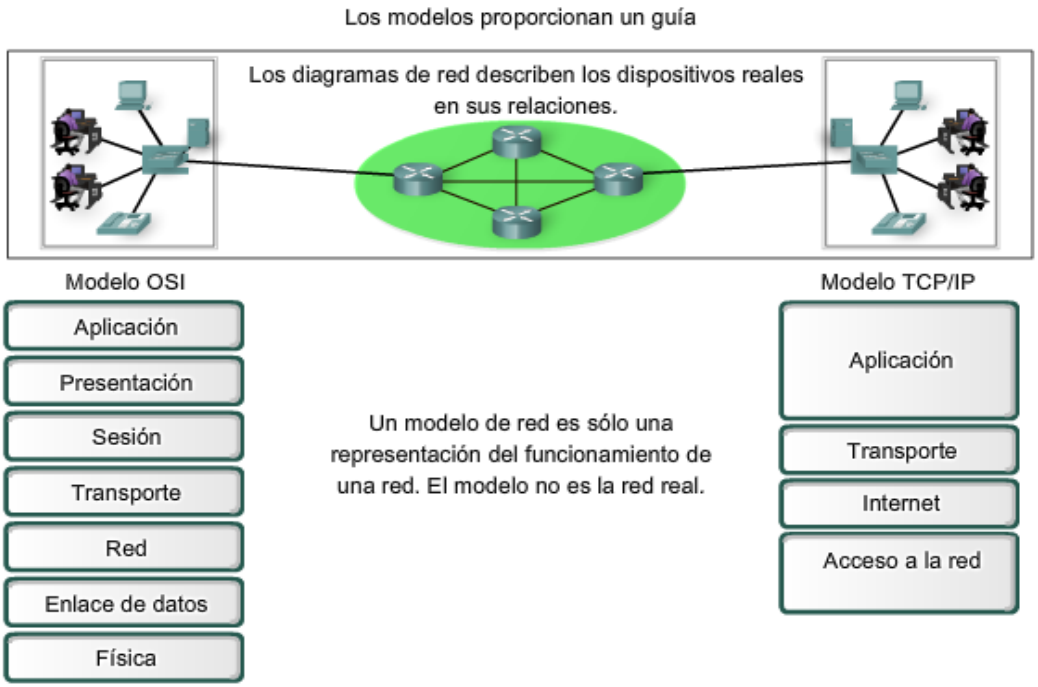


Figura 3
Modelo de protocolos y modelo de referencia
Fuente: http://cisco.netacad.net

Un modelo de referencia proporciona una referencia común para mantener consistencia en todos los tipos de protocolos y servicios de red. Un modelo de referencia no está pensado para ser una especificación de implementación ni para proporcionar un nivel de detalle suficiente para definir de forma precisa los servicios de la arquitectura de red. El propósito principal de un modelo de referencia es asistir en la comprensión más clara de las funciones y los procesos involucrados.

2.3.1.1. MODELO TCP/IP

El modelo TCP/IP describe la funcionalidad de los protocolos que forman la suite de protocolos TCP/IP. Los que se implementan tanto en el host emisor como en el receptor, interactúan para proporcionar la entrega de aplicaciones de extremo a extremo a través de una red.

Un proceso completo de comunicación incluye los siguientes pasos:

- Creación de datos a nivel de la capa de aplicación del dispositivo final origen 2. Segmentación y encapsulación de datos cuando pasan por la stack de protocolos en el dispositivo final de origen.
- Generación de los datos sobre el medio en la capa de acceso a la red de la stack.
- Transporte de los datos a través de la internetwork, que consiste en el medio y/o cualquier dispositivo intermediario.
- Recepción de los datos en la capa de acceso a la red del dispositivo final de destino.
- Desencapsulación y rearmado de los datos cuando pasan por la stack en el dispositivo final.
- El traspaso de estos datos a la aplicación de destino en la capa de aplicación del dispositivo final de destino.

2.3.1.2. MODELO OSI

Como modelo de referencia, el modelo OSI proporciona una amplia lista de funciones y servicios que pueden producirse en cada capa. También describe la interacción de cada capa con las que pasan directamente por encima y por debajo de él. Aunque el contenido de este curso se estructurará en torno al modelo OSI, el eje del análisis serán los protocolos identificados en el stack de protocolos TCP/IP.

2.3.1.3. PROTOCOLO IPv4

El Protocolo de Internet fue diseñado como un protocolo con bajo costo. Provee sólo las funciones necesarias para enviar un paquete desde un origen a un destino a través de un sistema interconectado de redes. El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. Estas funciones son realizadas por otros protocolos en otras capas.

Características básicas de IPv4:

- *Sin conexión:*No establece conexión antes de enviar los paquetes de datos.
- *Máximo esfuerzo (no confiable):* No se usan encabezados para garantizar la entrega de paquetes.
- *Medios independientes:* Operan independientemente del medio que lleva los datos.

2.3.1.4. ENCABEZADO DEL PAQUETE IPv4

Como se muestra en la figura, un protocolo IPv4 define muchos campos diferentes en el encabezado del paquete. Estos campos contienen valores binarios que los servicios IPv4 toman como referencia a medida que envían paquetes a través de la red.

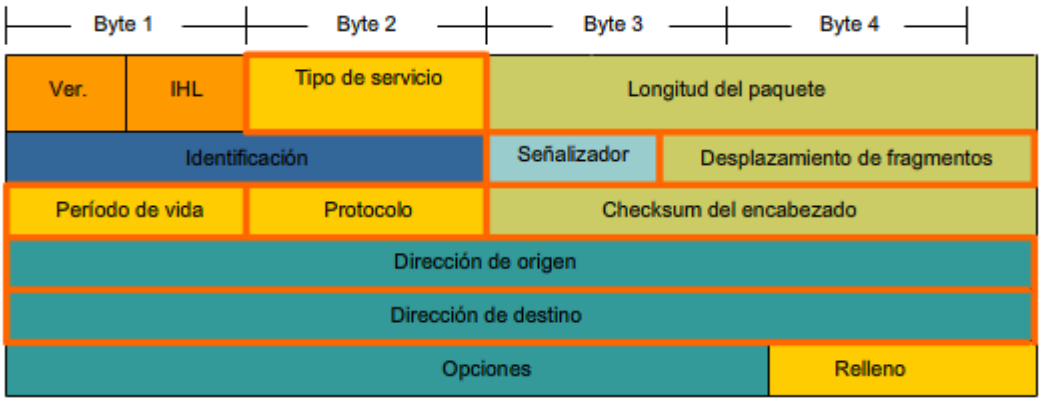


Figura 4
Encabezado de IPv4
Fuente: “Redes de Computadoras”, Tanenbaum

Los campos más importantes son:

- Dirección IP origen.
- Dirección IP destino.
- Tiempo de existencia (TTL).
- Versión
- Protocolo

2.4. DIRECCIONAMIENTO IPv4

Cada dispositivo de una red debe ser definido en forma exclusiva. En la capa de red es necesario identificar los paquetes de la transmisión con las direcciones de origen y de destino de los dos sistemas finales. Con IPv4, esto significa que cada paquete posee una dirección de origen de 32 bits y una dirección de destino de 32 bits en el encabezado de Capa 3.

Estas direcciones se usan en la red de datos como patrones binarios. Dentro de los dispositivos, la lógica digital es aplicada para su interpretación. Para quienes forman parte de la red humana, una serie de 32 bits es difícil de interpretar e incluso es más difícil de recordar. Por lo tanto, representamos direcciones IPv4 utilizando el formato decimal punteada. Ejemplo: ***172.16.4.20***

2.5. DIRECCIONES PÚBLICAS Y PRIVADAS

Aunque la mayoría de las direcciones IPv4 de host son direcciones públicas designadas para uso en redes a las que se accede desde Internet, existen bloques de direcciones que se utilizan en redes que requieren o no acceso limitado a Internet. A estas direcciones se las denomina direcciones privadas.

2.5.1 DIRECCIONES PRIVADAS

Los bloques de direcciones privadas son:

10.0.0.0 a 10.255.255.255 (10.0.0.0 /8)

172.16.0.0 a 172.31.255.255 (172.16.0.0 /12)
192.168.0.0 a 192.168.255.255 (192.168.0.0 /16)

Los bloques de direcciones de espacio privadas, como se muestra en la figura, se separa para utilizar en redes privadas. No necesariamente el uso de estas direcciones debe ser exclusivo entre redes externas. Por lo general, los hosts que no requieren acceso a Internet pueden utilizar las direcciones privadas sin restricciones. Sin embargo, las redes internas aún deben diseñar esquemas de direcciones de red para garantizar que los hosts de las redes privadas utilicen direcciones IP que sean únicas dentro de su entorno de networking.

