ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

IMPLEMENTACIÓN DE VLANS EN LA RED DE TELCONET PARA UNA INTERCONEXIÓN SEGURA ENTRE LAS AGENCIAS Y LA MATRIZ DE UNA INSTITUCIÓN BANCARIA

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO EN INGENIERIA INFORMATICA
MENCIÓN REDES DE INFORMACION

MILTON SANTIAGO TIPÁN LEMA

DIRECTOR: ING. DANIEL MANANGÓN

Quito, Octubre 2005

DECLARACIÓN

Yo, Milton Santiago Tipán Lema, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Milton Santiago Tipán Lema

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el Sr. Milton Santiago Tipán Lema, bajo mi supervisión.

Ing. Daniel Manangón

DIRECTOR DE PROYECTO

AGRADECIMIENTOS

Son muchos los amigos y profesionales que de forma directa o indirecta contribuyeron a la realización de este trabajo, no podría nombrar a todos de forma particular pero si quiero recalcar que cada uno de ellos con cada palabra de aliento y de sabiduría estuvieron fortaleciendo mis sentidos para poder llevar a cabo esta tesis.

Quiero agradecer de manera especial a una persona, que llenó mi espíritu y me ayudo a la realización de esta tesis, mi hermano Luis Guillermo, que siempre a estado pendiente de todas mis actividades en el transcurso de mi vida, en las buenas y en las malas, y ahora no pudo ser la excepción, a él mi mas sincero agradecimiento.

También agradezco la colaboración de Telconet y todo su personal técnico, que más de ser compañeros de trabajo han sido todos como una verdadera familia, siempre apoyándose y fortaleciéndose los unos a los otros.

Agradezco infinitamente a Dios por haberme permitido llegar al final de esta meta, puesto que él con sus bendiciones diarias han guiado cada paso de mi vida.

DEDICATORIA

Dedico esta tesis a mi familia, a mis padres Guillermo y Mariana, a mis hermanos Alexandra, Edgar y Luis, y las lucecitas de mis ojos, mis sobrinitos Carlitos Andrés, Jessica Brigitte y Lisbeth Estefanía.

Más importante que todo, dedico esta tesis a Dios, por las bondades recibidas y por el regalo de la vida, ya que sin él nada es posible y con él nada es imposible.

CONTENIDO

CAPITULO 3.

DISEÑO DE LA RED BANCARIA

CAPITULO 4.

IMPLEMENTACIÓN DE LA RED BANCARIA

CAPITULO 5.

CONCLUSIONES Y RECOMENDACIONES

INDICE DE TABLAS

INDICE DE GRAFICOS

RESUMEN

Telconet, es una empresa dedicada a comercializar los servicios principalmente de Internet y de transmisión de datos entre otros, por lo que brinda soluciones para diferentes empresas de diferente índole.

Se presenta la necesidad de transmisión de datos por parte de una Institución Bancaria, que es interconectar las agencias con la matriz para realizar sus transacciones, esto implica necesariamente por la naturaleza financiera de la institución, que la transmisión de datos sea segura y confiable.

Telconet asume la necesidad y presenta una alternativa basada en VLANS, esta solución cubre las necesidades del banco tanto en el aspecto funcional como en el aspecto relacionado a los costos, ya que el valor de los enlaces dedicados provistos por Telconet a la Institución Bancaria están acorde al mercado actual de las comunicaciones.

Se resume a continuación un breve esquema sobre los capítulos incorporados en el presente trabajo:

Capitulo 1. Las redes virtuales VLANS

Las VLANS son agrupaciones de red, que tienen su propio dominio de broadcast, esto indica que solo los equipos que pertenecen a una VLAN determinada podrán compartir información.

La ventaja de tener VLANS en una red es principalmente para dividir segmentos de red de forma lógica y administrado remotamente, con lo que se puede tener varias redes lógicas sobre una misma red física. El hecho de poder administrar varias VLANS incluye que se administra seguridad en la red.

Para poder formar las VLANS es necesario tener equipos switches que permitan realizar estas configuraciones, actualmente en el mercado hay muchas soluciones que permiten realizar VLANS. El estándar para la creación de una VLAN es IEEE 802.1Q.

Capitulo 2. Infraestructura actual de Telconet.

Telconet es una empresa dedicada a comercializar servicios de comunicaciones de datos, Internet, etc., por lo que cada vez es necesario obtener tecnología de punta para brindar las mejores soluciones a las necesidades de sus clientes.

Cuenta principalmente con un Backbone MEN (Metro Ethernet Network), formado con switches cisco catalyst 3550, es como una LAN gigante, sobre la misma se encuentran incorporados todos sus clientes.

Tiene dos tipos principales de enlaces, de fibra óptica, con fibra monomodo tendida sobre varios sectores de la ciudad de Quito, y enlaces de radio, por

medio de la tecnología Wireless, con la que soporta enlaces internos de la ciudad y en las afueras de la misma, por la complejidad de llegar con enlaces de fibra debido a su ubicación geográfica.

Capitulo 3. Diseño de la red bancaria.

En el diseño de la red bancaria se indican los equipos que serán necesarios incorporar al backbone de Telconet para poder brindar los enlaces a la institución bancaria, esto amerita la compra de dos dispositivos cisco catalyst 3550, que serán incorporados en lugares estratégicos para ofrecer la comunicación al banco y también para ampliar la red y abarcar mas sectores.

Se indican los dispositivos necesarios para poder diseñar la red bancaria de manera física, y se muestran los mapas para la distribución de los dispositivos de forma lógica, esto es direcciones IP, identificadores asignados para las VLANS, etc., indicando la forma en la que se formará y funcionará la red bancaria.

Capitulo 4. Implementación de la red bancaria.

La implementación se refiere a la forma en la que se realizarán los enlaces de última milla, por medio de fibra óptica, en la parte física, y el la parte lógica se indican las configuraciones de los dispositivos para formar las VLANS a nivel de capa 2 y la configuración de las redes y rutas para alcanzar las agencias bancarias desde la matriz, esto a nivel de capa 3.

Se realizan las pruebas de conexión desde la matriz bancaria (Servidor VLAN) hacia cada una de las agencias, tomando en cuenta los tiempos de respuesta, perdidas y duplicados al enviar paquetes icmp.

También se indica a cerca de dos formas de monitoreo una vez que se levantan los enlaces, esto es utilizando software específico, como WhatsUP para el monitoreo en forma real, con el que se puede sacar reportes de uptime y; MRTG con el que se obtiene estadísticas del tráfico de cada puerto de los switches catalyst por donde depende cada localidad bancaria.

Capitulo 5. Conclusiones y Recomendaciones.

Se concluye de forma general que la seguridad de la red bancaria formada por VLANS y controlada el acceso por medio de direcciones MAC es segura, siempre que la administración de la misma sea realizada por personal técnico capacitado y de confianza tanto en Telconet como el la institución bancaria.

Se recomienda realizar el monitoreo con las alarmas que sean necesarias configurar en WhatsUP para poder ofrecer al banco un soporte rápido, eficiente y oportuno, que haga que la red bancaria y el servicio prestado por Telconet sea confiable.

PRESENTACIÓN

Los sistemas de comunicación se han convertido en una necesidad imprescindible en cualquier área, principalmente de servicios, y mas aún en los sistemas de información es una forma de trabajo y de vida de muchas personas, ya sea que se involucren directa o indirectamente.

La transmisión de datos en los últimos años ha crecido de manera significativa con la aparición del Internet y los servicios que se pueden ofrecer sobre éste, pero también han crecido las necesidades de muchas empresas de realizar sus transmisiones de datos de forma segura ya que cada vez hay muchas maneras y formas de querer vulnerar las seguridades para causar fraudes o robos a través de la tecnología informática.

El presente trabajo presenta una solución para la transmisión de datos segura, por medio de la infraestructura de Telconet. Esta solución esta basada en VLANS, puesto que son adaptables a la infraestructura de Telconet y cubren las necesidades de la Institución Bancaria.

Esta tesis puede ser referenciada como un ejemplo de transmisión de información por medio de VLANS, los requerimientos de tecnología que se necesitan para implementarlas y la necesidad de tener varias redes lógicas sobre una misma red física.

Cabe señalar que garantizar la seguridad en la transmisión datos depende de forma primordial de las políticas de seguridad que estén establecidas tanto en Telconet como prestataria del servicio, así como en la Institución Bancaria, puesto que si no se tiene una buena administración de dichas políticas, no se podría brindar seguridades incluso con tecnologías de punta o con otro tipo de soluciones técnicas.

CAPITULO 1.

REDES VIRTUALES VLANS

1.1 INTRODUCCION

Hasta ahora, los grupos de trabajo en una red, han sido distribuidos por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo concentrador o hub.

Como consecuencia, estos grupos de trabajo comparten el ancho de banda disponible y los dominios de broadcast entre todos, y con la dificultad de gestión cuando se producen cambios en los miembros del grupo. Más aún, la limitación geográfica que supone que los miembros de un determinado grupo deben de estar situados adyacentemente, por su conexión al mismo concentrador o segmento de la red.

Los esquemas de comunicación por medio de VLAN (Virtual LAN o red virtual), proporcionan los medios adecuados para solucionar esta problemática, por medio de la agrupación realizada de una forma lógica en lugar de física. Sin embargo, las redes virtuales siguen compartiendo las características de los grupos de trabajo físicos, en el sentido de que todos los usuarios tienen conectividad entre ellos y comparten sus dominios de broadcast.

La principal diferencia con la agrupación física, como se mencionada, es que los usuarios de las redes virtuales pueden ser distribuidos a través de una red LAN, incluso situándose en diferentes concentradores de la misma, esto depende al grupo de VLAN que pertenezca. Los usuarios pueden, así, comunicarse a través de la red, manteniendo su pertenencia al grupo de trabajo lógico.

Por otro lado, al distribuir usuarios de un mismo grupo lógico a través de diferentes segmentos, se logra, como consecuencia directa, el incremento del ancho de banda en dicho grupo de usuarios.

También, al poder distribuir a los usuarios en diferentes segmentos de la red, se puede situar puentes y routers entre ellos, separando segmentos con diferentes topologías y protocolos. Por ejemplo, se puede mantener diferentes usuarios del mismo grupo, unos con FDDI y otros con Ethernet, en función tanto de las instalaciones existentes como del ancho de banda que cada uno precise, por su función específica dentro del grupo.

Todo lo mencionado, manteniendo la seguridad deseada en cada configuración por el administrador de la red: Se puede permitir o no que el tráfico de una VLAN que entre y salga desde/hacia otras redes.

Las redes virtuales permiten que la ubicuidad geográfica no se limite a diferentes concentradores o plantas de un mismo edificio, sino a diferentes oficinas intercomunicadas mediante redes WAN o MAN, a lo largo de países y continentes, sin limitación ninguna más que la impuesta por el administrador de dichas redes.

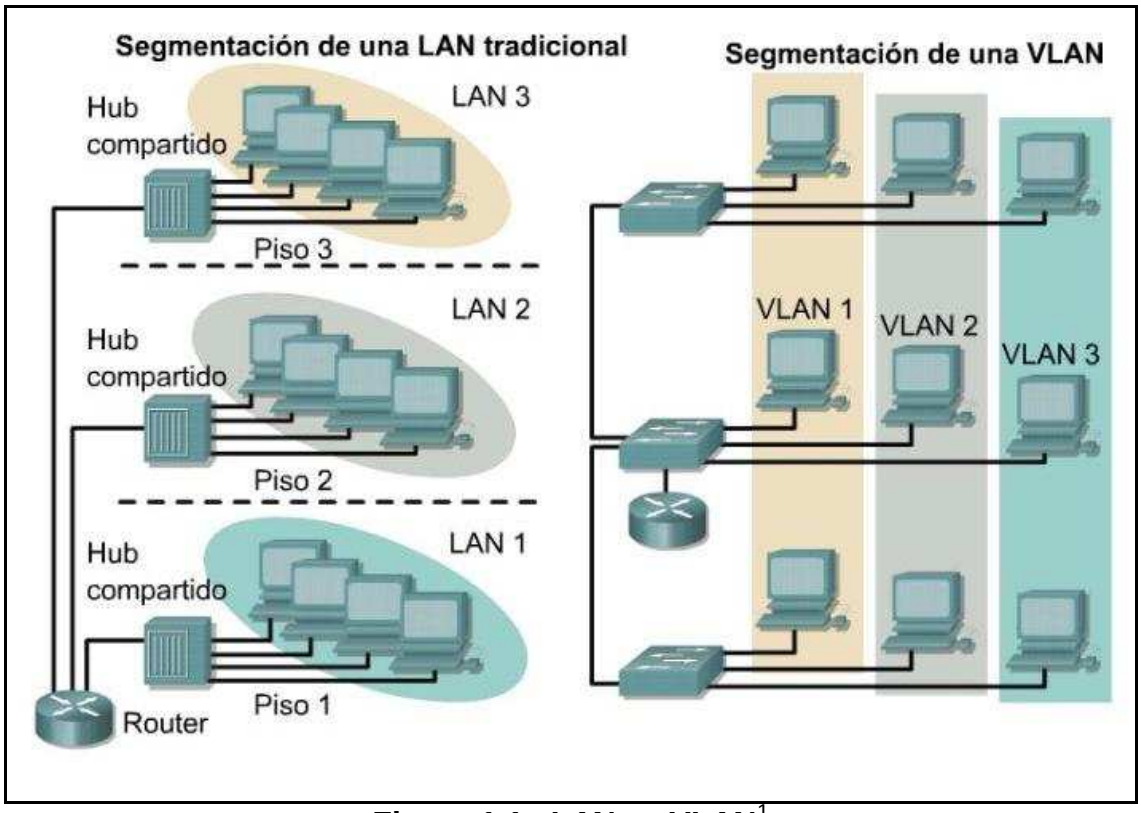


Figura 1.1 LAN y VLAN[1]

1.2 DEFINICIÓN DE 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[2].

[1] http://www.tlm.unavarra.es/asignaturas/aro/ccna3-8.ppt
[2] http://polaris.lcc.uma.es/~eat/services/rvirtual/rvirtual.html#link1

Figura 1.2 Ejemplo de VLAN[3]

Que hacen las redes virtuales (VLANS)?. 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

[3] http://www.tlm.unavarra.es/asignaturas/aro/ccna3-8.ppt

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[4].

Existen tres métodos principales de definición de pertenencia a VLAN:

- VLAN por puerto
- VLAN por dirección MAC
- VLAN por filtros

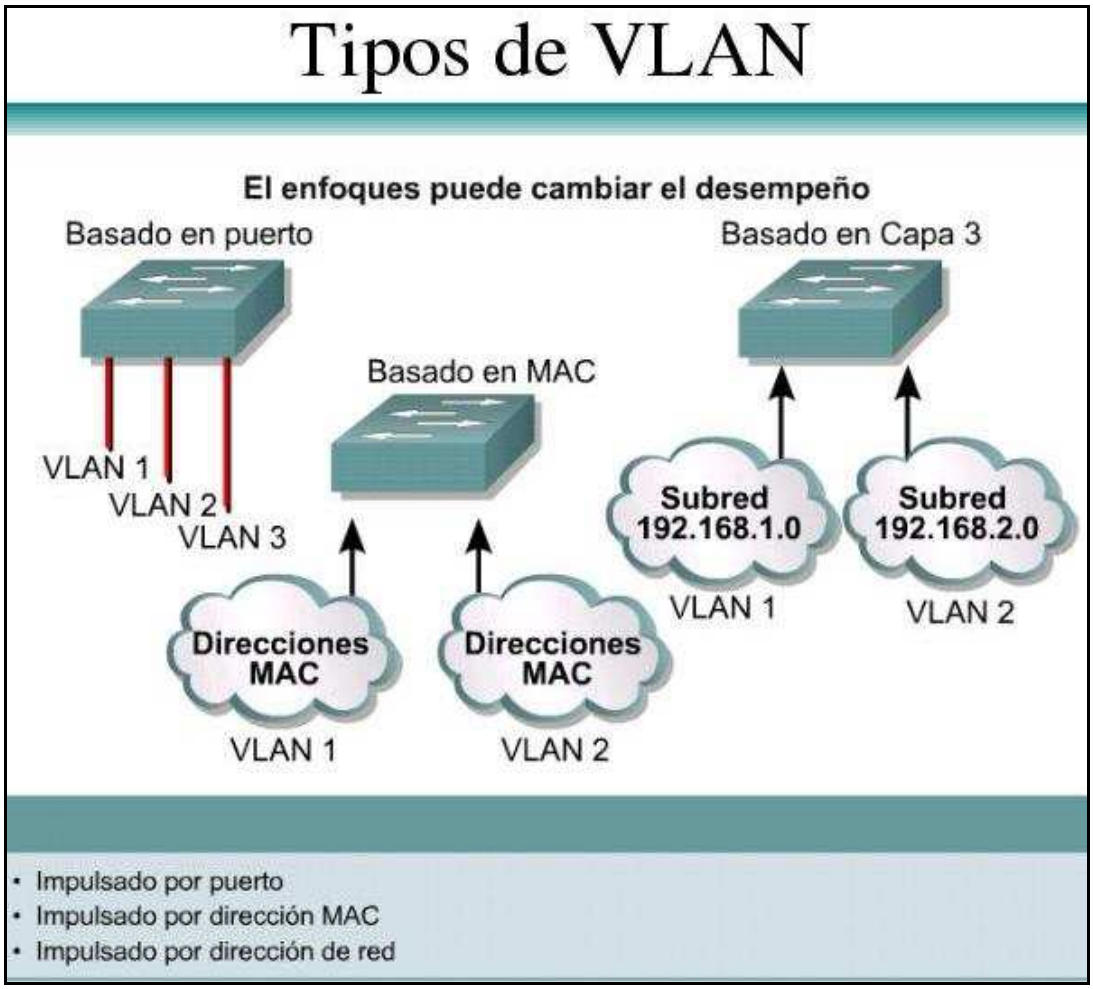


Figura 1.3 Tipos de VLAN[5]

[4] http://polaris.lcc.uma.es/~eat/services/rvirtual/rvirtual.html#link1
[5] http://www.tlm.unavarra.es/asignaturas/aro/ccna3-8.ppt

1.2.1 VLAN POR PUERTO

Cada puerto del conmutador puede asociarse a una VLAN.

Ventajas[6]:

Facilidad de movimientos y cambios.- un movimiento supone que la estación cambia de ubicación física pero sigue perteneciendo a la misma VLAN. Requiere reconfiguración del puerto al que se conecta la estación salvo si se utilizan técnicas de asignación dinámica a VLAN. Un cambio implica pertenencia a una nueva VLAN sin movimiento físico. El puerto del conmutador ha de configurarse como perteneciente a la nueva VLAN y la estación puede precisar reconfiguración (por ejemplo si se utiliza protocolo IP sin servidor DHCP). La reconfiguración de la estación no será necesaria si la subred (IP, IPX, etc) a la que pertenece esta totalmente contenida en la VLAN. Cualquier operación de añadir, mover o cambiar un usuario se traduce normalmente en la reconfiguración de un puerto y algunas aplicaciones gráficas de gestión de VLANs automatizan totalmente esta reasignación.

Microsegmentación y reducción del dominio de broadcast.- aunque los conmutadores permiten dividir la red en pequeños segmentos, el tráfico broadcast sigue afectando al rendimiento de las estaciones y se precisan routers o VLANs para aislar los dominios de broadcast. La definición de VLANs por puerto implica que el tráfico de broadcast de una VLAN no afecta a las estaciones en el resto de VLANs puesto que es siempre interno a la VLAN en la que se origina.

Multiprotocolo.- la definición de VLANs por puerto es totalmente independiente del protocolo o protocolos utilizados en las estaciones. No existen pues limitaciones para protocolos de uso poco común como VINES, OSI, etc. o protocolos dinámicos como DHCP.

[6] http://www.ibw.com.ni/~alanb/campus.html

Desventajas[7]:

Administración.- los movimientos y cambios implican normalmente una reasignación del puerto del conmutador a la VLAN a la que pertenece el usuario. Aunque las aplicaciones de gestión facilitan esta tarea es recomendable combinar dichas aplicaciones con mecanismos de asignación dinámica de VLAN de forma que se asignen los puertos a la VLAN en función de la dirección MAC o de otros criterios como la dirección de nivel 3. Cisco ha desarrollado un método de asignación dinámica de red VLAN a puerto basándose en las direcciones MAC de las estaciones de red.

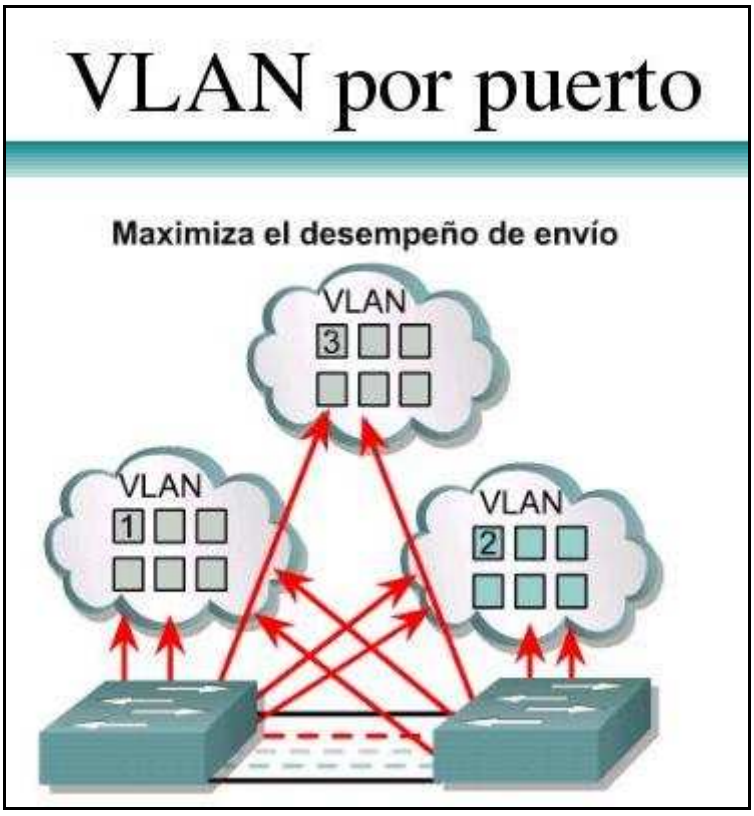


Figura 1.4 VLAN basadas en puertos[8]

[7] http://www.ibw.com.ni/~alanb/campus.html
[8] http://www.tlm.unavarra.es/asignaturas/aro/ccna3-8.ppt

1.2.2 VLAN DIRECCIÓN MAC

La relación de pertenencia a VLAN se basa en la dirección MAC.

Ventajas[9]:

Facilidad de movimientos.- las estaciones pueden moverse a cualquier ubicación física perteneciendo siempre en la misma VLAN sin que se necesite ninguna reconfiguración del conmutador.

Multiprotocolo.- no presenta ningún problema de compatibilidad con los diversos protocolos y soporta incluso la utilización de protocolos dinámicos tipo DHCP.

Desventajas[10]:

Problemas de rendimiento y control de broadcast.- éste método de definición de VLANs implica que en cada puerto del conmutador coexisten miembros de distintas VLANs (se evita el problema si se utilizan puertos dedicados a estaciones pues cada puerto pertenecerá a una única VLAN) por lo que cualquier tráfico broadcast afecta al rendimiento de todas las estaciones. El tráfico multicast y broadcast se propaga por todas las VLANs.

Complejidad en la administración.- todos los usuarios deben configurarse inicialmente en una VLAN. El administrador de la red introduce de forma manual, en la mayoría de los casos, todas las direcciones MAC de la red en algún tipo de base de datos. Cualquier cambio o nuevo usuario precisa modificación de la base de datos. Todo ello puede complicarse extremadamente en redes con un gran numero de usuarios o conmutadores.

Existen soluciones alternativas para automatizar esta definición y normalmente se utiliza un servidor de configuración de forma que las direcciones MAC se copian de las tablas de direcciones de los conmutadores a la base de datos del

[9] http://www.ibw.com.ni/~alanb/campus.html
[10] http://www.ibw.com.ni/~alanb/campus.html

servidor. La asignación dinámica de VLAN en base a dirección MAC es también posible si bien su implementación puede ser muy compleja.

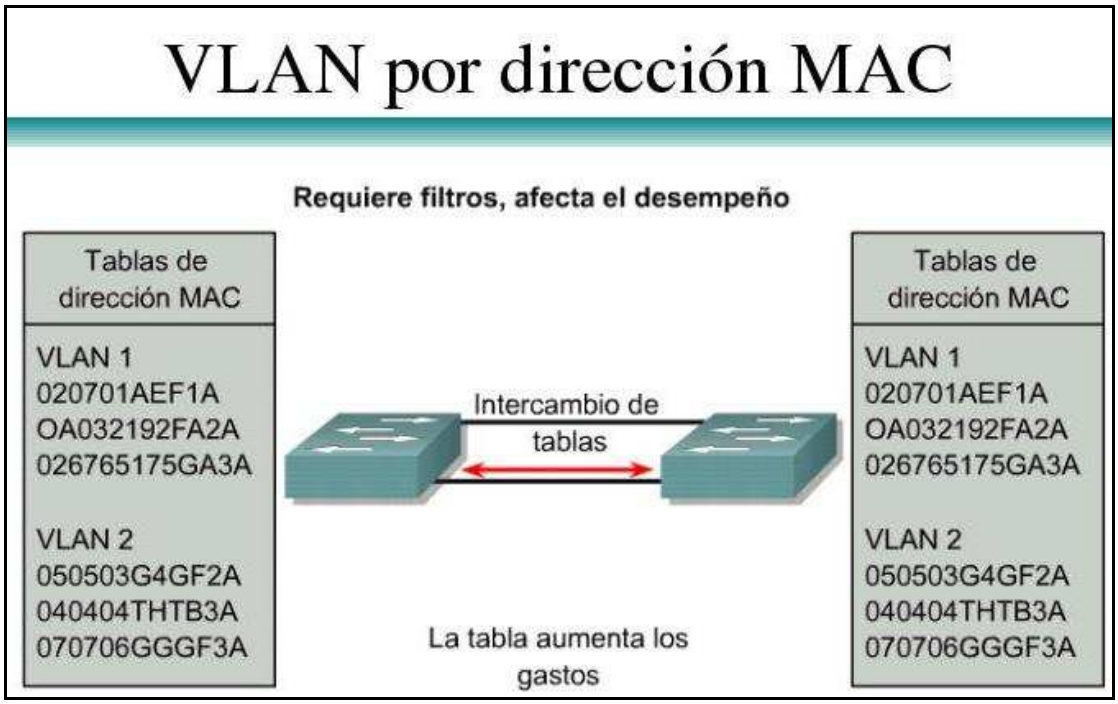


Figura 1.5 VLAN basadas en MAC[11]

1.2.3 VLANS POR FILTROS

La asignación a las VLANs se basa en información de protocolos de red (por ejemplo dirección IP o dirección IPX y tipo de encapsulación). La pertenencia a la VLAN se basa en la utilización de unos filtros que se aplican a las tramas para determinar su relación de pertenencia a la VLAN. Los filtros han de aplicarse por cada trama que entre por uno de sus puertos del conmutador.

Ventajas[12]:

Segmentación por protocolo.- es el método apropiado solo en aquellas redes en las que el criterio de agrupación de usuarios esté basado en el tipo de

[11] http://www.tlm.unavarra.es/asignaturas/aro/ccna3-8.ppt
[12] http://www.ibw.com.ni/~alanb/campus.html

protocolo de nivel 3 y la segmentación física existente sea muy diferente a los patrones de direccionamiento.

Asignación dinámica.- tanto la definición de VLANs por dirección MAC como por protocolo de nivel 3 ayudan a automatizar la configuración del puerto del conmutador en una VLAN determinada.

Desventajas[13]:

Problemas de rendimiento y control de broadcast.- la utilización de VLANs de nivel 3 requiere complejas búsquedas en tablas de pertenencia que afectan al rendimiento global del conmutador. Los retardos de transmisión pueden aumentar entre un 50 y un 80%.

El problema de control de broadcast surge con las estaciones multiprotocolo o sistemas multistack (por ejemplo estaciones con stacks TCP/IP, IPX y AppleTalk) que pertenecen a tantas VLANs como protocolos utilizan y por lo tanto recibirán todos los broadcast provenientes de las diversas VLANs en las que están incluidas.

No soporta protocolos de nivel 2 ni protocolos dinámicos.- la estación necesita una dirección de nivel 3 para que el conmutador la asigne a una VLAN. Las estaciones que utilicen protocolos de nivel 2 como NetBios y LAT no podrán asignarse a una VLAN. Si existen protocolos dinámicos como DHCP y la estación no tiene configurada su dirección IP ni su router por defecto el conmutador no puede clasificar la estación dentro de una VLAN.

Una premisa esencial en la definición de VLANs es que el rendimiento del conmutador no debe degradarse debido a la existencia de VLANs. Las técnicas de marcado (identificación de paquetes pertenecientes a cada VLAN) utilizadas en la definición de VLANs por puerto permiten mantener una velocidad de transmisión según el ancho de banda disponible (wire speed performance – rendimiento de velocidad en el cable) y por ello ha prevalecido dicha solución en la definición del estándar 802.1Q. Estas técnicas permiten además la

[13] http://www.ibw.com.ni/~alanb/campus.html

asignación de un mismo puerto o tarjeta de red a varias VLANs (routers o servidores pueden aprovechar esta ventaja evitándose la utilización de tantos interfaces o tarjetas de red como VLANs). ISL (Inter-Switch Link) para Fast Ethernet/Token Ring y 802.10 para FDDI son dos ejemplos de técnicas de marcado.

1.2.4 DOMINIO DE BROADCAST

Una VLAN es un dominio de broadcast que se crea en uno o más switches.

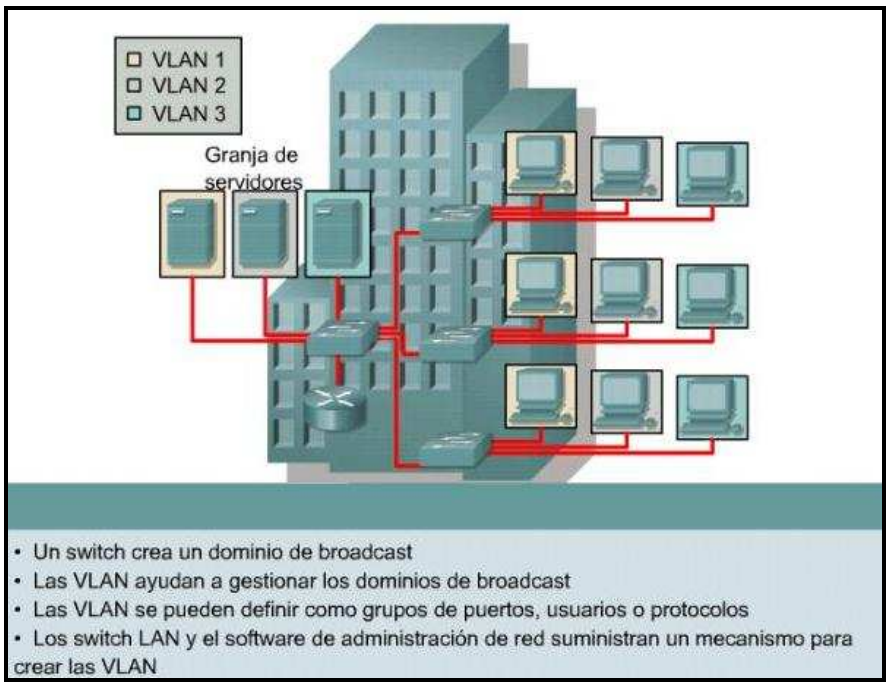


Figura 1.6 Dominio de Broadcast en las VLANS[14]

Para poder asimilar de mejor manera lo que significa el dominio de broadcast se utilizará algunos ejemplos.

Ejemplo 1[15]: En la siguiente figura se muestra como los tres dominios de broadcast se crean usando tres switches. El enrutamiento de capa 3 permite que el router mande los paquetes a tres dominios de broadcast diferentes.

[14] http://www.tlm.unavarra.es/asignaturas/aro/ccna3-8.ppt
[15] http://www.tlm.unavarra.es/asignaturas/aro/ccna3-8.ppt

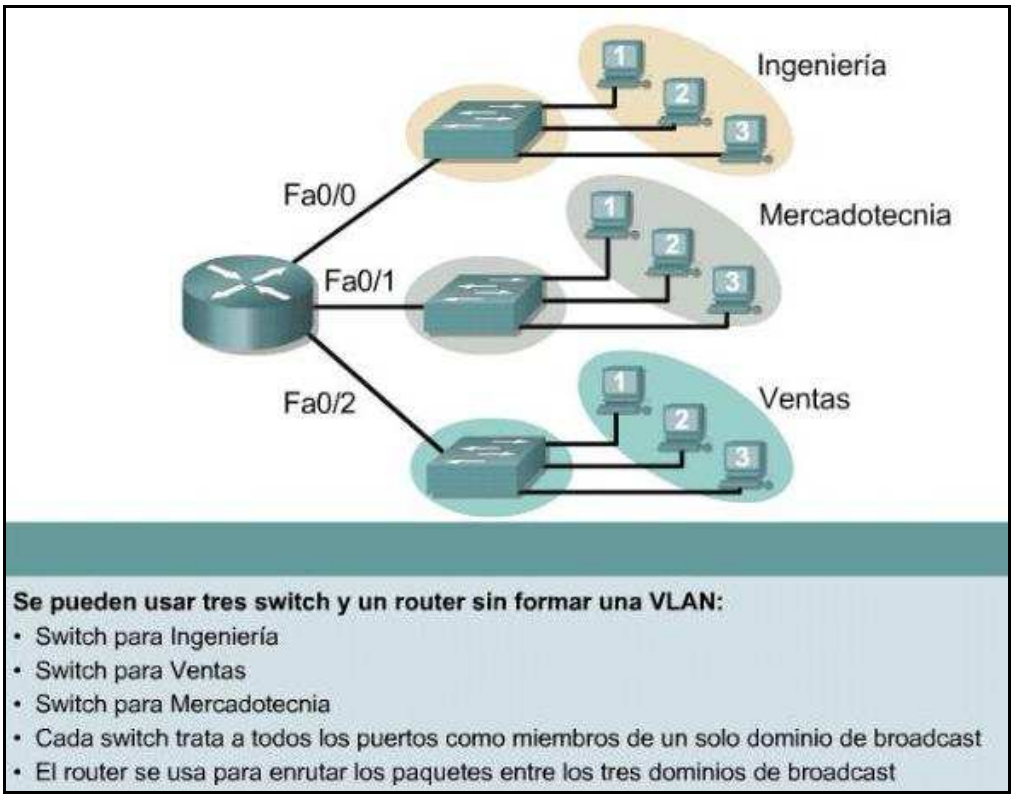


Figura 1.7 Ejemplo de la utilización de un router con VLAN[16]

Ejemplo 2[17]:

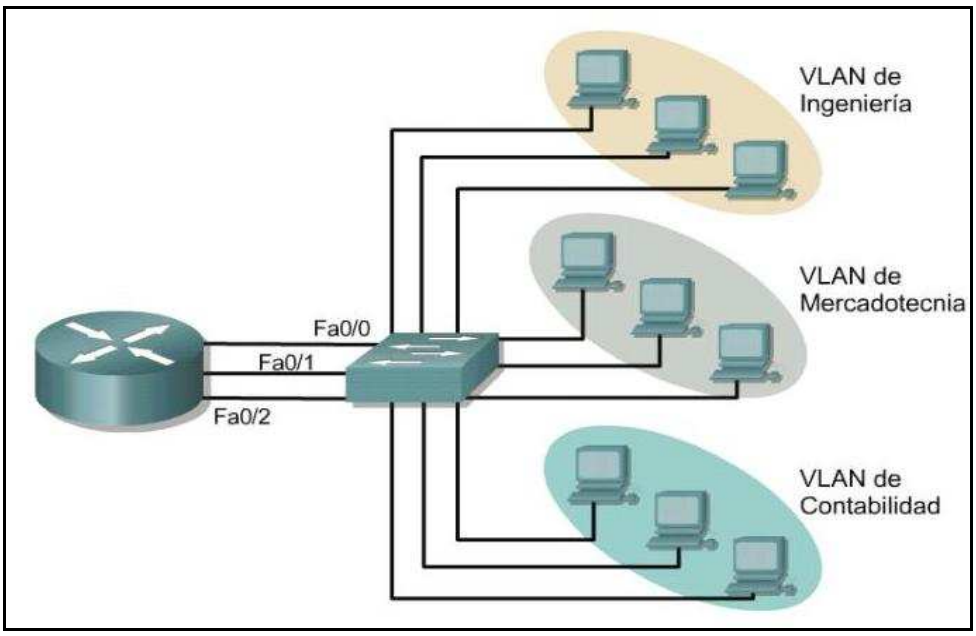


Figura 1.8 Ejemplo de tres dominios de broadcast separados[18]

[16] http://www.tlm.unavarra.es/asignaturas/aro/ccna3-8.ppt
[17] http://www.tlm.unavarra.es/asignaturas/aro/ccna3-8.ppt

En esta figura se crea una VLAN con un router y un switch. Existen tres dominios de broadcast separados. El router enruta el tráfico entre las VLAN mediante enrutamiento de Capa 3. El switch en la figura envía tramas a las interfaces del router cuando se presentan ciertas circunstancias:

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

Si la Estación de Trabajo 1 de la VLAN de Ingeniería desea enviar tramas a la Estación de Trabajo 2 en la VLAN de Ventas, las tramas se envían a la dirección MAC Fa0/0 del router. El enrutamiento se produce a través de la dirección IP de la interfaz del router Fa0/0 para la VLAN de Ingeniería.

Si la Estación de Trabajo 1 de la VLAN de Ingeniería desea enviar una trama a la Estación de Trabajo 2 de la misma VLAN, la dirección MAC de destino de la trama es la de la Estación de Trabajo 2 .

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

- El switch mantiene una tabla de puenteo o separada para cada VLAN.
- Si la trama entra en un puerto en la VLAN 1, el switch busca la tabla de puenteo para la VLAN 1.
- Cuando se recibe la trama, el switch agrega la dirección origen a la tabla de puenteo si es desconocida en el momento.
- Se verifica el destino para que se pueda tomar una decisión de envío.
- Para aprender y enviar se realiza la búsqueda en la tabla de direcciones para esa VLAN solamente.

[18] http://www.tlm.unavarra.es/asignaturas/aro/ccna3-8.ppt

1.3 COMPONENTES DE LAS VLANS

Los componentes físicos de las VLAN son los equipos que soporten los estándares de comunicación de las VLANS, esto incluye switches, puentes, interfaces de red, etc., todos los dispositivos con los que se implante un modelo de red con VLAN.

El componente principal de una VLAN es el estándar de comunicación que utiliza, en el caso particular es el estándar IEEE 802.1Q.

El estándar IEEE 802.1Q define una arquitectura para las LAN con puentes virtuales, los servicios proporcionados en las VLAN, y los protocolos y algoritmos que participan en la oferta de estos servicios.

A continuación de presenta un ejemplo del estándar 802.1Q:
Problema:
Transportar tráfico de varias LANs sobre ethernet.

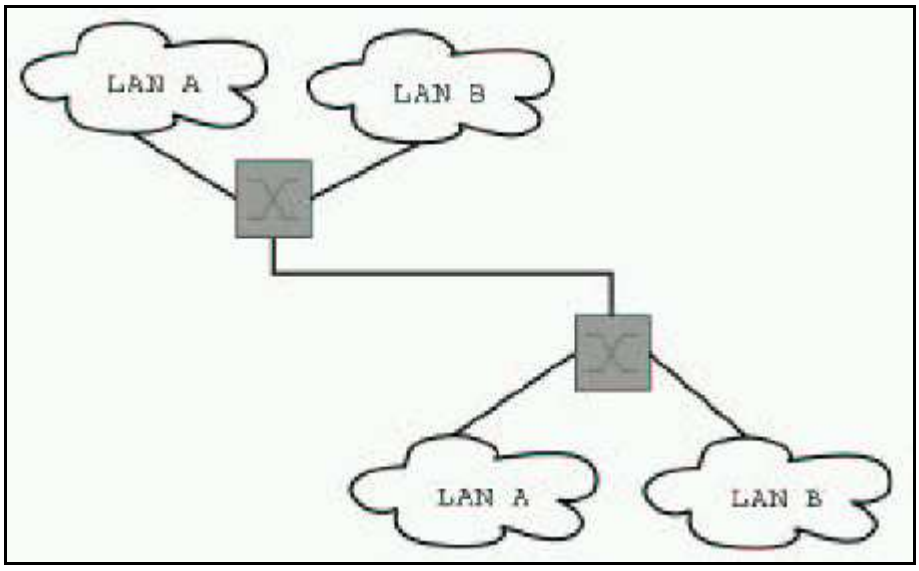


Figura 1.9 Ejemplo gráfico de problema de LANS[19]

[19] http://www.si.uji.es/bin/ponencies/ipp.pdf

Solución con 802.1Q:

Cada trama se marca con el id de la LAN a la que pertenece.