Muchos hosts en diferentes redes pueden utilizar las mismas direcciones de espacio privado. Los paquetes que utilizan estas direcciones como la dirección de origen o de destino no deberían aparecer en la Internet pública. El router o el dispositivo de firewall del perímetro de estas redes privadas deben bloquear o convertir estas direcciones. Incluso si estos paquetes fueran a hacerse camino hacia Internet, los routers no tendrían rutas para enviarlos a la red privada correcta.

2.5.2. DIRECCIONES PÚBLICAS

La amplia mayoría de las direcciones en el rango de host unicast IPv4 son direcciones públicas. Estas direcciones están diseñadas para ser utilizadas en los hosts de acceso público desde Internet. Aun dentro de estos bloques de direcciones, existen muchas direcciones designadas para otros fines específicos.

2.5.3. TRADUCCIÓN DE DIRECCIONES DE RED (NAT)

Con servicios para traducir las direcciones privadas a direcciones públicas, los hosts en una red direccionada en forma privada pueden tener acceso a recursos a través de Internet. Estos servicios, llamados Traducción de dirección de red (NAT), pueden ser implementados en un dispositivo en un extremo de la red privada. NAT permite a los hosts de la red "pedir prestada" una dirección pública

para comunicarse con redes externas. A pesar de que existen algunas limitaciones y problemas de rendimiento con NAT, los clientes de la mayoría de las aplicaciones pueden acceder a los servicios de Internet sin problemas evidentes.

2.6. REDES DE ÁREA LOCAL (LAN)

Como su nombre lo indica, constituye una forma de interconectar una serie de equipos informáticos y represento uno de los sucesos más críticos para la conexión de equipos de cómputo entre sí.

Una LAN no es más que un medio compartido junto con una serie de reglas que rigen el acceso a dicho medio, las LAN modernas también proporcionan al usuario multitud de funciones avanzadas como por ejemplo, controlar la configuración de equipos dentro de este medio, mediante gestiones de *software*, administración de usuarios y recursos de la red.

Todas las LAN comparten la característica de poseer un alcance ilimitado (normalmente abarcan un edificio) y de tener una velocidad suficiente para que la red de conexión resulte invisible para los equipos que la utilizan.

Una de las LAN más difundida es la Ethernet.

2.7. RED VIRTUAL - VLAN

Las LANs virtuales (VLANs) 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 campus. 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.

Una red virtual es un dominio de broadcast, es decir, cada VLAN tiene su propio dominio de broadcast. Como en un concentrador, todos los dispositivos en una red virtual ve todos los broadcast así como también todas las tramas con dirección de destino desconocida, sólo que los broadcast y tramas desconocidas son originadas dentro de esta red virtual.

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 campus, este cambio físico será transparente gracias a la visión lógica de la red virtual. Así mismo, 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.

2.7.1. VENTAJAS DE LAS VLAN

La productividad del usuario y la adaptabilidad de la red son impulsores clave para el crecimiento y el éxito del negocio. La implementación de la tecnología de VLAN permite que una red admita de manera más flexible las metas comerciales. Los principales beneficios de utilizar las VLAN son los siguientes:

Seguridad: los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial. Las computadoras del cuerpo docente se encuentran en la VLAN 10 y están completamente separadas del tráfico de datos del Invitado y de los estudiantes.

Reducción de costo: el ahorro en el costo resulta de la poca necesidad de actualizaciones de red caras y más usos eficientes de enlaces y ancho de banda existente.

Mejor rendimiento: la división de las redes planas de Capa 2 en múltiples grupos lógicos de trabajo (dominios de broadcast) reduce el tráfico innecesario en la red y potencia el rendimiento.

Mitigación de la tormenta de broadcast: la división de una red en las VLAN reduce la cantidad de dispositivos que pueden participar en una tormenta de broadcast. Como se analizó en el capítulo "Configure un switch", la segmentación de LAN impide que una tormenta de broadcast se propague a toda la red. En la figura puede observar que, a pesar de que hay seis computadoras en esta red, hay sólo tres dominios de broadcast: Cuerpo docente, Estudiante y Invitado.

Mayor eficiencia del personal de TI: las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN. Cuando proporciona un switch nuevo, todas las políticas y procedimientos que ya se configuraron para la VLAN particular se implementan cuando se asignan los puertos. También es fácil para el personal de TI identificar la función de una VLAN proporcionándole un nombre. En la figura, para una identificación más fácil se nombró "Estudiante" a la VLAN 20, la VLAN 10 se podría nombrar "Cuerpo docente" y la VLAN 30 "Invitado ".

Administración de aplicación o de proyectos más simples: las VLAN agregan dispositivos de red y usuarios para admitir los requerimientos geográficos o comerciales. Tener funciones separadas hace que gestionar un proyecto o trabajar con una aplicación especializada sea más fácil, por ejemplo una plataforma de desarrollo de e-learning para el cuerpo docente. También es fácil determinar el alcance de los efectos de la actualización de los servicios de red.

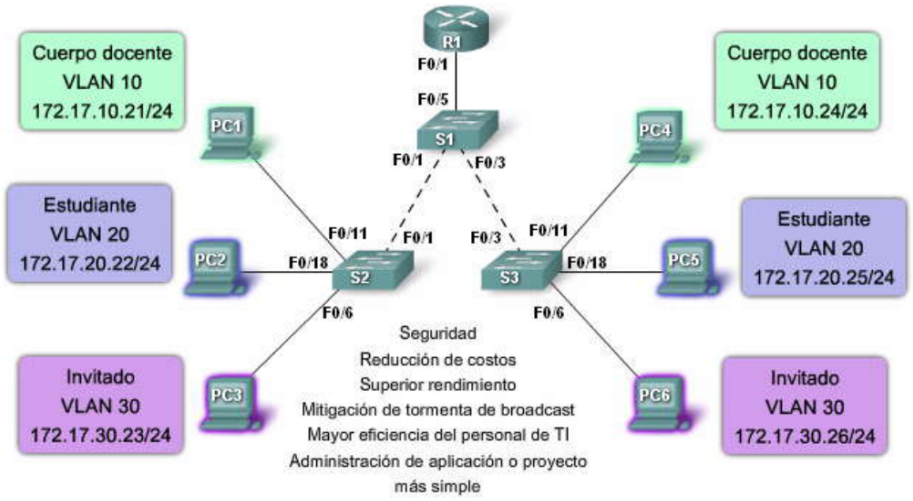


Figura 5
Ventajas de las VLAN
Fuente: http://cisco.netacad.net

2.7.2. RANGOS DEL ID DE LA VLAN

El acceso a las VLAN está dividido en un rango normal o un rango extendido.

2.7.2.1 VLAN DE RANGO NORMAL

- Se utiliza en redes de pequeños y medianos negocios y empresas.
- Se identifica mediante un ID de VLAN entre 1 y 1005.
- Los ID de 1002 a 1005 se reservan para las VLAN Token Ring y FDDI.
- Los ID 1 y 1002 a 1005 se crean automáticamente y no se pueden eliminar.
- Las configuraciones se almacenan dentro de un archivo de datos de la VLAN, denominado vlan.dat. El archivo vlan.dat se encuentra en la memoria flash del switch.
- El protocolo de enlace troncal de la VLAN (VTP), que ayuda a gestionar las configuraciones de la VLAN entre los switches, sólo puede asimilar las VLAN de rango normal y las almacena en el archivo de base de datos de la VLAN.

2.7.2.2 VLAN DE RANGO EXTENDIDO

- Posibilita a los proveedores de servicios que amplíen sus infraestructuras a una cantidad de clientes mayor. Algunas empresas globales podrían ser lo suficientemente grandes como para necesitar los ID de las VLAN de rango extendido.
- Se identifican mediante un ID de VLAN entre 1006 y 4094.
- Admiten menos características de VLAN que las VLAN de rango normal.
- Se guardan en el archivo de configuración en ejecución.
- VTP no aprende las VLAN de rango extendido.

2.7.3. 255 VLAN CONFIGURABLES

Un switch de Cisco Catalyst 2960 puede admitir hasta 255 VLAN de rango normal y extendido, a pesar de que el número configurado afecta el rendimiento del hardware del switch. Debido a que la red de una empresa puede necesitar un switch con muchos puertos, Cisco ha desarrollado switches a nivel de empresa que se pueden unir o apilar juntos para crear una sola unidad de conmutación que consiste en nueve switches separados. Cada switch por separado puede tener 48 puertos, lo que suma 432 puertos en una sola unidad de conmutación. En este caso, el límite de 255 VLAN por un solo switch podría ser una restricción para algunos clientes de empresas.

2.7.4. TIPOS DE VLAN

Hoy en día, existe fundamentalmente una manera de implementar las VLAN: VLAN basada en puerto. Una VLAN basada en puerto se asocia con un puerto denominado acceso VLAN.

Sin embargo, en las redes existe una cantidad de términos para las VLAN. Algunos términos definen el tipo de tráfico de red que envían y otros definen una función específica que desempeña una VLAN. A continuación, se describe la terminología común de VLAN:

2.7.4.1. VLAN De DATOS

Una VLAN de datos es una VLAN configurada para enviar sólo tráfico de datos generado por el usuario. Una VLAN podría enviar tráfico basado en voz o tráfico utilizado para administrar el switch, pero este tráfico no sería parte de una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos. La importancia de separar los datos del usuario del tráfico de voz y del control de administración del switch se destaca mediante el uso de un término específico para identificar las VLAN que sólo pueden enviar datos del usuario: una "VLAN de datos". A veces, a una VLAN de datos se la denomina VLAN de usuario.

2.7.4.2. VLAN PREDETERMINADA

Todos los puertos de switch se convierten en un miembro de la VLAN predeterminada luego del arranque inicial del switch.

Hacer participar a todos los puertos de switch en la VLAN predeterminada los hace a todos parte del mismo dominio de broadcast. Esto admite cualquier dispositivo conectado a cualquier puerto de switch para comunicarse con otros dispositivos en otros puertos de switch. La VLAN predeterminada para los switches de Cisco es la VLAN 1. La VLAN 1 tiene todas las características de cualquier VLAN, excepto que no la puede volver a denominar y no la puede eliminar. El tráfico de control de Capa 2, como CDP y el tráfico del protocolo spanning tree se asociará siempre con la VLAN 1: esto no se puede cambiar. En la figura, el tráfico de la VLAN1 se envía sobre los enlaces troncales de la VLAN conectando los switches S1, S2 y S3. Es una optimización de seguridad para cambiar la VLAN predeterminada a una VLAN que no sea la VLAN 1; esto implica configurar todos los puertos en el switch para que se asocien con una VLAN predeterminada que no sea la VLAN 1. Los enlaces troncales de la VLAN admiten la transmisión de tráfico desde más de una VLAN. A pesar de que los enlaces troncales de la VLAN se mencionan a lo largo de esta sección, se explican a detalle en la próxima sección.

Nota: Algunos administradores de red utilizan el término "VLAN predeterminada" para referirse a una VLAN que no sea la
VLAN 1 que el administrador de red definió como la VLAN a la que se asignan todos los puertos cuando no están en uso.
En este caso, la única función que cumple la VLAN 1 es la de manejar el tráfico de control de Capa 2 para la red.

2.7.4.3 VLAN NATIVA

Una VLAN nativa está asignada a un puerto troncal 802.1Q. Un puerto de enlace troncal 802.1 Q admite el tráfico que llega de muchas VLAN (tráfico etiquetado) como también el tráfico que no llega de una VLAN (tráfico no etiquetado). El puerto de enlace troncal 802.1Q coloca el tráfico no etiquetado en la VLAN nativa. En la figura, la VLAN nativa es la VLAN 99. El tráfico no etiquetado lo genera una computadora conectada a un puerto de switch que se configura con la VLAN nativa. Las VLAN se establecen en la especificación IEEE 802.1Q para mantener la compatibilidad retrospectiva con el tráfico no etiquetado común para los ejemplos de LAN antigua. Para nuestro fin, una VLAN nativa sirve como un identificador común en extremos opuestos de un enlace troncal. Es una optimización usar una VLAN diferente de la VLAN 1 como la VLAN nativa.

2.7.4.4. VLAN DE ADMINISTRACIÓN

Una VLAN de administración es cualquier VLAN que usted configura para acceder a las capacidades de administración de un switch. La VLAN 1serviría como VLAN de administración si no definió proactivamente una VLAN única para que sirva como VLAN de administración. Se asigna una dirección IP y una máscara de subred a la VLAN de administración. Se puede manejar un switch mediante HTTP, Telnet, SSH o SNMP. Debido a que la configuración lista para usar de un switch de Cisco tiene a VLAN 1 como la VLAN predeterminada, puede notar que la VLAN 1 sería una mala opción como VLAN de administración; no querría que un usuario arbitrario se conectara a un switch para que se configurara de manera predeterminada la VLAN de administración.

2.7.4.5. VLAN DE VOZ

Es fácil apreciar por qué se necesita una VLAN separada para admitir la Voz sobre IP (VoIP). Imagine que está recibiendo una llamada de urgencia y de repente la calidad de la transmisión se distorsiona tanto que no puede comprender lo que está diciendo la persona que llama. El tráfico de VoIP requiere:

- Ancho de banda garantizado para asegurar la calidad de la voz
- Prioridad de la transmisión sobre los tipos de tráfico de la red
- Capacidad para ser enrutado en áreas congestionadas de la red
- Demora de menos de 150 milisegundos (ms) a través de la red

Para cumplir estos requerimientos, se debe diseñar la red completa para que admita VoIP. Los detalles sobre cómo configurar una red para que admita VoIP están más allá del alcance del curso, pero es útil resumir cómo una VLAN de voz funciona entre un switch, un teléfono IP de Cisco y una computadora.

En la figura, la VLAN 150 se diseña para enviar tráfico de voz. La computadora del estudiante PC5 está conectada al teléfono IP de Cisco y el teléfono está conectado al switch S3. La PC5 está en la VLAN 20 que se utiliza para los datos de los estudiantes. El puerto F0/18 en S3 se configura para que esté en modo de voz a fin de que diga al teléfono que etiquete las tramas de voz con VLAN 150. Las tramas de datos que vienen a través del teléfono IP de Cisco desde la PC5 no se marcan. Los datos que se destinan a la PC5 que llegan del puerto F0/18 se etiquetan con la VLAN 20 en el camino al teléfono, que elimina la etiqueta de la VLAN antes de que los datos se envíen a la PC5. Etiquetar se refiere a la adición de bytes a un campo en la trama de datos que utiliza el switch para identificar a qué VLAN se debe enviar la trama de datos.

2.8.5. MODOS DE MEMBRESIS DEL PUERTO DE SWTICH

2.8.5.1 PUERTOS DE SWITCH

Los puertos de switch son interfaces de Capa 2 únicamente asociados con un puerto físico. Los puertos de switch se utilizan para manejar la interfaz física y los

protocolos asociados de Capa 2. No manejan enrutamiento o puenteo. Los puertos de switch pertenecen a una o más VLAN.

2.8.5.2. MODOS DE PUERTOS DE SWITCH DE VLAN

Cuando configura una VLAN, debe asignarle un número de ID y le puede dar un nombre si lo desea. El propósito de las implementaciones de la VLAN es asociar con criterio los puertos con las VLAN particulares. Se configura el puerto para enviar una trama a una VLAN específica. Como se mencionó anteriormente, el usuario puede configurar una VLAN en el modo de voz para admitir tráfico de datos y de voz que llega desde un teléfono IP de Cisco. El usuario puede configurar un puerto para que pertenezca a una VLAN mediante la asignación de un modo de membresía que especifique el tipo de tráfico que envía el puerto y las VLAN a las que puede pertenecer. Se puede configurar un puerto para que admita estos tipos de VLAN:

- ***VLAN estática***: los puertos en un switch se asignan manualmente a una VLAN. Las VLAN estáticas se configuran por medio de la utilización del CLI de Cisco. Esto también se puede llevar a cabo con las aplicaciones de administración de GUI, como el Asistente de red Cisco. Sin embargo, una característica conveniente del CLI es que si asigna una interfaz a una VLAN que no existe, se crea la nueva VLAN para el usuario. Para ver un ejemplo de configuración de VLAN estática, haga clic en el botón Ejemplo de Modo Estático en la figura. Cuado haya finalizado, haga clic en el botón Modos de Puertos en la figura. Esta configuración no se examinará en detalle ahora. Se presentará más adelante en este capítulo.
- ***VLAN dinámica***: este modo no se utiliza ampliamente en las redes de producción. Sin embargo, es útil saber qué es una VLAN dinámica. La membresía de una VLAN de puerto dinámico se configura utilizando un servidor especial denominado Servidor de política de membresía de VLAN (VMPS). Con el VMPS, asigna puertos de switch a las VLAN basadas en forma dinámica en la dirección MAC de origen del dispositivo conectado al puerto. El beneficio llega cuando traslada un host desde un puerto en un

switch en la red hacia un puerto sobre otro switch en la red. El switch asigna en forma dinámica el puerto nuevo a la VLAN adecuada para ese host.

- ***VLAN de voz***: el puerto está configurado para que esté en modo de voz a fin de que pueda admitir un teléfono IP conectado al mismo. Antes de que configure una VLAN de voz en el puerto, primero debe configurar una VLAN para voz y una VLAN para datos. En la figura, la VLAN 150 es la VLAN de voz y la VLAN 20 es la VLAN de datos. Se supone que la red ha sido configurada para garantizar que el tráfico de voz se pueda transmitir con un estado prioritario sobre la red. Cuando se enchufa por primera vez un teléfono en un puerto de switch que está en modo de voz, éste envía mensajes al teléfono proporcionándole la configuración y el ID de VLAN de voz adecuado. El teléfono IP etiqueta las tramas de voz con el ID de VLAN de voz y envía todo el tráfico de voz a través de la VLAN de voz.