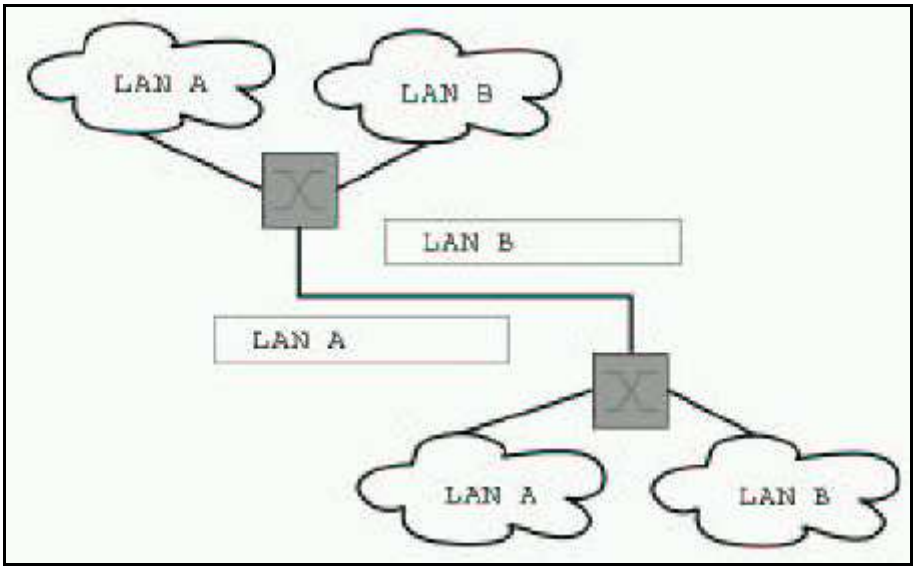


Figura 1.10 Ejemplo gráfico de la solución con 802.1Q[20]

La identificación de la LAN a la que pertenece cada red se identifica por el id, el formato de la trama 802.1Q es:

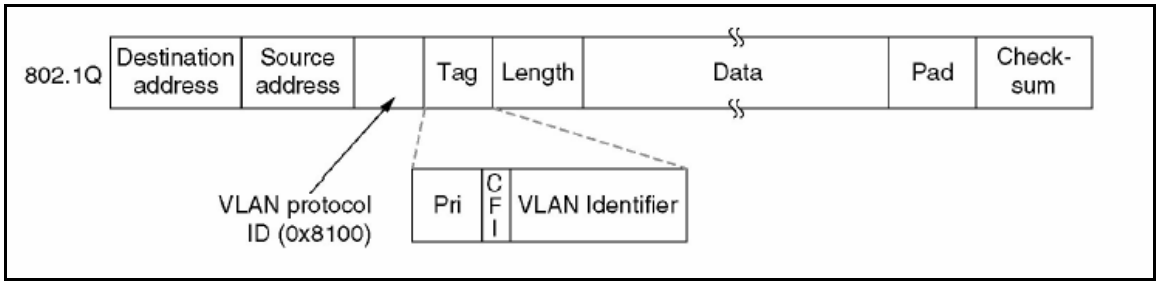


Figura 1.11 Formato de la trama 802.1Q[21]

1.4 SEGURIDAD EN VLANS

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Conviene aclarar que no siendo posible la certeza absoluta, el elemento de riesgo esta siempre presente, independiente de las medidas que se tomen, por

[20] http://www.si.uji.es/bin/ponencies/ipp.pdf

[21] http://www.si.uji.es/bin/ponencies/ipp.pdf

lo que se debe hablar de niveles de seguridad. La seguridad absoluta, la seguridad informática es un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos.

Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque hardware, software y datos son los datos y la información los sujetos principales de protección de las técnicas de seguridad. La seguridad informática se dedica principalmente a proteger la confidencialidad, la integridad y disponibilidad de la información. La confidencialidad se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos[22].

La seguridad en las VLANS depende de forma primordial de la administración, y de las prestaciones de los equipos que se utilicen para formar las VLANS, cabe indicar que mientras más segura y con menos accesos es una red, la administración de la misma es más compleja.

La seguridad que se tiene en una VLAN específica es muy elevada, puesto que solo los miembros que pertenecen a dicha VLAN podrán compartir recursos, como si fuese una LAN creada solo para ese grupo determinado.

Es necesario indicar que si no hay una distribución correcta de los usuarios que pertenecen a una VLAN determinada o, si se empiezan a trasladar usuarios de una VLAN general a la VLAN específica segura, subirá el riesgo de inseguridad de los datos a través de dicha VLAN.

1.5 BENEFICIOS DE LA IMPLEMENTACIÓN DE VLANS

Para poder comprender de mejor manera los beneficios qué tienen las redes virtuales (VLANs) se debe tener claro como funciona una red basada en enrutadores. Los enrutadores utilizan la capa tres del modelo OSI para mover tráfico en la red local LAN a otra red.

[22] http://www.solocursosgratis.com/curso_gratis_seguridad_informatica_-_conceptos_basicos-slccurso1029234.htm

Cada capa contiene campos en los cuales se identifica el dominio de broadcast en el cual el destino puede ser encontrado. Estas direcciones están asignadas por un administrador de red, y son generalmente registradas dentro de los archivos de configuración de las estaciones de red.

En una red basada en concentradores y enrutadores la dirección de red identifica un segmento de la misma[23].

Teniendo claro esto, cuando se cambia a una red virtual se obtienen los siguientes beneficios[24]:

- Las redes virtuales hacen que se reduzca el costo de manejo de usuarios que se mueven y cambian, éste beneficio se obtiene principalmente en las VLANs que han sido implementadas en el nivel 3 con direcciones IP, debido a que la estación cambia de sitio conserva su dirección IP; cosa que no sucede en las redes LAN pues si el dispositivo o estación de red es movido de un concentrador a otro, la dirección de red ya no será valida y el administrador de la red deberá corregir los archivos de configuración.
- Con las redes virtuales se pueden establecer Grupos de Trabajo Virtuales, esto es, miembros de un mismo departamento que están conectados en la misma LAN, es decir, físicamente contiguos pueden estar en diferentes VLANs. Así, si se cambia la estación de sitio pero en el mismo departamento no se tiene qué reconfigurar la máquina; si el equipo cambia de VLAN solo hay qué cambiar su número de red virtual y no su lugar físico.
- Otra ventaja es que se pueden establecer estos grupos con el criterio de 80/20 el cual consiste en que el 80% del tráfico de información es en la misma VLAN o grupo de trabajo y solamente el 20% restante es entre VLANs y por lo tanto no se requieren muchos enrutadores.
- Acceso a recursos: Un recurso y servidor puede estar en dos redes virtuales diferentes al mismo tiempo, es decir las VLANs permiten

[23] http://lauca.usach.cl/~lsanchez/Vlan
[24] http://lauca.usach.cl/~lsanchez/Vlan

superposición lo que reduce considerablemente el tráfico entre redes virtuales diferentes.

- Uno de los beneficios principales es la reducción de enrutadores, cuando se tiene una LAN los dominios de broadcast, son determinados por los enrutadores, en cambio, en una VLAN un switch sabe cuales puertos pertenecen al dominio de broadcast y por lo tanto solamente envía información a esos puertos, sin necesidad de un enrutador.
- Las VLANs pueden llegar a ser muy seguras cuando se implementan en conjunto con switches con puerto privado. Se puede implementar un firewall en cada VLAN fácilmente, éste es un servidor encargado de la seguridad, estableciendo permisos de entrada a cada red virtual.
- Dependiendo de la inteligencia de los switches se puede hacer filtrado e intercambio de decisiones respecto a los paquetes que pertenecen al tráfico, basados en medidas adoptadas por los administradores de la red. Esto se puede realizar a través de métodos como el filtrado de paquetes y la identificación de paquetes (encapsulado).
- Control y conservación del ancho de banda, las redes virtuales puede restringir los broadcast a los dominios lógicos donde han sido generados. Además añadir usuarios a un dominio determinado o grupo de trabajo no reduce el ancho de banda disponible para el mismo, ni para otros.
- Protección de la inversión, las capacidades VLAN están, por lo general, incluidas en el precio de los conmutadores que las ofrecen, y su uso no requiere cambios en la estructura de la red o cableado, sino mas bien los evitan, facilitando las reconfiguraciones de la red sin costos adicionales.
- Otro punto a destacar es que la tecnología ATM prevé, como parte importante de sus protocolos, grandes facilidades para las redes virtuales, lo que equivaldrá sin duda a grandes ventajas frente a la competencia para aquellos equipos que actualmente ya soportan sistemas VLAN.

- Se puede controlar el tráfico de broadcast de 2 maneras: limitando el número de puertos en el switch o limitando el número de personas que usan los puertos.

Estas diferencias entre los 2 tipos de redes hacen de las redes virtuales una solución más económica desde el punto de vista de desempeño y rapidez del flujo de información. Como los enrutadores no se usan para crear y separar cada dominio de broadcast, la disposición entre sus funciones principales es:

- Proveer conectividad entre las diferentes VLANs.
- Ser un filtro de broadcast para los enlaces WAN.

CAPITULO 2.

INFRAESTRUCTURA ACTUAL DE TELCONET

2.1 INTRODUCCION

Telconet, es una empresa dedicada a brindar varios servicios en el ámbito de las telecomunicaciones e Internet, su crecimiento y desarrollo se basa de manera fundamental en los siguientes aspectos:

2.1.1 MISIÓN

Buscar la excelencia en la provisión de la comunicación de datos, a través del uso de la mejor tecnología disponible y la preparación continua de nuestros recursos humanos en beneficio de la comunidad, cliente y empresas[25].

2.1.2 VISIÓN

Ser la mejor alternativa e integrar al Ecuador a través de la provisión de servicios de comunicación de video, voz y datos; siguiendo estándares internacionales de calidad y usando la mejor y más moderna tecnología en telecomunicaciones[26].

2.1.3 POLÍTICA DE CALIDAD

Proveer Servicios de Telecomunicaciones con un Sistema de Gestión de Calidad Transparente basado en la Prevención, comprometidos con el mejoramiento continuo para maximizar la satisfacción de cada cliente[27].

2.1.4 INFRAESTRUCTURA ACTUAL

Telconet cuenta principalmente con un backbone MEN (Metro Ethernet Network), el mismo que esta formado por varios nodos o vértebras principales, cada nodo cuenta con un equipo de conmutación Switch Cisco Catalyst 3550, estos equipos tienen 24 puertos Fast Ethernet y 2 puertos GBIC (Convertidor

[25] Misión - Telconet S.A.
[26] Visión - Telconet S.A.
[27] Política de Calidad – Telconet S.A.

de Interfaz Gigabit), el estándar utilizado para la configuración de los puertos es:

- Puertos GBIC: para conexión al backbone.
- Puertos Fast Ethernet del 1 al 5: para formar anillos de respaldo del Backbone.
- Puertos Fast Ethernet del 6 al 24: para conexión de clientes.

Los enlaces utilizados para la interconexión de los nodos dentro de la ciudad son casi en su totalidad por medio de fibra óptica, habiendo también radio enlaces utilizados en lugares alejados a la ciudad, pero ya se está trabajando en el tendido de fibra óptica para alcanzar esos lugares y poder tener el Backbone completamente con enlaces de fibra óptica.

A cada uno de los nodos se enlazan o conectan los clientes ya sea por medio de enlaces de fibra óptica o enlaces de radio, dependiendo de las necesidades del cliente, de la factibilidad de la instalación de uno u otro enlace y del costo representado de acuerdo a la negociación del mismo.

Todos los enlaces convergen en el nodo principal de Telconet, que se denomina nodo Gosseal, y es donde están ubicadas la oficinas y desde donde se realiza toda la administración de la red de forma remota.

Además Telconet cuenta con varios tipos de servidores:

- Servidores DNS, primario y secundario.
- Servidores Web, uno sobre Windows 2000 Server y otro sobre Linux Fedora Core 2.
- Servidores de Correo, un servidor utilizado para envío de correo, un servidor utilizado para recepción de correo y el último que realiza las dos funciones y es utilizado para almacenar correos de clientes que cuentan con su propio dominio, siempre que los clientes no tengan su propio servidor de correo.
- Servidor de acceso remoto, para conexiones Dial Up.

El esquema básico de conexión de un cliente al backbone de Telconet es el siguiente:

- Instalación de la última milla, o enlace desde el cliente hacia uno de los nodos.
- Instalación de un equipo de comunicación al cliente, esto es de acuerdo a la negociación y costos, por lo general se colocan equipos con sistema operativo Linux Fedora Core 2, con 2 interfaces de red, la primera es la interfaz con el backbone y la segunda es para la conexión de la red interna del cliente.
- Habilitación y configuración del puerto del switch catalyst por donde se enlaza el cliente, esto se lo realiza de forma retoma.
- Pruebas de conexión, verificación del correcto funcionamiento de los servicios contratados por el cliente.
- Monitoreo del enlace del cliente.

Para la conexión a Internet tiene arrendados dos canales DS3, que convergen con Telconet por medio de un Router Cisco 7513, el mismo se conecta a la fibra óptica de Colombia para luego pasar por el canal panamericano y llegar a los Estados Unidos.

En forma global se muestra la infraestructura actual de Telconet:

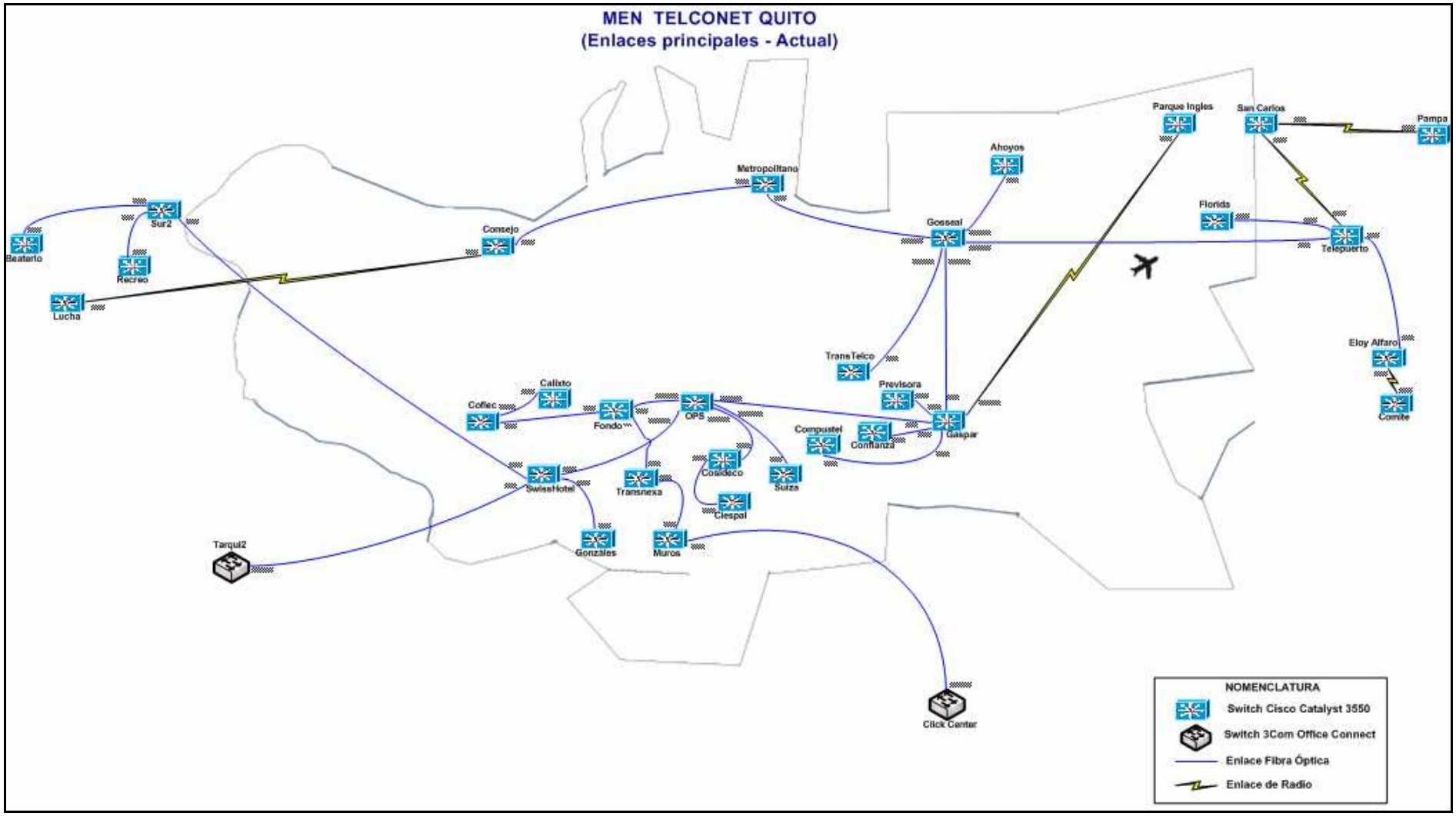


Figura 2.1 MEN Telconet Quito Actual

2.1.5 SERVICIOS QUE PRESTA TELCONET

Los principales servicios ofrecidos por Telconet se clasifican de acuerdo al cliente:

- Carriers e ISP
    - Con 15 clientes, de los mismos se puede mencionar algunos como Brigthcell y Onnet.
- Corporativos
    - Alrededor de 280 clientes, entre ellos, Seguros Colonial, Seguros Confianza y Cooperativa Andalucía.
- Dial Up
    - Clientes individuales, alrededor de 2000 usuarios.
- Hosting
    - Se administran 40 sitios Web.
- Diseño de Webs

Clientes Carries e ISP: como carrier de carriers, Telconet cuenta con un entusiasta y dedicado equipo, enfocado exclusivamente en cada una de las necesidades específicas de cada cliente, planteando soluciones y brindando respuestas ágiles. Cuenta con los siguientes servicios:

- Tránsito al Backbone de Internet por Fibra Óptica hasta el NAP de las Américas.
- Servicios de Enlaces de Transmisión de Datos locales, nacionales e internacionales.
- Servicios de VPN locales, nacionales e internacionales.
- Servicios de Segmento Espacial sobre Satmex para enlaces SCPC y VSAT.

Clientes Corporativos: el cliente corporativo ha sido un pilar importante en el crecimiento de la empresa, es por eso que Telconet asume el compromiso de brindarle acceso a una potente gama de servicios y soluciones inteligentes para satisfacer sus necesidades:

- Servicio de Internet Dedicado 1.1.
- Servicios de Internet Dedicado por Fibra Óptica.

- Servicios de Enlaces de Transmisión de Datos locales y nacionales.
- Servicios de VPN locales, nacionales e internacionales.
- Servicios de Certificación y Firmas Digitales.
- Servicios de administración de servidores de correo.

Clientes Dial Up: los principales servicios ofrecidos son:

- Servicio de conexión a Internet.
- Servicio de Correo Electrónico

Hosting: las soluciones en servicios de Hosting ofrecen la confiabilidad y seguridad que el cliente requiere para mantener su información. Los servidores de Telconet cuentan con las más avanzadas tecnologías y altos estándares de rendimiento para brindar un servicio 100% libre de preocupaciones.

Diseño de Webs: La imagen y presentación de una empresa a nivel de Internet es la prioridad para el trabajo de sitios Web. Telconet cuenta con las herramientas necesarias para desarrollar sitios Web de alto rendimiento.

2.1.6 CLIENTES DE TELCONET

Existen variedad de clientes que utilizan los servicios de Telconet, a continuación se nombran algunos clientes principales:

- Seguros Colonial
- Seguros Confianza
- Cooperativa Ilalo
- Cooperativa Andalucía
- Superdespensas AKI
- Artefacta
- Datafast
- Brigthcell
- Onnet

2.2 EQUIPOS DE COMUNICACIÓN UTILIZADOS POR TELCONET

La utilización de diferentes equipos ha sido una forma de poder sobresalir ante los diversos problemas de comunicación, es decir, se acuerdo a la necesidad

del cliente se utiliza equipamiento que pueda garantizar un buen servicio y con esto poder lograr la satisfacción del cliente.

Los equipos utilizados en la infraestructura de Telconet se clasifican en:

- Equipos de última milla.
- Equipos del backbone.
- Servidores y Ruteadores.
- Equipos terminales.

2.2.1 EQUIPOS DE ULTIMA MILLA

Los equipos de última milla se clasifican básicamente en dos tipos:

- De radio
- De fibra óptica

Entre la gran variedad de equipos de radio utilizados para comunicación de datos en el mercado, Telconet utiliza los siguientes:

Trendnet TEW-210APB

Esta familia de productos cumple con la normativa de comunicaciones IEEE de última generación, más avanzada, que conecta una red de ordenadores mediante las normas de encriptación 128-bits WEP. Con la transmisión mediante la normativa 802.11b de los datos enviados, los productos TRENDNET llevan a cabo la comunicación de una forma automática a la velocidad óptima de transmisión en cada momento, es decir, a 1, 2, 5.5, y 11Mbps[28].

[28] http://www.noticias.com/articulo/14-03-2002/redaccion/nuevos-productos-inalambricos-red-31mb.html

Figura 2.1 Equipo TrendNet TEW-210 APB[29]

Teletronics 11 Mbps Access Point Inter-Building

Utilizado en enlaces de redes de computo de forma inalámbrica en aplicaciones punto-punto y punto-multipunto.

Estos equipos son útiles también para monitoreo inalámbrico de CCTV, disponibles en las bandas de 2.4GHz.

Figura 2.2 Equipo Teletronics 11 Mbps

[29] http://www.noticias.com/articulo/14-03-2002/redaccion/nuevos-productos-inalambricos-red-31mb.html

Información Técnica:

Configuración típica, para uso dentro de la oficina.

Configuración antena externa, para aumentar la potencia y ser usado en ambientes externos.

Modos operativos:

Access Point

Bridge (Inter.-building with repeating)

Ad-Hoc

Velocidad: 11 Mbps

Potencia de salida: 15 dBm (30mW)

Modulación: DSSS

Banda: 2.412-2.462 GHz; 11 Canales

Sensibilidad: -83dBm a 11 Mbps.

Conector: SMA Inverso (para aplicaciones con antenas externas).

Provee conexión entre una red Ethernet (PC's) cableada operando como Access Point o Bridge para enlazar redes de forma inalámbrica. En conjunción con antenas externas de ganancia y amplificadores (SmartAmp) se puede incrementar la potencia y rango de alcance del enlace[30].

Motorola Canopy.

La plataforma inalámbrica Canopy es una solución de banda ancha de alta velocidad lista para una conectividad de costo efectivo a redes privadas, tales como las de los gobiernos o empresas, así como a los operadores y proveedores de servicios de Internet. El sistema Canopy es escalable, sólido, confiable y da soporte a las aplicaciones de banda ancha de mayor demanda. Su desempeño superior ofrece uno de los menores costos totales y puede reducir de manera significativa los costos de arranque, mantenimiento y líneas alquiladas (*leased-lines*) de los proveedores[31].

Información Técnica:

Método de Acceso: TDD/TDMA

Velocidad de señalización: 10 Mbps

[30] http://www.teletronics.com/Firmware.html

[31] http://motorola.canopywireless.com/es/

Tipo de Modulación: Alto Índice de Modulación BFSK(Optimizado para rechazar la interferencia)

Portadora a Interferencia (C/I): 3dB

Sensibilidad Receptora: -83dBm

Margen de Funcionamiento: Hasta 3 kilómetros (2 millas) con antena integrada en la banda de 5.2 GHz. Hasta 16 kilómetros (10 millas) con reflector pasivo en la banda de 5.7 GHz.

Potencia Transmisora: Cumple el Límite FCC UNII ERP

Alimentación de CC: 24 VCC a 0.3 Amp (estado activo)

Interfaz: 10/100 BaseT, dúplex medio/completo. Velocidad autonegociada (en conformidad con 802.3)

Protocolos Usados por CANOPY: IPV4, UDP, TCP, ICMP, Telnet, HTTP, FTP, SNMP

Ruta de Actualización del Software: Descarga a distancia en FLASH mediante enlace de RF

Administración de la Red: HTTP, TELNET, FTP, SNMP

Viento: 190 km/hr (118 millas/hr)

Temperatura de Funcionamiento: 30℃ a +55℃ (-40℉ - +131℉)

Peso: 0.45 kg (1 libra)

Dimensiones: 29.9 cm Al x 8.6 cm An x 8.6 cm P (11.75 x 3.4 x 3.4 pulg.)

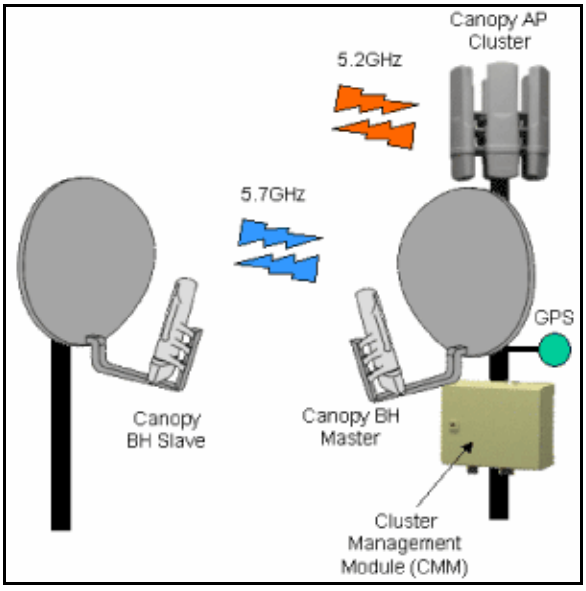


Figura 2.3 Equipos Canopy[32]

[32] http://motorola.canopywireless.com/es/

TrangoBroadband

El puente Ethernet inalámbrico para exteriores TrangoLINK-10 ofrece un rendimiento superior, largo alcance, flexibilidad de banda doble y fácil instalación a un precio asequible.

Figura 2.4 Equipos TrangoLINK-10[33]

Ideal para aplicaciones de redes de retroceso ISP y para extensiones WAN de punto a punto de clase empresarial, el sistema TrangoLINK-10 es versátil, fiable y sólido. El sistema TrangoLINK-10 funciona tanto a 5,8 GHz como a 5,3 GHz y proporciona a los operadores de red un puente Ethernet de punto a punto para exteriores económico pero eficaz. El sistema proporciona con fiabilidad 10 Mbps a una distancia de hasta 16 kilómetros (10 millas) con antenas integradas y de 64 kilómetros (40 millas) con antenas externas. El sistema TrangoLINK-10 se puede implementar como sistema de red de retroceso o como alternativa a las líneas alquiladas y a los múltiples circuitos T1[34].

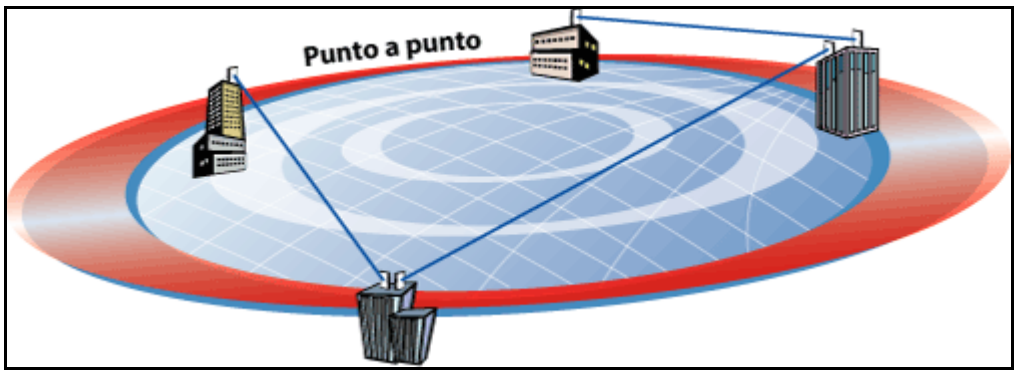


Figura 2.5 Enlace con equipos Trango[35]

[33] http://www.trangobroadband.com/sp/products/trangolink_10.htm
[34] http://www.trangobroadband.com/sp/products/quickspecs.htm
[35] http://www.trangobroadband.com/sp/products/trangolink_10.htm

Puntos importantes del equipo:

- El sistema TrangoLINK-10 proporciona canales de funcionamiento tanto en la banda ISM de 5,8 GHz como en la banda U-NII de 5,3 GHz.
- La tecnología del espectro ensanchado por secuencia directa proporciona un alcance excelente e inmunidad a las interferencias.
- La autenticación MAC propia, junto con la codificación de las transmisiones, proporciona un alto grado de seguridad durante las comunicaciones.
- La configuración es sencilla y se puede realizar en minutos.
- Las antenas de polarización doble combinadas con los 11 canales sin solapamiento proporcionan 22 combinaciones de canal y polaridad para conseguir una capacidad de ubicación conjunta máxima. Las selecciones de polaridad y canal se pueden conmutar de forma remota.
- Existe disponible una gran variedad de antenas, incluidas la antena integrada de 16 kilómetro (10 millas) y las antenas externas de 32 y 64 kilómetros (20 y 40 millas) (banda de 5,8 GHz).

Información Técnica:

Frecuencia de funcionamiento: 5725 MHz a 5850 MHz (banda alta), 5250 MHz a 5350 MHz (banda baja).

Rendimiento de datos de usuario: 10 Mbps

Polarización de antena: Horizontal / Vertical (conmutable por software)

Formato de modulación: Espectro ensanchado por secuencia directa (DSSS) con RAKE

Seguridad: Esquema de autenticación MAC propio, codificación de datos durante la comunicación

Configuración y administración: Telnet, SNMP (a través de AP), TFTP, http

Interfaces físicas: Detección automática de Ethernet 10/100, puerto serie (RJ11)

Método de alimentación: PoE

Límites de voltaje: 10,5 V CC – 24 V CC

Tipo de carcasa: Policarbonato resistente a todo tipo de situaciones meteorológicas

Intervalo de temperaturas: -40°a 60°C (-40°a 140°F)

Dimensiones de la radio: 12,5" × 8" × 2 ¾"

Peso de la radio: 1,8 Kg (4 libras)

Interfaces: RJ-45 y RJ-11

Los equipos utilizados por Telconet para transmisión mediante fibra óptica son:

Tipo de fibra óptica

Fibra óptica monomodo de 9 micrones, generalmente de 4 hilos para la instalación de ultima milla desde el cliente hacia el nodo dependiente, para otros enlaces utiliza de 12 y 24 hilos, con este tipo de fibra se alcanza distancias de 3 a 10Km.

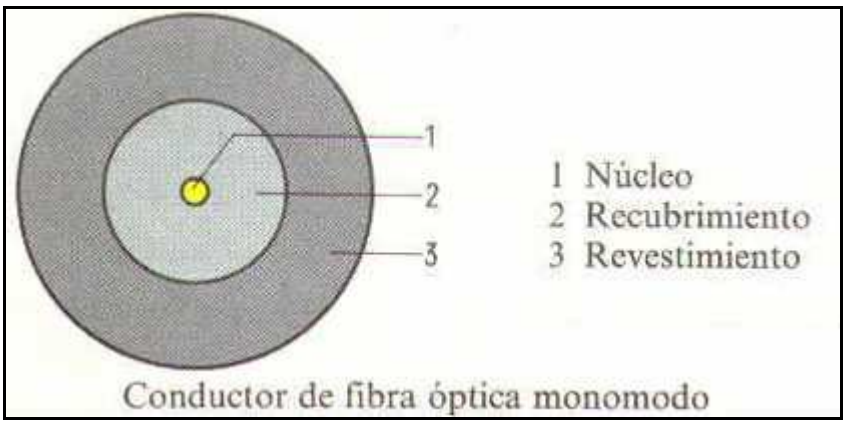


Figura 2.6 Fibra Óptica Monomodo[36]

Transceivers

Son equipos D-LINK, de dos hilos, un hilo para transmisión y otro para recepción de datos (Tx/Rx), respectivamente.

[36] http://orbita.starmedia.com/ygalarza/Ciencia.html

Figura 2.7 Transceiver D-LINK[37]

Conectores

Se utilizan conectores tipo SC.

Figura 2.8 Conectores SC[38]

2.2.2 EQUIPOS DEL BACKBONE

Los equipos del backbone de Telconet están representados directamente por los Switch Cisco Catalyst que forman parte primordial de la MEN (Metro Ethernet Network) de Telconet.

Metro Ethernet[39]**.-** Actualmente, Metro Ethernet es un servicio ofrecido por los proveedores de telecomunicaciones para interconectar LANs ubicadas a grandes distancias dentro de una misma ciudad; es decir, realizando un transporte WAN.

Los beneficios que Metro Ethernet ofrece son:

Fácil uso: Interconectando con Ethernet se simplifica las operaciones de red, administración, manejo y actualización.

---

[37] http://www.conecsion.es/index.asp?nivel=32&idcateg=36
[38] http://cubitel.es/web/images/stories/fibra_optica/conectores_sc_pc-apc.jpg
[39] http://www.monografias.com/trabajos17/metro-ethernet/metro-ethernet.shtml#metro

Economía: los servicios Ethernet reducen el capital de suscripción y operación de tres formas:

- Amplio uso: se emplean interfaces Ethernet que son las más difundidas para las soluciones de Networking.
- Bajo costo: Los servicios Ethernet ofrecen un bajo costo en la administración, operación y funcionamiento de la red.
- Ancho de banda: Los servicios Ethernet permiten a los usuarios acceder a conexiones de banda ancha a menor costo.

Flexibilidad: Las redes de conectividad mediante Ethernet permiten modificar y manipular de una manera más dinámica, versátil y eficiente, los anchos de banda y cantidad de usuarios en corto tiempo.

Servicio Metro Ethernet.- El modelo básico de los servicios Metro Ethernet, esta compuesto por una Red switcheada (Metro Ethernet Network -MEN-), ofrecida por el proveedor de servicios; los usuarios acceden a la red mediante CEs (Customer Equipement) que se conectan a través de UNIs (User Network Interface) a velocidades de 10Mbps, 100Mbps, 1Gbps o 10Gbps.
Es posible tener múltiples UNIs conectadas al MEN de una simple localización. Los servicios pueden soportar una variedad de tecnologías y protocolos de transporte en el MEN tales como SONET, DWDM, MPLS, GFP, etc.

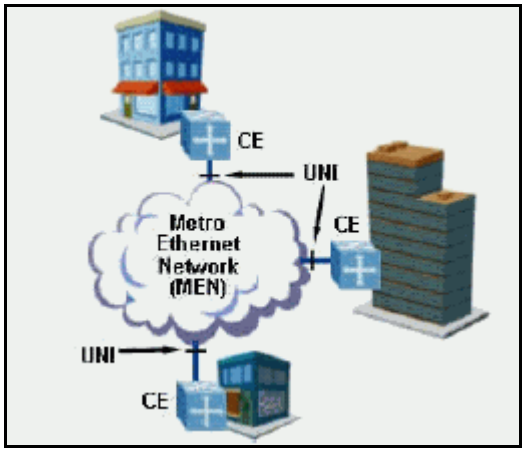


Figura 2.9 Metro Ethernet Network[40]

Cisco Catalyst 3550-24 SMI.- esta diseñado para ayudar a los usuarios a que pasen de forma sencilla de las redes LAN compartidas tradicionales a redes

[40] http://www.monografias.com/trabajos17/metro-ethernet/metro-ethernet.shtml#metro

completamente conmutadas. Los switches Catalyst de Cisco ofrecen un amplio espectro para aplicaciones de usuarios, desde switches para pequeños grupos de trabajo hasta switches multicapa para aplicaciones empresariales escalables en el centro de datos o en el backbone. Los switches Catalyst ofrecen rendimiento, administración y escalabilidad, se puede encontrar equipos Ethernet, Fast Ethernet y con opciones modulares las cuales permiten adaptarlos a las necesidades del negocio[41].

24-10/100 + 2 GBIC PORTS: SMI

Figura 2.10 Switch Cisco Catalyst 3550

Descripción del producto Cisco Catalyst 3550-24 SMI - conmutador - 24 puertos
Factor de forma Externo - 1 U
Características:

- Capacidad duplex, Encaminamiento IP, soporte VLAN, activable.
- Dimensiones (Ancho x Profundidad x Altura) 36.6 cm x 44.5 cm x 4.5 cm.
- Peso 5 kg.
- Alimentación CA 110/230 V CA 100/240 V (50/60 Hz).
- Memoria RAM 64 MB (instalados) / 64 MB (máx.).
- Tipo de dispositivo Conmutador.
- Cantidad de puertos 24 x Ethernet 10Base-T, Ethernet 100Base-TX.

[41] http://www.cisco.com/en/US/products/hw/switches/ps646/ps3814/

- Velocidad de transferencia de datos 100 Mbps.
- Protocolo de interconexión de datos Ethernet, Fast Ethernet.
- Cumplimiento de normas IEEE 802.3, IEEE 802.3U, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.1w, IEEE 802.1x, IEEE 802.1s.
- Modo comunicación Semidúplex, dúplex pleno.
- Memoria Flash 16 MB (instalados) / 16 MB (máx.).
- Protocolo de gestión remota SNMP 1, SNMP 2, RMON 1, RMON 2, SNMP 3.
- Ranuras vacías 2 x GBIC.

2.2.3 SERVIDORES Y RUTEADORES

Los equipos utilizados como servidores de datos, aplicaciones, etc., son Servidores Supermicro, con el sistema operativo instalado, de acuerdo a la función que desempeña.

Supermicro.-El SuperServer Supermicro 6113L-8 es el servidor para montaje en rack de formato 1U. Equipado con una placa base que utiliza el chipset E8770, el servidor 6113L-8 se sitúa por delante del resto al soportar velocidades de bus de 400MHz y procesadores Itanium 2 de hasta 1,50 GHz y hasta 16GB de memoria DDR-200 ECC registrada. El 6113L-8 incluye también dos puertos de red Gigabit, una ranura de expansión PCI-X y cuatro bahías de disco Ultra320 SCSI para intercambio "en caliente" (hasta 724GB de capacidad de almacenamiento). Para mayor seguridad, se ha implementado un sistema de protección térmica para el procesador para prevenir daños en la CPU o "caídas" del sistema por sobrecalentamientos anormales. Una fuente de alimentación intercambiable de 500W y una ranura IPMI 1.5 para gestión avanzada de servidores completan las increíbles características de este servidor. Este robusto y brillante equipo ofrece prestaciones de primera línea para servidores de alto rendimiento, servidores SQL y sistemas HPCCs (High Performance Computer Cluster) y EPICs (Explicitly Parallel Instruction Computing). Construido con los niveles de calidad y las prestaciones que han

hecho famoso a Supermicro, el servidor Supermicro 6113L-8 es una solución optimizada para el formato 1U en la que se puede confiar a largo plazo[42].

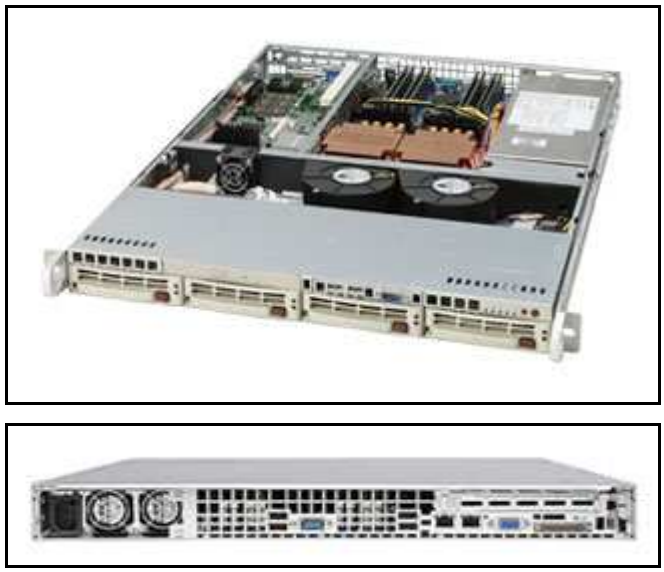


Figura 2.11 Servidor Supermicro[43]

Ruteadores.- El router (enrutador o encaminador) es un dispositivo hardware o software de interconexión de redes de ordenadores/computadoras que opera en la capa 3 (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando como base la información de la capa de red.

Los routers toman decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirigen los paquetes hacia el segmento y el puerto de salida adecuados. Los routers toman decisiones basándose en diversos parámetros. Lo más importante es decidir la dirección de la red hacia la que va destinado el paquete (En el caso del protocolo *IP* esta sería la dirección IP). Otras serían la carga de tráfico de red en los distintos interfaces de red del router y la velocidad de cada uno de ellos, dependiendo del protocolo que se utilice[44].

[42] http://www.flytech.es/supermicro/Productos/Servidores/supermicro%20itanium%202%206113L-8.htm
[43] http://www.flytech.es/supermicro/Productos/Servidores/supermicro%20itanium%202%206113L-8.htm
[44] http://es.wikipedia.org/wiki/Router

Son algunos modelos de ruteadores utilizados por Telconet, de acuerdo a cada necesidad, pero su estándar es de la familia Cisco, entre los mismos el de más relevancia es el Router 7513 de Cisco.

Cisco 7513.- soporta multiprotocolo, las conexiones routing multimedia y bridging con una amplia variedad de protocolos y cualquier combinación de Asynchronous Transfer Mode - Modo de Transferencia Asincrónico (ATM), Ethernet, Fast Ethernet, Token Ring, Fiber Distributed Data Interface - Interfaz de Distribución de Datos por Fibras (FDDI), High-Speed Serial Interface - Interfaz Serial de Alta Velocidad (HSSI), accesorios del canal y medios. Las interfaces de red usan los procesadores de interfaz que proporcionan una conexión directa entre dos Cisco Extended Buses - Buses Extendidos Cisco (CyBuses) y las redes externas[45].

Figura 2.12 Cisco 7513[46]

2.2.4 EQUIPOS TERMINALES

Los equipos utilizados como terminales (CE Customer Equipement) son servidores de comunicación con Sistema Operativo Linux, en la actualidad se implementan los Phoenix Router.