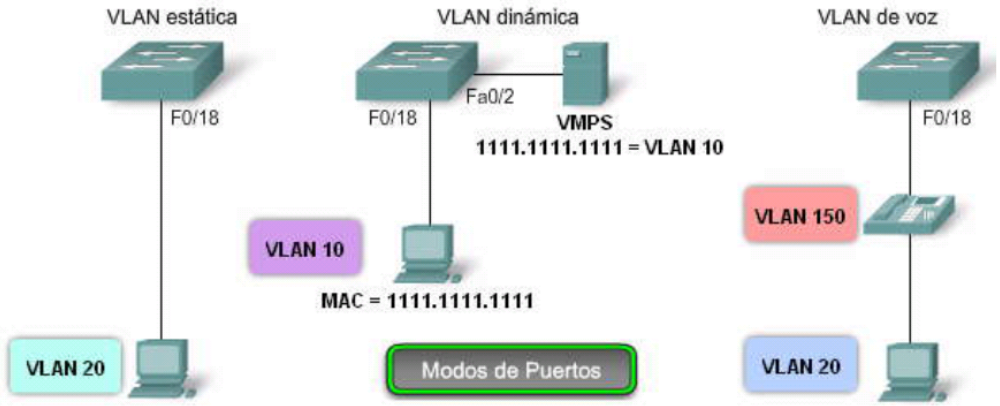


Figura 6
Modos de Membresia
Fuente: http://cisco.netacad.net

2.8.6. CONTROL DE LOS DOMINIO DE BROADCAST CON LAS VLAN

- ***Red sin VLAN***

En funcionamiento normal, cuando un switch recibe una trama de broadcast en uno de sus puertos, envía la trama a todos los demás puertos. En la figura, toda la red está configurada en la misma subred, 172.17.40.0/24. Como resultado,

cuando la computadora del cuerpo docente, PC1, envía una trama de broadcast, el switch S2 envía esa trama de broadcast a todos sus puertos. La red completa la recibe finalmente; la red es un dominio de broadcast.

- ***Red con VLAN***

En la figura, se dividió la red en dos VLAN: Cuerpo docente como VLAN 10 y Estudiante como VLAN 20. Cuando se envía la trama de broadcast desde la computadora del cuerpo docente, PC1, al switch S2, el switch envía esa trama de broadcast sólo a esos puertos de switch configurados para admitir VLAN 10.

En la figura, los puertos que componen la conexión entre los switches S2 y S1 (puertos F0/1) y entre S1 y S3 (puertos F0/3) han sido configurados para admitir todas las VLAN en la red. Esta conexión se denomina enlace troncal. Más adelante en este capítulo aprenderá más acerca de los enlaces troncales.

Cuando S1 recibe la trama de broadcast en el puerto F0/1, S1 envía la trama de broadcast por el único puerto configurado para admitir la VLAN 10, puerto F0/3. Cuando S3 recibe la trama de broadcast en el puerto F0/3, envía la trama de broadcast por el único puerto configurado para admitir la VLAN 10, puerto F0/11. La trama de broadcast llega a la única otra computadora en la red configurada en la VLAN 10, la computadora PC4 del cuerpo docente.

Cuando las VLAN se implementan en un switch, la transmisión del tráfico de unicast, multicast y broadcast desde un host en una VLAN en particular, se limitan a los dispositivos presentes en la VLAN.

2.8.7. ENLACE TRONCAL DE LAS VLAN.-

2.8.7.1 ¿Qué es un enlace troncal?

Es difícil describir las VLAN sin mencionar los enlaces troncales de la VLAN. Aprendió acerca de controlar broadcasts de la red con segmentación de la VLAN y observó la manera en que los enlaces troncales de la VLAN transmitieron tráfico a diferentes partes de la red configurada en una VLAN. En la figura, los enlaces entre los switches S1 y S2 y entre S1 y S3 están configurados para transmitir el tráfico que proviene de las VLAN 10, 20, 30 y 99. Es posible que esta red no funcione sin los enlaces troncales de la VLAN. El usuario descubrirá que la

mayoría de las redes que encuentra están configuradas con enlaces troncales de la VLAN. Esta sección une su conocimiento previo sobre el enlace troncal de la VLAN y proporciona los detalles necesarios para poder configurar el enlace troncal de la VLAN en una red.

2.8.7.2. DEFINICIÓN DE ENLACE TRONCAL DE LA VLAN

Un enlace troncal es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN. Un enlace troncal de VLAN le permite extender las VLAN a través de toda una red. Cisco admite IEEE 802.1Q para la coordinación de enlaces troncales en interfaces Fast Ethernet y Gigabit Ethernet. Más adelante en esta sección, aprenderá acerca de 802.1Q.

Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre switches y routers.

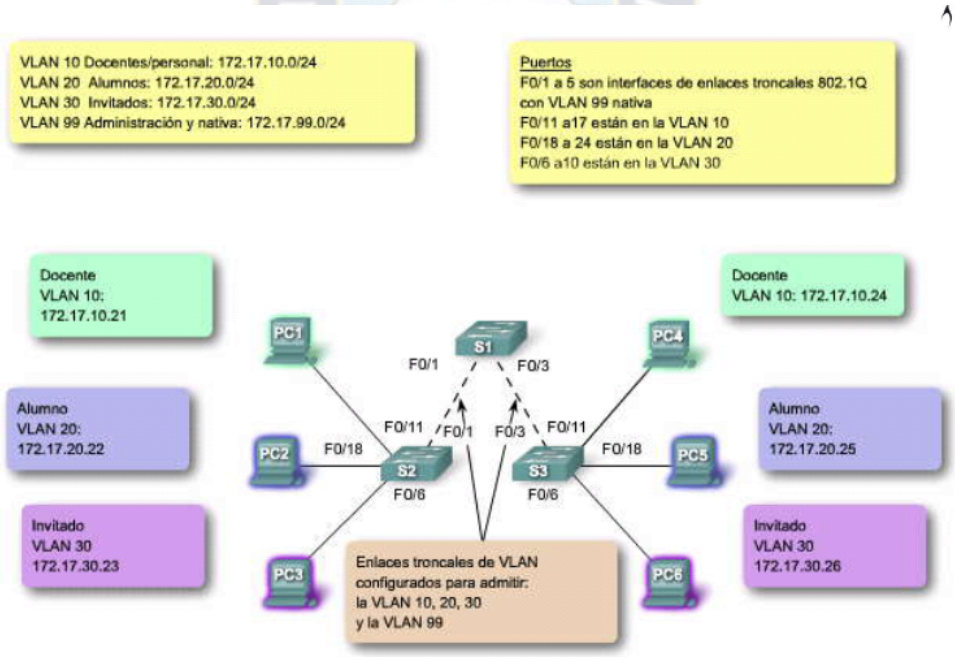


Figura 7
Enlace Troncal en una VLAN
Fuente: http://cisco.netacad.net

2.9. REDES DE ÁREA AMPLIA - WAN

Cuando una compañía o una organización tienen ubicaciones separadas por grandes distancias geográficas es posible que deba utilizar un proveedor de servicio de telecomunicaciones (TSP) para interconectar las LAN en las distintas ubicaciones. Los proveedores de servicios de telecomunicaciones operan grandes redes regionales que pueden abarcar largas distancias. Tradicionalmente, los TSP transportaban las comunicaciones de voz y de datos en redes separadas.

Cada vez más, estos proveedores ofrecen a sus subscriptores servicios de red convergente de información.

Por lo general, las organizaciones individuales alquilan las conexiones a través de una red de proveedores de servicios de telecomunicaciones. Estas redes que conectan las LAN en ubicaciones separadas geográficamente se conocen como

Redes de área amplia (WAN). Aunque la organización mantiene todas las políticas y la administración de las LAN en ambos extremos de la conexión, las políticas dentro de la red del proveedor del servicio de comunicaciones son controladas por el TSP.

Las WAN utilizan dispositivos de red diseñados específicamente para realizar las interconexiones entre las LAN. Dada la importancia de estos dispositivos para la red, la configuración, instalación y mantenimiento de éstos son aptitudes complementarias de la función de una red de la organización.

Las LAN y WAN son de mucha utilidad para las organizaciones individuales. Conectan a los usuarios dentro de la organización. Permiten gran cantidad de formas de comunicación que incluyen intercambio de e□mails, capacitación corporativa y acceso a recursos.

Las LAN separadas por una distancia geográfica están conectadas por una red que se conoce como Red de área extensa (WAN).

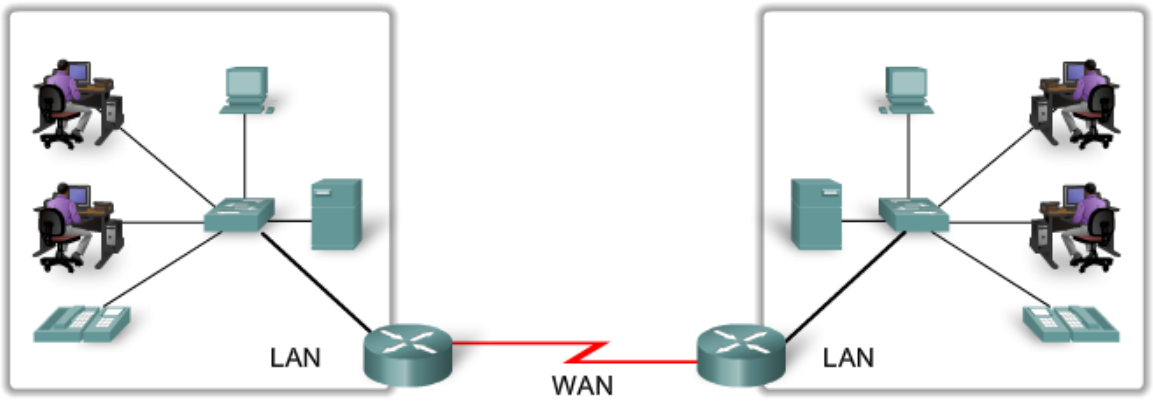


Figura 8
Enlace WAN
Fuente: http://cisco.netacad.net

2.10. CONFIGURACIÓN DE CONTRASEÑAS Y USO DE MENSAJES

La limitación física del acceso a los dispositivos de red con armarios o bastidores con llave resulta una buena práctica; sin embargo, las contraseñas son la principal defensa contra el acceso no autorizado a los dispositivos de red. Cada dispositivo debe tener contraseñas configuradas a nivel local para limitar el acceso. En un curso futuro, analizaremos cómo reforzar la seguridad al exigir una ID de usuario junto con una contraseña. Por ahora, presentaremos precauciones de seguridad básicas mediante el uso de contraseñas únicamente.

Como se comentó anteriormente, el IOS usa modos jerárquicos para colaborar con la seguridad del dispositivo. Como parte de este cumplimiento de seguridad, el IOS puede aceptar diversas contraseñas para permitir diferentes privilegios de acceso al dispositivo.

Las contraseñas ingresadas son:

• Contraseña de consola: limita el acceso de los dispositivos mediante la conexión de consola.

• Contraseña de enable: limita el acceso al modo EXEC privilegiado.

• Contraseña enable secret: encriptada, limita el acceso del modo EXEC privilegiado.

• Contraseña de VTY: limita el acceso de los dispositivos que utilizan Telnet.

Siempre conviene utilizar contraseñas de autenticación diferentes para cada uno de estos niveles de acceso. Si bien no es práctico iniciar sesión con varias contraseñas diferentes, es una precaución necesaria para proteger adecuadamente la infraestructura de la red ante accesos no autorizados.

Además, utilice contraseñas seguras que no se descubran fácilmente. El uso de contraseñas simples o fáciles de adivinar continúa siendo un problema de seguridad en muchas facetas del mundo empresarial.

Considere estos puntos clave cuando elija contraseñas:

• Use contraseñas que tengan más de 8 caracteres.

• Use en las contraseñas una combinación de secuencias de letras mayúsculas y minúsculas o numéricas.

• Evite el uso de la misma contraseña para todos los dispositivos.

• Evite el uso de palabras comunes como contraseña o administrador, porque se descubren fácilmente.

Nota: En la mayoría de las prácticas de laboratorio, usaremos contraseñas simples como cisco o clase. Estas contraseñas se consideran simples y fáciles de adivinar, y deben evitarse en un entorno de producción. Sólo usamos estas contraseñas por comodidad en el entorno instructivo.

Como se muestra en la figura, cuando se le solicita una contraseña, el dispositivo no repetirá la contraseña mientras se ingresa. En otras palabras, los caracteres de la contraseña no aparecerán cuando el usuario los ingrese. Esto se hace por cuestiones de seguridad; muchas contraseñas se obtienen por ojos espías.

2.10.1. CONTRASEÑA DE CONSOLA

El puerto de consola de un dispositivo Cisco IOS tiene privilegios especiales. El puerto de consola de dispositivos de red debe estar asegurado, como mínimo, mediante el pedido de una contraseña segura al usuario. Así se reducen las posibilidades de que personal no autorizado conecte físicamente un cable al dispositivo y obtenga acceso a éste.

Los siguientes comandos se usan en el modo de configuración global para establecer una contraseña para la línea de consola:

Switch(config)#line console 0

Switch(config□line)#password password

Switch(config□line)#login

Desde el modo de configuración global, se usa el comando line console 0 para ingresar al modo de configuración de línea para la consola. El cero se utiliza para representar la primera (y, en la mayoría de los casos, la única) interfaz de consola para un router.

El segundo comando, password especifica una contraseña en una línea.

El comando login configura al router para que pida la autenticación al iniciar sesión. Cuando el login está habilitado y se ha configurado una contraseña, habrá una petición de entrada de una contraseña.

Una vez que se han ejecutado estos tres comandos, aparecerá una petición de entrada de contraseña cada vez que un usuario intente obtener acceso al puerto de consola.

2.10.2. CONTRASEÑA DE ENABLE Y CONTRASEÑA ENABLE SECRET

Para proporcionar una mayor seguridad, se utiliza el comando enable password o el comando enable secret. Puede usarse cualquiera de estos comandos para establecer la autenticación antes de acceder al modo EXEC privilegiado (enable).

Si es posible, debe usarse siempre el comando enable secret, no el comando anterior enable password. El comando enable secret provee mayor seguridad porque la contraseña está encriptada. El comando enable password puede usarse sólo si enable secret no se ha configurado aún.

El comando enable password se ejecutaría si el dispositivo usa una versión anterior del software IOS de Cisco que no reconoce el comando enable secret.

Los siguientes comandos se utilizan para configurar las contraseñas:

Router(config)#enable password contraseña

Router(config)#enable secret contraseña

Nota: Si no se configura una contraseña enable password o enable secret, IOS impide el acceso EXEC privilegiado desde una sesión Telnet.

Si no se ha establecido una contraseña de enable, podría aparecer una sesión Telnet de esta forma:

Switch>enable

% No se ha establecido contraseña

Switch>

2.10.3. CONTRASEÑA DE VTY

Las líneas vty permiten el acceso a un router a través de Telnet. En forma predeterminada, muchos dispositivos Cisco admiten cinco líneas VTY con numeración del 0 al 4. Es necesario configurar una contraseña para todas las líneas vty disponibles. Puede configurarse la misma contraseña para todas las

conexiones. Sin embargo, con frecuencia conviene configurar una única contraseña para una línea a fin de proveer un recurso secundario para el ingreso administrativo al dispositivo si las demás conexiones están en uso.

Los siguientes comandos se usan para configurar una contraseña en líneas vty:

Router(config)#line vty 0 4

Router(config□line)#password contraseña

Router(config□line)#login

Por defecto, el IOS incluye el comando login en las líneas VTY. Esto impide el acceso Telnet al dispositivo sin la previa solicitud de autenticación. Si por error, se configura el comando no login, que elimina el requisito de autenticación, personas no autorizadas podrían conectarse a la línea a través de Telnet. Esto representaría un gran riesgo de seguridad.

CAPITULO III

3. MARCO PRÁCTICO

3.1. ESTADO DE LA RED DE TIGO EN EL ALTO

La sucursal de TIGO en la ciudad de El Alto, se encuentra ubicada en la avenida 6 de Marzo, entre calles 3 y 4, esta sucursal se enlaza con la Sucursal principal de HANSA, la sucursal de Calacoto, la Planta Alpacoma y HANSA SWITCH; sin embargo, el servidor principal donde se encuentran todos los programas con los que interactúa se encuentran en la sucursal principal de HANSA.

Los programas que se utilizan en la sucursal de TIGO en El Alto son habilitados en correspondencia con los usuarios, es decir que existen ciertas ventajas y características que son habilitadas únicamente para las áreas que involucren su función correspondiente.

La mayoría de las aéreas manejan la “BSC_LPZ 20” y “BSC_LPZ 30”, estos programas poseen un Backup en caso de actualizaciones o algún otro percance, las cuales son reemplazadas por la “BSC_SCZ 22” y la “BSC_SCZ 32” respectivamente. La diferencia entre estas es sencilla, ya que la BSC_LPZ 30 y la BSC_SCZ 32 son utilizadas exclusivamente para los cajeros, mientras que la BSC_LPZ 20 y la BSC_SCZ 22 son utilizadas por Servicio de Atención al Cliente, Logística y todas las aéreas involucradas con Ventas.

En ninguna de las áreas mencionadas se utiliza del mismo modo, es decir:

El área de Ventas lo utiliza primordialmente para el registro de nuevos usuarios, la habilitación de nuevos chips, tanto en 2G y 3G, también es utilizado allí para rehabilitar los números que no han sido utilizados y fueron caducados por el sistema.

Logística lo utiliza para el registro, control y despacho de suministros, material de oficina y el ingreso de equipos móviles, tanto en 2G y 3G.