Los Phoenix Router son dispositivos que tienen instalado el sistema operativo Linux en una memoria que es utilizada como disco duro, sus prestaciones de

[45] http://www.cisco.com/en/US/products/hw/routers/ps359/ps362/
[46] http://www.cisco.com/en/US/products/hw/routers/ps359/ps362/

almacenamiento de datos son limitadas y son utilizados específicamente para la transmisión de datos, es decir, como si fuesen ruteadores, la gran ventaja de su utilización es que tienen un costo muy inferior que un equipo router específico y su tamaño es pequeño y fácil de ubicar en cualquier lugar.

Figura 2.13 Phoenix Router

2.3 TIPOS DE ENLACES DE COMUNICACIÓN UTILIZADOS POR TELCONET

Básicamente los enlaces de comunicación se dividen en dos formas de acuerdo al medio de transmisión:

- Enlaces mediante Fibra Óptica
- Radio enlaces (Wireless)

2.3.1 ENLACES MEDIANTE FIBRA OPTICA

En un sistema de transmisión por fibra óptica existe un transmisor que se encarga de transformar las ondas electromagnéticas en energía óptica o en luminosa, por ello se le considera el componente activo de este proceso. Una vez que es transmitida la señal luminosa por las minúsculas fibras, en otro extremo del circuito se encuentra un tercer componente al que se le denomina detector óptico o receptor, cuya misión consiste en transformar la señal luminosa en energía electromagnética, similar a la señal original. El sistema básico de transmisión se compone en este orden, de señal de entrada, amplificador, fuente de luz, corrector óptico, línea de fibra óptica (primer tramo), empalme, línea de fibra óptica (segundo tramo), corrector óptico, receptor, amplificador y señal de salida[47].

[47] http://www.monografias.com/trabajos13/fibropt/fibropt.shtml

Se puede decir que en el proceso de comunicación la fibra óptica funciona como medio de transportación de la señal luminosa, generado por el transmisor de LED'S (diodos emisores de luz) y láser.

Los diodos emisores de luz y los diodos láser son fuentes adecuadas para la transmisión mediante fibra óptica, debido a que su salida se puede controlar rápidamente por medio de una corriente de polarización. Además su pequeño tamaño, su luminosidad, longitud de onda y el bajo voltaje necesario para manejarlos son características principales.

Los principales elementos de un enlace de comunicaciones de fibra óptica son: transmisor, receptor y guía de fibra. El transmisor consiste de una interfase analógica o digital, un conversor de voltaje a corriente, una fuente de luz y un adaptador de fuente de luz a fibra. La guía de fibra es un vidrio ultra puro o un cable plástico. El receptor incluye un dispositivo conector detector de fibra a luz, un foto detector, un conversor de corriente a voltaje un amplificador de voltaje y una interfase analógica o digital. En un transmisor de fibra óptica la fuente de luz se puede modular por una señal análoga o digital, acoplando impedancias y limitando la amplitud de la señal o en pulsos digitales. El conversor de voltaje a corriente sirve como interfase eléctrica entre los circuitos de entrada y la fuente de luz.

La fuente de luz por lo general es un diodo emisor de luz LED o un diodo de inyección láser ILD, la cantidad de luz emitida es proporcional a la corriente de excitación, por lo tanto el conversor de voltaje a corriente, convierte el voltaje de la señal de entrada en una corriente que se usa para dirigir la fuente de luz. La conexión de fuente a fibra es una interfase mecánica cuya función es acoplar la fuente de luz al cable.

La fibra óptica esta compuesta de un núcleo de fibra de vidrio o plástico, una cubierta y una capa protectora. El dispositivo de acoplamiento del detector de fibra a luz también es un acoplador mecánico.

El detector de luz generalmente es un diodo PIN o un APD (fotodiodo de avalancha), ambos convierten la energía de luz en corriente. En consecuencia, se requiere un conversor corriente a voltaje que transforme los cambios en la corriente del detector a cambios de voltaje en la señal de salida[48].

2.3.2 RADIO ENLACES (WIRELESS)

El concepto de WLAN (Wireless Local Area Network) se interpreta como un sistema de comunicación de datos flexible utilizado como alternativa a la redes cableadas. Este tipo de redes se diferencia de las convencionales principalmente en la capa física y en la capa de enlace de datos, según el modelo de referencia OSI.

La capa Física (PHY) indica cómo son enviados los bits de una estación a otra. La capa de Enlace de Datos (MAC) se encarga de describir cómo se empaquetan y verifican los bits de manera que no tengan errores. Las demás capas se encargan de los protocolos, de los puentes, encaminadores o puertas de enlace que se utilizan para conectarse[49].

Los dos métodos que se emplean para reemplazar la capa física en una red inalámbrica son la transmisión de Radio Frecuencia y la Luz Infrarroja.
Los sistemas por infrarrojos, según el ángulo de apertura con que se emite la información, pueden clasificarse en:

- Sistemas de corta apertura, también denominados de rayo dirigido o de línea de visión (LOS, line of sight).
- Sistemas de gran apertura, también denominados reflejados o difusos[50].

Por otra parte, las comunicaciones inalámbricas que utilizan radiofrecuencia pueden clasificarse en:

- Sistemas de banda estrecha (narrow band) o de frecuencia dedicada. Este tipo trabaja de una forma similar a las ondas de una estación de radio. Esta señal puede atravesar paredes por lo que puede alcanzar

[48] http://www.monografias.com/trabajos13/fibropt/fibropt.shtml
[49] http://www.maxitrucos.com/articulos/montse/wireless_la_conexion_sin_cables.htm
[50] http://www.maxitrucos.com/articulos/montse/wireless_la_conexion_sin_cables.htm

una red bastante amplia, sin embargo tienen problemas con las reflexiones que sufren las ondas de radio, para establecer esto hay que evitar las posibles interferencias.

- Sistemas basados en espectro disperso o extendido (spread spectrum). La FCC (Comisión Federal de Comunicaciones) a partir de 1985 permitió la operación sin licencia de dispositivos que utilicen 1 watio de energía o menos, en tres bandas de frecuencias: 902 a 928 MHz, 2.400 a 2.483,5 MHz y 5.725 a 5.850 MHz[51].

WLAN 802.11.- Este estándar está desarrollado por el Instituto de Ingeniería Eléctrica y Electrónica IEEE 802.11, describe las normas a seguir por cualquier fabricante de dispositivos Wireless para que puedan ser compatibles entre si. El 802.11 es una red local inalámbrica que usa la transmisión por radio en la banda de 2.4 GHz, o infrarroja, con regímenes binarios de 1 a 2 Mbit/s. El método de acceso al medio es mediante escucha pero sin detección de colisión, que se conoce como DFWMAC (Distributed Foundation Wireless MAC).

Los estándares más importantes son:

- IEEE802.11a: hasta 54 Mbps (megabits por segundo) de ancho de banda disponible, trabajando en la frecuencia de 5GHz.
- IEEE802.11b: hasta 11 Mbps. Este es el más usual y el más utilizado, trabaja en la frecuencia de 2,4GHz.
- IEEE802.11g: futuro estándar hasta 54 Mbps, trabajando en la frecuencia de 2,4 GHz como 802.11a.

Al ser un estándar mundial, muchos fabricantes de hardware están creando equipos Wireless para poder conectar ordenadores, y van mucho más allá, utilizando Wireless para otras aplicaciones como pueden ser: servidores de impresión o cámaras Web. Un mundo lleno de posibilidades[52].

[51] http://www.maxitrucos.com/articulos/montse/wireless_la_conexion_sin_cables.htm
[52] http://www.maxitrucos.com/articulos/montse/wireless_la_conexion_sin_cables.htm

2.4 ESTRUCTURA DEL BACKBONE

Las redes de telecomunicación constituyen la infraestructura básica de transporte para el intercambio de información entre dos puntos. Una red queda identificada cuando se conoce:

- La naturaleza de los elementos físicos que la forman: nodos, medios de transmisión y sistemas de conmutación.
- La topología o disposición básica de dichos elementos.
- Las normas operativas que establecen los protocolos de acceso y funcionamiento de la red.

La naturaleza de los elementos físicos de la red.- en Telconet los elementos físicos del Backbone se componen por:

- Switch Cisco Catalyst 3550, que forman la MEN (Metro Ethernet Network).
- Enlaces por medio de Fibra Óptica y de Radio (Wireless).
- La conmutación es automática en el caso de cortes de enlace en el backbone a través de anillos formados con los diferentes nodos utilizando el protocolo Spannig Tree para éste propósito.

Topología de la red.- es la forma en que los equipos terminales y los nodos se conectan entre sí, a través de los enlaces. Es posible distinguir cuatro topologías básicas:

- **Estrella.-**diseñada con un nodo central al que se encuentran conectados todos los terminales y que actúa como distribuidor del tráfico de las comunicaciones. Posee la estructura más simple y permite una comunicación rápida. Resulta especialmente apta para áreas geográficas concentradas con un número de terminales no muy elevado. Su principal problema es la escasa fiabilidad pues si falla el nodo central los terminales quedan incomunicados[53].

[53] http://trajano.us.es/~rafa/ARSS/apuntes/tema2.pdf

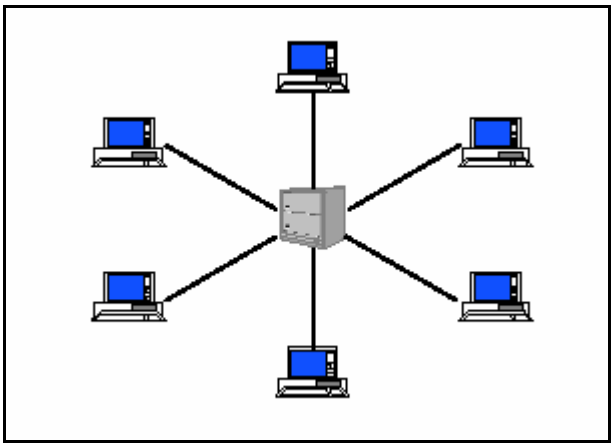


Figura 2.14 Topología en Estrella[54]

- **Malla.-** en ella todos los equipos se encuentran conectados entre sí (mallado total), aunque a veces pueden faltar ciertos enlaces (mallado parcial).

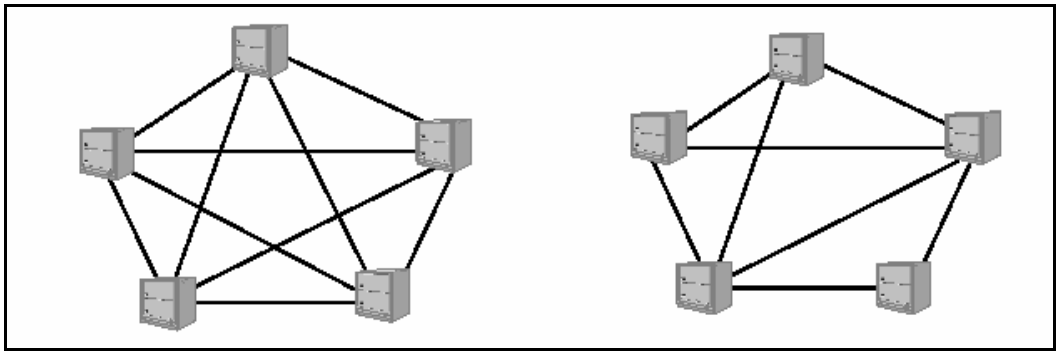


Figura 2.15 Topología en Malla, total y parcial respectivamente[55]

- El número de medios de transmisión necesarios en esta topología es elevado (para N nodos se necesitará N*(N-1)/2). La eficiencia de los enlaces es baja, pues éstos permanecen inactivos gran parte del tiempo. Por el contrario es una estructura muy fiable, pues existen caminos alternativos para llevar la información a los nodos. Suele utilizarse en el núcleo de las redes[56].

- **Anillo.-** cada equipo se conecta con los dos adyacentes hasta formar entre ellos un anillo. Para incrementar la fiabilidad de la red se utiliza el

[54] http://trajano.us.es/~rafa/ARSS/apuntes/tema2.pdf
[55] http://trajano.us.es/~rafa/ARSS/apuntes/tema2.pdf
[56] http://trajano.us.es/~rafa/ARSS/apuntes/tema2.pdf

anillo doble, que permite continuar las comunicaciones caso de fallar un enlace o un nodo.

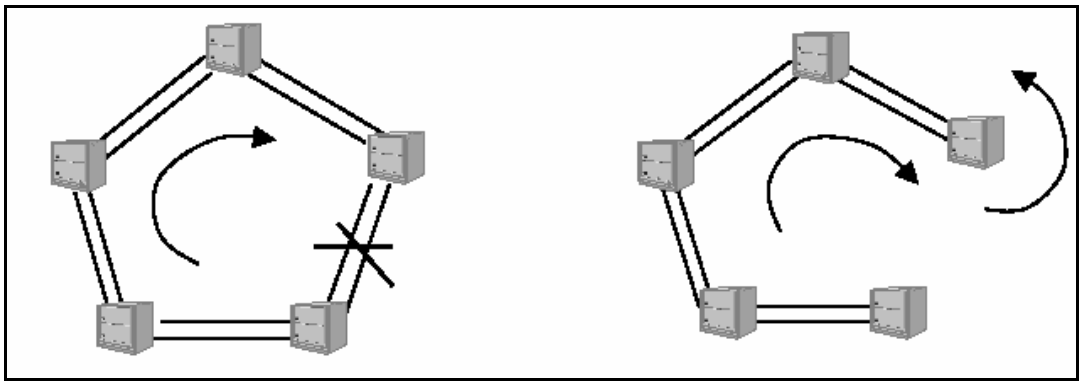


Figura 2.16 Topología en Anillo[57]

Esta topología resulta adecuada cuando la separación entre nodos es muy grande. Es muy utilizada en las redes de transporte de fibra óptica de operadores públicos de telefonía y televisión por cable[58].

- **Bus.-** todos los equipos terminales se encuentran conectados a un mismo medio de transmisión, normalmente metálico, por el cual se difunde la información. Es necesario arbitrar una técnica para acceder al medio compartido a fin de enviar información. Un nodo no depende del resto para que la información circule, por lo que su fiabilidad aumenta notablemente.

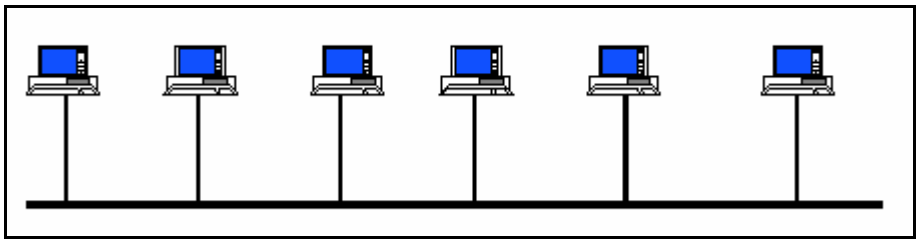


Figura 2.17 Topología en Bus[59]

Utiliza la transmisión punto a multipunto. El canal o medio de transmisión se usa de forma muy eficiente, pues todas las transmisiones circulan por él. Esto mismo puede provocar problemas de saturación cuando el

[57] http://trajano.us.es/~rafa/ARSS/apuntes/tema2.pdf
[58] http://trajano.us.es/~rafa/ARSS/apuntes/tema2.pdf
[59] http://trajano.us.es/~rafa/ARSS/apuntes/tema2.pdf

número de equipos que desean transmitir en el medio compartido es excesivo. La localización de fallos en la comunicación es difícil y la longitud máxima del Bus se encuentra acotada por falta de regeneración en la señal.

Es una topología de bajo coste, y muy utilizada en las redes de área local, dónde el número de usuarios no resulta muy elevado y se encuentran concentrados en un espacio reducido[60].

En Telconet se utiliza una topología hibrida de acuerdo a las necesidades del backbone para ampliar la cobertura del mismo, es así que se utilizan varias topologías básicas combinadas para lograr este propósito.

[60] http://trajano.us.es/~rafa/ARSS/apuntes/tema2.pdf

CAPITULO 3.

DISEÑO DE LA RED BANCARIA

3.1 EQUIPOS DE COMUNICACIÓN A IMPLANTARSE AL BACKBONE DE TELCONET

Como se indicó en el capítulo anterior, Telconet tiene una infraestructura de backbone basada en la tecnología MEN, a la que se incorporarán 2 nuevos nodos, denominados ClickCenter y Tarqui2.

Actualmente se tiene estos nodos solo como parte de la red, pero no como parte del backbone, de los cuales dependen varios clientes. Los enlaces de cada nodo se concentran en switches 3com office connect de 8 puertos.

Clientes que dependen de ClickCenter:

Cliente	Ancho de Banda (Kbps)
Colegio Alemán	512
Cyber Click	128
Colegio Mediterráneo	256
Seguros Colonial – Presidencia	64

Tabla 3.1 Clientes nodo ClickCenter (actual)

Clientes que dependen de Tarqui2

Cliente	Ancho de Banda (Kbps)
Cabinatel	128
Cliente Cueva	64
Cliente Montaquiza	128
Cliente Argotti	128
Micomisariato Villaflora	128

Tabla 3.2 Clientes nodo Tarqui2 (actual)

El control de los anchos de banda respectivos se los realiza directamente en los equipos Linux instalados en cada cliente, pero esto no garantiza un control 100% efectivo, ya que se trabaja con los paquetes de CBQ en Linux para el control de ancho de banda y con esto se tiene un 30% +/- de efectividad.

Todos estos enlaces se añaden a nodos principales de Telconet, por medio de los respectivos switches 3com office connect, y trabajan en la VLAN por defecto de Telconet.

Para poder ofrecer el servicio de conexión a la institución bancaria y a otros clientes es necesario fortalecer estos nodos, actualizando la infraestructura de los mismos.

Los clientes pendientes por instalar son:

Dependientes del nodo ClickCenter:

Cliente	Ancho de Banda (Kbps)
Agencia Cumbaya (Banco)	128
Cyber Xavier	128
Puembo	512
Fybeca Cumbaya	128
Juan Marcet Cumbaya	128

Tabla 3.3 Clientes nodo ClickCenter (por instalar)

Dependientes del nodo Tarqui2:

Cliente	Ancho de Banda (Kbps)
Agencia San Rafael (Banco)	128
Aki Conocoto	128
Etranspi	128

Tabla 3.4 Clientes nodo Tarqui2 (por instalar)

De los datos citados en las tablas anteriores, se puede observar los siguientes datos de forma gráfica:

Tráfico nodo ClickCenter:

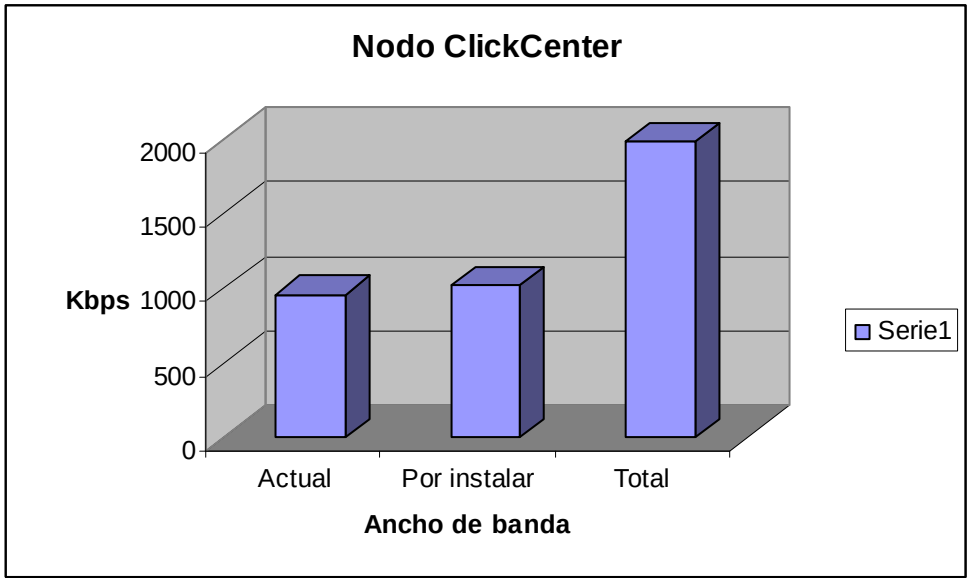


Figura 3.1 Datos de tráfico del nodo ClickCenter

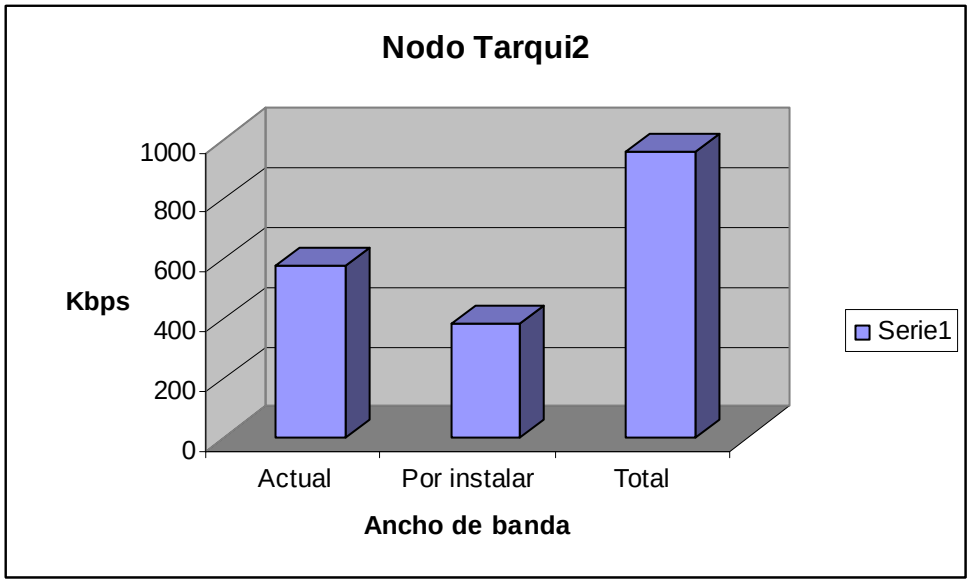


Figura 3.2 Datos de tráfico del nodo Tarqui2

Como se observa la tendencia de estos nodos es creciente, tanto en ancho de banda como en nuevos clientes, que por la ubicación estratégica abarca los valles principales de Quito.

En base a estas nuevas demandas se presentan dos alternativas de enlaces para los clientes, y en especial para la institución bancaria:

- Enlaces de Fibra óptica, que ente sus ventajas están proporcionar estabilidad, soportar altos volúmenes de tráfico, no es susceptible a interferencias en la transmisión de información, etc.
- Enlaces de Radio, con los que se puede alcanzar sitios o lugares que por su ubicación geográfica son inaccesibles para llegar con cableado de fibra óptica.

De estas dos alternativas con las que cuenta Telconet, para las agencias bancarias, se elige la transmisión de datos por medio de fibra óptica, por las ventajas antes mencionadas.

3.1.1 EQUIPOS DE COMUNICACIÓN PARA LOS NODOS

De acuerdo a la tecnología MEN utilizada en el backbone se debe adaptar equipos que tengan las características necesarias para cubrir las necesidades de Telconet.

Entre algunos equipos que podrían utilizarse están:

	3Com SuperStack 3 Switch 3870	Nortel BaySack 450-24T Switch	Switch Cisco Catalyst 3550
Puertos Ethernet	24	24	24
Puertos GBIC	4	0	2
Spanning Tree	IEEE 802.1w Rapid Spanning Tree, IEEE 802.1s Multiple Spanning Tree	No ofrece enlaces redundantes	Redundancia totalmente a fallos con soporte para bucle de prueba y Uplink Fast para funcionar con spanning tree robusto
VLAN	Utiliza 255 VLANs para controlar y asegurar el tráfico de red, 802.1Q	Soporta 802.1Q	Se puede crear enlaces VLAN desde cualquier puerto, utilizando tanto trunking basado en el estándar 802.1Q, como la arquitectura ISL VLAN propia de cisco
Capa en la que trabaja	2 para control por MAC Address, capa 3 para control por direcciones IP, capa 4 para control por puerto de servicio	2 para control por MAC Address, capa 3 para control por direcciones IP	2 para control por MAC Address, capa 3 para control por direcciones IP, capa 4 para control por puerto de servicio
Garantía	De por vida	1 año	De por vida
Precio USD	3100	1495	2639

Tabla 3.5 Comparación entre 3 marcas de switches

Se escogió entre estas 3 marcas de switches principalmente porque son los que tienen mayor aceptación en el mercado de las comunicaciones.

De las 3 alternativas se escogió los switches cisco catalyst 3550, los que se incorporarán al Backbone de Telconet en los lugares o nodos en donde no se los ha implementado y que son primordiales para la dependencia de las agencias del banco. Esto es para formar las VLANs que darán la conectividad a las diferentes agencias con la matriz bancaria.

Los switches catalyst 3550 serán implementados en los siguientes nodos:

Nodo ClickCenter: Para la agencia Cumbayá.

Nodo Tarqui2: Para la agencia San Rafael.

Los switches catalyst 3550 reemplazarán a los switches 3com office connect, ya que estos equipos están funcionando solo para difundir la señal, son equipos no administrables y no se puede hacer ninguna configuración sobre ellos.

Se eligió poner los switches cisco catalyst 3550 por las siguientes razones:

- De acuerdo a la ubicación de los nodos y al crecimiento del backbone de Telconet para poder llegar a los valles de la ciudad de Quito, es necesario fortalecer los nodos, tanto para poder ofrecer la conectividad a la institución bancaria como para poder expandir el backbone y abarcar mas clientes en dichos sectores.
- Son equipos administrables, que trabajan tanto a nivel de capa 2 y capa 3 de acuerdo al modelo OSI, esto ofrece muchos beneficios al momento de administrar la red y brindar soluciones de acuerdo a las necesidades de los clientes.
- Los switches catalyst 3550 tienen ventajas relacionados con sus homólogos catalyst 2950 (inferior) y catalyst de la familia 4000 (superior) que básicamente son:
    - El switch catalyst 2950 no maneja control de ancho de banda por puerto, y no tiene implementado funciones de ruteo, el switch catalyst 3550 si hace funciones de router y también maneja QoS (Calidad de Servicio) para poder controlar políticas de ancho de banda por cada uno de sus puertos, esto es necesario para poder garantizar el ancho de banda contratado por los clientes.
    - El switch catalyst 3550, en esta época, se esta promocionando por parte de Cisco a nivel latinoamericano, con reducción de costos de 10 y 20 % del precio normal, y sobre todo ofrece las funcionalidades requeridas por Telconet sin necesidad de adquirir switches catalyst de la familia 4000 que por sus funcionalidades y capacidades tienen costos muy elevados.
- Para poder brindar el servicio a la institución bancaria es necesario formar VLANS independientes para ofrecer la seguridad de las conexiones, los switches catalyst 3550 permiten ésta funcionalidad.
- Para poder ofrecer confiabilidad a la red bancaria es necesario tener backups de conexión en todos los nodos de los que dependa una localidad bancaria, así, con los switches catalyst 3550 se podrá formar anillos de backup por medio del protocolo spanning tree.

- El estándar de Telconet en la infraestructura de su backbone son switches catalyst 3550, los nodos en donde se ubicarán los nuevos switches serán parte del backbone.

3.2 DISEÑO FISICO DE LA RED BANCARIA

Para llevar acabo el diseño físico de la red bancaria se tomarán en cuenta los siguientes puntos:

- Selección de la tecnología.
- Selección de los dispositivos de red.
- Diseño de la infraestructura de la red.
- Costos de instalación.

3.2.1 SELECCIÓN DE LA TECNOLOGÍA

La tecnología que se utilizará en la interconexión de las agencias con la matriz del banco es MEN (Metro Ethernet Network), ya que el backbone de Telconet utiliza este tipo de infraestructura, en decir, se añadirán VLANS a la MEN que sean exclusivas para estas comunicaciones por medio de los dispositivos switches catalyst 3550, los mismos que permiten configurar VLANS.

Se implementará la tecnología de VLANS por las siguientes razones:

- Seguridad de las comunicaciones entre las agencias con la matriz bancaria.
- Independencia de los dominios de broadcast.
- Es adaptable a la infraestructura de Telconet.
- Configuración y administración remota de las VLANS.

Se utilizarán enlaces de fibra óptica desde el nodo de Telconet asignado hacia la agencia bancaria que dependerá del mismo. La tecnología de transmisión por fibra óptica a utilizarse se deriva de las siguientes ventajas:

- Velocidad en la transmisión de datos, necesaria para la comunicación de las operaciones bancarias.
- Amplia capacidad de transmisión de datos, para las operaciones bancarias que necesiten realizar backups o transferencia de datos en gran cantidad.

- Confiabilidad en la comunicación, puesto que con los enlaces de fibra óptica se cuenta con tiempos de respuesta muy bajos (velocidad), y no se tienen perdidas en el canal (perdidas o duplicados de paquetes), con lo que asegura la confiabilidad de los datos transmitidos.
- Cabe indicar que los enlaces de fibra óptica requieren personal técnico especializado para realizarlo, pero las ventajas y la disponibilidad que se obtiene brindan las garantías a la comunicación entre las agencias con la matriz bancaria.

3.2.2 SELECCIÓN DE LOS DISPOSITIVOS DE RED

Como se menciona anteriormente el backbone de Telconet esta formado por una MEN con switches catalyst 3550, por lo tanto los principales dispositivos son estos switches, a los cuales se conectarán los enlaces de fibra óptica de cada nodo de la red bancaria.

La fibra óptica a utilizase es monomodo de 9 micras con conectores SC, es parte también del estándar de Telconet, cabe señalar que este es el medio físico de transmisión por tanto pertenece a la capa física de acuerdo al modelo de referencia OSI.

A continuación se muestra una tabla de valores de acuerdo al medio de transmisión:

Estándar	Sub Capa MAC	Medio Físico	Distancia Máxima	Observaciones
1Base5	802.3	Cable Coaxial	500 m	
10 Base2	802.3	Cable Coaxial de 50 ohms (thin coaxial) RG58	185 m	Soporta hasta 30 terminales conectadas. Conectores AUI. Topología en bus serial
10Base5	802.3	Cable Coaxial de 50 ohms (tick coaxial)	500 m	Soporta hasta 208 usuarios. Conectores AUI. Utilizando repetidores, 2500 m máximo y 1024 usuarios
10BaseT	802.3	UTP categoría 3,4 ó 5	100 m	Conectores RJ-45. Topología en estrella. Utiliza 2 pares de cables de un cable de par trenzado
10Broad36	802.3	Cable Coaxial	3.600 m	Servicio de 10 Mbps de banda ancha
100BaseFX	802.3	Dos hilos de fibra óptica multimodo de 62.5/125 micrones	400 m	Conectores ST o SC. Topología punto a punto
100BaseFX	802.3u	Fibra óptica monomodo	10.000 m	
100BaseT	802.3	Cable UTP		Utiliza la misma frecuencia de transmisión que 10BaseT, enviando mayor cantidad de información en cada pulso.
100BaseT2	802.3u	Cable UTP cat. 3,4 ó 5	100 m	
100BaseT4	802.3u	Cable UTP cat. 3,4 ó 5	100 m	Utiliza los 4 pares de cables
100BaseTX	802.3u	Cable UTP cat. 5,6 ó 7 ó STP	100 m	Fast-Ethernet utiliza 2 pares de cables
1000BaseT	802.3ab	UTP categoría 5	100 m	
1000BaseCX	802.3z	Par trenzado de cobre blindado	25 m	
1000BaseSX	802.3z	Fibra óptica multimodo de 62.5 y 50 micrones		260 m
1000BaseLX	**802.3z**	**Fibra óptica monomodo de 9 micrones**	**3.000 a 10.000 m**	
ARCnet		Coaxial		Bus LAN de token de 2.5 Mb desarrollado por Datapoint Corporation.

Tabla 3.6 Valores de transmisión estándar de acuerdo al medio físico[61]

[61] http://www.ufps.edu.co/cisco/docs/docCCNA/fastnoteccnav22.pdf

Como se puede observar en la tabla anterior, la fibra óptica monomodo de 9 micrones alcanza distancias de 3 a 10 Km., éstos valores en el área metropolitana brinda muy buena cobertura.

Los conectores de fibra óptica que se utilizarán son tipo SC ya que por la forma cuadrada del conector existen menos posibilidades de un desfase que pueda afectar la conectividad de los equipos.

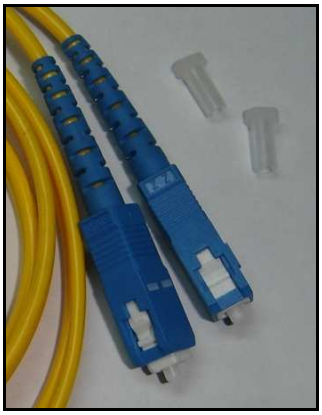


Figura 3.3 Conectores SC

Los dispositivos para la conectividad de fibra óptica muy importantes son los transceivers, encargados de convertir la energía luminosa en eléctrica y viceversa, en este caso los dispositivos a utilizarse son transceivers de 2 hilos(Tx/Rx) monomodo, uno en cada extremo de la conexión.
Los cables de conexión entre los transceivers hasta los switches catalyst por un lado y por el otro desde los transceivers hacia los dispositivos del banco, son patch-cord RJ45 CAT-5 con el estándar 568B.

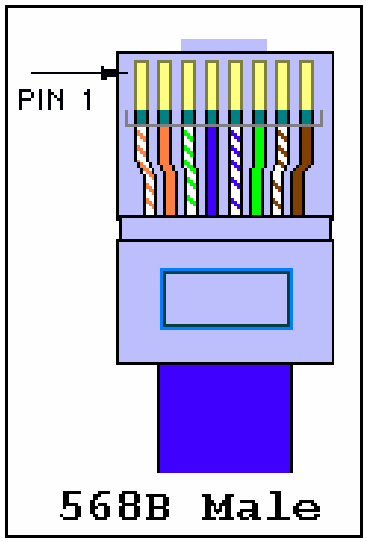


Figura 3.4 Conector RJ45 estándar 568B[62]

Con los dispositivos ya mencionados se realizará las conexiones físicas de última milla por medio de fibra óptica.

3.2.3 DISEÑO DE LA INFRAESTRUCTURA DE LA RED

En el diseño de la infraestructura de la red bancaria básicamente se identifican los nodos de los cuales dependerán cada uno de los enlaces, así se tiene el siguiente cuadro de distribución:

Localidad Bancaria	Nodo Dependiente	Distancia (Km.)
Matriz Bancaria	Fondo	0,8
Agencia Cotocollao	Telepuerto	3
Agencia América	OPS	2,5
Agencia Amazonas	Cofiec	1,5
Agencia San Rafael	Tarqui2	14
Agencia Issac Barrera	Gaspar	0,8
Agencia Villaflora	Sur2	2
Agencia Cumbaya	ClickCenter	0,5
Agencia Iñaquito	Gosseal	2
Agencia Parkenor	Telepuerto	1,5
Agencia Alameda	SwissHotel	3

Tabla 3.7 Dependencias bancarias con cada nodo

Por lo detallado en la tabla se tiene la conectividad de los enlaces graficados de la siguiente manera:

[62] http://www.coopconesa.com.ar/coopconesa/red/

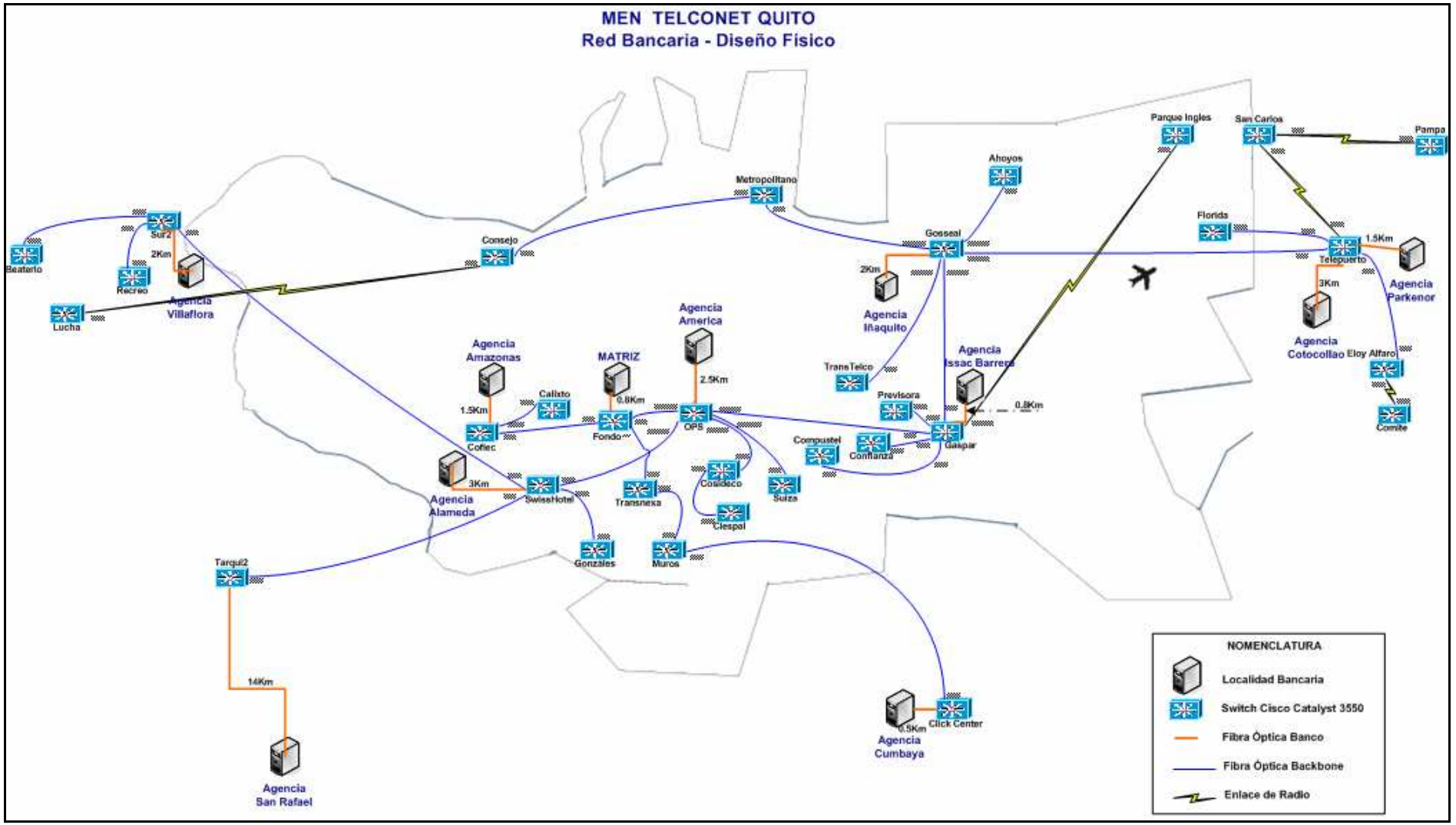


Figura 3.5 Diseño Físico – Red Bancaria

Como se observa en el mapa, cada localidad bancaria depende de un switch catalyst, por la ubicación geográfica estarán enlazados al nodo más cercano, que forman parte de la MEN.

3.2.4 COSTOS DE INSTALACIÓN

Para describir de manera detallada los costos se los ha divido en 3 tipos:

- Costos de Equipos
- Costos de Recursos Humanos
- Costos de Materiales

Costos de equipos:

Cantidad	Descripción	Utilización	Precio Unitario	Precio Total
2	Switches cisco catalyst 3550	Infraestructura del backbone	2639	5278
1	PC con Windows 2000 Professional	Monitoreo de la red bancaria	715	715
1	Servidor supermicro	Servidor VLAN	910	910
			TOTAL:	**6903**

Tabla 3.8 Costos de equipos

Costos de Recursos Humanos:

Cantidad	Descripción	Utilización	Precio Unitario	Precio Total
10	Diseño del proyecto, costo por día.	Técnico de Telconet	50	500
31600	Mano de obra del tendido de fibra óptica, costo por metro	Tendido de Fibra óptica	0,6	18960
632	Mano de obra de la colocación de herrajes en la postería	Cada 50 metros se coloca un herraje	1,5	948
44	Mano de obra de fusión de hilos de fibra, costo por cada hilo fusionado	Fusión de fibra óptica	18	792
			TOTAL:	**21200**

Tabla 3.9 Costos de recursos humanos

Costos de Materiales:

Cantidad	Descripción	Utilización	Precio Unitario	Precio Total
31600	Fibra óptica monomodo de 9 micrones, costo por metro	Tendido de Fibra óptica	0,55	17380
632	Herrajes para poste	Cada 50 metros se coloca un herraje	5	3160
22	Patch Cord de fibra óptica	Para fusionar con los hilos de fibra óptica de la acometida externa	25	550
22	Patch Cord de cable UTP Cat. 5	Conectorización	3	66
11	Caja para empalmes de fibra óptica	Empalmado de fibra óptica	38	418
22	Transeivers de fibra óptica monomodo	Conectorización de la fibra óptica	130	2860
160	Hojas impresas a tinta	Impresión del diseño del proyecto	0,25	40
320	Copias	2 copias de la impresión del diseño del proyecto	0,05	16
3	Anillados	1 original y 2 copias	2	6
2	CD RW	Respaldos de configuración de equipos y diseño del proyecto	2	4
			TOTAL:	**24500**

Tabla 3.10 Costos de Materiales

Costo total del proyecto:

Tipo de Costo	Precio
Equipos	6903
Recursos Humanos	21200
Materiales	24500
TOTAL USD	**52603**

Tabla 3.11 Costo total del proyecto

De los costos especificados, y de acuerdo a un breve análisis se estima que la inversión será recuperable en aproximadamente 10 meses, sin embargo se tendrá más disponibilidad en los nuevos nodos y más cobertura para nuevos clientes, también subirá el status presencial de Telconet en comunicaciones, prestando servicios confiables y seguros a empresas financieras.

El costo mensual que Telconet cobrará por los enlaces dedicados, no depende del número de transacciones que el banco realice en cada agencia, simplemente se cobrará por el arriendo de los enlaces por el ancho de banda provisto.

Así, Telconet recaudará la suma de 5000 USD mensuales a la Institución Bancaria por los siguientes enlaces dedicados:

Localidad Bancaria	Ancho de banda (Kbps)
Agencia Cotocollao	128
Agencia América	128
Agencia Amazonas	1536
Agencia San Rafael	128
Agencia Issac Barrera	128
Agencia Villaflora	128
Agencia Cumbaya	128
Agencia Iñaquito	128
Agencia Parkenor	128
Agencia Alameda	512
Matriz Bancaria	2560

Tabla 3.12 Ancho de banda contratado por localidad bancaria

3.3 DISEÑO LÓGICO DE LA RED BANCARIA

En el diseño de la red lógica bancaria se tomaran en cuenta varios ítems:

- Diseño de la topología de red.
- Diseño del modelo de direccionamiento.
- Enrutamiento de redes.

3.3.1 DISEÑO DE LA TOPOLOGÍA DE RED

La topología de la red bancaria de manera lógica será en estrella, ya que la tendencia de las conexiones es centralizada desde la matriz hacia las agencias bancarias y viceversa. El siguiente mapa de red muestra la topología en estrella de la red bancaria:

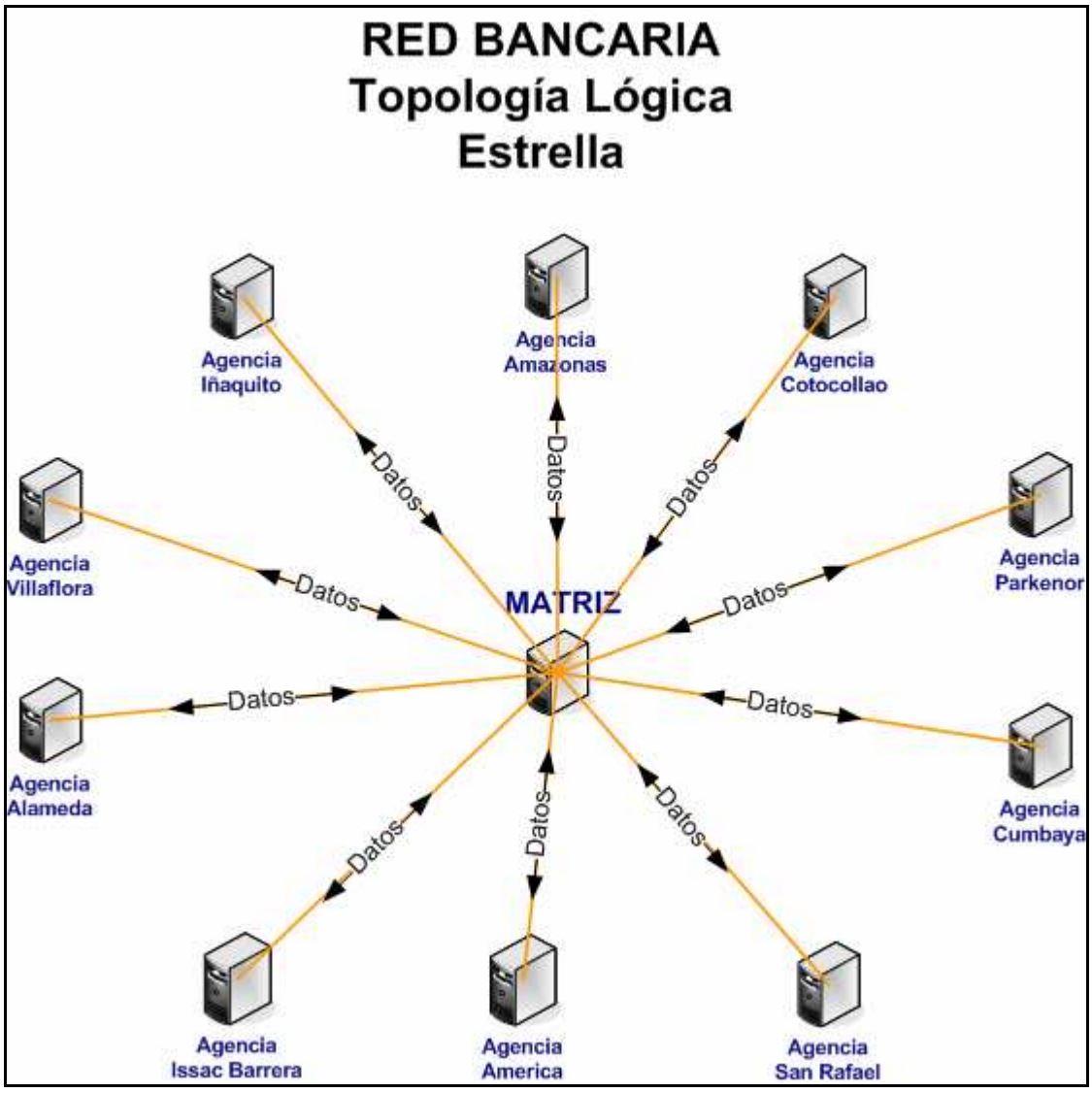


Figura 3.6 Topología lógica en estrella

Básicamente se observa que los datos fluyen desde la matriz hacia cada una de las agencias, puede ser cualquier información ya que no hay restricciones en el canal de comunicación de cada agencia, pero en particular es la conexión a los servidores de BBD, por lo mismo se forma una topología centralizada.

3.3.2 DISEÑO DEL MODELO DE DIRECCIONAMIENTO

El modelo de direccionamiento se basa en el protocolo TPC/IP, puesto que las direcciones IP con las que se interactúa pertenecen a éste protocolo.

La familia de protocolos TCP/IP fue diseñada para permitir la interconexión entre distintas redes. El mejor ejemplo de interconexión de redes es Internet: se trata de un conjunto de redes unidas mediante encaminadores o routers.

El siguiente es un ejemplo de interconexión de 3 redes. Cada host (ordenador) tiene una dirección física que viene determinada por su adaptador de red. Estas direcciones se corresponden con la capa de acceso al medio y se utilizan para comunicar dos ordenadores que pertenecen a la misma red. Para identificar globalmente un ordenador dentro de un conjunto de redes TCP/IP se utilizan las direcciones IP (capa de red). Observando una dirección IP se sabe si pertenece a la propia red o a una distinta[63].

Host	Dirección física	Dirección IP	Red
A	00-60-52-0B-B7-7D	192.168.0.10	
	00-E0-4C-AB-9A-FF	192.168.0.1	Red 1
R1	A3-BB-05-17-29-D0	10.10.0.1	
B	00-E0-4C-33-79-AF	10.10.0.7	
	B2-42-52-12-37-BE	10.10.0.2	Red 2
R2	00-E0-89-AB-12-92	200.3.107.1	
C	A3-BB-08-10-DA-DB	200.3.107.73	
D	B2-AB-31-07-12-93	200.3.107.200	Red 3

Tabla 3.13 Direcciones IP del ejemplo de interconexión de 3 redes[64]

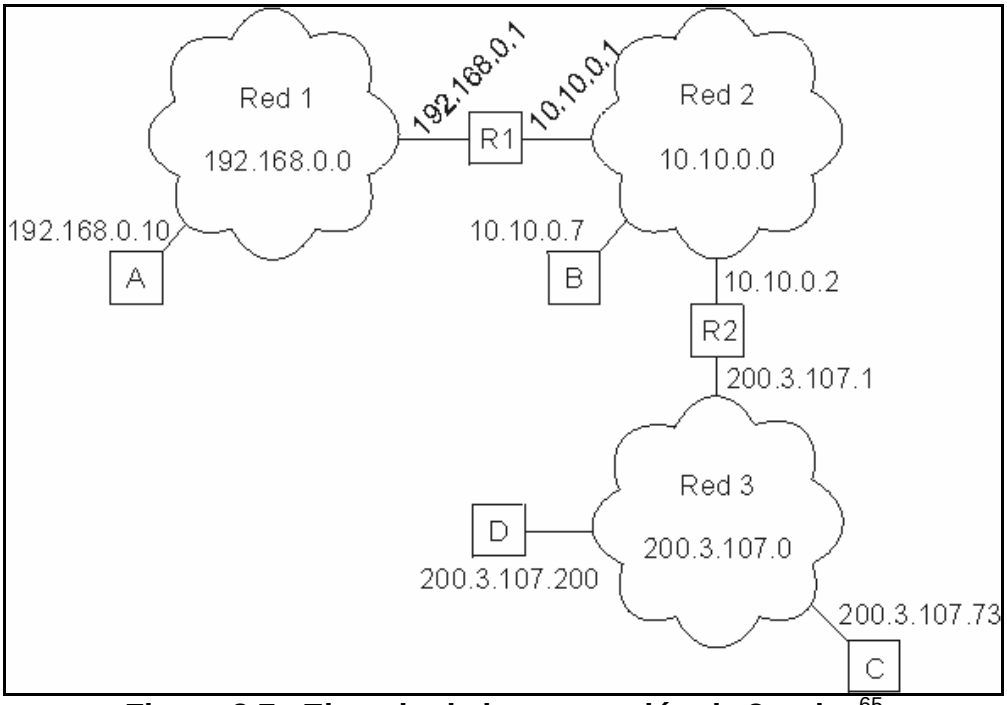


Figura 3.7 Ejemplo de interconexión de 3 redes[65]

[63] http://www.saulo.net/pub/tcpip/a.htm#2
[64] http://www.saulo.net/pub/tcpip/a.htm#2

El concepto de red está relacionado con las direcciones IP que se configuran en cada ordenador, no con el cableado. Es decir, si se tiene varias redes dentro del mismo cableado solamente los ordenadores que permanezcan a una misma red podrán comunicarse entre sí. Para que los ordenadores de una red puedan comunicarse con los de otra red es necesario que existan routers que interconecten las redes. Un router o encaminador no es más que un ordenador con varias direcciones IP, una para cada red, que permita el tráfico de paquetes entre sus redes.

La capa de red se encarga de fragmentar cada mensaje en paquetes de datos llamados datagramas IP y de enviarlos de forma independiente a través de la red de redes. Cada datagrama IP incluye un campo con la dirección IP de destino. Esta información se utiliza para enrutar los datagramas a través de las redes necesarias que los hagan llegar hasta su destino.

En el ejemplo anterior, el ordenador 200.3.107.200 (D) envía un mensaje al ordenador con IP 200.3.107.73 (C). Como ambas direcciones comienzan con los mismos números, D sabrá que ese ordenador se encuentra dentro de su propia red y el mensaje se entregará de forma directa. Sin embargo, si el ordenador 200.3.107.200 (D) tuviese que comunicarse con 10.10.0.7 (B), D advertiría que el ordenador destino no pertenece a su propia red y enviaría el mensaje al router R2 (es el ordenador que le da salida a otras redes). El router entregaría el mensaje de forma directa porque B se encuentra dentro de una de sus redes (la Red 2).

3.3.2.1 Direcciones IPv4

El protocolo IPv4 utiliza un modelo de direccionamiento, de forma que a cada interface de cada dispositivo se le asigna una dirección independientemente de su dirección MAC, que es la que utilizan los protocolos de nivel de enlace. La dirección IP destino es un dato que debe ser suministrado por las aplicaciones que corren en el propio dispositivo al protocolo IP. La dirección IP origen la obtiene de los datos de configuración de la interfaz. Estas direcciones IP constan de 32 bits y para su representación se emplea la notación decimal de puntos

[65] http://www.saulo.net/pub/tcpip/a.htm#2

(X.X.X.X). Ésta consiste en 4 números decimales separados por un punto, por ejemplo:
@IP = 194.110.100.200

El ámbito de cada valor es de 0 a 255, dado que corresponden a 1 octeto, es decir, 8 bits. Su representación hexadecimal sería:
@IP = C2.6E.64.C8

y la representación binaria:
@IP = 11000010.01101110.01100100.11001000

El valor más a la derecha sólo puede oscilar entre 1 y 254 porque el 255 está reservado a la dirección de broadcast y el 0 es indicativo de toda la red.
Todos los dispositivos tienen como dirección local propia 127.0.0.1, y que se identifica como localhost.
En Internet, para acomodar la estructura de direccionamiento a las diferentes necesidades de utilización, el ámbito de direcciones IP se ha agrupado en clases de forma que la simple inspección de una dirección IP permite conocer a que clase pertenece[66].
Estas clases son:

Clase	Prefijo
A	0
B	10
C	110
D	1110
E	1111

Tabla 3.14 Clases de las direcciones IP[67]

[66] http://people.ac.upc.edu/asalaver/cbxc_ip.pdf
[67] http://people.ac.upc.edu/asalaver/cbxc_ip.pdf

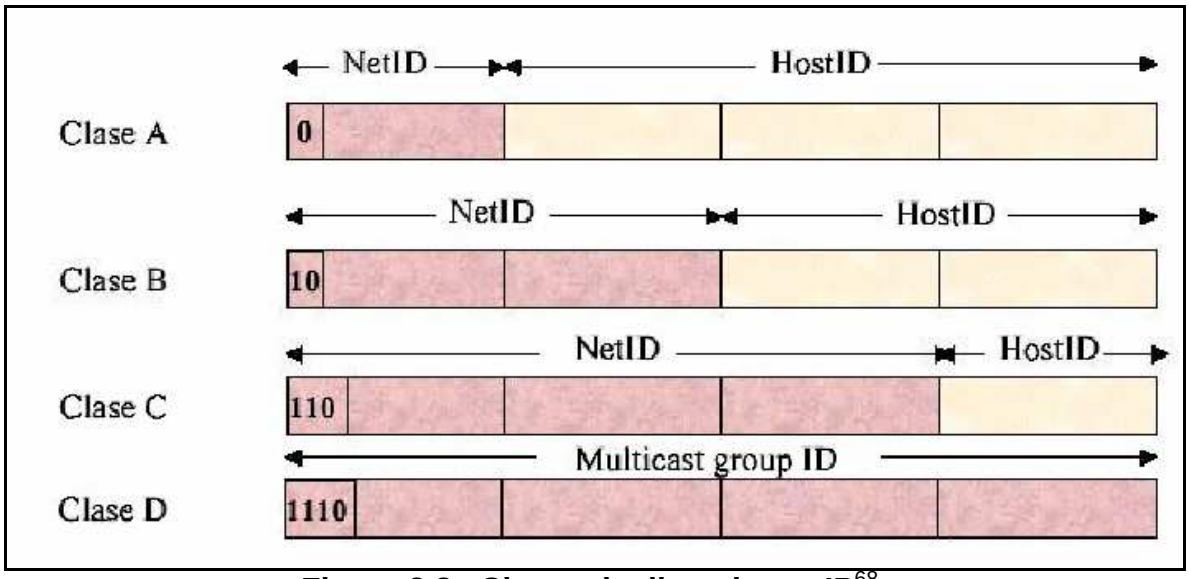


Figura 3.8 Clases de direcciones IP[68]

Clase A

7 bits para red y 24 bits para los dispositivos

Rango: de la 0.0.0.0 a la 127.255.255.255

Número de redes = 2 7 = 128

Número de dispositivos = 2 24 –2 = 16777214

Clase B

14 bits para red y 16 bits para los dispositivos

Rango: de la 128.0.0.0 a la 191.255.255.255

Número de redes = 2 14 = 16384

Número de dispositivos = 2 16 –2 = 65534

Clase C

21 bits para red y 8 bits para los dispositivos

Rango: de la 192.0.0.0 a la 223.255.255.255

Número de redes = 2 21 = 2097152

Número de dispositivos = 2 8 –2 = 254

[68] http://people.ac.upc.edu/asalaver/cbxc_ip.pdf

Clase D

28 bits para multicasting

Rango: de la 224.0.0.0 a la 238.255.255.255

Clase E

28 bits experimental

Rango: de la 240.0.0.0 a la 247.255.255.255

3.3.2.2 Máscaras

Con posterioridad a la definición inicial del protocolo IP aparecen las máscaras, y es como consecuencia de la necesidad de subdividir las redes en varias subunidades y cada una de ellas con un grupo de direcciones IP distinto (RFC 950).

Estas máscaras constan de 4 octetos (32 bits), igual que una dirección IP y por como se utilizan deben contener unos a la izquierda y ceros a la derecha, es decir, no pueden haber mezclas de unos y ceros. Por ejemplo

Máscara = 1111 1111.1111 1111.1111 0000.0000 0000

Como siempre la máscara va asociada a la dirección IP, en estos casos se indica con /XX a continuación de la dirección IP, siendo XX el número de unos de la máscara. En el ejemplo sería /20.

En Internet es habitual el empleo de las siguientes máscaras para cada clase:

Clase	Máscara
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Tabla 3.15 Máscaras de Red[69]

Es característico del protocolo IP el hecho de que las máscaras no viajan en los mensajes IP, es decir, se emplean de forma local en cada dispositivo[70].

[69] http://people.ac.upc.edu/asalaver/cbxc_ip.pdf
[70] http://people.ac.upc.edu/asalaver/cbxc_ip.pdf

3.3.2.3 A.R.P.

El sistema de direccionamiento del protocolo IP plantea un problema desde el punto de vista de direccionamiento del nivel físico. Por ejemplo en una red local Ethernet, dos dispositivos solo pueden comunicarse si se conocen sus respectivas direcciones físicas (MAC).

En base a su funcionamiento, el protocolo ARP es de nivel de red según el modelo de referencia OSI y sus especificaciones están desarrolladas en la RFC 826.

El protocolo ARP permite encontrar las direcciones físicas basándose en las direcciones IP de los dispositivos. Para ello se realiza:

- Primero, una solicitud de tipo broadcast de un paquete ARP conteniendo entre otros datos la dirección IP que se desea localizar. Todos los dispositivos de la red reciben este mensaje.
- Segundo, solamente aquel dispositivo cuya dirección IP coincida con la recibida, responde con otro paquete de respuesta del protocolo ARP. Este paquete contiene la dirección física (MAC) de dicho dispositivo. Al recibirse la respuesta, el primer dispositivo "aprende" la dirección física (MAC) del segundo.

Esta información se mantiene en memoria caché para posteriores envíos. Las entradas en la memoria caché se asocian a un temporizador para permitir la modificación dinámica de la dirección física de los dispositivos porque:

- La dirección IP puede ser cambiada por necesidades de operación y;
- La dirección física MAC también cambia si se cambia su tarjeta de red.

Las llamadas al protocolo ARP proceden de los protocolos de nivel de enlace, ya que estos son los que reciben los paquetes del protocolo IP con sus direcciones IP, y que para construir su trama requieren de las direcciones MAC equivalentes a estas direcciones IP.

El protocolo ARP cuando recibe la solicitud de una dirección MAC sigue el procedimiento siguiente:

- Primero consulta en la tabla ARP del propio dispositivo.
- Si se encuentra dicha dirección IP en la tabla ARP, responde con la correspondiente dirección física.
- Sí no está en la tabla ARP, envía una solicitud ARP de broadcasting.
- Cuando recibe la respuesta, almacena la dirección IP y la física correspondiente en su tabla ARP para posibles usos futuros.

Estructura del paquete.- El mensaje ARP corresponde al campo de datos del protocolo de nivel de enlace de la red en cuestión. Así si es una red 802.3/Ethernet con protocolo 802.2 SNAP, los campos SAP origen y destino contienen el número 170, y el campo de tipo de Ethernet 2054, indicativo de que se trata de un mensaje ARP. Por esta razón se considera que es un protocolo de nivel de red según el modelo de referencia OSI.
Los campos de la dirección física del destino van a 0 en el mensaje de búsqueda. El dispositivo destino insertará aquí su dirección física en el mensaje ARP de respuesta[71].

3.3.2.4 R.A.R.P. (Reverse A.R.P.)

Las especificaciones de este protocolo RARP están descritas en la RFC 903.
El protocolo RARP permite asignar direcciones IP a dispositivos sin unidades de disco y así resolver este problema. Para ello se utilizan mensajes del mismo tipo que los del protocolo ARP.
Todos los dispositivos con interface de red tiene una dirección física MAC pero en nuestro caso, estos dispositivos no disponen de dirección IP, por lo que no pueden comunicarse con protocolos de niveles superiores al de enlace. Por esta razón este protocolo RARP funciona a nivel de red según el modelo de referencia OSI.
El proceso comienza cuando un dispositivo envía una solicitud de dirección IP. En la respuesta se indica además de la dirección IP, la dirección física del dispositivo y a continuación se pone en estado de espera de una respuesta por parte de uno o varios servidores RARP que le indiquen su dirección IP.

[71] http://people.ac.upc.edu/asalaver/cbxc_ip.pdf

También debemos tener en cuenta, de que si los servidores RARP están fuera de servicio, los dispositivos pendientes de ellos, no podrán conectarse a la red.

El mensaje RARP corresponde al campo de datos del protocolo de nivel de enlace de la red en cuestión. Así si es una red 802.3/Ethernet con protocolo 802.2 SNAP, los campos SAP origen y destino contienen el número 170, y el campo de tipo de Ethernet 32821, indicativo de que se trata de un mensaje RARP. Por esta razón se considera que es un protocolo de nivel de red según el modelo de referencia OSI.

El protocolo RARP tiene “frame type = 0x8035” y “op= 3” en los mensajes de request y “op=4” en los mensajes de reply.

A diferencia de los mensajes de reply del protocolo ARP son del tipo broadcast, los mensajes de reply de RARP son unicast[72].

3.3.2.5 Direccionamiento de la red bancaria

De lo mencionado en los párrafos anteriores con respecto a las direcciones IP, la distribución de redes para la comunicación de las agencias con la matriz será dispuesta de la siguiente manera:

Red	Agencias	# VLAN
172.26.117.172/30	Agencia Cotocollao	160
172.26.117.152/30	Agencia América	161
172.26.117.156/30	Agencia Amazonas	162
172.26.117.160/30	Agencia San Rafael	163
172.26.117.164/30	Agencia Issac Barrera	164
172.26.117.176/30	Agencia Villaflora	166
172.26.114.252/30	Agencia Cumbaya	168
172.26.113.232/30	Agencia Iñaquito	169
172.26.114.240/30	Agencia Parkenor	175
172.26.114.248/30	Agencia Alameda	177

Tabla 3.16 Distribución de redes

Como se observa en la distribución de redes, se formarán redes que contengan solamente 2 direcciones IPs válidas, esto es, una IP será levantada sobre el servidor central (Servidor VLAN) de comunicación en el banco y la siguiente será asignada al equipo de comunicación de la agencia, el mismo que sirve de puerta de enlace para la red interna de la agencia.

[72] http://people.ac.upc.edu/asalaver/cbxc_ip.pdf

Además se formarán VLANS, una por cada agencia, todas las VLANS convergen en el servidor central (Servidor VLAN), que estará ubicado en la matriz del banco, y que a su vez interconectará todas las agencias con la matriz bancaria independientemente.

El Servidor VLAN, es un equipo con sistema operativo Linux Fedora Core 2, en el mismo que se crearán las VLANS y sobre las mismas se subirán las interfaces virtuales en el servidor para la conectividad de las agencias, se escogió este sistema operativo por las múltiples ventajas que tiene:

- Adaptable con TCP/IP.
- La configuración no es compleja.
- Esta versión de Linux esta probada y no se han tenido inconvenientes por parte de Telconet.
- Realiza con facilidad funciones de firewall, ruteo, entre otras.

Se escogió poner un servidor, en lugar de algún otro dispositivo (router, etc.), principalmente por los costos que representa, además en los equipos con sistema operativo Linux se puede realizar varias funciones, puesto que se llega hasta el nivel de aplicación, en cambio un router llega hasta el nivel de red,

El siguiente gráfico muestra la estructura de las direcciones IP y VLANS:

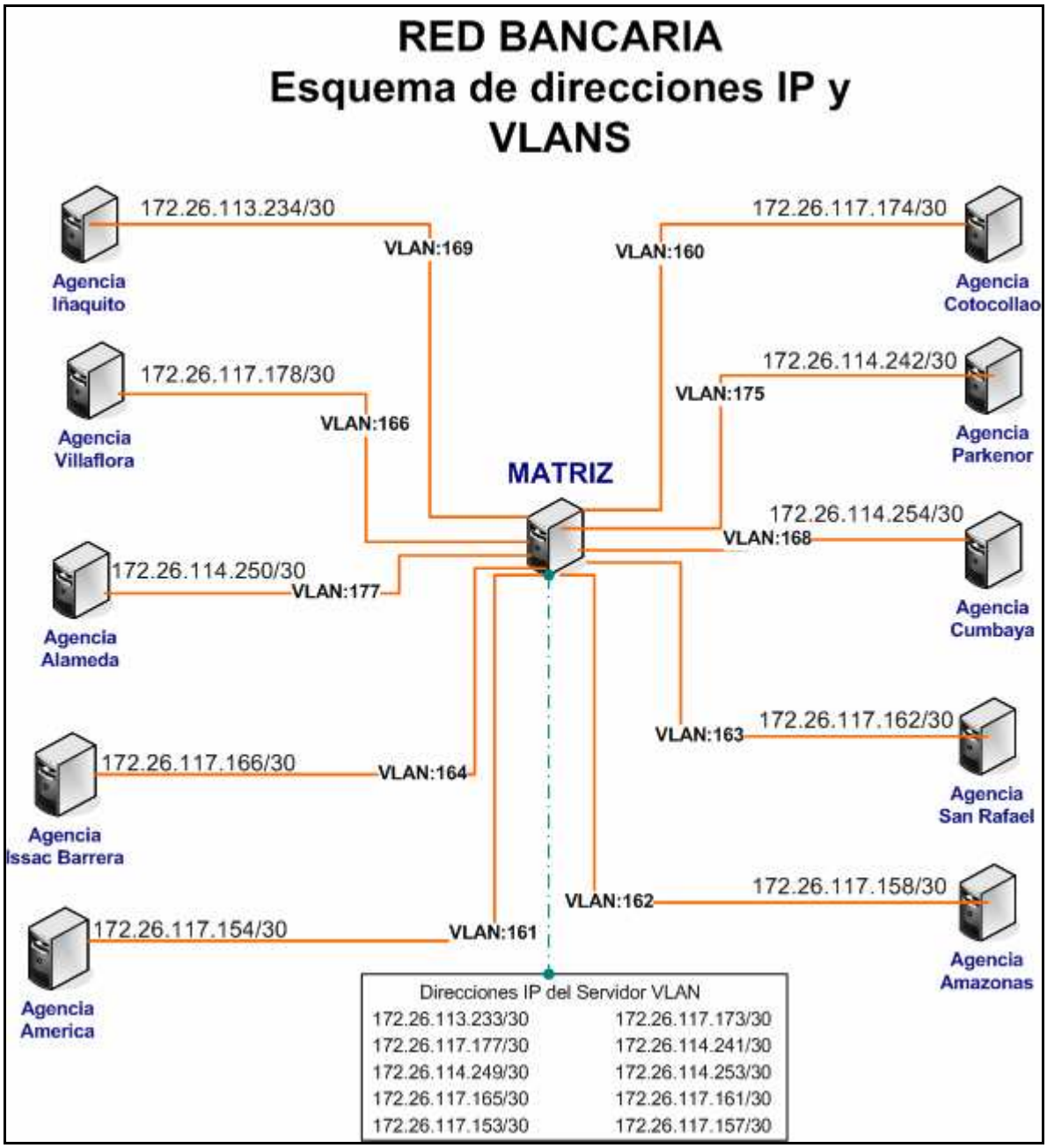


Figura 3.9 Esquema de direcciones IP y VLANS

Es necesario mencionar que los equipos a donde llegará cada enlace de cada agencia pertenecen a la institución bancaria, la misma que ha asignado las direcciones IP y el número de VLAN para la interconexión.

Las VLANS estarán implementadas entre el Servidor VLAN y el puerto del switch catalyst 3550, es decir, se debe configurar el número de VLAN en dicho puerto.

3.3.3 ENRUTAMIENTO DE REDES

Para realizar el ruteo de las direcciones IP's de las agencias se utilizará enrutamiento estático, ya que no se administrarán muchas redes, y porque los destinos a alcanzar de los paquetes son cortos, solamente deberán decidir por que VLAN encaminarse para alcanzar su destino final, éste enrutamiento se lo realizará en el Servidor VLAN.

Una interconexión de redes IP con enrutamiento estático no utiliza protocolos de enrutamiento como RIP para IP u OSPF para comunicar información de enrutamiento entre enrutadores. Toda la información de enrutamiento se almacena en una tabla de enrutamiento estático en cada enrutador. Debe asegurarse de que cada enrutador dispone de las rutas adecuadas en su tabla de enrutamiento, de manera que se pueda intercambiar tráfico entre dos extremos cualesquiera de la interconexión de redes IP[73].

Para una mejor comprensión a cerca de la forma de enrutamiento en la red bancaria se muestra un ejemplo de la comunicación de una agencia con la matriz:

[73] http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/2f31b4c2-b1ba-4d20-a18f-b7c9eb11649c.mspx

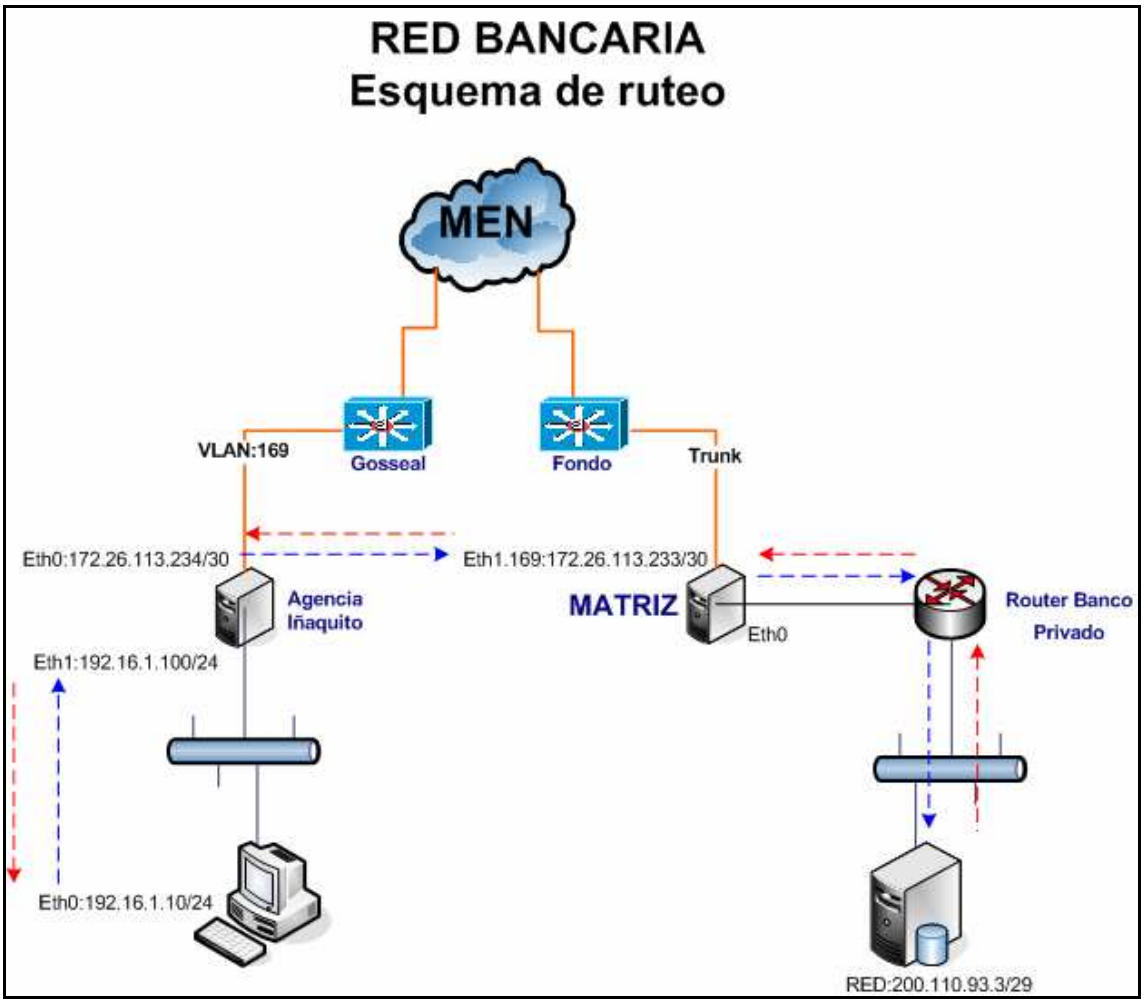


Figura 3.10 Esquema de ruteo estático

La PC (192.16.1.10) hace una petición al servidor de base de datos (BDD: 200.110.93.3) para alcanzar su destino y conseguir respuesta a su pedido realiza los siguientes saltos:

- Verifica que no es una dirección IP que esta dentro de su red, por lo que toma como camino su puerta de enlace, en este caso el equipo de comunicación con dirección IP 192.16.1.100 en la interfaz de red interna.
- El equipo de comunicación al no encontrar la dirección IP solicitada en sus interfaces, lo envía por su puerta de enlace a la interfaz levantada en el Servidor VLAN con dirección IP 172.26.113.233.
- El Servidor VLAN también envía el paquete por su puerta de enlace, en el caso del gráfico lo envía al Router Banco, este equipo es privado, que su a su vez alcanza la dirección IP solicitada por la PC.

- Una vez realizada la petición, el servidor de base de datos envía la respuesta por su puerta de enlace, que es el router privado, quien a su vez envía la información al Servidor VLAN.
- El Servidor VLAN que es administrado por Telconet verifica que el paquete esta dirigido para la dirección IP 192.16.1.10 por lo que busca en la tabla de rutas estáticas que para llegar a una instancia de esa red debe tomar el camino que tiene la dirección IP 172.26.113.234. La ruta agregada en el servidor dice lo siguiente:
    - Para alcanzar una dirección IP de la red 192.16.1.0/24 vaya por la dirección IP 172.26.113.234.
- Una vez que el paquete llega hacia el equipo de comunicación encuentra que la dirección IP 192.16.1.10 esta en su red, y a través de su interfaz interna hace llegar la información a la PC.

Este mismo esquema de ruteo se implementará en todas las agencias bancarias para interconectarlas con la matriz.

3.4 SEGURIDAD DE LA RED BANCARIA

La seguridad de la red bancaria estará garantizada por varios aspectos:

- VLANS Privadas.
- Acceso a la red por direcciones MAC.
- Seguridad de acceso a los equipos de comunicación.

3.4.1 VLANS PRIVADAS

Las VLANS creadas en los equipos de Telconet serán de utilización exclusiva para la red bancaria, así como los puertos en los switch catalyst 3550 de los que dependerá cada enlace.

En la configuración del puerto del switch catalyst para la matriz bancaria se configurarán solo las VLANS que sean pertenecientes a cada agencia, para este propósito el puerto debe estar configurado como trunk. Un puerto configurado como trunk puede escuchar varias VLANS.

La configuración de las VLANS en los switch catalyst 3550 será de la siguiente manera de acuerdo a la dependencia de las agencias:

Nombre Banco	Nombre Catalyst 3550	# VLAN
Agencia Cotocollao	Telepuerto	160
Agencia América	OPS	161
Agencia Amazonas	Cofiec	162
Agencia San Rafael	Tarqui2	163
Agencia Isaac Barrera	Gaspar	164
Agencia Villaflora	Sur2	166
Agencia Cumbaya	ClickCenter	168
Agencia Iñaquito	Gosseal	169
Agencia Parkenor	Telepuerto	175
Agencia Alameda	SwissHotel	177
Matriz Bancaria	Fondo	Trunk: 160,161,162,163,164,166,168,169,175,177

Tabla 3.17 Distribución de VLANS

El identificador de VLAN es único, tanto para cada agencia como también en el Backbone de Telconet, esto garantiza la independencia y seguridad de datos.

Para ver la distribución de forma gráfica se tiene el siguiente esquema:

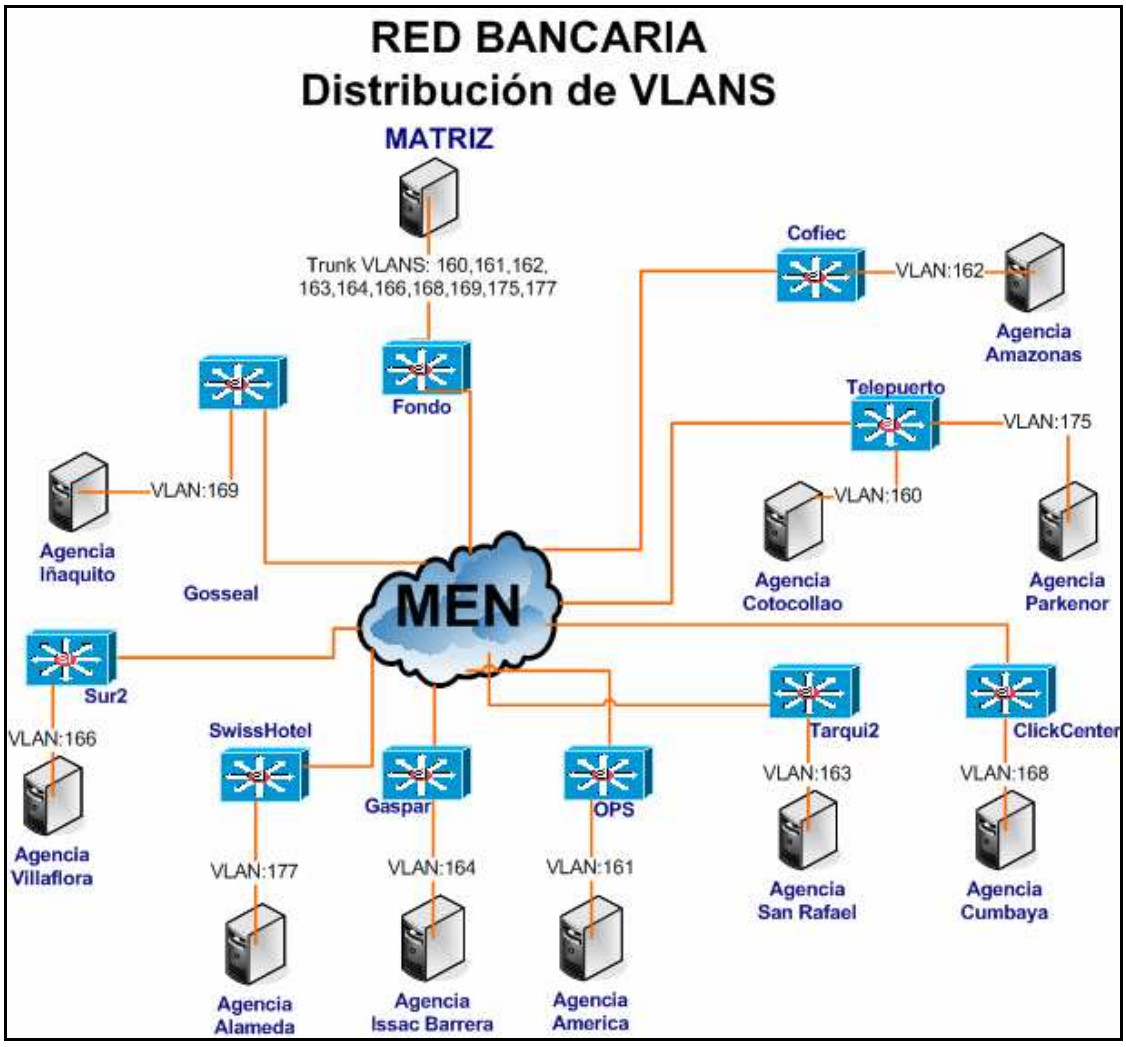


Figura 3.11 Distribución de VLANS

3.4.2 ACCESO A LA RED POR DIRECCIONES MAC

El acceso a la red bancaria en los puertos de los switch catalyst se controla por medio de direcciones MAC, es decir mediante la dirección física del dispositivo de red.

La capa de enlace de acuerdo al modelo OSI se subdivide en dos subcapas:

- Control lógico de enlace LLC ("Logical Link Control"), define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores.
- Control de acceso al medio MAC ("Medium Access Control"), esta subcapa actúa como controladora del hardware subyacente (el adaptador de red). De hecho el controlador de la tarjeta de red es denominado a veces "MAC

driver", y la dirección física contenida en el hardware de la tarjeta es conocida como dirección MAC ("MAC address"). Su principal tarea consiste en arbitrar la utilización del medio físico para facilitar que varios equipos puedan competir simultáneamente por la utilización de un mismo medio de transporte.

Para obtener seguridad en los puertos de los switch catalyst se configurará solo la dirección MAC del dispositivo de comunicación del banco en dicho puerto. Esto garantiza que ningún otro dispositivo de red, que no sea el admitido, pueda acceder a través de los puertos de los diferentes switches catalyst.