Servicio de Atención al Cliente tiene la particularidad de incluir todas las funciones y beneficios del área de ventas, incluyendo en esta el detalle de llamadas, extracto de la cuenta, habilitación y cierre de paquetes y/o promociones.

Como se desarrollo anteriormente cada área trabaja con características muy particulares que evidencian su importancia en el trabajo cotidiano de la sucursal.

3.2. CONTRASEÑAS DE USUARIOS

La red de cualquiera de las sucursales de la empresa de Telecomunicaciones TIGO proporciona un grado de seguridad en base a las contraseñas por usuario, estas contraseñas se encuentran almacenadas en el servidor principal, la creación de las mismas se encuentra basada en el primer apellido y la inicial de su primer nombre, por ejemplo: el nombre de usuario de José Pérez seria "perezj"; de forma similar se genera el nombre de correo electrónico, en este caso sería: perezj@tigo.net.bo.

Estos usuarios tienen los permisos adecuados para sus labores al momento de ingresar a algún programa. Estos datos son ingresados al inicio de sesión de cada computadora y al momento de ingresar a cualquiera de los programas.

3.3. ESTADO ACTUAL DE LA RED

El estado actual de la red se encuentra distribuido en cuatro Plantas, que conllevan nueve Aéreas de Trabajo, las cuales se describen según el siguiente detalle y se encuentran graficadas en Anexos.

Servicio de Atención al Cliente (SAC)

6 pts. (Planta 1)

7 pts. (Planta 2)

3 pts. Impresoras (Planta 1 y 2)

1 pts. Servidor (Planta 1)

1 pts. Ticket (Planta 1)

1 pts. Servicio Técnico SAC (Planta 1)

Logística

2 pts. (Planta 1) con Impresora USB

1 pts. Impresora

Cajas

2pts. (Planta 1) con Impresoras USB

Ventas Prepago

4 pts. (Planta 4 y 2)

Ventas Banda Ancha

4 pts. (Planta 4 y 2)

Ventas Postpago

2 pts. (Planta 4 y 2)

Ventas Indirectas

2 pts. (Planta 4 y 2)

2 pts. Impresoras

Sistemas

3 pts. (Planta 3)

Distribución

4 pts. (Planta 3) con impresoras USB

Registro Biométrico

1 pts. (Planta 1)

Seguridad Policía

1 pts. (Planta 1)

Todas estas hacen un total de 47 puntos de Red y conformarían según un total de siete Áreas de Trabajo independiente, las mismas que estarían distribuidas en las cuatro plantas mencionadas.

3.4. DISTRIBUCIÓN Y DISEÑO DE SUBRREDES

Según el detalle anteriormente mencionado, se realizará la distribución de Direcciones IP en el proceso de elaboración de Subredes. Se debe tomar en cuenta que los detalles respecto a cada una de las Plantas con las que se conforma la sucursal se muestran detalladamente en los Anexos.

La dirección de red matriz con la que se procederá al subneteo es la 172.30.106.0/24, con esta realizaremos la distribución de direcciones IP para cada una de las Subredes.

Para SAC:

Con la Dirección: 172.30.106.0/24 tomando 3 bits para la parte de Red, con lo que conseguimos 8 Dir. de Subred, cada una con 30 Host. Las Direcciones obtenidas son:

172.30.106.0 /27

172.30.106.32 /27

172.30.106.64 /27

172.30.106.96 /27

172.30.106.128 /27

172.30.106.160 /27

172.30.106.192 /27

172.30.106.224 /27

Utilizaremos la 172.30.106.0 /27

Para Ventas:

Con la Dirección: 172.30.106.32 /27 tomando 1 bit adicional a los 3 bits anteriores para la parte de Red, con lo que conseguimos 2 Dir. de Subred, cada una con 14 Host. Las Direcciones obtenidas son:

172.30.106.32 /28

172.30.106.48 /28

Utilizaremos la 172.30.106.32 /28

Para Distribución:

Con la Dirección: 172.30.106.48 /28 tomando 1 bit adicional a los 4 bits anteriores para la parte de Red, con lo que conseguimos 2 Dir. de Subred, cada una con 6 Host. Las Direcciones obtenidas son:

172.30.106.48 /29

172.30.106.56 /29

Utilizaremos la 172.30.106.48 /29

Para Logística:

Utilizaremos la 172.30.106.56 /29

Para Sistemas:

Con la Dirección: 172.30.106.64 /27 tomando 2 bits adicionales a los 3 bits anteriores para la parte de Red, con lo que conseguimos 4 Dir. de Subred, cada una con 6 Host. Las Direcciones obtenidas son:

172.30.106.64 /29

172.30.106.72 /29

172.30.106.80 /29

172.30.106.88 /29

Utilizaremos la 172.30.106.64 /29

Para Cajas:

Utilizaremos la 172.30.106.72 /29

Para el Registro Biométrico y Seguridad Policía:

Con la Dirección: 172.30.106.80 /29 tomando 1 bits adicionales a los 5 bits anteriores para la parte de Red, con lo que conseguimos 2 Dir. de Subred, cada una con 2 Host. Las Direcciones obtenidas son:

172.30.106.80 /30

172.30.106.84 /30

Utilizaremos la 172.30.106.80 /30

Para Seguridad Policía:

Utilizaremos la 172.30.106.84 /30

3.5. CONFIGURACIÓN EN CADA DISPOSITIVO

3.5.1 ROUTER 0

En la configuración realizada se establecieron las contraseñas de consola, contraseña encriptada, establecimiento de direcciones IP y configuración para las redes Virtuales, el detalle de los mismos es el siguiente:

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RC
RC#conf t
Router(config)#line console 0
Router(config-line)#password r0e
Router(config-line)#login
Router(config)#enable secret tigoed
RC(config)#int fa0/0
RC(config-if)#no ip address
RC(config-if)#no shut
RC(config-if)#int fa0/0.1
RC(config-subif)#encapsulation dot1Q 10
RC(config-subif)#ip address 172.30.106.1 255.255.255.224
RC(config-subif)#int f0/0.2
RC(config-subif)#encapsulation dot1q 20
RC(config-subif)#ip address 172.30.106.33 255.255.255.240
RC(config-subif)#int f0/0.3
RC(config-subif)#encapsulation dot1q 30
RC(config-subif)#ip address 172.30.106.49 255.255.255.248
Router(config)#interface Serial0/0/0
```

Router(config-if)# ip address 172.30.101.81 255.255.255.252

Router(config-if)# clock rate 64000

Router(config)# ip route 172.30.107.0 255.255.255.0 Serial0/0/0

3.5.2. SWITCH 0

En este switch se realizo la configuración de las contraseñas de administración, del enlace troncal y la creación de las VLANs correspondientes

Switch>en

Switch#conf t

Switch(config)#interface FastEthernet0/1

Switch(config-if)# switchport mode trunk

Switch(config)#hostname SW0

SW0(config)#enable secret tigoed

SW0(config)#line console 0

SW0(config-line)#password sw0e

SW0(config-line)#login

SW0(config)#vlan 10

SW0(config-vlan)#name VLAN1

SW0(config-vlan)#vlan 20

SW0(config-vlan)#name VLAN2

SW0(config-vlan)#vlan 30

SW0(config-vlan)#name VLAN3

SW0(config-vlan)#vlan 40

SW0(config-vlan)#name VLAN4

SW0(config-vlan)#vlan 50

SW0(config-vlan)#name VLAN5

SW0(config-vlan)#vlan 60

SW0(config-vlan)#name VLAN6

SW0(config-vlan)#vlan 70

SW0(config-vlan)#name VLAN7

SW0(config)#vlan 99

SW0(config-vlan)#name NATIVA

3.5.3. SWITCH 1

En este switch se realizó la configuración de las contraseñas de administración, del enlace troncal y la creación de las VLANs correspondientes.

Switch>en

Switch#conf t

Switch(config)#interface FastEthernet0/1

Switch(config-if)# switchport mode trunk

Switch(config)#hostname SW1

SW1(config)#enable secret tigoed

SW1(config)#line console 0

SW1(config-line)#password sw1e

SW1(config-line)#login

SW1(config)#vlan 10

SW1(config-vlan)#name VLAN1

SW1(config-vlan)#vlan 20

SW1(config-vlan)#name VLAN2

SW1(config-vlan)#vlan 30

SW1(config-vlan)#name VLAN3

SW1(config-vlan)#vlan 40

SW1(config-vlan)#name VLAN4

SW1(config-vlan)#vlan 50

SW1(config-vlan)#name VLAN5

SW1(config-vlan)#vlan 60

SW(config-vlan)#name VLAN6

SW1(config-vlan)#vlan 70

SW1(config-vlan)#name VLAN7

SW1(config)#vlan 99

SW1(config-vlan)#name NATIVA

SW1(config)#interface FastEthernet0/1

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 10

SW1(config)#interface FastEthernet0/2

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 10

SW1(config)#interface FastEthernet0/3

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 10

SW1(config)#interface FastEthernet0/4

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 10

SW1(config)#interface FastEthernet0/5

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 10

SW1(config)#interface FastEthernet0/6

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 10

SW1(config)#interface FastEthernet0/7

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 10

SW1(config)#interface FastEthernet0/8

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 10

SW1(config)#interface FastEthernet0/9

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 10

SW1(config)#interface FastEthernet0/10

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 10

SW1(config)#interface FastEthernet0/11

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 20

SW1(config)#interface FastEthernet0/12

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 20

SW1(config)#interface FastEthernet0/13

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 20

SW1(config)#interface FastEthernet0/14

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 20

SW1(config)#interface FastEthernet0/15

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 20

SW1(config)#interface FastEthernet0/16

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 20

SW1(config)#interface FastEthernet0/17

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 20

SW1(config)#interface FastEthernet0/18

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 20

SW1(config)#interface FastEthernet0/19

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 20

SW1(config)#interface FastEthernet0/20

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 20

SW1(config)#interface FastEthernet0/21

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 20

SW1(config)#interface FastEthernet0/22

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 23

SW1(config)#interface FastEthernet0/20

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 20

SW1(config)#interface FastEthernet0/20

SW1(config-if)# switchport mode trunk

SW1(config-if)# switchport trunk native 99

3.5.4. SWITCH 2

En este switch se realizo la configuración de las contraseñas de administración, del enlace troncal y la creación de las VLANs correspondientes.