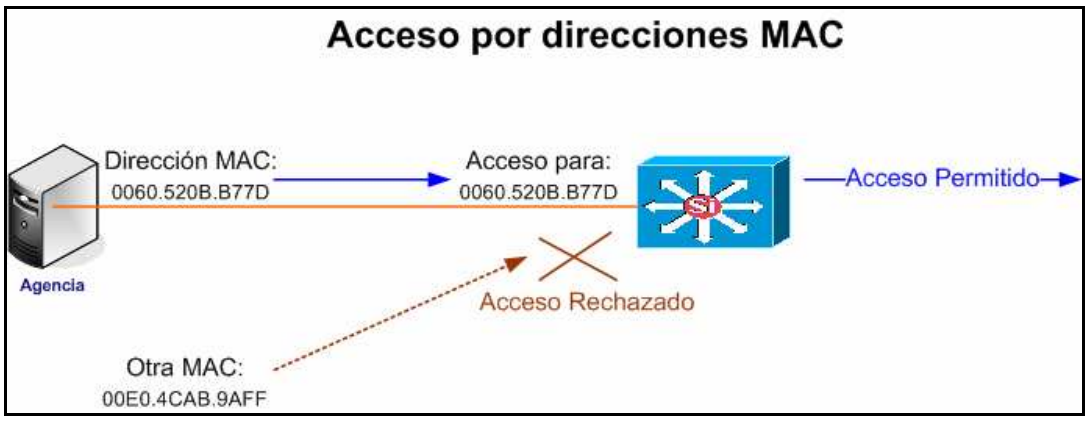


Figura 3.12 Ejemplo de acceso por direcciones MAC

3.4.3 SEGURIDAD DE ACCESO A LOS EQUIPOS DE COMUNICACIÓN

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Conviene aclarar que no siendo posible la certeza absoluta, el elemento de riesgo esta siempre presente, independiente de las medidas que se tomen, por lo que se debe hablar de niveles de seguridad. La seguridad absoluta no es posible, la seguridad es un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos.

Además, la seguridad informática precisa de un nivel organizativo, por lo que se dirá que:

Sistema de Seguridad = TECNOLOGIA + ORGANIZACION

Para brindar seguridad a los equipos de comunicación, la institución bancaria solo permitirá acceder a los mismos de acuerdo a sus políticas de seguridad. Estas políticas de acceso son físicas directamente con los equipos y lógicas por cuanto se administran claves de acceso y solo tráfico de datos permitido por sus políticas[74].

La seguridad administrada por Telconet es específicamente en 2 puntos:

- Seguridad de los enlaces, que no puedan acceder a la red equipos o personas no autorizadas, y las personas autorizadas a hacerlo sean de exclusiva confianza y con los conocimientos necesarios para hacerlo.

- Seguridad del Servidor VLAN, teniendo acceso y las claves del mismo solo personal autorizado, además de filtros y firewall de protección levantados también en el servidor.

3.5 CONFIABILIDAD DE LA RED BANCARIA

La confiabilidad de una red es una medida que refleja la capacidad de la misma de continuar operativa frente a posibles fallos de algunos de sus componentes, y se define como la probabilidad de comunicación exitosa entre cierto conjunto de nodos de la red, dadas las probabilidades de funcionamiento de los componentes y la topología de la red.

La confiabilidad de los enlaces de la red bancaria se los tomará en cuenta de acuerdo los siguientes aspectos:

- Cláusulas del contrato de los enlaces.
- Anillos de backup en el Backbone de Telconet.

3.5.1 CLÁUSULAS DEL CONTRATO DE LOS ENLACES

[74] http://www.eurologic.es/conceptos/conbasics.htm

El punto principal a tocar en las cláusulas del arrendamiento de los enlaces se deriva de que cada enlace desde cada agencia hacia algún nodo de Telconet, es único por medio de fibra óptica, esto implica que si por cualquier motivo el enlace falla Telconet no brindará un backup automático, puesto que el banco asume su backup por medio de otro proveedor u otras instancias propias al banco. Esto se deriva principalmente del costo o negociación.

Pero lo dicho anteriormente no quita la responsabilidad a Telconet de resolver el problema de una manera rápida y efectiva, así Telconet esta en la obligación y responsabilidad de levantar un enlace caído por cualquier motivo desde la agencia hacia el nodo del que depende en un máximo de 3 horas. El tiempo es considerable puesto que pueden existir problemas de ruptura de fibra óptica, que de ser el caso se debe hacer las fusiones necesarias para solventar el problema.

3.5.2 ANILLOS DE BACKUP EN EL BACKBONE DE TELCONET

Los anillos en la MEN de Telconet garantizan la confiabilidad del backbone, puesto que éstos son el sistema automático de backup de los enlaces entre los nodos de Telconet.

Los anillos están formados entre los diferentes switch catalyst 3550, y configurados con el protocolo spanning tree (STP), para la conmutación automática.

3.5.2.1 Protocolo Spanning Tree (STP)

Tan pronto como cada dispositivo ha aprendido la configuración de la red, un bucle presenta la información de conflictos en el segmento en que una dirección específica se localiza y obliga al dispositivo a remitir todo el tráfico. El Algoritmo Spanning Tree Protocol es una norma del software (especificaciones IEEE 802.1d) para describir cómo los puentes y conmutadores pueden comunicarse para evitar bucles en la red.

Intercambiando paquetes denominados BPDU, los puentes y conmutadores establecen un único camino para alcanzar cada segmento de la red. En algunos casos, un puerto de un conmutador o puente puede ser desconectado si existe otro camino al mismo segmento. El proceso de transmitir los paquetes BPDU es continuo, por lo que si un puente o conmutador falla repentinamente, el resto de

los dispositivos reconfiguran sus rutas para permitir que cada segmento sea alcanzado. En algunos casos, los administradores de la red diseñan bucles en redes con puentes, de forma que si un puente o conmutador falla, el algoritmo Spanning Tree calculará la ruta alternativa en la configuración de la red. Para que esto funcione correctamente, todos los conmutadores y puentes de la red deben de soportar este protocolo[75].

Las características principales del funcionamiento de STP son:

- Evitar loops en una red de puentes (switches).
- Respaldo automático de conexión.
- Elección de un puente o conmutador raíz (uno por red).
- Mensajes por Bridge Protocol Data Units (BPDU).
- Todos los otros puentes o conmutadores determinan por que puerto es el camino mas corto al puente o conmutador raíz. Sus demás puertos hacia éste o que puedan causar un loop se dan de baja.
- Todos los puentes o conmutadores intercambian paquetes de Hello, BPDU, los cuales proveen información como bridge IP, Root ID, y root path cost.
- Esta información sirve para que unánimamente elijan un puente o conmutador raíz. Se comparan los bridge ID y el que tenga el ID menor (mayor prioridad es el elegido). Cabe señalar que a mayor prioridad, menor ID.
- Si existen puentes o conmutadores con el mismo ID, se toma el de la menor MAC address.
- Se selecciona un puente o conmutador designado para cada LAN. Si más de un puente o conmutador esta conectado a la LAN, el puente con el path cost más corto al raíz es el elegido. En caso de duplicidad de path cost, el puente con el ID menor es el elegido.
- Los puentes o conmutadores no designados en la LAN, ponen sus puertos no seleccionados en estado blocked. En estado blocked los puertos escuchan para cambiar a forwarding en un posible cambio de topología.

[75] http://www.consulintel.es/Html/Tutoriales/Lantronix/guia_et_p2.html

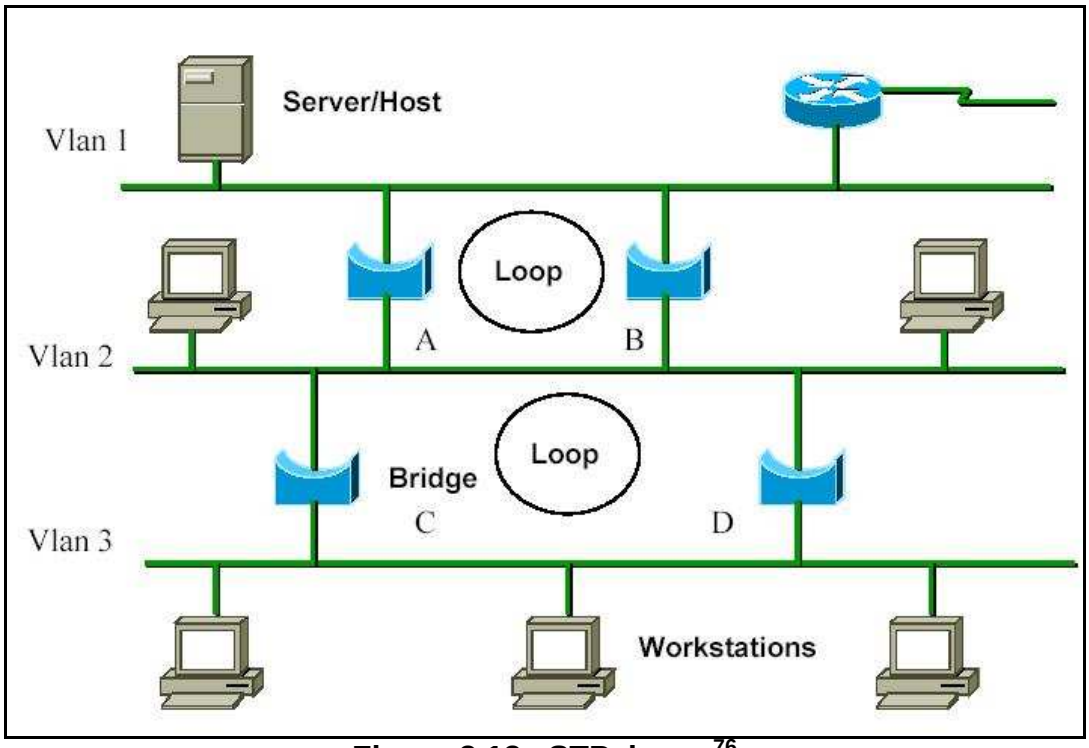


Figura 3.13 STP loops[76]

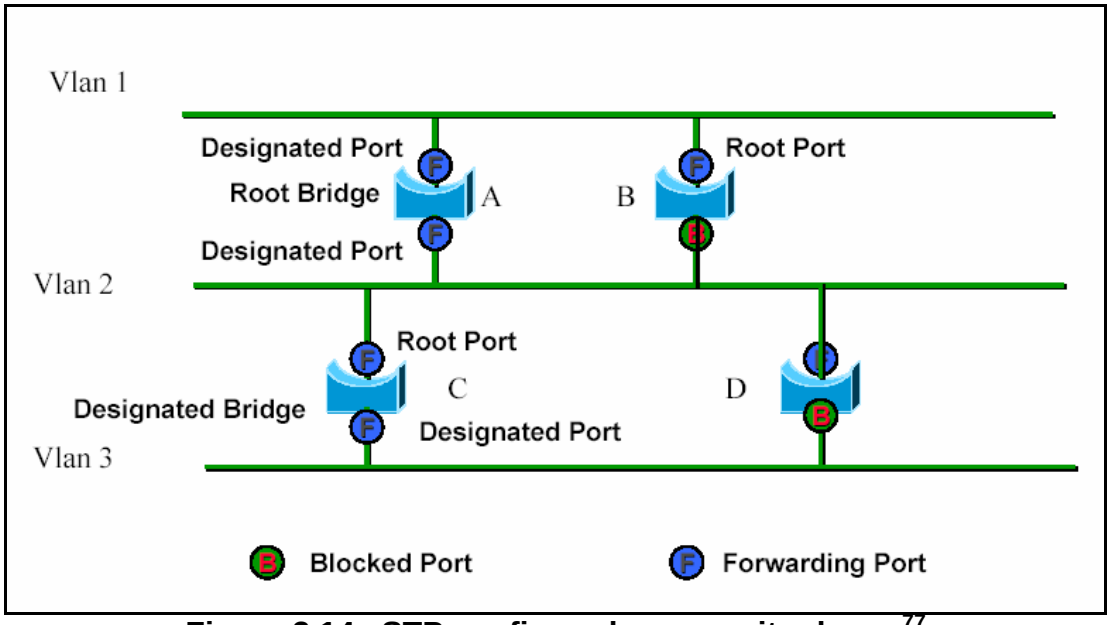


Figura 3.14 STP configurado para evitar loops[77]

3.5.2.2 Anillos STP en el Backbone de Telconet

[76] http://www.itesm.mx/viti/servicios/soporte_red/TYR-CCS-P2.pdf
[77] http://www.itesm.mx/viti/servicios/soporte_red/TYR-CCS-P2.pdf

Para brindar la confiabilidad de la red bancaria Telconet a implementado varios anillos de backup en su backbone por medio del protocolo spanning tree, cada nodo tiene por lo menos un anillo de respaldo, y en los principales nodos existen hasta 3 anillos.

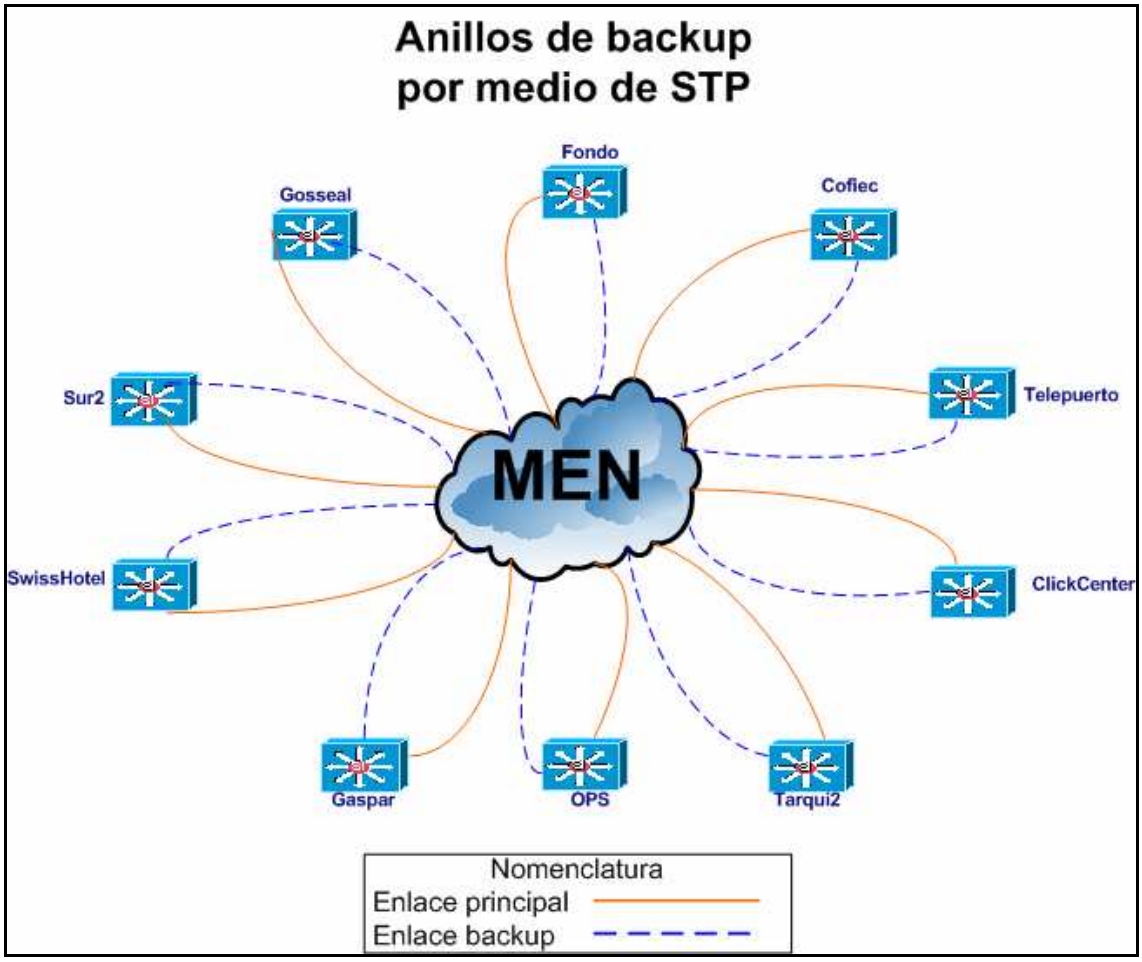


Figura 3.15 Anillos backup utilizando el Protocolo Spanning Tree

Esta infraestructura garantiza al banco la confiabilidad de los enlaces desde cada una de las agencias hacia la matriz bancaria.

CAPITULO 4.

IMPLEMENTACIÓN DE LA RED BANCARIA

4.1 INSTALACIÓN DE ÚLTIMA MILLA

La instalación de la ultima milla, es decir, los enlaces desde cada entidad bancaria hacia cada nodo de Telconet será realizada por el departamento de tendido e instalación de fibra óptica.

Básicamente se llevan a cabo los siguientes trabajos:

- Creación del mapa de tendido de la fibra óptica.
- Inspección de las acometidas en las entidades bancarias.
- Tendido de la fibra óptica.
- Fusión de los hilos de fibra óptica.
- Conectorización de dispositivos.

4.1.1 CREACIÓN DEL MAPA DE TENDIDO DE FIBRA OPTICA

Los mapas del tendido de fibra óptica los administra el departamento de su mismo nombre, sobre los mapas principales de la ciudad se añaden los trazados de fibra por donde se tenderá la misma, estos mapas están realizados en AutoCad, y dimensionados a escala para poder obtener con exactitud la distancia de los enlaces.

4.1.2 INSPECCIÓN DE LAS ACOMETIDAS EN LAS ENTIDADES BANCARIAS

Al respecto de las acometidas, se realiza una inspección previa por donde ingresará el cable de fibra hacia la entidad bancaria, esto puede darse ya sea por las ducterías propias de la localidad o por medios externos adecuando mangueras protectoras y estéticas para tal propósito.

4.1.3 TENDIDO DE LA FIBRA OPTICA

Telconet realiza el tendido de la fibra óptica en la ciudad de 2 formas:

- Acoplada a los postes eléctricos, esto es a la altura de los cables eléctricos, para lo cual es necesario abrazaderas que sostengan de manera segura el cable de fibra óptica, el mismo que esta diseñado para exteriores y para soportar las variaciones climáticas.

- Subterránea, por lo general este tipo de instalaciones se las realiza para el acceso a las localidades, es decir, desde el último poste en donde esta la fibra aérea se asienta a los ductos subterráneos de las afueras de las localidades para luego ingresar a las mismas por sus ducterías apropiadas para estos trabajos.

Para el tendido se toma en cuenta el siguiente procedimiento:

Herramientas y Materiales:

- Cinta para el tendido reutilizable (lanzadera).
- Eslabón giratorio (máximo de 2,22 cm de diámetro).
- Acoples para subductos.
- Acoples para postería.
- Dispositivos de monitores de tensión, como dinamómetro y equipo de tendido mecánico con capacidad de monitores.
- Lubricante apropiado.
- Carrete para cables que tenga un radio igual a 20 veces el diámetro del mismo.
- Trapos limpios.
- Equipos estándar para colocación de cable aéreo y subterráneo.

Figura 4.1 Herraje para poste

Precauciones de Seguridad:

- Evitar dañar el cable durante su manejo y utilización.
- Evitar hacer dobleces muy pronunciados y/o aplastarlo.

- Sustituir la sección de cable dañada, ya que puede cambiar las características de transmisión.
- Asegurar el espacio suficiente durante la distribución de los equipos (vehículos, remolques, etc.), para:
- Tráfico peatonal y de vehículos.
- Estacionamiento.
- Propiedad Privada.
- Asegurarse de seguir las precauciones establecidas, en caso de utilizar fibra óptica.

- No corte los cables de fibra óptica por conveniencias de instalación.
- En la colocación de los cables de fibra:

    - Trabajar de acuerdo a las especificaciones y planos de ingeniería.
    - Inspeccionar visualmente todos los carretes de cable de fibra a ser utilizados, para asegurarse que no existan daños físicos.

Métodos de Tendido:

- Para monitorear la tensión de tendido aplicada durante todo el proceso, se utiliza un dinamómetro (o equipo equivalente).
- De acuerdo a la dificultad para realizar el tendido, se puede tender:

    - Algunas secciones de cable mutuamente, de cámara a cámara.
    - El resto mecánicamente.

- Planificar con anterioridad la ubicación o localización de los carretes y su manejo en la vía.
- Al instalar cables de fibra óptica se deben tener en cuenta las siguientes consideraciones de diseño:

    - Tensión límite a la cual puede ser sometido el cable de fibra óptica: 272 Kg (600 libras).
    - Mínimos radios de curvaturas: - Diez (10) veces el diámetro del cable cuando el cable no está bajo tensión. - Veinte (20) veces el

diámetro del cable cuando el cable está bajo tensión. Se debe mantener además, un tendido recto y uniforme.

Colocación del Carrete de Cable:

- Ubicación: Depende del poste en el cual se instalará el cable.
- Posicionamiento del carrete:
    - Número de codos o curvas de 90°.
    - Cambios de ruta de los postes.
    - Condiciones del terreno en el tramo.
- Reducción de Tensión en el Tendido:
    - Colocación del carrete en una posición estratégica (dirección de tendido).
    - Uso del método "Tendido Bidireccional".
- Dificultades en el Tendido:
    - Colocar lubricante adicional para un tendido de desviaciones variadas.
    - En el caso de un tramo de altas desviaciones, se recomienda pasar una cinta de poliéster reutilizable usando la guía original para introducirla, y con esta se procede al tendido del cable de fibra óptica.
    - Proveer asistencia durante el tendido mediante el tendido manual en cámaras intermedias.

Disminución de la Tensión en el Cable:

- Colocar el vehículo de tendido a un lado del poste lo más cerca posible al extremo del cable.
- Enderezar el cable y continuar instalando de poste a poste hasta el final del tramo o sección.

Procedimiento para el tendido del cable:

- Se incrementa gradualmente la tensión en la línea hasta que el cable se comienza a mover y se sube gradualmente la velocidad y se continua tirando uniformemente (máximo 3,5 Km/hr).
- Se tira los cables de fibra óptica tan uniformemente como sea posible mientras dure la instalación y se observa constantemente la tensión durante la operación de tendido.
- Se toma en cuenta los postes donde se tengan curvaturas de 90° y se coloca un marcador en la línea de tendido a 12m. del extremo unido al cable. Esto servirá como un indicador de que:
- El cable está rápidamente acercándose al poste, la velocidad de tendido debe ser reducida.

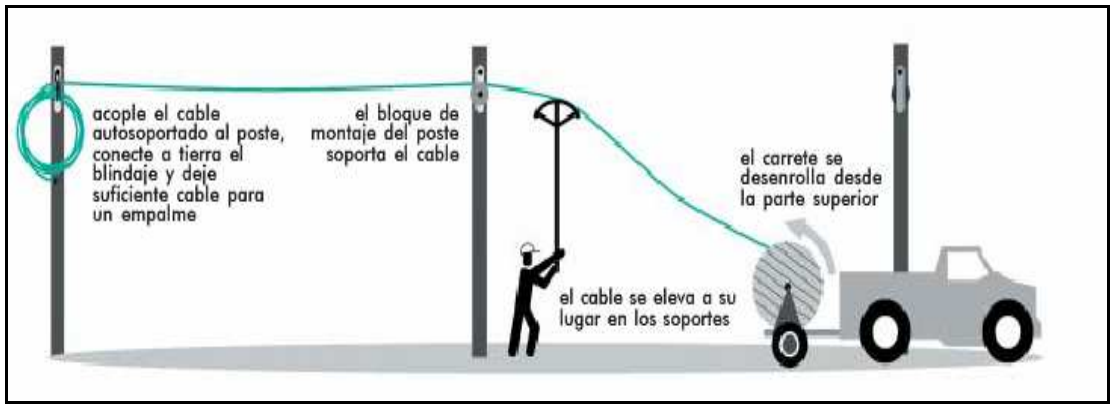


Figura 4.2 Tendido del cable de fibra óptica[78]

Medidas de precaución:

- Equipos apropiados de seguridad (enrollador de cables).
- Mantener tensión en la línea de tendido si es necesario parar la operación de tendido de cables y monitorear la tensión de tendido.
- Cuando el marcador de la línea este cerca del último poste, disminuir la velocidad gradualmente.
- Tirar la cantidad de cable requerida para soportarlo en el herraje y para el empalmado (aproximadamente 15 m) en los postes intermedios y en le

[78] http://www.commscope.com/docs/fiber_manual_sp.pdf

último poste. Para tener suficiente cantidad de cable para empalmar, extender el pescante del camión de tendido sobre la cámara y tirar el cable hasta el tope del pescante.

- Retirar el equipo de tendido.

Recomendaciones:

- Si el número de fibras contenida en el cable no está marcado en la cubierta, se debe verificar físicamente el número de fibras para asegurar el uso del cable apropiado.
- Prever un sistema de comunicaciones entre el personal.
- Proveer de barricadas de protección en zonas de mucho tráfico.
- Probar los equipos de tendido y corte con una carga inicial predeterminada.
- Aplicar lubricación en el extremo de alimentación (periódicamente), durante el tendido.
- Equipotenciar y poner a tierra 25 ohms o menos, en los puntos de empalme que así lo requieran, si se utilizan cables con armadura (acorazados).
- Todo el personal tiene que conocer las condiciones locales de trabajo, las señales de comunicación, procedimientos de seguridad para construcciones subterráneos y aéreos, antes de comenzar los trabajos.

4.1.4 FUSIÓN DE LOS HILOS DE FIBRA ÓPTICA

Una vez realizada la acometida de la fibra óptica tanto a la localidad bancaria como al nodo de Telconet, es necesario fusionar los hilos, esto se lo realiza en ambos extremos, y con el siguiente procedimiento:

Preparación de puntas de cable:

- Para comenzar con la preparación se corta el cable dejando la longitud apropiada de acuerdo al tipo de empalme a realizar.
- Desde el extremo del cable se mide una longitud de 1.5 m, se efectúa un corte en forma circular y transversal al cable en todo el espesor de la cubierta externa.

- Las cintas de ligadura y envoltura del núcleo se cortan, y una vez eliminado el compuesto de relleno se procede a secar los tubos. Finalmente se procede a identificar las ataduras que contienen las fibras.

Preparación de caja de empalmes:

- Comprende las operaciones de apertura de la caja, remoción de bandejas, selección de bocas de entrada y salida para los cables, remoción de obturadores de bocas, etc.
- Se procede a la fijación de los cables, según se trate de un cable cortado o una sangría para un empalme de derivación.
- En el caso de cable cortado, se suplementa la cubierta del cable en el extremo, para lograr su adaptación al tamaño de la brida de sujeción, sí el diámetro fuese menor al de la brida, y se adaptará también a la altura de la boca de obturación.
- Se sujeta el cable con la brida y se anclan las fibras y los elementos de refuerzo. En caso de existir más cables se repetirán las operaciones detalladas.
- Los dispositivos que servirán de fijación a los tubos de fibras sin cortar, se los acondicionará luego en el interior.

Ejecución y cierre de empalmes por sistema de fusión:

- Antes de proceder al empalme de las fibras, se distribuye uniformemente los tubos en las bandejas. Eliminando hasta unos 2 cm. hasta el punto de fijación en la bandeja, removiendo por lo menos 20 cm. y dejando las fibras al descubierto con su primera protección.
- Se realiza la limpieza de las fibras con alcohol. Una vez fijados los tubos se procede a realizar los empalmes por fusión.
- Las fibras se cortan utilizando un cleaver, que asegura una buena calidad de corte. Es necesario colocar las fibras dentro de la máquina de empalmar para lograr la alineación correcta, tomando como referencia el núcleo de la fibra. El equipo mencionado permite esta precisa alineación, utilizando ópticas de aumento. El empalme es asistido a su vez por una cámara

controlada por computadora y un procesado de imagen, de esta manera se asegura la calidad final del mismo.

- Una vez unida, se coloca un manguito termocontraíble o tubito de soporte, en las partes desnudas de la fibra empalmada. El equipo se encarga también de contraer este manguito, a través de un horno dispuesto en el frente del mismo. También realiza una prueba de tracción. El empalme es sometido a 200gr. de tracción para comprobar su robustez.

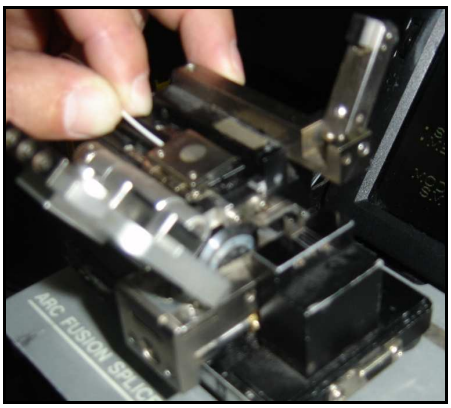


Figura 4.3 Fusión de la fibra óptica

Acondicionamiento y cierre de las cajas de empalmes:

- Se dispone las fibras respetando un orden según la codificación y comenzando desde el punto más alejado de la bandeja.
- Luego se enrolla la fibra en los discos de la bandeja en su totalidad. Una vez que se halla completado la tarea de ordenamiento para cada uno de los empalmes se procede al cierre de la caja.
- Se coloca un elemento higroscópico antes de cerrar (Gel de Silicona). Se asegura un cerrado estanco antes de proceder al ajuste de los tornillos de fijación. Se verifica que se encuentren selladas también las bocas de cables no utilizados.

Testeo de empalmes:

- OTDR - Optical Time Domain Reflectometer - Reflectómetro Óptico es el equipo utilizado para realizar el testeo de los empalmes.

Figura 4.4 OTDR

- Para testear las fibras en una dirección, se conecta el OTDR a un extremo de la fibra óptica para adquirir una lectura que proveerá información sobre la continuidad del tramo de fibra, sobre la pérdida en cada empalme, la pérdida total (punta a punta), la atenuación característica de cada segmento de fibra en la red y la reflectancia de empalmes o conexiones, etc.
- Si no se conoce el valor del índice de refracción, el valor adoptado es 1.4650.

Aceptación del empalme:

- Se entiende por sección a toda longitud de cable óptico comprendido entre dos terminaciones a nivel del distribuidor de fibra óptica o Patch Panel.
- El valor máximo de atenuación aceptado por empalme es de 0,03 dB. Sí el valor de atenuación del empalme resulta mayor de 0,03 dB, el mismo se rehace hasta un mínimo de tres intentos.
- Todas las medidas de atenuación se efectúan en las longitudes de onda de 1310 y 1550nm y en ambos sentidos, y se considera como valor absoluto de pérdida el promedio obtenido en ambas mediciones.

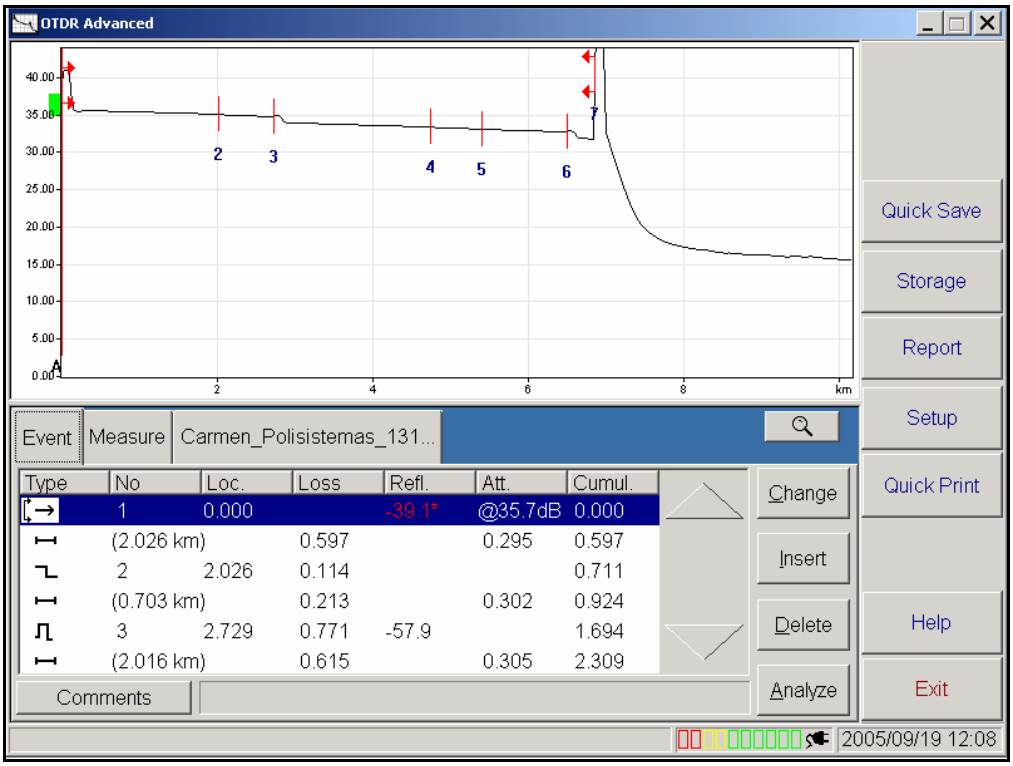


Figura 4.5 Resultado del testeo con el OTDR

4.1.5 CONECTORIZACIÓN DE DISPOSITIVOS

Realizada la fusión y comprobación del correcto testeo de los empalmes de fibra óptica se procede a realizar la conectorización, esto simplemente consiste en insertar los conectores de fibra en los transceivers y también conectar los patch cord de UTP que van desde el transceiver hacia el dispositivo con interfaz RJ45, esto se lo realiza en dos sentidos, es decir, en la agencia bancaria y en el nodo del que depende, debiendo iluminarse los leds del transceiver (indicadores de conexión) tanto de Fx como de Tx, el led de Fx indica la conectividad de la fibra óptica, mientras que el de Tx indica la conectividad de los dispositivos con interfaz RJ45.

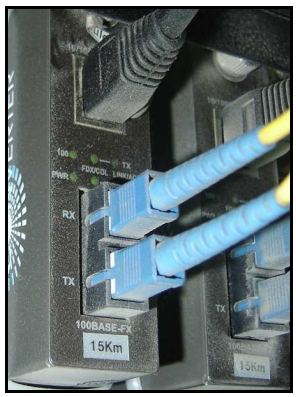


Figura 4.6 Conectorización

4.2 CONFIGURACIÓN DE DISPOSITIVOS

Los dispositivos que estarán bajo la responsabilidad de Telconet y que serán configurados para poder brindar la interconexión de las agencias con la matriz bancaria son:

- Switch Cisco Catalyst 3550.
- Servidor VLAN.

4.2.1 CONFIGURACIÓN DE LOS SWITCHES CISCO CATALYST 3550

En primera instancia es necesario indicar que éstos dispositivos están ya configurados y en funcionamiento en el Backbone de Telconet, por lo que se presentarán las configuraciones que se realizarán para que la red bancaria funcione sobre la infraestructura de Telconet.

A continuación se indican los equipos switch catalyst con el respectivo puerto por medio del cual se realizará la interconexión de la red bancaria:

Nombre Banco	Nombre Catalyst 3550	Puerto Asignado	# VLAN
Agencia Cotocollao	Telepuerto	Fa0/20	160
Agencia América	OPS	Fa0/24	161
Agencia Amazonas	Cofiec	Fa0/23	162
Agencia San Rafael	Tarqui2	Fa0/12	163
Agencia Issac Barrera	Gaspar	Fa0/10	164
Agencia Villaflora	Sur2	Fa0/13	166
Agencia Cumbaya	ClickCenter	Fa0/19	168
Agencia Iñaquito	Gosseal	Fa0/24	169
Agencia Parkenor	Telepuerto	Fa0/21	175
Agencia Alameda	SwissHotel	Fa0/19	177
Matriz Bancaria	Fondo	Fa0/13	160,161,162,163, 164,166,168,169, 175,177

Tabla 4.1 Puertos asignados para la interconexión

Los comandos a utilizarse en la configuración del los puertos de los que dependen las agencias son similares, por lo que se revisará los comandos a ejecutarse en un puerto del que depende una agencia y en el puerto del que depende la matriz.

4.2.1.1 Configuración de los puertos de los switch catalyst 3550 de los que dependen cada una de las agencias bancarias.

Para ejemplo se muestra la configuración del puerto 20 del catalyst 3550 denominado Telepuerto, del mismo que depende la agencia bancaria Cotocollao. Las sentencias a utilizarse son las siguientes:

Configuración Global:

sw1telepuerto#**configure terminal** (Ingresa en el modo de configuración)
Enter configuration commands, one per line. End with CNTL/Z.
sw1telepuerto(config)#**vlan 160** (Añade la VLAN 160)
sw1telepuerto(config-vlan)#**name VLAN0160** (Asigna un nombre a la VLAN)
sw1telepuerto(config-vlan)#**end** (Sale del modo de configuración)
sw1telepuerto#**write** (Graba las configuraciones realizadas)

Configuración en la interface:

sw1telepuerto#**configure terminal** (Ingresa en modo de configuración)
Enter configuration commands, one per line. End with CNTL/Z.
sw1telepuerto(config)#**interface fastEthernet 0/20** (Ingresa en la configuración del puerto fast ethernet 20)
sw1telepuerto(config)#**no shutdown** (Habilita el puerto)
sw1telepuerto(config-if)#**description cce_agencia-cotocollao_eth0_fib** (Descripción o nombre del puerto)
sw1telepuerto(config-if)#**switchport access vlan 160** (Asigna la VLAN al puerto)
sw1telepuerto(config-if)#**switchport mode access** (Define VLANS en modo estático)
sw1telepuerto(config-if)#**switchport nonegotiate** (Acelera los tiempos de convergencia en la conectividad)
sw1telepuerto(config-if)#**switchport block multicast** (bloquea multicast desconocido)
sw1telepuerto(config-if)#**switchport block unicast** (bloquea unicast desconocido)

sw1telepuerto(config-if)#**switchport port-security** (Activa la seguridad al puerto)
sw1telepuerto(config-if)#**switchport port-security maximum 1** (Activa para que máximo ingrese 1 mac por el puerto)
sw1telepuerto(config-if)#**switchport port-security violation restrict** (Si existe una violación de una MAC que no esta declarada el puerto no deja pasar a dicha MAC pero no se deshabilita el puerto y muestra el intento de violación en los LOG del catalyst)
sw1telepuerto(config-if)#**switchport port-security aging static** (Seguridad del puerto estática)
sw1telepuerto(config-if)#**switchport port-security mac-address 0040.f467.8868** (Setea la MAC en el puerto)
sw1telepuerto(config-if)#**ip access-group 135 in** (Levanta un Access List ACL, políticas de ingreso y salida al puerto)
sw1telepuerto(config-if)#**service-policy input policy_port20_in** (Seteo para control de ancho de banda de entrada)
sw1telepuerto(config-if)#**service-policy output policy_port20_out** (Seteo para el control de ancho de banda de salida)
sw1telepuerto(config-if)#**storm-control broadcast level 5.00** (Limita el tráfico a las tormentas de broadcast)
sw1telepuerto(config-if)#**storm-control multicast level 5.00** (Limita el tráfico a las tormentas multicast)
sw1telepuerto(config-if)# **storm-control unicast level 2.00** (Limita el tráfico a las tormentas unicast)
sw1telepuerto(config-if)#**no cdp enable** (deshabilita el Protocolo de Descubrimiento de Cisco CDP)
sw1telepuerto(config-if)# **spanning-tree portfast** (Deshabilita STP haciendo que si ocurre un loop, éste no se detecte)
sw1telepuerto(config-if)#**spanning-tree bpduguard enable** (hace que no envíe paquetes BPDU (Bridge Packet Data Unit), parte de la deshabilitación del STP)
sw1telepuerto(config-if)# **spanning-tree guard root** (Mantiene el switch root configurado para que otros no accedan como root)
sw1telepuerto(config-if)#**end** (Sale del modo de configuración)
sw1telepuerto#**write** (Graba las configuraciones realizadas)

La configuración descrita será la misma para todos los puertos de los cuales dependa cada una de las agencias bancaria, por lo que se tiene las siguientes configuraciones:

Catalyst Telepuerto: Puerto 20

```
sw1telepuerto#show running-config interface fastEthernet 0/20
Building configuration...

Current configuration : 699 bytes
!
interface FastEthernet0/20
 description cce_agencia-cotocollao_eth0_fib
 switchport access vlan 160
 switchport mode access
 switchport nonegotiate
 switchport block multicast
 switchport block unicast
 switchport port-security
 switchport port-security violation restrict
 switchport port-security aging static
 switchport port-security mac-address 0040.f467.8868
 ip access-group 135 in
 service-policy input policy_port20_in
 service-policy output policy_port20_out
 storm-control broadcast level 5.00
 storm-control multicast level 5.00
 storm-control unicast level 2.00
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree guard root
end
```

Catalyst OPS: Puerto 24

```
sw1ops# show running-config interface fastEthernet 0/24
Building configuration...

Current configuration : 696 bytes
!
interface FastEthernet0/24
 description cce_agencia-america_eth0_fib
 switchport access vlan 161
 switchport mode access
 switchport nonegotiate
 switchport block multicast
 switchport block unicast
 switchport port-security
 switchport port-security violation restrict
 switchport port-security aging static
 switchport port-security mac-address 0003.2200.7705
 ip access-group 135 in
 service-policy input policy_port24_in
 service-policy output policy_port24_out
 storm-control broadcast level 5.00
 storm-control multicast level 5.00
 storm-control unicast level 2.00
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree guard root
end
```

Catalyst Cofiec: Puerto 23

```
sw1cofiec# show running-config interface fastEthernet 0/23
Building configuration...
```

```
Current configuration : 697 bytes
!
interface FastEthernet0/23
 description cce_agencia-amazonas_eth0_fib
 switchport access vlan 162
 switchport mode access
 switchport nonegotiate
 switchport block multicast
 switchport block unicast
 switchport port-security
 switchport port-security violation restrict
 switchport port-security aging static
 switchport port-security mac-address 0000.9334.4e88
 ip access-group 135 in
 service-policy input policy_port23_in
 service-policy output policy_port23_out
 storm-control broadcast level 5.00
 storm-control multicast level 5.00
 storm-control unicast level 2.00
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree guard root
end
```

Catalyst Tarqui2: Puerto 12

```
sw1tarqui2# show running-config interface fastEthernet 0/12
Building configuration...

Current configuration : 699 bytes
!
interface FastEthernet0/12
 description cce_agencia-san-rafael_eth0_fib
```

```
 switchport access vlan 163
 switchport mode access
 switchport nonegotiate
 switchport block multicast
 switchport block unicast
 switchport port-security
 switchport port-security violation restrict
 switchport port-security aging static
 switchport port-security mac-address 0000.e8d8.1ec2
 ip access-group 135 in
 service-policy input policy_port12_in
 service-policy output policy_port12_out
 storm-control broadcast level 5.00
 storm-control multicast level 5.00
 storm-control unicast level 2.00
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree guard root
end
```

Catalyst Gaspar: Puerto 10

```
sw1gaspar#show running-config interface fastEthernet 0/10
Building configuration...

Current configuration : 702 bytes
!
interface FastEthernet0/10
 description cce_agencia-issac-barrera_eth0_fib
 switchport access vlan 164
 switchport mode access
 switchport nonegotiate
 switchport block multicast
```

```
 switchport block unicast
 switchport port-security
 switchport port-security violation restrict
 switchport port-security aging static
 switchport port-security mac-address 0000.e8de.f1cb
 ip access-group 135 in
 service-policy input policy_port10_in
 service-policy output policy_port10_out
 storm-control broadcast level 5.00
 storm-control multicast level 5.00
 storm-control unicast level 2.00
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree guard root
end
```

Catalyst Sur2: Puerto 13

```
sw1sur2# show running-config interface fastEthernet 0/13
Building configuration...

Current configuration : 699 bytes
!
interface FastEthernet0/13
 description cce_agencia-villaflora_eth0_fib
 switchport access vlan 166
 switchport mode access
 switchport nonegotiate
 switchport block multicast
 switchport block unicast
 switchport port-security
 switchport port-security violation restrict
 switchport port-security aging static
```

```
 switchport port-security mac-address 000d.60e6.99d8
 ip access-group 135 in
 service-policy input policy_port13_in
 service-policy output policy_port13_out
 storm-control broadcast level 5.00
 storm-control multicast level 5.00
 storm-control unicast level 2.00
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree guard root
end
```

Catalyst ClickCenter : Puerto 19

```
sw1clickcenter#show running-config interface fastEthernet 0/19
Building configuration...

Current configuration : 696 bytes
!
interface FastEthernet0/19
 description cce_agencia-cumbaya_eth0_fib
 switchport access vlan 168
 switchport mode access
 switchport nonegotiate
 switchport block multicast
 switchport block unicast
 switchport port-security
 switchport port-security violation restrict
 switchport port-security aging static
 switchport port-security mac-address 0004.ac8a.1130
 ip access-group 135 in
 service-policy input policy_port19_in
 service-policy output policy_port19_out
```

```
 storm-control broadcast level 5.00
 storm-control multicast level 5.00
 storm-control unicast level 2.00
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree guard root
end
```

Catalyst Gosseal : Puerto 24

```
sw1gosseal# show running-config interface fastEthernet 0/24
Building configuration...

Current configuration : 697 bytes
!
interface FastEthernet0/24
 description cce_agencia-inaquito_eth0_fib
 switchport access vlan 169
 switchport mode access
 switchport nonegotiate
 switchport block multicast
 switchport block unicast
 switchport port-security
 switchport port-security violation restrict
 switchport port-security aging static
 switchport port-security mac-address 0009.6b27.3b72
 ip access-group 135 in
 service-policy input policy_port24_in
 service-policy output policy_port24_out
 storm-control broadcast level 5.00
 storm-control multicast level 5.00
 storm-control unicast level 2.00
 no cdp enable
```

```
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree guard root
end
```

Catalyst Telepuerto : Puerto 21

```
sw1telepuerto#show running-config interface fastEthernet 0/21
Building configuration...

Current configuration : 697 bytes
!
interface FastEthernet0/21
 description cce_agencia-parkenor_eth0_fib
 switchport access vlan 175
 switchport mode access
 switchport nonegotiate
 switchport block multicast
 switchport block unicast
 switchport port-security
 switchport port-security violation restrict
 switchport port-security aging static
 switchport port-security mac-address 0000.e8df.3527
 ip access-group 135 in
 service-policy input policy_port21_in
 service-policy output policy_port21_out
 storm-control broadcast level 5.00
 storm-control multicast level 5.00
 storm-control unicast level 2.00
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree guard root
end
```

Catalyst SwissHotel : Puerto 19

```
sw1swisshotel# show running-config interface fastEthernet 0/19
Building configuration...

Current configuration : 696 bytes
!
interface FastEthernet0/19
 description cce_agencia-alameda_eth0_fib
 switchport access vlan 177
 switchport mode access
 switchport nonegotiate
 switchport block multicast
 switchport block unicast
 switchport port-security
 switchport port-security violation restrict
 switchport port-security aging static
 switchport port-security mac-address 0200.6000.8888
 ip access-group 135 in
 service-policy input policy_port19_in
 service-policy output policy_port19_out
 storm-control broadcast level 5.00
 storm-control multicast level 5.00
 storm-control unicast level 2.00
 no cdp enable
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree guard root
end
```

4.2.1.2 Configuración del puerto del switch catalyst 3550 del que depende la matriz bancaria

La configuración de este puerto es diferente que la configuración de los anteriores, puesto que por el mismo debe aceptar las diferentes VLANS de la conexión de cada agencia, entonces es necesario configurarlo para tal propósito.
La configuración se la realiza en el switch catalyst 3550 denominado fondo en el puerto número 13.