```
Switch>en
Switch#conf t
Switch(config)#hostname SW2
SW2(config)#enable secret tigoed
SW2(config)#line console 0
SW2(config-line)#password sw1e
SW2(config-line)#login
SW2(config)#vlan 10
SW2(config-vlan)#name VLAN1
SW2(config-vlan)#vlan 20
SW2(config-vlan)#name VLAN2
SW2(config-vlan)#vlan 30
SW2(config-vlan)#name VLAN3
SW2(config-vlan)#vlan 40
SW2(config-vlan)#name VLAN4
SW2(config-vlan)#vlan 50
SW2(config-vlan)#name VLAN5
SW2(config-vlan)#vlan 60
SW2(config-vlan)#name VLAN6
SW2(config-vlan)#vlan 70
SW2(config-vlan)#name VLAN7
SW2(config)#vlan 99
SW2(config-vlan)#name NATIVA
SW2(config)#interface FastEthernet0/1
```

SW2(config-if)# switchport mode access

SW2(config-if)# switchport access vlan 10

SW2(config)#interface FastEthernet0/2

SW2(config-if)# switchport mode access

SW2(config-if)# switchport access vlan 10

SW2(config)#interface FastEthernet0/3

SW2(config-if)# switchport mode access

SW2(config-if)# switchport access vlan 10

SW2(config)#interface FastEthernet0/4

SW2(config-if)# switchport mode access

SW2(config-if)# switchport access vlan 10

SW2(config)#interface FastEthernet0/5

SW2(config-if)# switchport mode access

SW2(config-if)# switchport access vlan 10

SW2(config)#interface FastEthernet0/6

SW2(config-if)# switchport mode access

SW2(config-if)# switchport access vlan 10

SW2(config)#interface FastEthernet0/7

SW2(config-if)# switchport mode access

SW2(config-if)# switchport access vlan 10

SW2(config)#interface FastEthernet0/8

SW2(config-if)# switchport mode access

SW2(config-if)# switchport access vlan 10

SW2(config)#interface FastEthernet0/9

SW2(config-if)# switchport mode access

SW2(config-if)# switchport access vlan 10

SW2(config)#interface FastEthernet0/10

SW2(config-if)# switchport mode access

SW2(config-if)# switchport access vlan 30

SW2(config)#interface FastEthernet0/11

SW2(config-if)# switchport mode access

SW2(config-if)# switchport access vlan 30

SW2(config)#interface FastEthernet0/12

SW2(config-if)# switchport mode access

SW2(config-if)# switchport access vlan 30

SW2(config)#interface FastEthernet0/13

SW2(config-if)# switchport mode access

SW2(config-if)# switchport access vlan 30

SW2(config)#interface FastEthernet0/14

SW2(config-if)# switchport mode access

SW2(config-if)# switchport access vlan 40

SW2(config)#interface FastEthernet0/15

SW2(config-if)# switchport mode access

SW2(config-if)# switchport access vlan 40

SW2(config)#interface FastEthernet0/16

SW2(config-if)# switchport mode access

SW2(config-if)# switchport access vlan 40

El diagrama final de la Red Virtual es el siguiente:

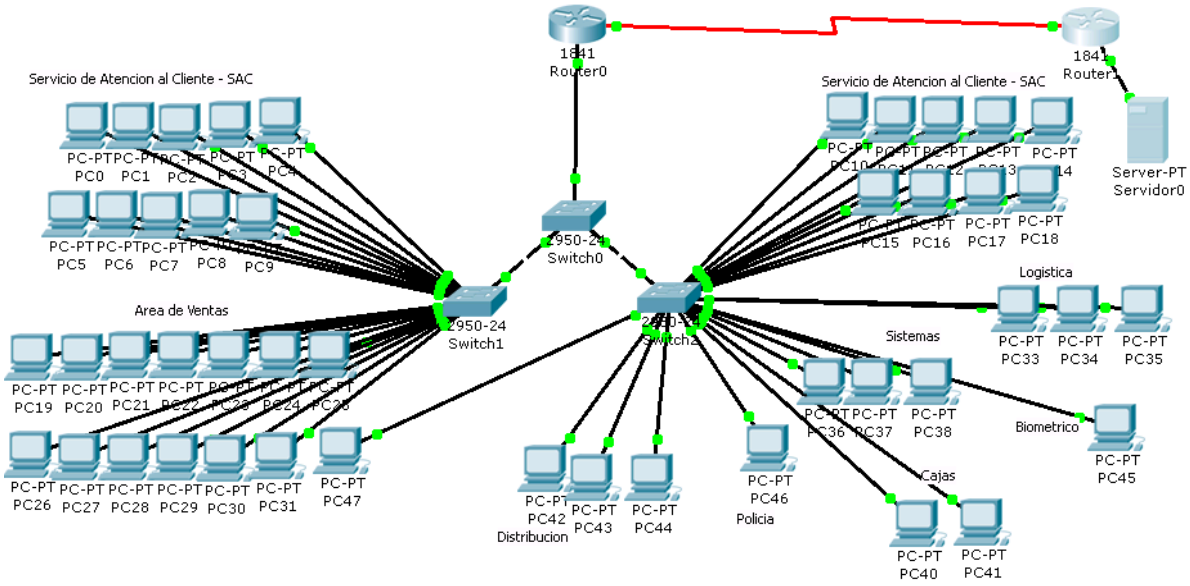


Figura 9
Enlace WAN

Fuente: Diseño en PacketTracer

CAPITULO IV

4.1. CONCLUSIONES