Las sentencias son las siguientes:

sw1fondo#**configure terminal** (Ingresa en modo de configuración)
Enter configuration commands, one per line. End with CNTL/Z.
sw1fondo(config)#**interface fastEthernet 0/13** (Ingresa en la configuración del puerto fast ethernet 13)
sw1fondo(config-if)#**no shutdown** (Habilita el puerto)
sw1fondo(config-if)#**description cce_servervlan_eth1_fib** (Descripción o nombre del puerto)
sw1fondo(config-if)#**switchport trunk encapsulation dot1q** (Se elige como encapsulamiento el protocolo de trunking IEEE 802.1Q (dot1q))
sw1fondo(config-if)#**switchport trunk allowed vlan 100,160-164,166,168,169,175,177** (Asigna las VLAN que se permitirá el acceso a través del puerto)
sw1fondo(config-if)#**switchport mode trunk** (Setea al puerto de modo trunk, para permitir pasar más de una VLAN)
sw1fondo(config-if)#**switchport nonegotiate** (Acelera los tiempos de convergencia en la conectividad)
sw1fondo(config-if)#**ip access-group 135 in** (Levanta un Access List ACL, políticas de ingreso y salida al puerto)
sw1fondo(config-if)#**service-policy input policy_port13_in** (Seteo para control de ancho de banda de entrada)
sw1fondo(config-if)#**service-policy output policy_port13_out** (Seteo para el control de ancho de banda de salida)

sw1fondo(config-if)#**storm-control broadcast level 5.00** (Limita el tráfico a las tormentas de broadcast)
sw1fondo(config-if)#**storm-control multicast level 5.00** (Limita el tráfico a las tormentas multicast)
sw1fondo(config-if)#**storm-control unicast level 2.00** (Limita el tráfico a las tormentas unicast)
sw1fondo(config-if)#**no cdp enable** (deshabilita el Protocolo de Descubrimiento de Cisco CDP)
sw1fondo(config-if)#**spanning-tree portfast trunk** (Deshabilita STP haciendo que si ocurre un loop, éste no se detecte)
sw1fondo(config-if)#**spanning-tree bpduguard enable** (hace que no envíe paquetes BPDU (Bridge Packet Data Unit), parte de la deshabilitación del STP)
sw1fondo(config-if)#**spanning-tree guard root** (Mantiene el switch root configurado para que otros no accedan como root)
sw1fondo(config-if)#**end** (Sale del modo de configuración)
sw1fondo#**write** (Graba las configuraciones realizadas)

Es necesario indicar que se ha configurado una VLAN adicional con número 100, ésta será utilizada exclusivamente por Telconet para el monitoreo de los enlaces, una vez terminada la configuración se puede observar la misma:

Catalyst Fondo : Puerto 13

```
sw1fondo#show running-config interface fastEthernet 0/13
Building configuration...

Current configuration : 547 bytes
!
interface FastEthernet0/13
 description cce_servervlan_eth1_utp
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,160-164,166,168,169,175,177
 switchport mode trunk
 switchport nonegotiate
```

```
 ip access-group 135 in
 service-policy input policy_port13_in
 service-policy output policy_port13_out
 storm-control broadcast level 5.00
 storm-control multicast level 5.00
 storm-control unicast level 2.00
 no cdp enable
 spanning-tree portfast trunk
 spanning-tree bpduguard enable
 spanning-tree guard root
end
```

4.2.2 CONFIGURACIÓN DEL SERVIDOR VLAN

El servidor para VLANS es un equipo Supermicro, el mismo que tiene instalado el sistema operativo Linux Fedora Core 2, y que tiene 2 interfaces de red, la primera (eth0) será utilizada para la conexión con el router del banco y la segunda (eth1) se conectará con el puerto del switch cisco catalyst 3550 (Fondo, puerto 13).

Figura 4.7 Esquema de conexión del Servidor VLAN

Este equipo es la interfaz entre todas las agencias y la matriz bancaria, sobre el mismo se configuran los siguientes parámetros:

- Configuración de las interfaces de red
- Creación de VLANS
- Asignación de direcciones IP
- Implementación de rutas estáticas
- Configuraciones de seguridad

4.2.2.1 Configuración de las interfaces de red

La configuración de las tarjetas de red del servidor se encuentra en el siguiente path:

[root@tnnel-uio network-scripts]# pwd

/etc/sysconfig/network-scripts/etc/sysconfig/network-scripts

Para ver la configuración de cada una de las tarjetas de red:

eth0:

[root@tnnel-uio network-scripts]# more ifcfg-eth0

Realtek|RTL-8139/8139C/8139C+

DEVICE=eth0

ONBOOT=yes

BOOTPROTO=static

IPADDR=200.193.230.2

NETMASK=255.255.255.252

GATEWAY=200.193.230.1

eth1:

[root@tnnel-uio network-scripts]# more ifcfg-eth1

Realtek|RTL-8139/8139C/8139C+

DEVICE=eth1

ONBOOT=yes

BOOTPROTO=static

IPADDR=172.168.109.1

NETMASK=255.255.255.0

Esta es la configuración inicial de las direcciones IP al momento de arrancar el sistema operativo y de levantar las interfaces de red, estas configuraciones fueron creadas al momento de la instalación del sistema operativo, pero pueden ser modificadas editando los archivos y grabando nuevas configuraciones, luego de esto se puede reiniciar el servidor para que los cambios realizados tomen efecto.

4.2.2.2 Creación de VLANS

La creación de las VLANS en el servidor sirve para la interconexión con cada una de las agencias, es decir, para enlazarse con los puertos de los switch catalyst, en una misma VLAN.

Para levantar las VLANS se realizan los siguientes pasos:

1.- En la eth1 del servidor se baja la interfaz y se quita la dirección IP que se levanta por defecto al arrancar el sistema operativo, para luego levantar nuevamente la interfaz eth1 pero sin dirección IP, es decir, se levanta físicamente solo con la dirección MAC.

```
[root@tnnel-uio root]# ifconfig eth1 down
[root@tnnel-uio root]# ifconfig eth1 0.0.0.0 up
[root@tnnel-uio root]# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:40:F4:91:8A:7B
          inet6 addr: fe80::240:f4ff:fe91:8a7b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1267256 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1214305 errors:0 dropped:0 overruns:2 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:32290354 (30.7 Mb)  TX bytes:25850894 (24.6 Mb)
          Interrupt:5 Base address:0xb000
```

2.- Se procede a añadir la VLANS en la interfaz eth1.

```
[root@tnnel-uio root]# vconfig add eth1 100
[root@tnnel-uio root]# vconfig add eth1 160
[root@tnnel-uio root]# vconfig add eth1 161
[root@tnnel-uio root]# vconfig add eth1 162
[root@tnnel-uio root]# vconfig add eth1 163
[root@tnnel-uio root]# vconfig add eth1 164
[root@tnnel-uio root]# vconfig add eth1 166
[root@tnnel-uio root]# vconfig add eth1 168
```

[root@tnnel-uio root]# vconfig add eth1 169
[root@tnnel-uio root]# vconfig add eth1 175
[root@tnnel-uio root]# vconfig add eth1 177

4.2.2.3 Asignación de direcciones IP

Una vez creadas las VLANS se levanta las direcciones IP sobre cada una de ellas.

[root@tnnel-uio root]# ifconfig eth1.100 172.26.3.1 netmask 255.255.255.128 broadcast 172.26.3.127 up
[root@tnnel-uio root]# ifconfig eth1.160 172.26.117.173 netmask 255.255.255.252 broadcast 172.26.117.175 up
[root@tnnel-uio root]# ifconfig eth1.161 172.26.117.153 netmask 255.255.255.252 broadcast 172.26.117.155 up
[root@tnnel-uio root]# ifconfig eth1.162 172.26.117.157 netmask 255.255.255.252 broadcast 172.26.117.159 up
[root@tnnel-uio root]# ifconfig eth1.163 172.26.117.161 netmask 255.255.255.252 broadcast 172.26.117.163 up
[root@tnnel-uio root]# ifconfig eth1.164 172.26.117.165 netmask 255.255.255.252 broadcast 172.26.117.167 up
[root@tnnel-uio root]# ifconfig eth1.166 172.26.117.177 netmask 255.255.255.252 broadcast 172.26.117.179 up
[root@tnnel-uio root]# ifconfig eth1.168 172.26.114.253 netmask 255.255.255.252 broadcast 172.26.114.255 up
[root@tnnel-uio root]# ifconfig eth1.169 172.26.113.233 netmask 255.255.255.252 broadcast 172.26.113.235 up

[root@tnnel-uio root]# ifconfig eth1.175 172.26.114.241 netmask 255.255.255.252 broadcast 172.26.114.243 up
[root@tnnel-uio root]# ifconfig eth1.177 172.26.114.249 netmask 255.255.255.252 broadcast 172.26.114.251 up

La configuración de las direcciones IP levantadas sobre cada una de las VLANS se muestra de la siguiente manera:

```
[root@tnnel-uio root]# ifconfig |more

eth1.100  Link encap:Ethernet  HWaddr 00:40:F4:91:8A:7B
          inet addr:172.26.3.1  Bcast:172.26.3.127  Mask:255.255.255.128
          inet6 addr: fe80::240:f4ff:fe91:8a7b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:487245 errors:0 dropped:0 overruns:0 frame:0
          TX packets:77745 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:7479390 (7.1 Mb)  TX bytes:7932577 (7.5 Mb)

eth1.160  Link encap:Ethernet  HWaddr 00:40:F4:91:8A:7B
          inet addr:172.26.117.173  Bcast:172.26.117.175  Mask:255.255.255.252
          inet6 addr: fe80::240:f4ff:fe91:8a7b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:90124 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74179 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:6019371 (5.7 Mb)  TX bytes:6815548 (6.4 Mb)

eth1.161  Link encap:Ethernet  HWaddr 00:40:F4:91:8A:7B
          inet addr:172.26.117.153  Bcast:172.26.117.155  Mask:255.255.255.252
          inet6 addr: fe80::240:f4ff:fe91:8a7b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:118412 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97448 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:8125950 (7.7 Mb)  TX bytes:7876108 (7.5 Mb)

eth1.162  Link encap:Ethernet  HWaddr 00:40:F4:91:8A:7B
          inet addr:172.26.117.157  Bcast:172.26.117.159  Mask:255.255.255.252
          inet6 addr: fe80::240:f4ff:fe91:8a7b/64 Scope:Link
```

```
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:17472 errors:0 dropped:0 overruns:0 frame:0
        TX packets:17336 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:1547742 (1.4 Mb)  TX bytes:1991682 (1.8 Mb)

eth1.163  Link encap:Ethernet  HWaddr 00:40:F4:91:8A:7B
        inet addr:172.26.117.161  Bcast:172.26.117.163  Mask:255.255.255.252
        inet6 addr: fe80::240:f4ff:fe91:8a7b/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:49603 errors:0 dropped:0 overruns:0 frame:0
        TX packets:42005 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:3596648 (3.4 Mb)  TX bytes:3386410 (3.2 Mb)

eth1.164  Link encap:Ethernet  HWaddr 00:40:F4:91:8A:7B
        inet addr:172.26.117.165  Bcast:172.26.117.167  Mask:255.255.255.252
        inet6 addr: fe80::240:f4ff:fe91:8a7b/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:72962 errors:0 dropped:0 overruns:0 frame:0
        TX packets:57765 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:5176299 (4.9 Mb)  TX bytes:4353466 (4.1 Mb)

eth1.166  Link encap:Ethernet  HWaddr 00:40:F4:91:8A:7B
        inet addr:172.26.117.177  Bcast:172.26.117.179  Mask:255.255.255.252
        inet6 addr: fe80::240:f4ff:fe91:8a7b/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:91904 errors:0 dropped:0 overruns:0 frame:0
        TX packets:82556 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:6196219 (5.9 Mb)  TX bytes:6344755 (6.0 Mb)
```

```
eth1.168  Link encap:Ethernet  HWaddr 00:40:F4:91:8A:7B
          inet addr:172.26.114.253  Bcast:172.26.114.255  Mask:255.255.255.252
          inet6 addr: fe80::240:f4ff:fe91:8a7b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:817 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2458 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:118667 (115.8 Kb)  TX bytes:696889 (680.5 Kb)

eth1.169: Link encap:Ethernet  HWaddr 00:40:F4:91:8A:7B
          inet addr:172.26.113.233  Bcast:172.26.113.235  Mask:255.255.255.252
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

eth1.175  Link encap:Ethernet  HWaddr 00:40:F4:91:8A:7B
          inet addr:172.26.114.241  Bcast:172.26.114.243  Mask:255.255.255.252
          inet6 addr: fe80::240:f4ff:fe91:8a7b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:89692 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1577 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:8694381 (8.2 Mb)  TX bytes:187133 (182.7 Kb)

eth1.177  Link encap:Ethernet  HWaddr 00:40:F4:91:8A:7B
          inet addr:172.26.114.249  Bcast:172.26.114.251  Mask:255.255.255.252
          inet6 addr: fe80::240:f4ff:fe91:8a7b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2115 errors:0 dropped:0 overruns:0 frame:0
          TX packets:28597 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

RX bytes:105750 (103.2 Kb) TX bytes:4372634 (4.1 Mb)

En el siguiente gráfico se observan las configuraciones realizadas:

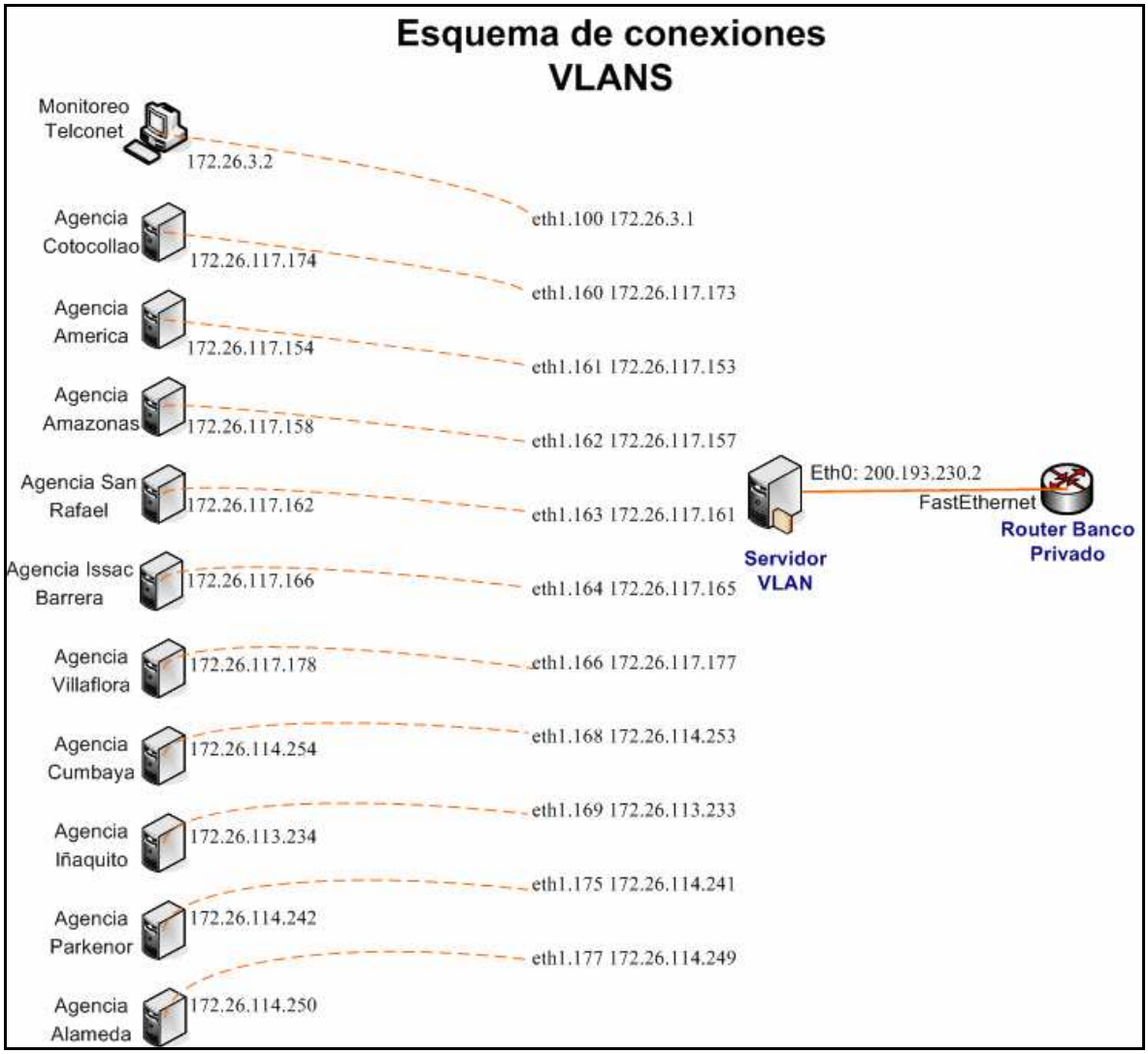


Figura 4.8 Esquema de conexiones por VLAN

4.2.2.4 Implementación de rutas estáticas

Las rutas estáticas que se levantan en el servidor VLAN son necesarias para direccionar los paquetes de cada una de las redes internas de las agencias bancarias, es decir, distinguir a que red pertenecen, y encaminar los paquetes por la VLAN asignada.

Las redes internas asignadas a las agencias bancarias son las siguientes:

Nombre Agencia Bancaria	Red Interna Asignada	# VLAN
Agencia Cotocollao	192.20.1.0/24	160
Agencia América	192.10.1.0/24	161
Agencia Amazonas	192.11.1.0/24	162
Agencia San Rafael	192.12.1.0/24	163
Agencia Issac Barrera	192.13.1.0/24	164
Agencia Villaflora	192.14.1.0/24	166
Agencia Cumbaya	192.15.1.0/24	168
Agencia Iñaquito	192.16.1.0/24	169
Agencia Parkenor	192.17.1.0/24	175
Agencia Alameda	192.22.1.0/24	177

Tabla 4.2 Asignación de redes internas.

Las rutas estáticas en el servidor VLAN para el encaminamiento de los paquetes hacia las redes internas son:

```
[root@tnnel-uio root]# ip route add 192.20.1.0/24 dev eth1.160
[root@tnnel-uio root]# ip route add 192.10.1.0/24 dev eth1.161
[root@tnnel-uio root]# ip route add 192.11.1.0/24 dev eth1.162
[root@tnnel-uio root]# ip route add 192.12.1.0/24 dev eth1.163
[root@tnnel-uio root]# ip route add 192.13.1.0/24 dev eth1.164
[root@tnnel-uio root]# ip route add 192.14.1.0/24 dev eth1.166
[root@tnnel-uio root]# ip route add 192.15.1.0/24 dev eth1.168
[root@tnnel-uio root]# ip route add 192.16.1.0/24 dev eth1.169
[root@tnnel-uio root]# ip route add 192.17.1.0/24 dev eth1.175
[root@tnnel-uio root]# ip route add 192.22.1.0/24 dev eth1.177
```

Se pueden divisar las rutas levantadas con:

```
[root@tnnel-uio root]# route -n |grep
192.20.1.0  0.0.0.0       255.255.255.0 U    0      0        0 eth1.160
192.10.1.0  0.0.0.0       255.255.255.0 U    0      0        0 eth1.161
192.11.1.0  0.0.0.0       255.255.255.0 U    0      0        0 eth1.162
192.12.1.0  0.0.0.0       255.255.255.0 U    0      0        0 eth1.163
192.13.1.0  0.0.0.0       255.255.255.0 U    0      0        0 eth1.164
192.14.1.0  0.0.0.0       255.255.255.0 U    0      0        0 eth1.166
```

```
192.15.1.0  0.0.0.0         255.255.255.0 U     0      0        0 eth1.168
192.16.1.0  0.0.0.0         255.255.255.0 U     0      0        0 eth1.169
192.17.1.0  0.0.0.0         255.255.255.0 U     0      0        0 eth1.175
192.22.1.0  0.0.0.0         255.255.255.0 U     0      0        0 eth1.177
```

4.2.2.5 Configuraciones de seguridad

En el servidor de VLANS se configuran los siguientes parámetros de seguridad:

1.- Acceso físico al servidor VLAN, tienen acceso solo personal autorizado del banco.

2.- Servicios que se levantan al iniciar el sistema operativo, esto es si por alguna razón es necesario reiniciar el servidor, solo deben subir los servicios configurados para que trabajen de acuerdo a las necesidades establecidas. Es necesario mencionar que las configuraciones realizadas están guardadas en un archivo, que se inicia de forma automática al iniciarse el sistema operativo.

```
[root@tnnel-uio etc]# pwd
/etc
[root@tnnel-uio etc]# ls -al reglas
-rwx------  1 root root 7 Jul  20 16:25 reglas
```

Este archivo con permisos de ejecución esta asociado con un link (enlace o encadenador) denominado S200net para que suban las sentencias escritas en el mismo, al momento de iniciar el sistema operativo.

```
[root@tnnel-uio rc3.d]# pwd
/etc/rc3.d
[root@tnnel-uio rc3.d]# ln -s /etc/reglas S200net

[root@tnnel-uio rc3.d]# ls -al S200net
lrwxrwxrwx  1 root root 11 Jul  20 18:36 S100net -> /etc/reglas
```

Esto indica que el link S200net, al momento de arrancar el sistema operativo del servidor VLAN se ejecuta automáticamente haciendo la llamada al archivo reglas,

en el mismo que se encuentran las configuraciones para que se levanten las VLANS, las direcciones IP y las rutas estáticas, además suben varios servicios del sistema operativo:

crond.- para realizar tareas automáticas, es utilizado para sacar respaldos de los archivos de configuraciones.

iptables.- es un sistema de firewall vinculado al kernel de Linux, es utilizado para crear reglas de firewall en el servidor VLAN.

kudzu.- este servicio se utiliza para que detecte de forma automática los cambios físicos de dispositivos en el servidor VLAN en caso de ser necesario.

network.- para levantar los servicios asociados a la red.

sshd.- es usado para acceso remoto seguro al servidor VLAN.

syslog.- es utilizado para que se guarden en el disco duro todos los logs del sistema operativo.

xfs.- para tener un sistema de archivos de alto rendimiento.

xinetd.- es utilizado para administrar los ficheros /etc/hosts.allow y /etc/hosts.deny para configurar el acceso a los servicios del sistema.

Para poder activar o desactivar que los servicios instalados se levanten al iniciar el sistema operativo se ejecuta lo siguiente en la pantalla de consola del servidor VLAN:

[root@tnnel-uio root]# ntsysv

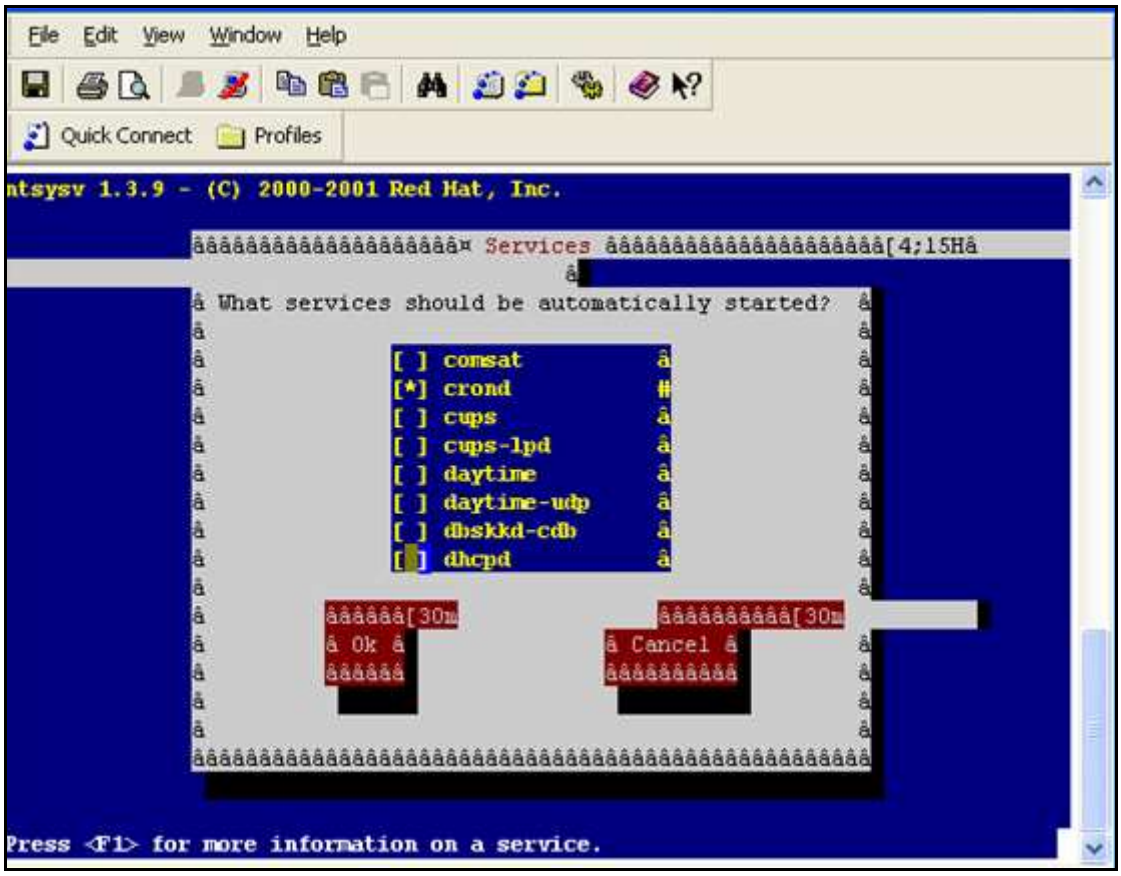


Figura 4.9 Pantalla de consola de servicios de Linux.

Con la barra espaciadora se selecciona o se quita el asterisco (*) que indica los servicios que se levantarán al inicial el sistema operativo, luego de seleccionar los necesarios se presiona el botón OK. Se puede levantar el servicio sin necesidad de reiniciar el servidor con la siguiente línea de comando:

[root@tnnel-uio root]# service crond start

donde crond es el nombre del servicio y la opción start inicia el mismo, se puede usar 3 opciones: start para inicial el servicio, stop para detener el servicio y restart para reiniciar el servicio.

3.- Acceso al servidor controlado por direcciones IP, esto se lo realiza a través de TCP-Wrappers, por lo que se utiliza dos archivos que se encuentran en el servidor VLAN, estos archivos son:

/etc/hosts.allow
/etc/hosts.deny

En el archivo hosts.allow se configura las direcciones IP que tendrán acceso a determinado servicio, en el archivo hosts.deny en cambio se restringe todo, quedando habilitados solo los accesos que estén configurados en el archivo hosts.allow. En el servidor VLAN se tiene:

```
[root@tnnel-uio root]# more /etc/hosts.allow
#
# hosts.allow   This file describes the names of the hosts which are
#               allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#
sshd : 172.26.3.2 172.26.3.3 172.26.3.4 172.26.3.5 172.26.3.6
```

```
[root@tnnel-uio root]# more /etc/hosts.deny
#
# hosts.deny    This file describes the names of the hosts which are
#               *not* allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#
# The portmap line is redundant, but it is left to remind you that
# the new secure portmap uses hosts.deny and hosts.allow.  In particular
# you should know that NFS uses portmap!
ALL : ALL
```

4.- Conexiones seguras hacia el servidor VLAN, que son realizadas por medio del servicio sshd, las sesiones de conexión al servidor para su administración son realizadas con sesiones seguras, el servicio sshd permite este requerimiento, y solo direcciones IP permitidas pueden conectarse.

4.3 PRUEBAS DE CONEXIÓN

Las pruebas de conexión se realizan entre los dispositivos de comunicación de las agencias bancarias con el servidor VLAN, para lo cual se utiliza el comando ping, el mismo que sirve para obtener el tiempo de respuesta de ida y vuelva de un paquete enviado desde el servidor VLAN hacia cada agencia bancaria.

Para la comprobación desde el servidor VLAN, se utiliza el ping extendido, es decir, se hace ping desde la dirección IP origen de la red en el servidor hacia la dirección IP destino que pertenece a la misma red. Para poder comprender mejor se tiene el siguiente ejemplo:

```
ping -I 172.26.117.173 172.26.117.174
```

En donde el parámetro –I indica desde que dirección IP origen sale en paquete para que sea devuelto a la misma, en este caso el paquete sale con dirección IP origen 172.26.117.173 hacia la dirección IP 172.26.117.174.

Para las pruebas se ingresa en el servidor VLAN mediante el servicio ssh y se realiza envío/recepción de paquetes por medio del comando ping, hacia cada agencia bancaria.

Agencia Cotocollao:

[root@tnnel-uio root]# ping -I 172.26.117.173 172.26.117.174

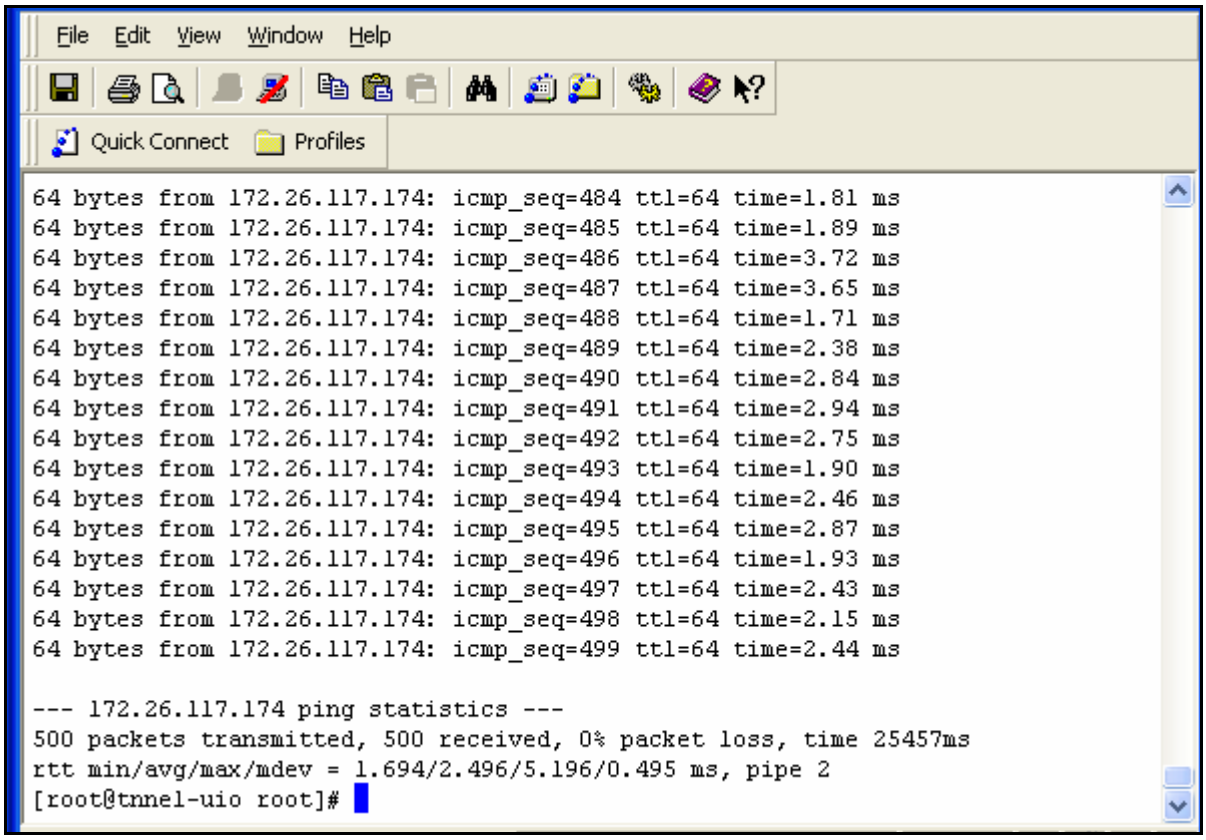


Figura 4.10 Prueba de conexión de la Agencia Cotocollao

Datos Obtenidos:

Paquetes transmitidos: 500

Paquetes recibidos: 500

Paquetes perdidos: 0

Tiempo promedio de respuesta: 2.4ms.

Agencia América:

[root@tnnel-uio root]# ping -I 172.26.117.153 172.26.117.154

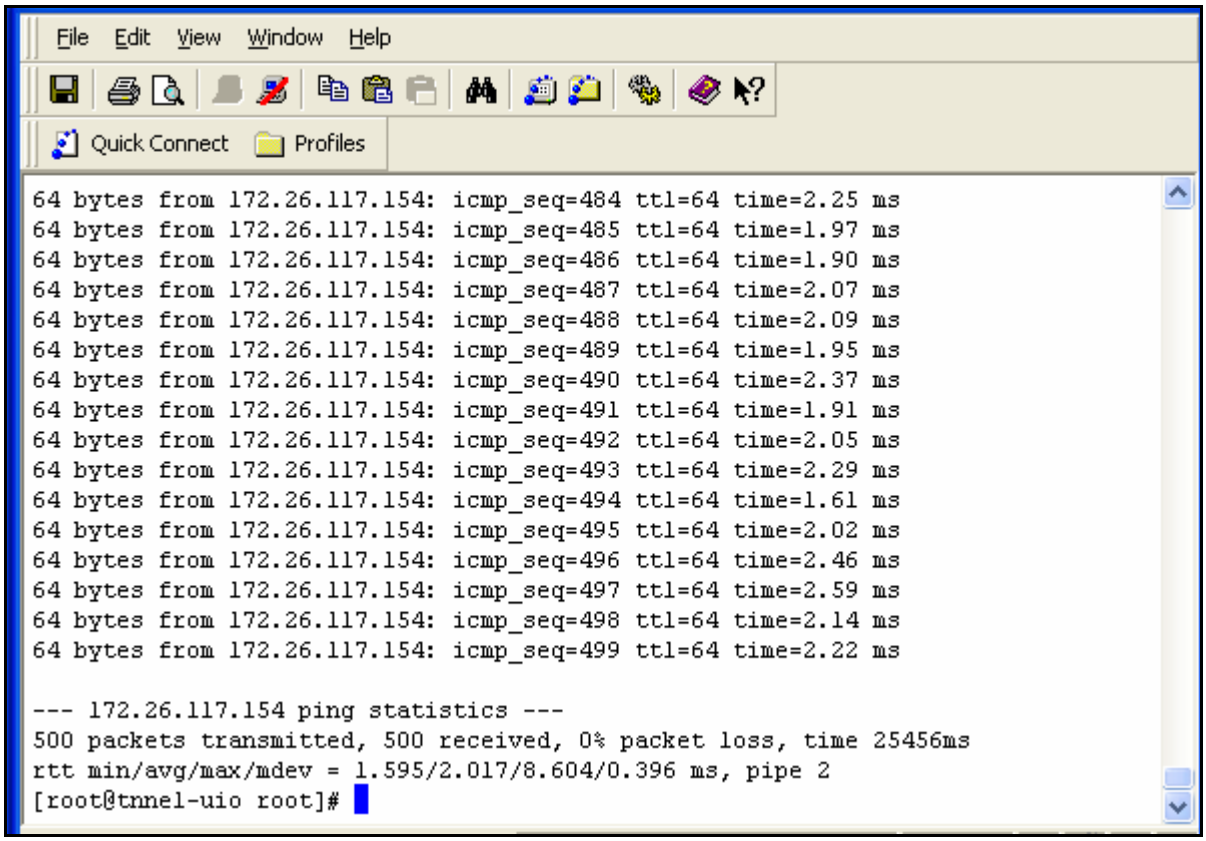


Figura 4.11 Prueba de conexión de la Agencia América

Datos Obtenidos:

Paquetes transmitidos: 500

Paquetes recibidos: 500

Paquetes perdidos: 0

Tiempo promedio de respuesta: 2.0ms.

Agencia Amazonas:

[root@tnnel-uio root]# ping -I 172.26.117.157 172.26.117.158

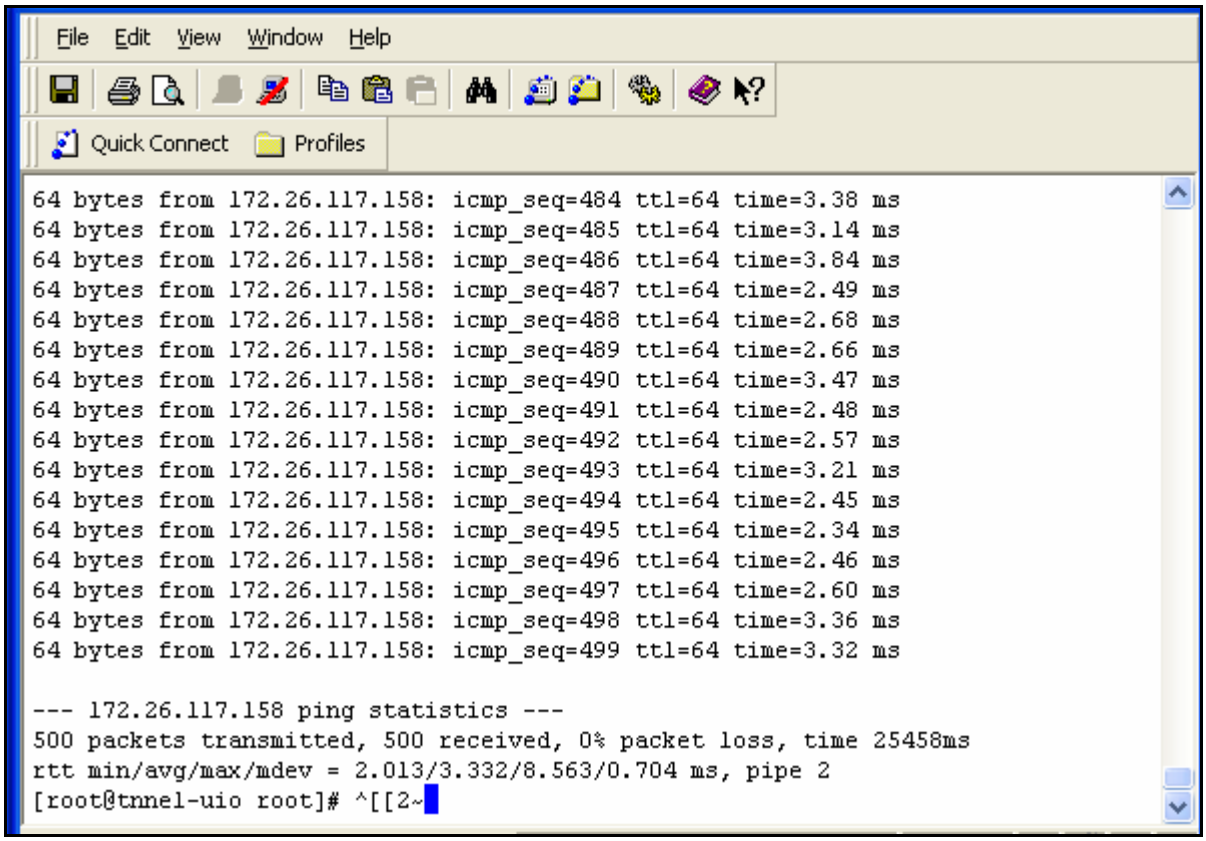


Figura 4.12 Prueba de conexión de la Agencia Amazonas

Datos Obtenidos:

- Paquetes transmitidos: 500
- Paquetes recibidos: 500
- Paquetes perdidos: 0
- Tiempo promedio de respuesta: 3.3ms.

Agencia San Rafael:

[root@tnnel-uio root]# ping -I 172.26.117.161 172.26.117.162

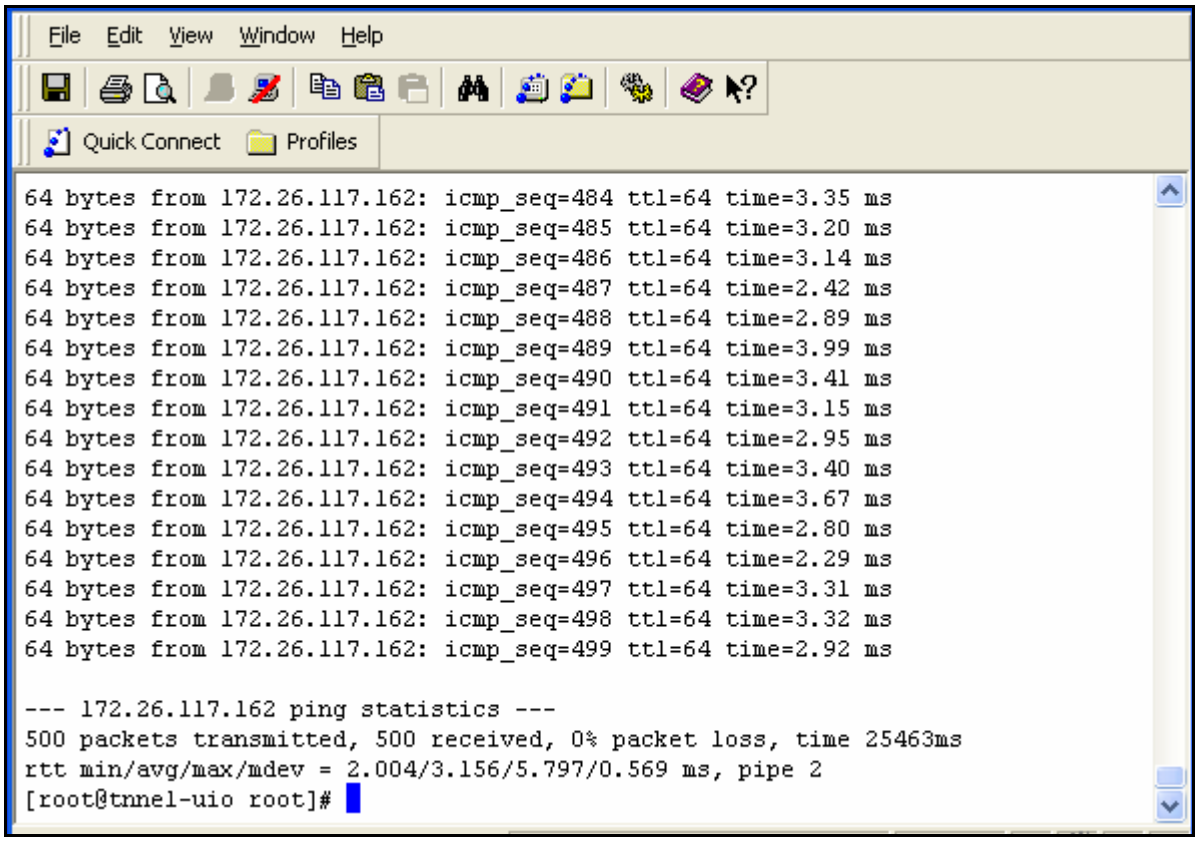


Figura 4.13 Prueba de conexión de la Agencia San Rafael

Datos Obtenidos:

Paquetes transmitidos: 500

Paquetes recibidos: 500

Paquetes perdidos: 0

Tiempo promedio de respuesta: 3.1ms.

Agencia Issac Barrera:

[root@tnnel-uio root]# ping -I 172.26.117.165 172.26.117.166

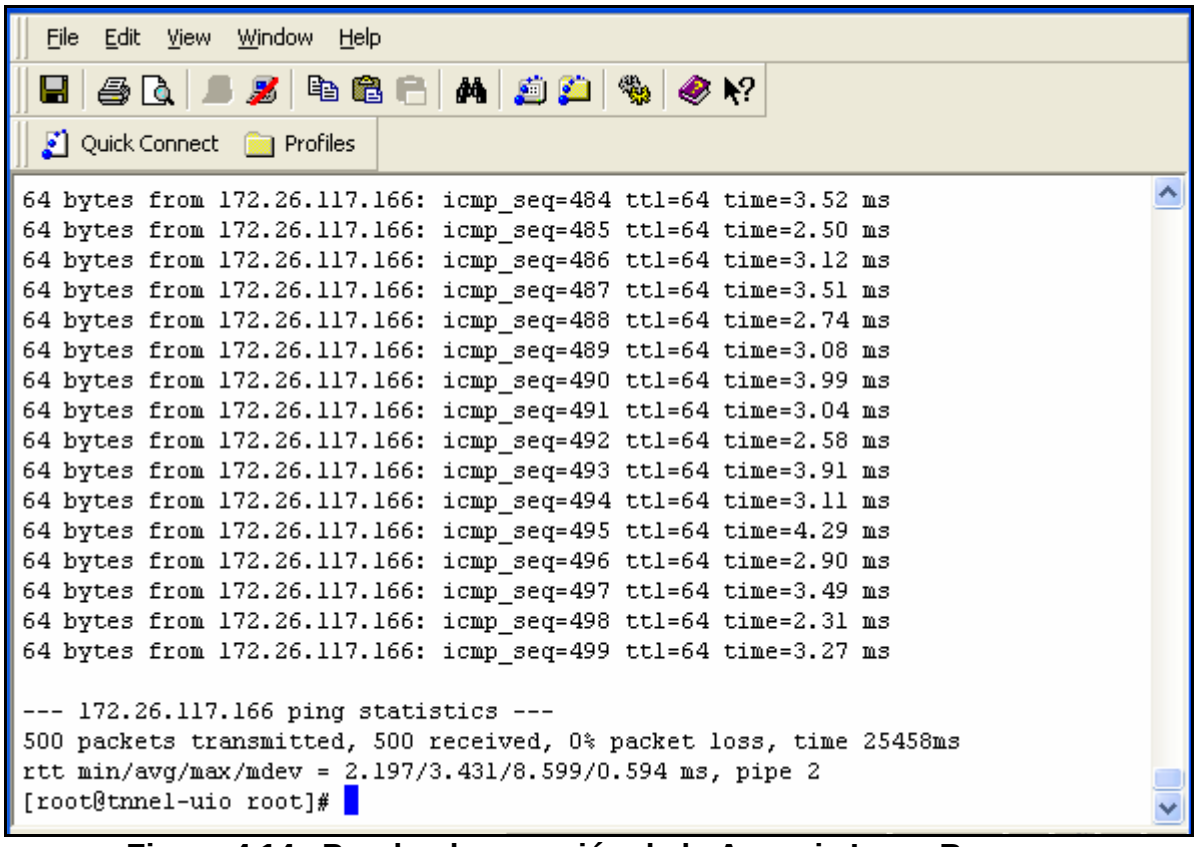


Figura 4.14 Prueba de conexión de la Agencia Issac Barrera

Datos Obtenidos:

Paquetes transmitidos: 500

Paquetes recibidos: 500

Paquetes perdidos: 0

Tiempo promedio de respuesta: 3.4ms.

Agencia Villaflora:

[root@tnnel-uio root]# ping -I 172.26.117.177 172.26.117.178

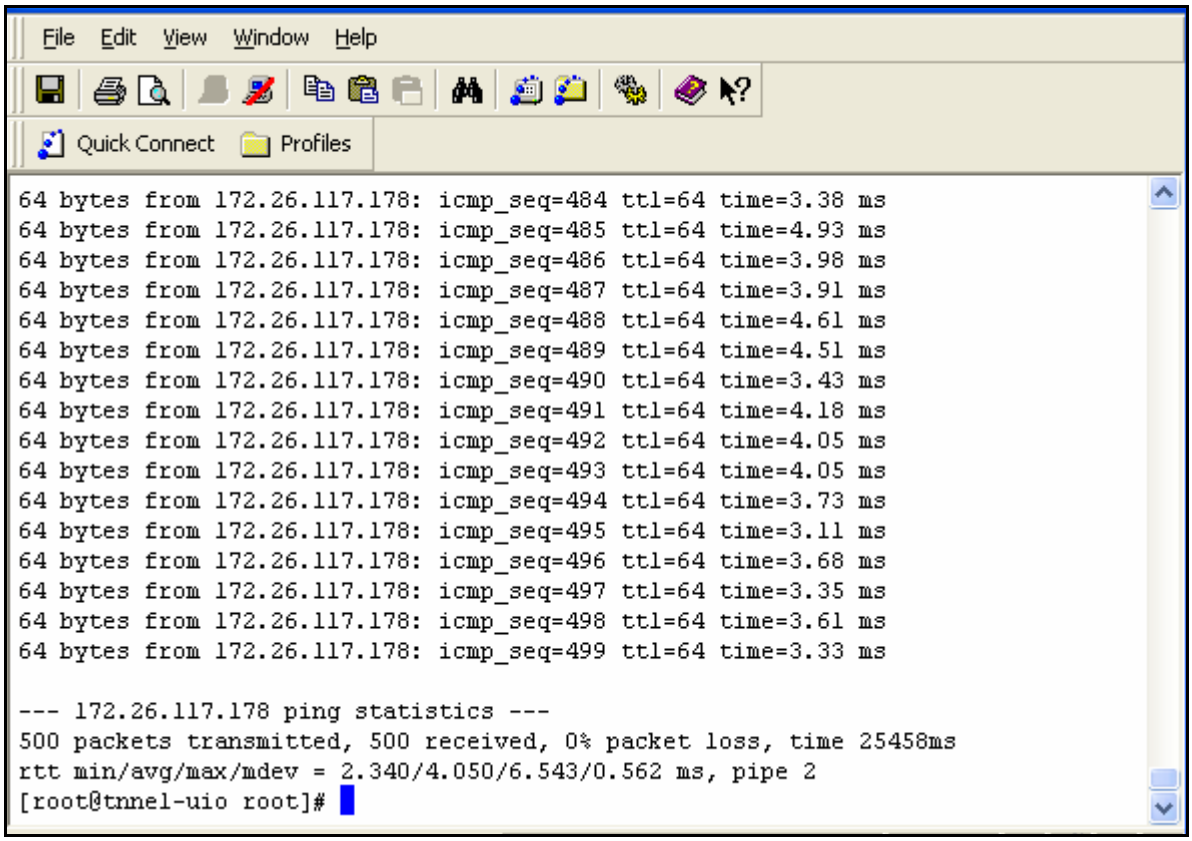


Figura 4.15 Prueba de conexión de la Agencia Villaflora

Datos Obtenidos:

Paquetes transmitidos: 500

Paquetes recibidos: 500

Paquetes perdidos: 0

Tiempo promedio de respuesta: 4.0ms.

Agencia Cumbaya:

[root@tnnel-uio root]# ping -I 172.26.114.253 172.26.114.254

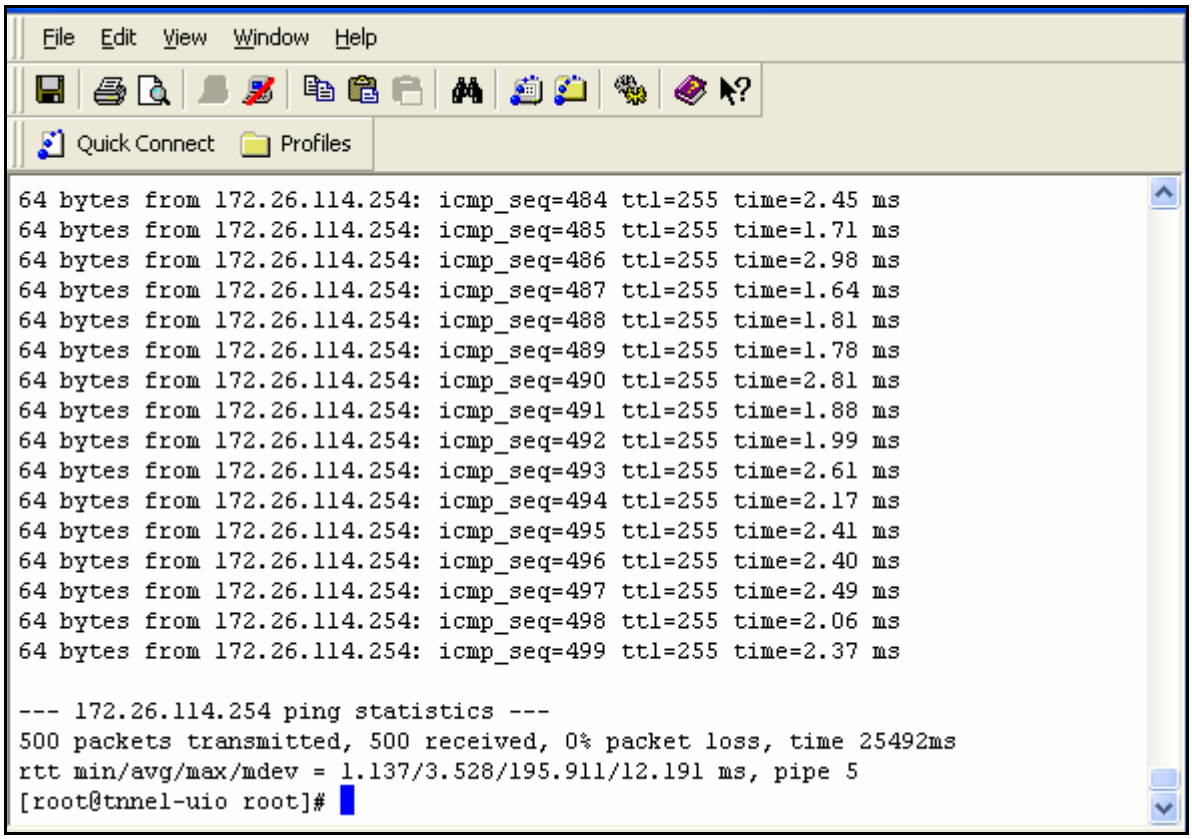


Figura 4.16 Prueba de conexión de la Agencia Cumbaya

Datos Obtenidos:

Paquetes transmitidos: 500

Paquetes recibidos: 500

Paquetes perdidos: 0

Tiempo promedio de respuesta: 3.5ms.

Agencia Iñaquito:

[root@tnnel-uio root]# ping -I 172.26.113.233 172.26.113.234

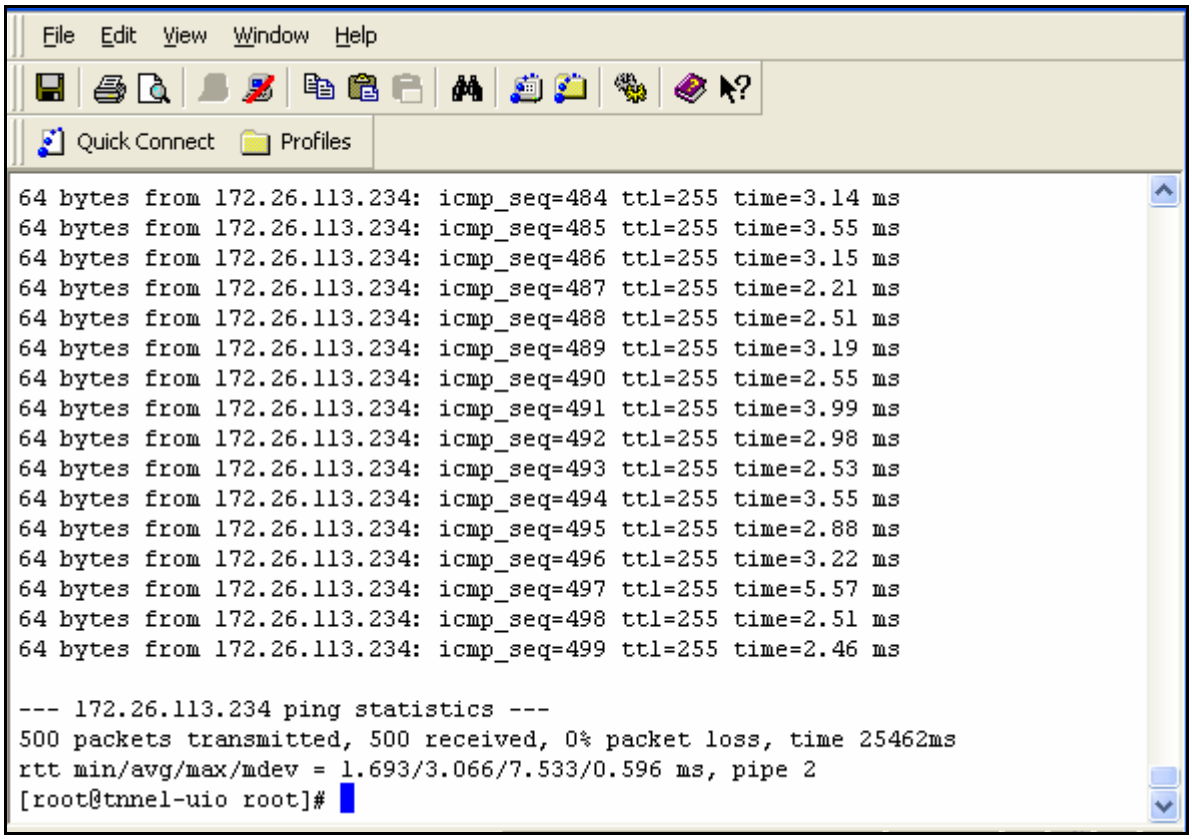


Figura 4.17 Prueba de conexión de la Agencia Iñaquito

Datos Obtenidos:

Paquetes transmitidos: 500

Paquetes recibidos: 500

Paquetes perdidos: 0

Tiempo promedio de respuesta: 3.0ms.

Agencia Parkenor:

[root@tnnel-uio root]# ping -I 172.26.114.241 172.26.114.242

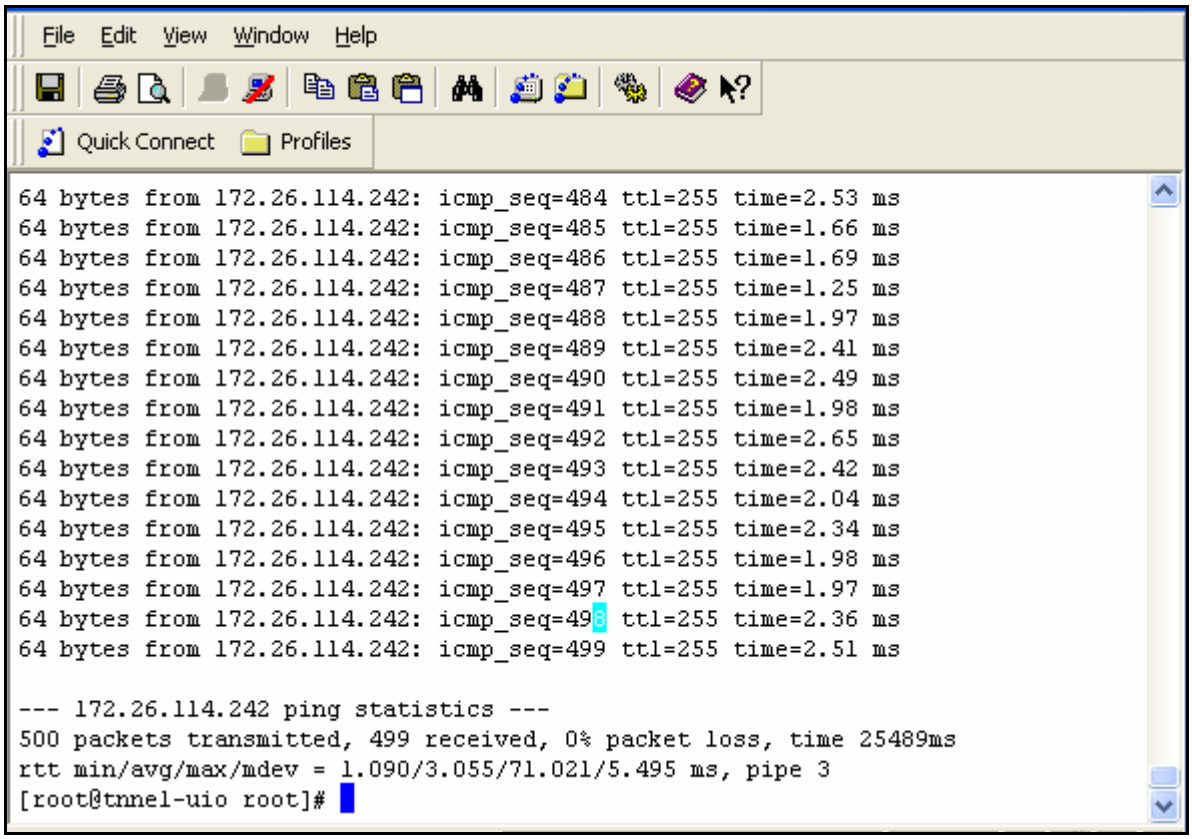


Figura 4.18 Prueba de conexión de la Agencia Parkenor

Datos Obtenidos:

Paquetes transmitidos: 500

Paquetes recibidos: 500

Paquetes perdidos: 0

Tiempo promedio de respuesta: 3.0ms.

Agencia Alameda:

[root@tnnel-uio root]# ping -I 172.26.114.249 172.26.114.250

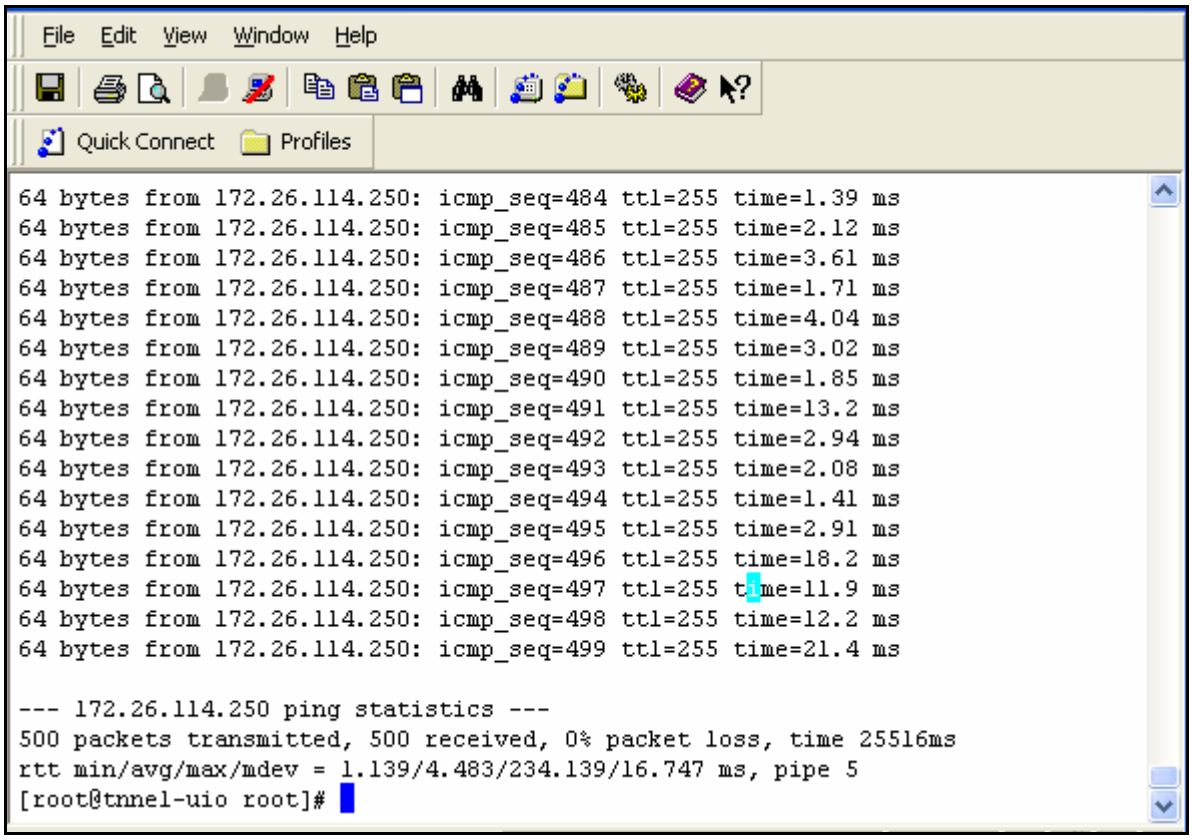


Figura 4.19 Prueba de conexión de la Agencia Alameda

Datos Obtenidos:

Paquetes transmitidos: 500

Paquetes recibidos: 500

Paquetes perdidos: 0

Tiempo promedio de respuesta: 4.4ms.

De las pruebas realizadas a cada una de las agencias, todos los enlaces están aptos para la transmisión de datos, los tiempos de respuesta son estables y no existen paquetes duplicados o perdidos.

4.4 INTERCONEXIÓN DE LAS AGENCIAS CON LA MATRIZ DEL BANCO

Este tema se refiere a la transmisión de datos desde la red interna de cada agencia hacia la matriz, a los servidores de la institución bancaria.

Una vez comprobados los enlaces desde el servidor VLAN hacia cada una de las agencias bancarias, en la matriz se procede a conectar el cable UTP que va desde la interfaz eth0 del servidor hacia la interfaz ethernet del router de la institución bancaria.

En el router se deberán configurar las rutas para poder alcanzar las redes internas de las agencias bancarias, esto se debe hacer indicando que la puerta de enlace para alcanzar las redes sea la dirección IP eth0 del servidor VLAN.

Una vez que los paquetes lleguen hacia el servidor, éste será el encargado de direccionarlos hacia la agencia correspondiente por medio de las rutas estáticas que ya fueron levantadas.

Por motivos de seguridad de la institución bancaria no se pueden observar las conexiones desde las redes internas de las agencias hacia las redes internas de la matriz, esto es exclusivo del banco, pero si hubiesen los accesos necesarios bastaría con hacer ping desde una maquina de la red interna de alguna agencia hacia uno de los servidores de la matriz.

4.5 SISTEMA DE MONITOREO DE LA RED BANCARIA

El sistema de monitoreo de la red bancaria por parte de Telconet se lo realizará utilizando software especializado para éste propósito:

- Monitoreo con WhatsUP
- Monitoreo con MRTG

4.5.1 MONITOREO CON WHATSUP

WhatsUp es una solución de mapeado, monitorización, notificación, e informes de rendimiento para redes, fácil de usar, que ayuda a los ingenieros y administradores de red a detectar y resolver los problemas de la red con rapidez.

El esquema de monitoreo de la red bancaria por medio de WhatsUP es el siguiente:

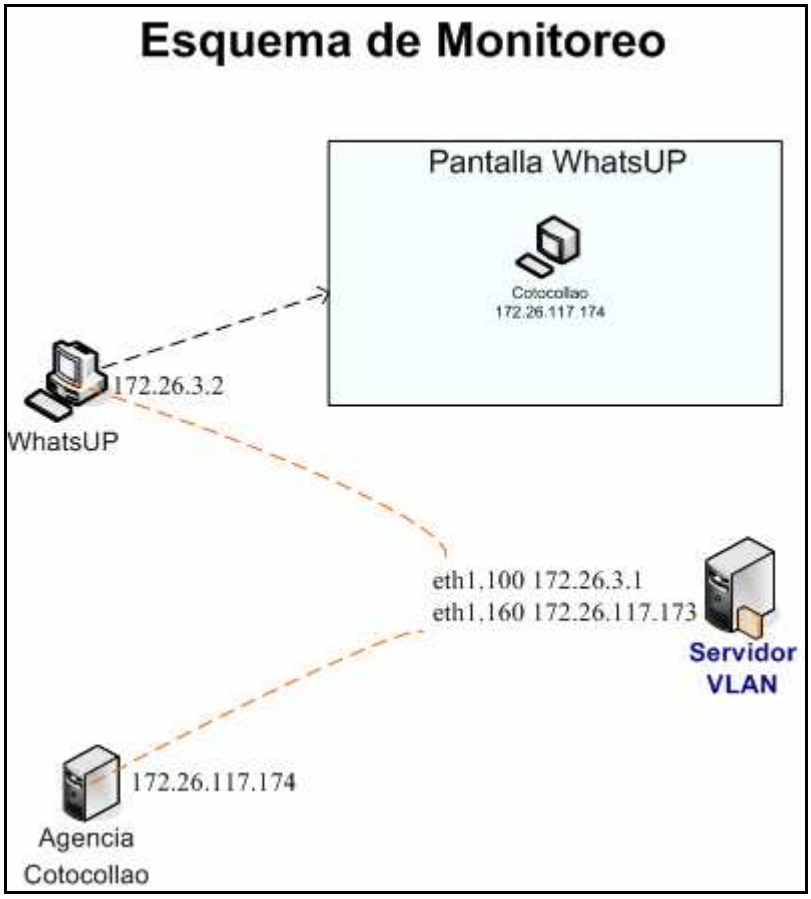


Figura 4.20 Esquema de monitoreo con WhatsUP

El equipo para monitoreo tiene instalado sistema operativo Windows 2000 profesional, y el software WhatsUP Gold versión 7.02, con licencia para uso de Telconet.

Este equipo tiene la dirección IP 172.26.3.2 con mascara de red 255.255.255.128 y con puerta de enlace 172.26.3.1, esta conectado al Backbone de Telconet sobre la VLAN 100, por medio de esta se enlaza al servidor VLAN, que es donde convergen todas las redes de la institución bancaria, y desde éste puede llegar a través del protocolo ICMP hacia cada una de las agencias y por ende poder monitorear el estado de los enlaces, que es lo que le corresponde a Telconet.

El software de monitoreo WhatsUP es fácil de instalar y de configurar, tan solo se necesita graficar los dispositivos a monitorear y especificar mediante que protocolo se realizará el monitoreo, para este caso se utiliza el protocolo ICMP Internet Control Messages Protocol - Protocolo de Control de Mensajes Internet), es básicamente como realizar ping desde la maquina de monitoreo hacia los equipos de comunicación de las agencias, esto de forma visualizada y en caso de problemas de los enlaces, con sus respectivas alarmas.

WhatsUP tiene dos funciones principales para su gestión que son edición y monitoreo.

En la función de edición se grafican los dispositivos a monitorear, simplemente se arrastra el tipo de dispositivo y se configura en la opción de las propiedades del mismo:

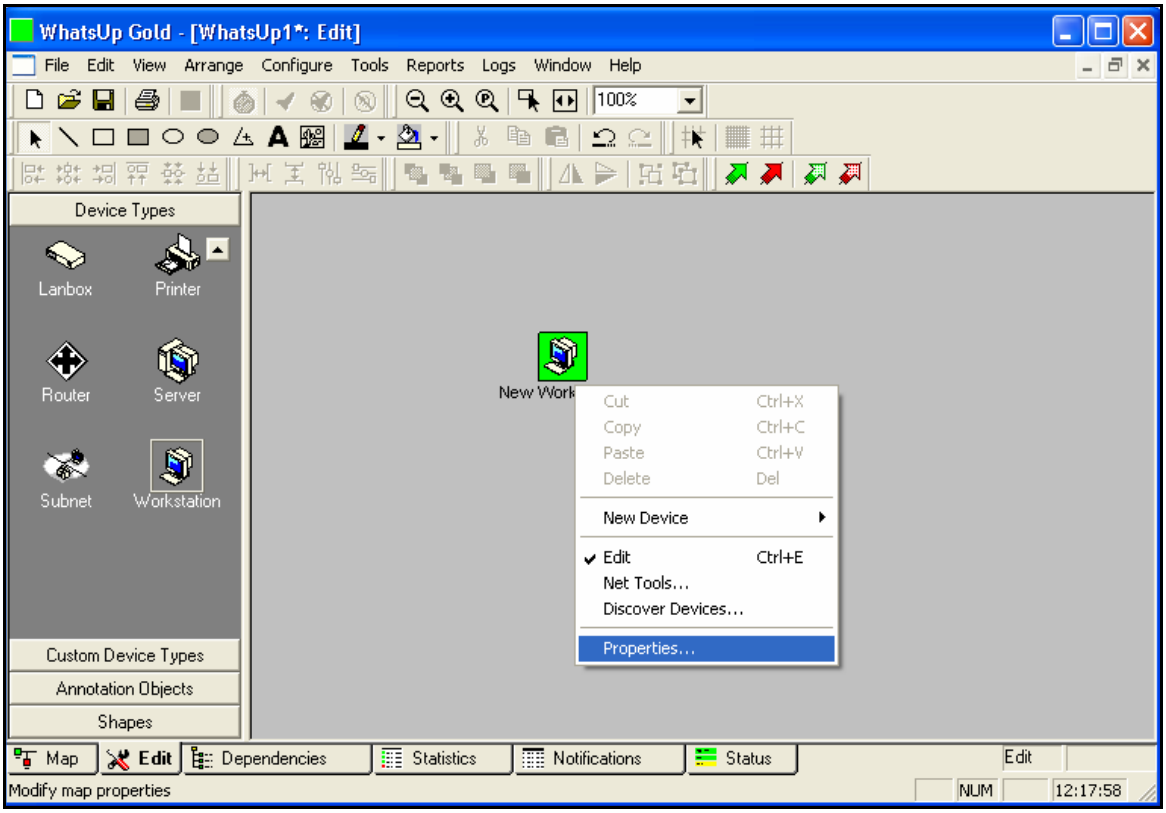


Figura 4.21 Modo de edición de WhatsUP

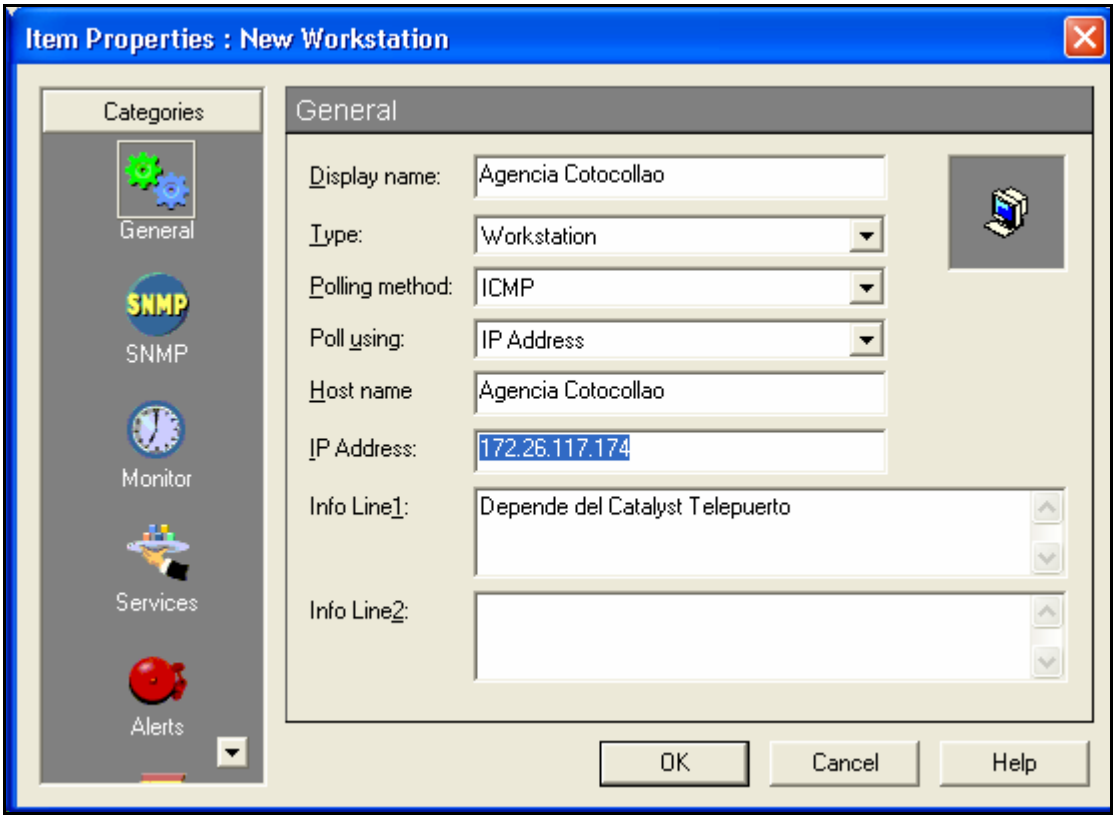


Figura 4.22 Propiedades del dispositivo

Además en la opción de alertas se escoge el tipo de alerta que se desea configurar para la notificación en el caso de caídas de los enlaces, Telconet utiliza la alerta de sonido para alarmar al personal de soporte técnico que están monitoreando los enlaces:

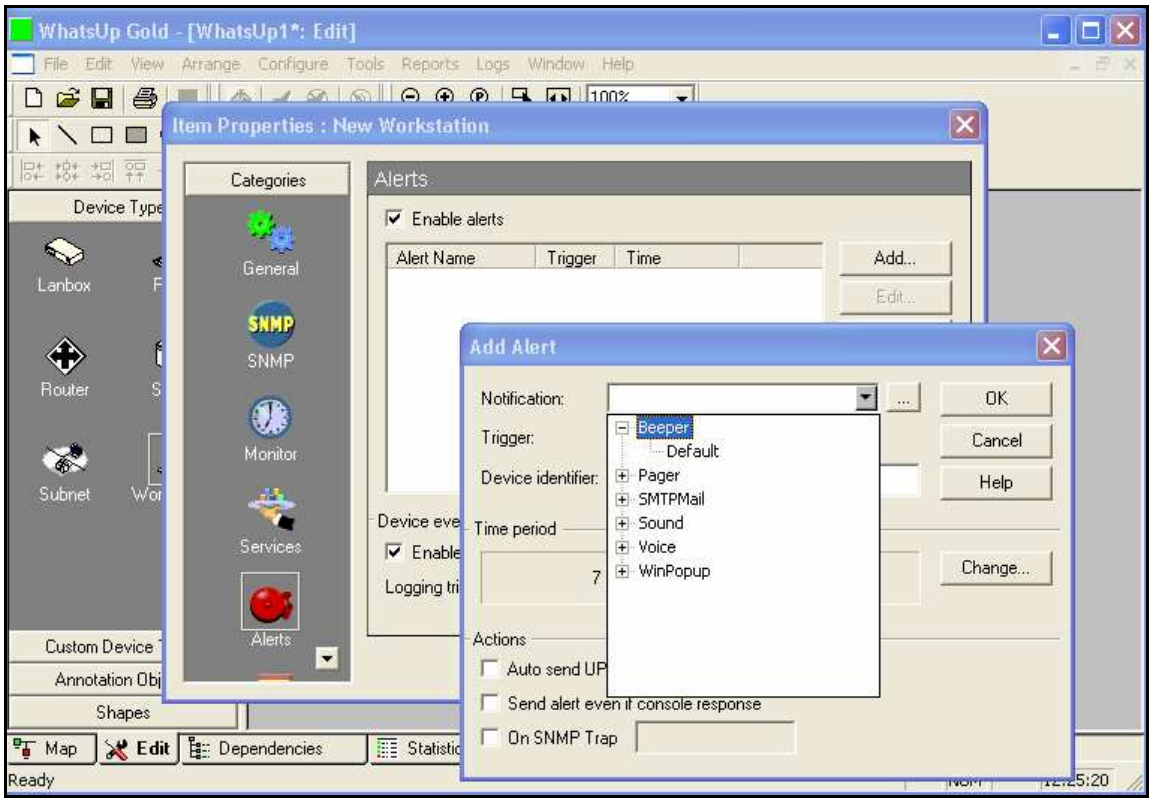


Figura 4.23 Funciones de alertas de WhatsUP

Terminado de graficar todos los dispositivos de la red bancaria a monitorearse, se utiliza la segunda función principal de WhatsUP que es el monitoreo de los dispositivos graficados, para esto simplemente se quita la función de edición y automáticamente WhatsUP empieza el monitoreo.

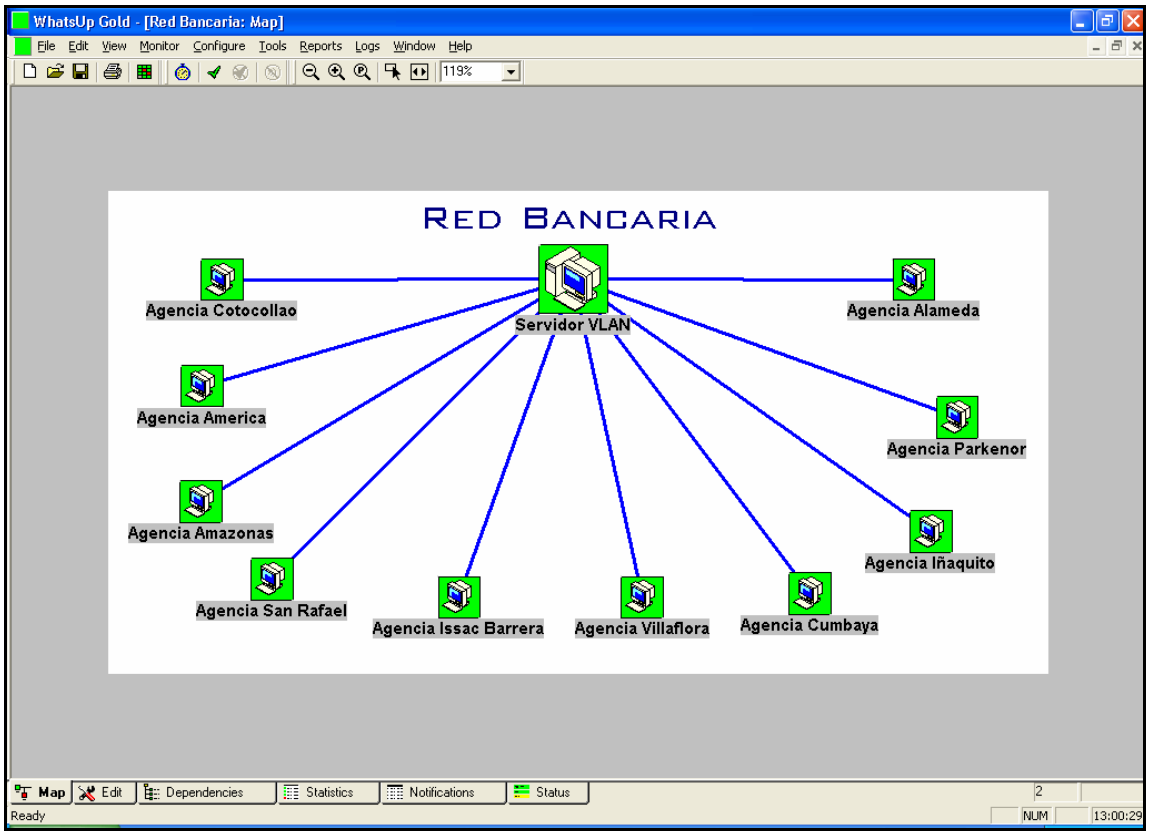


Figura 4.24 Función de monitoreo de WhatsUP

Todos los eventos ocurridos durante el monitoreo de la red bancaria mediante WhatsUP son registrados en los archivos logs propios del software, una de las herramientas de WhatsUP permite utilizar estos logs para poder sacar reportes de uptime de cada conexión, las mismas que son el respaldo de Telconet de la confiabilidad y estabilidad de los enlaces proporcionados al banco.

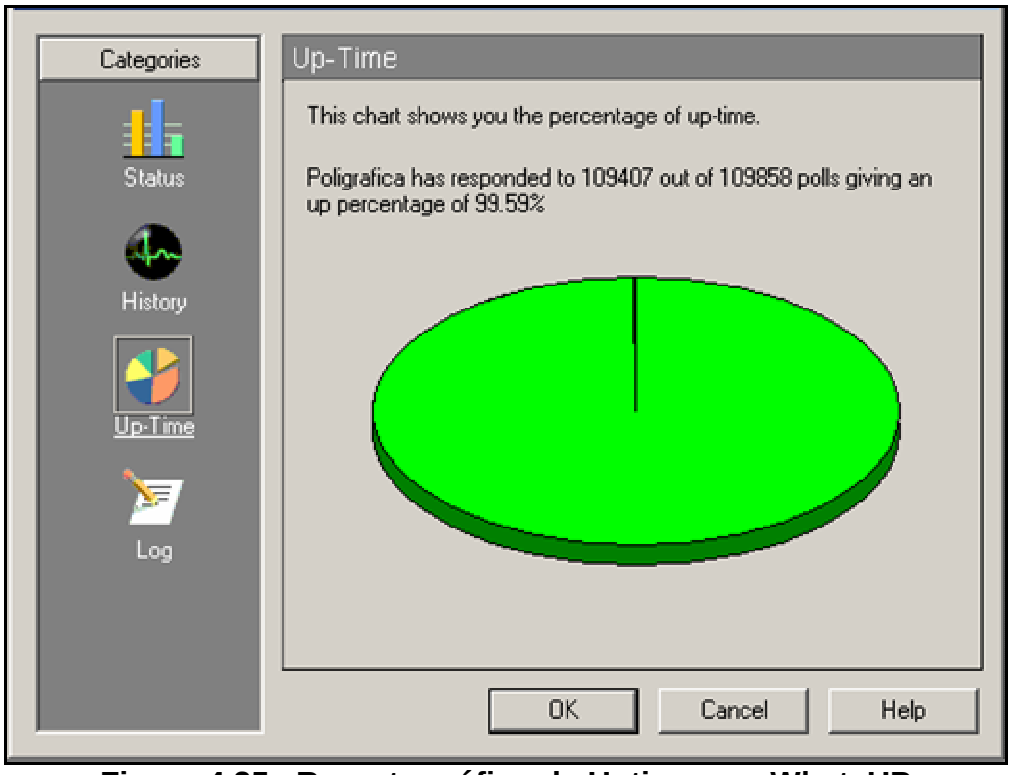


Figura 4.25 Reporte gráfico de Uptime con WhatsUP

4.5.2 MONITOREO CON MRTG

MRTG (Multi Router Traffic Grapher), es una herramienta para supervisar la carga de tráfico en los enlaces de red. MRTG genera páginas de HTML que contienen imágenes gráficas que proporcionan una representación visual de este tráfico.

MRTG está disponible gratuitamente según las condiciones de la Licencia pública GNU.

Se utiliza MRTG para monitorear el tráfico de los enlaces de las localidades bancarias, esto lo realiza Telconet monitoreando el tráfico de cada puerto de los switches cisco catalyst 3550 de donde depende cada entidad bancaria, el monitoreo se lo realiza por medio del protocolo SNMP (Simple Network Management Protocol) y con un servidor de MRTG en el que se tiene levantado el servicio httpd (servidor web linux) para poder divisar el tráfico a través de páginas Web.

El esquema del monitoreo mediante MRTG es el siguiente:

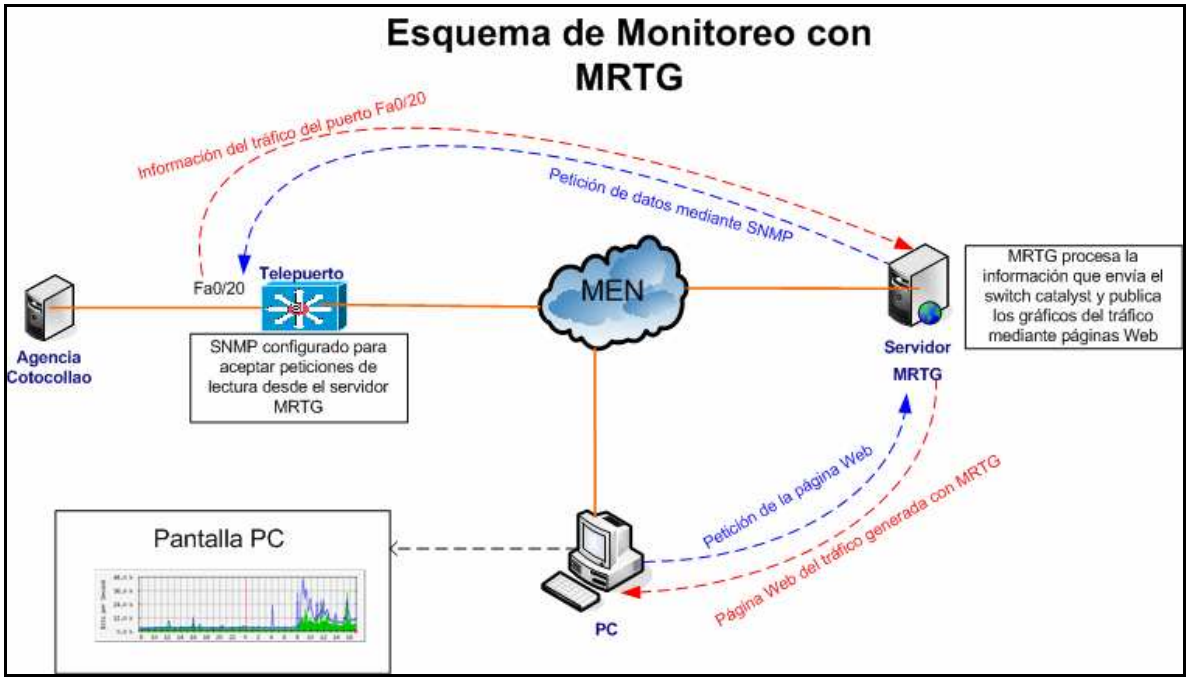


Figura 4.26 Esquema de monitoreo de tráfico utilizando MRTG

Como se observa en el gráfico, existe un servidor de MRTG de Telconet que monitorea mediante SNMP el tráfico de los puertos de los switch catalyst, el servidor hace la petición al switch y éste devuelve la información del tráfico generado en cada uno de los puertos, esta información es procesada en el servidor MRTG, el mismo que genera las paginas Web que muestran el tráfico.

Para la configuración del servicio SNMP en los switches cisco catalyst se debe crear una comunidad de lectura por medio de la cual el servidor MRTG pueda acceder a leer los datos.

El servidor MRTG tiene sistema operativo Linux Fedora Core 2, y están instalados los paquetes necesarios para que funcione el MRTG, el proceso de lectura de los datos lo realiza de manera automática cada 10 minutos, y las páginas Web que genera está publicadas mediante el servicio httpd en el mismo servidor.

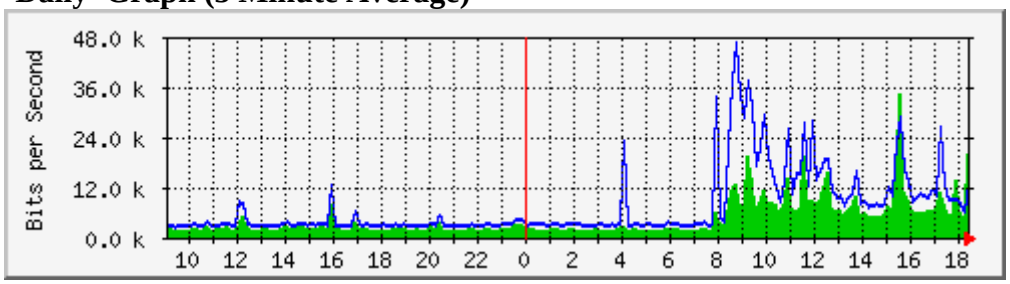
Mediante las páginas se puede observar las estadísticas de consumo del canal, en el caso de la entidad bancaria puede divisarlo para verificar si sus canales necesitan de ampliación del ancho de banda o no.

A continuación se muestra las gráficas del consumo diario de cada puerto del que depende cada entidad bancaria:

Agencia Cotocollao (128 Kbps): Catalyst Telepuerto: Fa0/20

The statistics were last updated **Monday, 10 October 2005 at 18:27**,
at which time **'sw1telepuerto.uio.telconet.net'** had been up for **5 days, 7:17:08**.

`Daily' Graph (5 Minute Average)

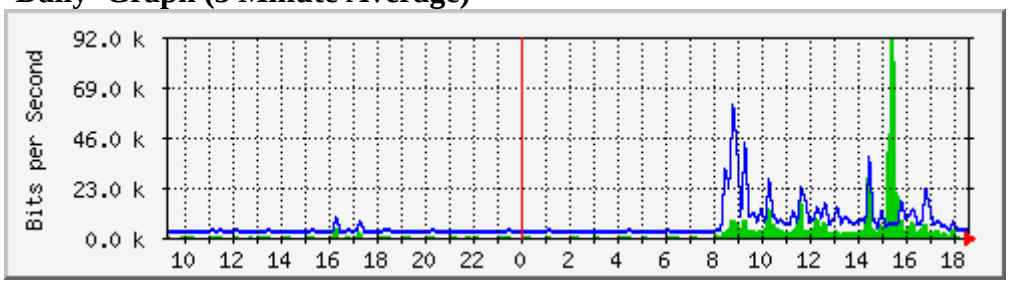


Max In:34.8 kb/s (0.3%) Average In:4632.0 b/s (0.0%) Current In:20.3 kb/s (0.2%)
Max Out:46.8 kb/s (0.5%) Average Out:7624.0 b/s (0.1%) Current Out:12.7 kb/s (0.1%)

Agencia América (128 Kbps): Catalyst OPS: Fa0/24

The statistics were last updated **Monday, 10 October 2005 at 18:39**,
at which time **'sw1ops.uio.telconet.net'** had been up for **46 days, 5:10:57**.

`Daily' Graph (5 Minute Average)

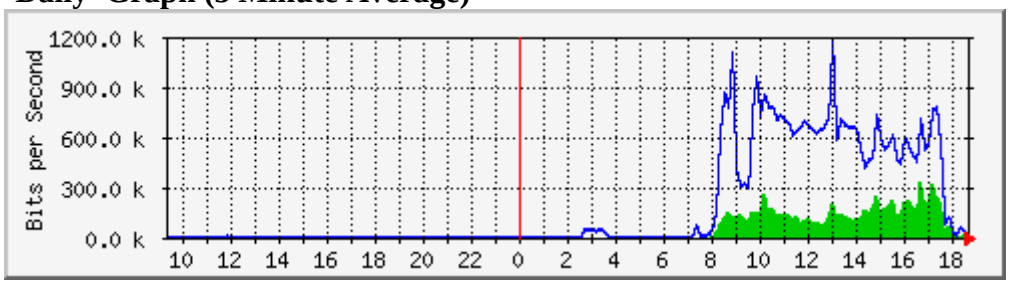


Max In:91.9 kb/s (0.9%) Average In:2848.0 b/s (0.0%) Current In: 432.0 b/s (0.0%)
Max Out:61.6 kb/s (0.6%) Average Out:6256.0 b/s (0.1%) Current Out:3416.0 b/s (0.0%)

Agencia Amazonas (1536 Kbps): Catalyst Cofiec: Fa0/23

The statistics were last updated **Monday, 10 October 2005 at 18:33**,
at which time **'sw1cofiec.uio.telconet.net'** had been up for **36 days, 8:36:06**.

`Daily' Graph (5 Minute Average)

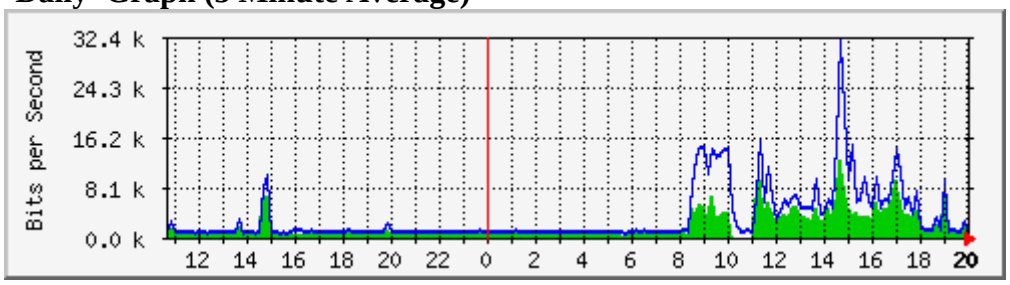


Max In: 337.5 kb/s (0.3%) Average In: 48.7 kb/s (0.0%) Current In:31.0 kb/s (0.0%)
Max Out:1197.9 kb/s (1.2%) Average Out:187.1 kb/s (0.2%) Current Out:25.6 kb/s (0.0%)

Agencia San Rafael (128 Kbps): Catalyst Tarqui2: Fa0/12

The statistics were last updated **Monday, 10 October 2005 at 20:02**,
at which time **'sw1tarqui2.uio.telconet.net'** had been up for **8 days, 3:32:06**.

`Daily' Graph (5 Minute Average)

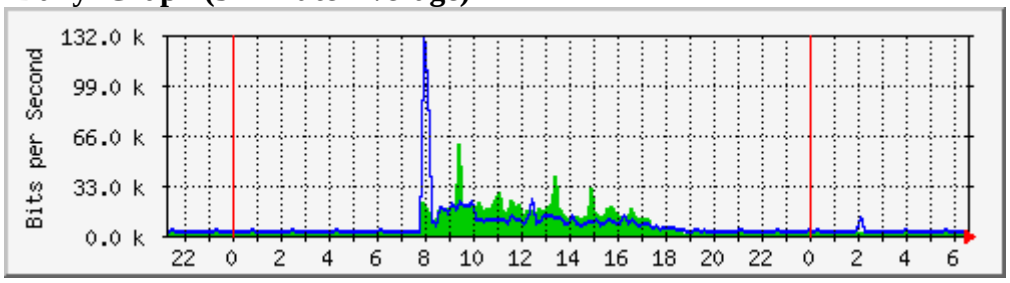


Max In:12.8 kb/s (0.0%) Average In:1952.0 b/s (0.0%) Current In:1016.0 b/s (0.0%)
Max Out:32.2 kb/s (0.0%) Average Out:3376.0 b/s (0.0%) Current Out:1024.0 b/s (0.0%)

Agencia Issac Barrera (128 Kbps): Catalyst Gaspar: Fa0/10

The statistics were last updated **Tuesday, 11 October 2005 at 6:38**,
at which time **'sw1gaspar.uio.telconet.net'** had been up for **32 days, 5:21:16**.

`Daily' Graph (5 Minute Average)

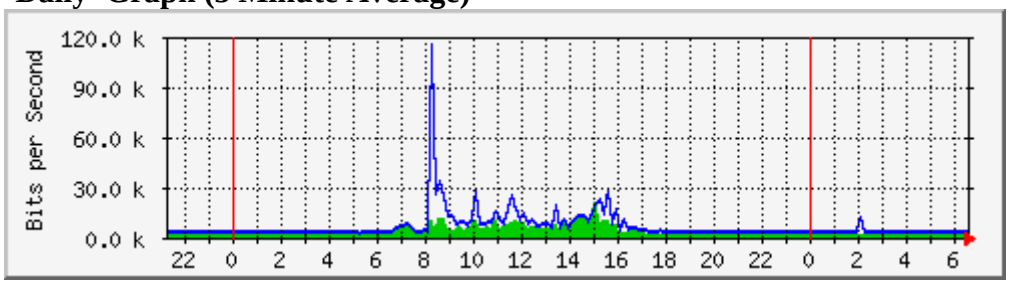


Max In: 60.9 kb/s (0.6%) Average In:7336.0 b/s (0.1%) Current In:2656.0 b/s (0.0%)
Max Out:131.7 kb/s (1.3%) Average Out:7288.0 b/s (0.1%) Current Out:3760.0 b/s (0.0%)

Agencia Villaflora (128 Kbps): Catalyst Sur2: Fa0/13

The statistics were last updated **Tuesday, 11 October 2005 at 6:37**,
at which time **'sw1sur2.uio.telconet.net'** had been up for **46 days, 16:08:13**.

`Daily' Graph (5 Minute Average)

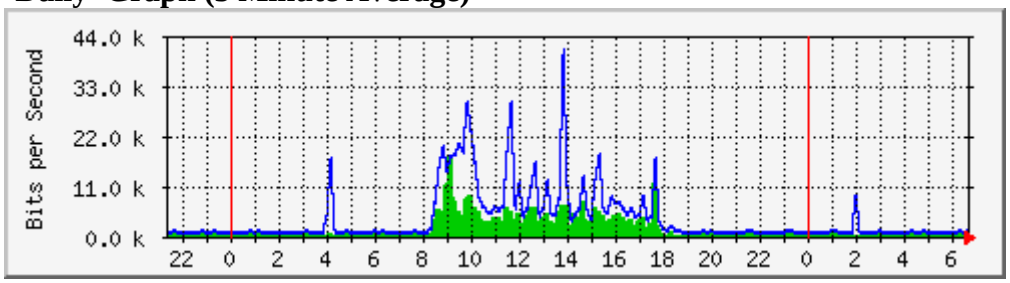


Max In: 22.0 kb/s (0.0%) Average In:4328.0 b/s (0.0%) Current In:2576.0 b/s (0.0%)
Max Out:115.5 kb/s (0.1%) Average Out:7024.0 b/s (0.0%) Current Out:3688.0 b/s (0.0%)

Agencia Cumbaya (128 Kbps): Catalyst ClickCenter: Fa0/19

The statistics were last updated **Tuesday, 11 October 2005 at 6:40**,
at which time **'sw1clickcenter.uio.telconet.net'** had been up for **6 days, 23:49:03**.