Finalizando con el presente proyecto solo se tendría que coordinar con el actual encargado de Sistemas para saber si existen algunos otros aspectos que no se tomaron en cuenta, como ser los planes de ampliaciones de aéreas y/o reordenamiento de ciertos puntos a otros lugares de los ambientes de la Sucursal.

Es necesario tomar en cuenta que los datos realizados en este proyecto solo abarcan la configuración del Router de salida, ya que el router donde se encuentra el servidor se configura con parámetros adicionales de los cuales no se posee información suficiente para abarcar dicho dispositivo.

También es necesario que sean informadas las sucursales de la regional de Santa Cruz, oficina principal de HANSA,HANSA Switch y la Planta Alpacoma, ya que son con estas las Sucursales con las que se interactúa constantemente, y no se realicen ningún tipo de dificultades al querer compartir y/o solicitar soporte en las mismas.

4.2.1 . BIBLIOGRAFÍA Y PÁGINAS WEB:

✓ Forouzan, Behrouz A. (2002). “Transmisión de datos y redes de comunicación”. (Segunda Edición). Madrid:McGraw-Hill.

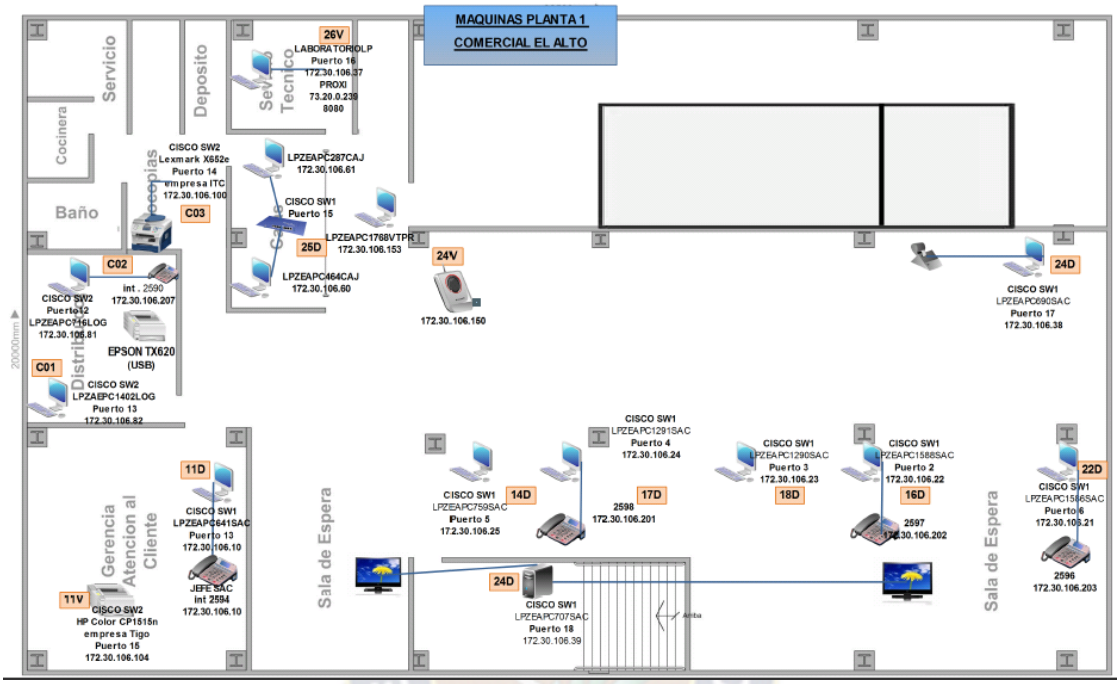
✓ TANENBAUM, Andrew S. (2003). “Redes de Computadoras”. (Cuarta Edición). Madrid: McGraw-Hill.

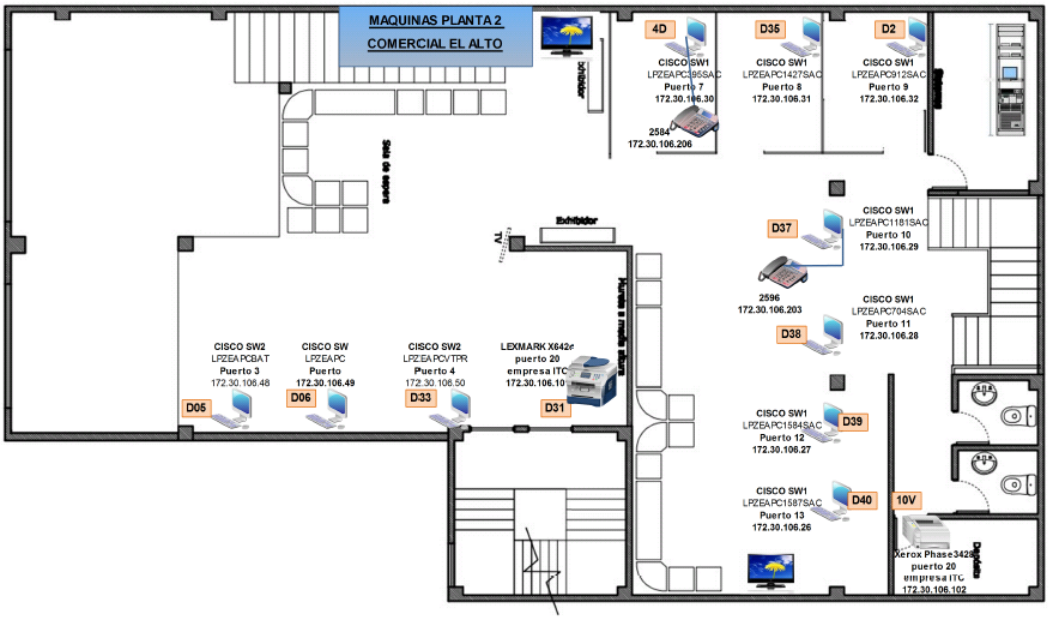
✓ CISCO CCNA EXPLORATION 1 “Aspectos básicos de Networking” Fuente: http://cisco.netacad.net

✓ CISCO CCNA EXPLORATION 3 “VLANs” Fuente: http://cisco.netacad.net

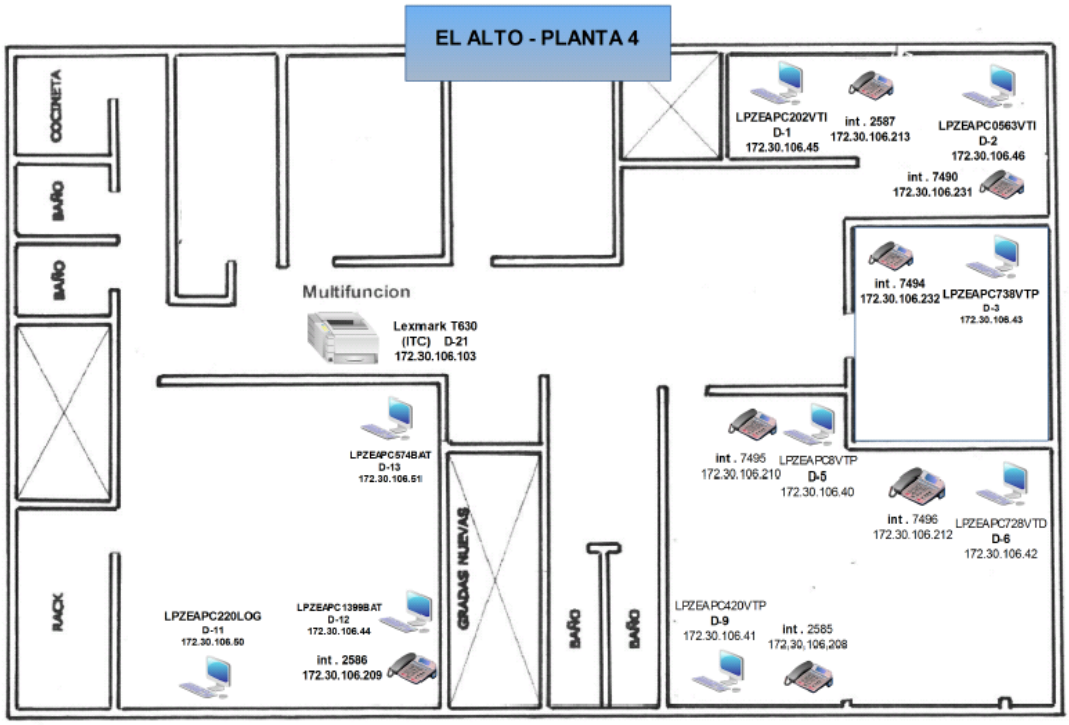
ANEXOS

PLANOS DE CADA UNA DE LA PLANTAS DE LA SUCURSAL DE TIGO:






MAQUINAS PLANTA 3
COMERCIAL EL ALTO
SW
LPZEAPC1398DIS
Puerto
172.30.106.65
int . 7477
172.30.106.230
CISCO SW2
LPZEAPC1177DIS
Puerto 7
172.30.106.66
09B
09A
CISCO SW2
Puerto 8
CP1515n
172.30.106.105
SW
LPZEAP841CDIS
Puerto
172.30.106.71
int . 2583
172.30.106.205
CISCO SW
LPZEAPC594DIS
Puerto
172.30.106.69
07A
Of. VENTAS POST PAGO
05A
03A
01A
Of. VENTAS BANDA ANCHA
Of. VENTAS INDIRECTAS
05B
SALA DESCANSO
14B
10A
07B
SALA DE CAPACITACION
Of. GERENCIA
CISCO SW2
LPZALPPC1441ot
Puerto 19,20
172.30.106.175
02B
02A
Of. SISTEMAS
15A
04A
CISCO SW2
LPZEAPC398it
Puerto 18
172.30.106.170


EL ALTO - PLANTA 4
COCINETA
BAÑO
BAÑO
Multifuncion
Lexmark T630
(ITC) D-21
172.30.106.103
LPZEAPC202VTI
D-1
172.30.106.45
int . 2587
172.30.106.213
LPZEAPC0563VTI
D-2
172.30.106.46
int . 7490
172.30.106.231
int . 7494
172.30.106.232
LPZEAPC738VTP
D-3
172.30.106.43
LPZEAPC574BAT
D-13
172.30.106.51
int . 7495
172.30.106.210
LPZEAPC8VTP
D-5
172.30.106.40
int . 7496
172.30.106.212
LPZEAPC728VTD
D-6
172.30.106.42
RACK
LPZEAPC220LOG
D-11
172.30.106.50
LPZEAPC1399BAT
D-12
172.30.106.44
int . 2586
172.30.106.209
GRADAS NUEVAS
BAÑO
BAÑO
LPZEAPC420VTP
D-9
172.30.106.41
int . 2585
172,30,106,208

UNIVERSITAS MAJOR PACENSIS DIVI ANDRE Æ