`Daily' Graph (5 Minute Average)

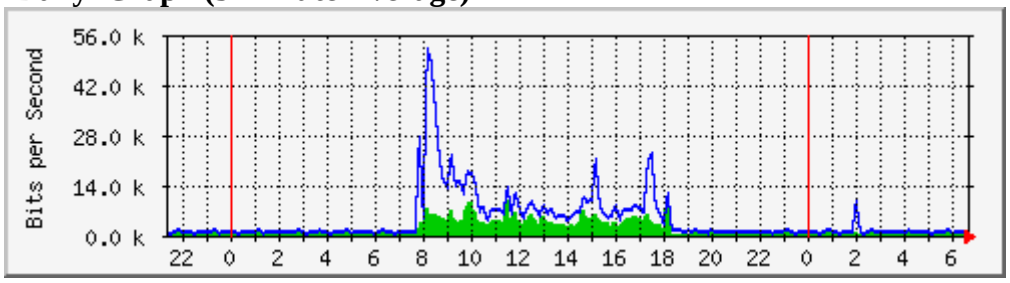


Max In:18.0 kb/s (0.2%) Average In:2096.0 b/s (0.0%) Current In:1240.0 b/s (0.0%)
Max Out:41.1 kb/s (0.4%) Average Out:4080.0 b/s (0.0%) Current Out:1688.0 b/s (0.0%)

Agencia Iñaquito (128 Kbps): Catalyst Gosseal: Fa0/24

The statistics were last updated **Tuesday, 11 October 2005 at 6:41**,
at which time **'sw1gosseal.uio.telconet.net'** had been up for **33 days, 20:21:08**.

`Daily' Graph (5 Minute Average)

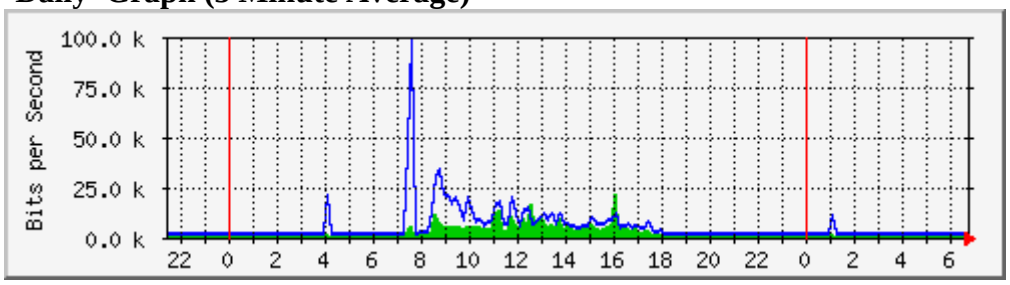


Max In:10.3 kb/s (0.0%) Average In:2128.0 b/s (0.0%) Current In: 768.0 b/s (0.0%)
Max Out:52.5 kb/s (0.1%) Average Out:4664.0 b/s (0.0%) Current Out:1312.0 b/s (0.0%)

Agencia Parkenor (128 Kbps): Catalyst Telepuerto: Fa0/21

The statistics were last updated **Tuesday, 11 October 2005 at 6:47**,
at which time '**sw1telepuerto.uio.telconet.net**' had been up for **5 days, 19:36:56**.

`Daily' Graph (5 Minute Average)

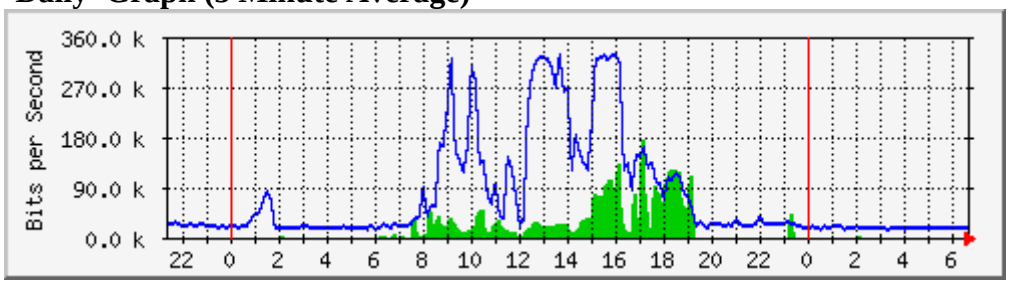


Max In:22.1 kb/s (0.0%) Average In:3136.0 b/s (0.0%) Current In:1464.0 b/s (0.0%)
Max Out:99.2 kb/s (0.1%) Average Out:5688.0 b/s (0.0%) Current Out:2216.0 b/s (0.0%)

Agencia Alameda (512 Kbps): Catalyst SwissHotel: Fa0/19

The statistics were last updated **Tuesday, 11 October 2005 at 6:41**,
at which time '**sw1swisshotel.uio.telconet.net**' had been up for **46 days, 17:03:25**.

`Daily' Graph (5 Minute Average)

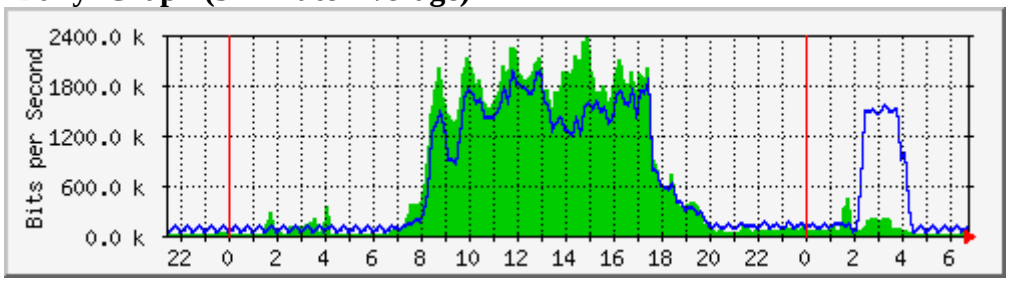


Max In:179.4 kb/s (1.8%) Average In:16.0 kb/s (0.2%) Current In:552.0 b/s (0.0%)
Max Out:328.8 kb/s (3.3%) Average Out:74.8 kb/s (0.7%) Current Out:18.0 kb/s (0.2%)

Matriz Bancaria (2560 Kbps): Catalyst Fondo: Fa0/13

The statistics were last updated **Tuesday, 11 October 2005 at 6:48**,
at which time '**sw1fondo.uio.telconet.net**' had been up for **33 days, 20:28:42**.

`Daily' Graph (5 Minute Average)



Max In:2386.0 kb/s (2.4%) Average In:614.0 kb/s (0.6%) Current In: 45.2 kb/s (0.0%)
Max Out:1974.6 kb/s (2.0%) Average Out:601.5 kb/s (0.6%) Current Out:130.9 kb/s (0.1%)

CAPITULO 5.

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Luego de realizar la implementación de la interconexión de las agencias con la matriz bancaria se han obtenido las siguientes conclusiones:

- Luego de haber aprendido los diferentes conceptos, tanto en redes de información, como en seguridades, y otros mas, en la carrera de Ingeniería Informática, es necesario recalcar que fueron de sustancial ayuda para poder realizar el diseño y la implementación del presente proyecto, puesto que se ha fortalecido la parte teórica de los estudios con la experiencia y parte técnica en el ámbito laborar.
- Las comunicaciones realizadas por medio de VLANS son seguras siempre que la administración de dicha seguridad sea realizada por personal técnico responsable tanto de la institución bancaria como de Telconet.
- Cada VLAN utiliza un dominio de broadcast, por lo que el tráfico de todo este dominio es independiente, con esto se elimina el riesgo de que un enlace que no pertenece al dominio de una VLAN en particular afecte los enlaces de otras VLANS.
- Telconet es una empresa en crecimiento y la tecnología MEN (Metro Ethernet Network) que utiliza, brinda grandes posibilidades de ampliación tanto del Backbone como de clientes, es similar que una LAN muy grande, y por tal motivo no es difícil de comprender su esquema de red, es adaptable para brindar soluciones de interconexión.
- Los switches cisco catalyst 3550 son equipos muy robustos que no solo funcionan como conmutadores, sino que también se puede configurar como router, es decir, se puede levantar direcciones IP en cada puerto y trabajar en capa 3 de acuerdo al modelo OSI, y sus seguridad por medio de direcciones MAC garantizan que a nivel de capa 2 solo puedan ingresar los equipos que son permitidos por el administrador de los switches.

- Actualmente las comunicaciones necesitan mas rapidez y capacidad de transportar datos, por lo tanto, los enlaces de fibra óptica son los más confiables para brindar éstas necesidades.
- Para formar las VLANS no es necesario tener equipos de las mismas características pero si es necesario que trabajen con el mismo protocolo, es decir, con 802.1q que es el estándar para formar las VLANS, esto hace que para formar redes VLANS no se deba utilizar un solo tipo de equipos de acuerdo al fabricante, sino que se pueda utilizar varios modelos de equipos y de diferentes marcas.
- El sistema operativo Linux Fedora Core 2, es muy estable y apropiado para trabajar en ambientes de redes TCP/IP, puede ser utilizado como router y la mayoría de aplicaciones y soluciones creadas son no comerciales, existe mucha información y es un sistema operativo abierto, es decir, se puede modificar el código fuente y recompilar el kernel de acuerdo a necesidades específicas.
- En la creación de rutas se debe tener muy claro el esquema de la red, para evitar equivocaciones, se debe tomar en cuenta el camino de ida y vuelva de un paquete, puesto que puede darse el caso que un paquete llegue a su destino pero no sepa por donde regresar hacia su origen.
- El sistema de monitoreo WhatsUP es un software muy sencillo de utilizar y configurar, y tiene altas prestaciones en el monitoreo de redes, además se puede emitir reportes de eventos suscitados de forma textual o gráfica, siendo muy fácil establecer el uptime de los enlaces y la disponibilidad de los mismos.

5.2 RECOMENDACIONES

A continuación se presentan algunas recomendaciones que fueron tomadas en cuenta en el desarrollo de este proyecto:

- En las acometidas de fibra óptica a las entidades bancarias es necesario tener accesos preestablecidos para evitar retrasos en los trabajos, las instituciones bancarias son muy seguras y no pueden permitir ningún tipo de trabajo que no este autorizado y vigilado, por esto es necesario realizar una planificación conjunta de los trabajos a realizarse en las acometidas.
- En el servidor VLAN es aconsejable instalar programas sniffers (iftop, jnettop, etc), que estén monitoreando a todo momento el tráfico que pasa por medio del servidor y detectar si en algún momento existe tráfico de direcciones IP no establecidas en la red para poder alarmar y verificar conjuntamente con la entidad bancaria si se trata de algún posible hueco de seguridad.
- Con la herramienta MRTG se puede observar el historial del tráfico que consume cada enlace, el canal es limitado, por lo que se debe verificar regularmente si el canal llega a saturarse para sugerir a la institución bancaria el incremento del canal y no tener problemas de lentitud de las aplicaciones por saturación.
- En el caso de tener alguna ruptura de fibra óptica o deterioro de algún dispositivo de comunicación perteneciente a Telconet, se debe tener en bodega el stock necesario para solventar falencias en caso de emergencia.
- Una vez realizada la instalación y pruebas, el monitoreo de los enlaces es el trabajo principal del departamento de gestión de redes NOC (Network Operation Center), puesto que el saber detectar a tiempo las alarmas y saber que hacer al respecto, implica dar las soluciones necesarias y rápidas en caso de problemas con los enlaces, representando en el cumplimiento del uptime garantizado a la institución bancaria.

REFERENCIAS BIBLIOGRAFICAS

GONCALVEZ, Marcus. Manual de Firewalls, McGrawHill-México, 2002.

HERRERA S., Juan Alberto. Interconexión de redes LAN de diferentes plataformas, EPN-Quito, 1996.

SANCHEZ P., Edwin Patricio. Metodología para el diseño de redes virtuales VLANS, EPN-Quito, 2000.

VARGAS G., Norma Patricia. Metodología para el diseño de redes de área local para pequeñas y medianas empresas en el Ecuador, EPN-Quito, 1997.

LISTA PARCIAL DE DOCUMENTOS EN EL WEB

Capitulo 1.

http://www.consulintel.es/Html/Tutoriales/Articulos/vlan.html

http://polaris.lcc.uma.es/~eat/services/rvirtual/rvirtual.html#link1

http://www.monografias.com/trabajos18/tipos-cables-redes/tipos-cables-redes.shtml#REDES

http://www.tlm.unavarra.es/asignaturas/aro/ccna3-8.ppt

http://www.ibw.com.ni/~alanb/campus.html

http://www.tlm.unavarra.es/asignaturas/aro/slides/3-8/img7.html

http://lauca.usach.cl/~lsanchez/Vlan/

http://www.linuxjournal.com/article/7268

http://www.solocursosgratis.com/curso_gratis_seguridad_informatica_-conceptos_basicos-slccurso1029234.htm

http://www.si.uji.es/bin/ponencies/ipp.pdf

Capitulo 2.

http://www.monografias.com/trabajos13/fibropt/fibropt.shtml

http://www.noticias.com/articulo/14-03-2002/redaccion/nuevos-productos-inalambricos-red-31mb.html

http://www.teletronics.com/Firmware.html

http://www.trangobroadband.com/sp/products/trangolink_10.htm

http://www.trangobroadband.com/sp/products/quickspecs.htm

http://motorola.canopywireless.com/es/

http://orbita.starmedia.com/ygalarza/Ciencia.html

http://www.conecsion.es/index.asp?nivel=32&idcateg=36

Capitulo 3.
http://support.3com.com/infodeli/tools/switches/ss/gig/duf1770-aaa01_spanish.pdf
http://www.cisco.com/warp/public/3/es/canal/docs/Nortel.PDF
http://www.monografias.com/trabajos17/metro-ethernet/metro-thernet.shtml#metro
http://www.flytech.es/supermicro/Productos/Servidores/supermicro%20itanium%202%206113L-8.htm
http://www.cisco.com/en/US/products/hw/switches/ps646/ps3814/
http://trajano.us.es/~rafa/ARSS/apuntes/tema2.pdf
http://www.monografias.com/trabajos13/fibropt/fibropt.shtml
http://www.maxitrucos.com/articulos/montse/wireless_la_conexion_sin_cables.htm
http://www.monografias.com/trabajos7/rela/rela2.shtml#meto
http://www.consulintel.es/Html/Tutoriales/Articulos/fast_eth.html
http://www.ufps.edu.co/cisco/docs/docCCNA/fastnoteccnav22.pdf
http://people.ac.upc.edu/asalaver/cbxc_ip.pdf
http://www.saulo.net/pub/tcpip/a.htm#2
http://www.ufps.edu.co/cisco/docs/docCCNA/fastnoteccnav22.pdf
http://www.coopconesa.com.ar/coopconesa/red/
http://www.cudi.edu.mx/otono2002/presentaciones/Hugo_Zamora.pdf
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/2f31b4c2-b1ba-4d20-a18f-b7c9eb11649c.mspx
http://www.zator.com/Hardware/H12_2.htm
http://www.eurologic.es/conceptos/conbasics.htm
http://www.fing.edu.uy/~mauttone/
http://www.itesm.mx/viti/servicios/soporte_red/TYR-CCS-P2.pdf
http://www.consulintel.es/Html/Tutoriales/Lantronix/guia_et_p2.html
http://www.optim.com.ar/es/policy.php

Capitulo 4.
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_configuration_guide_chapter09186a008019d0ee.html
http://studies.ac.upc.edu/FIB/XC/XC-Lab-10-Switches.pdf

http://www.europe.redhat.com/documentation/rhl7.2/rhl-cg-es-7.2/tcp-wrappers.php3
http://www.wsftp.com/international/spanish/whatsup_professional.asp
http://www.ciscoredaccionvirtual.com/redaccion/comunicados/ver_comunicados.asp?Id=436
http://www.commscope.com/docs/fiber_manual_sp.pdf

ANEXOS

GLOSARIO

Access Point, es la conexión que une dispositivos de comunicación inalámbricos en una red. También puede usarse en una configuración de red ad-hock.

ACL (Access Control List), es una lista de los servicios disponibles, cada uno con una lista de los host que permitieron usar el servicio.

Ancho de Banda, se refiere a la capacidad de transmisión de un canal. Indica la cantidad de información por unidad de tiempo que puede enviarse a través de una línea de transmisión, medida frecuentemente en bits por segundos (bps).

ARP (Address Resolution Protocol), protocolo de resolución de dirección. Protocolo usado por una computadora para correlacionar una dirección IP con una dirección de hardware. Las computadoras que llaman el ARP difunden una solicitud a la que responde la computadora objetivo.

ATM (Asynchronous Transfer Mode), modo de transferencia asíncrono. Tecnología de transmisión de datos en forma de paquetes. La información se divide en pequeñas células que se transmiten individualmente y se procesan de manera asíncrona.

Backbone, línea de transmisión de información de alta velocidad o una serie de conexiones que juntas forman una vía con gran ancho de banda. Un backbone conecta dos puntos o redes distanciados geográficamente, a altas velocidades.

Backups, es un computador diseñado para copiar datos con el propósito de tener una copia de seguridad de la fuente original en caso de daños en la fuente original.

Base T, un estándar IEEE (802.3) para operar a10 Mbps en las redes Ethernet (Lan), con cableado par trenzado conectado a un hub.

BFSK, tipo de modulación para los equipos canopy

BPDU(Bridge Protocol Data Unit), un tipo de mensaje utilizado por bridges para intercambiar dirección y control de la información.

Bridge, un dispositivo que conecta dos o más redes físicas y sirve para transmitir paquetes entre ellas. Puede utilizarse también para filtrar los paquetes que entran o salen, selectivamente. (Similar al router).

Broadcast (o en castellano "difusiones"), se producen cuando una fuente envía datos a todos los dispositivos de una red.

Carriers, operadores de telecomunicaciones los cuales son propietarios de los backbone de Internet y responsables del transporte de los datos. Proporciona una conexión a Internet de alto nivel.

Chipset, es un grupo de microprocesadores especialmente diseñados para funcionar como si fueran una única unidad y para desempeñar una o varias funciones.

Cortafuegos o firewall, mecanismo de seguridad en Internet frente a accesos no autorizados. Básicamente consiste en un filtro que mira la identidad de los paquetes y rechaza todos aquellos que no estén autorizados o correctamente identificados

DBm, es una unidad de medida utilizada, principalmente, en telecomunicaciónes para expresar la potencia absoluta mediante una relación logarítmica.

DDR (Double Data Rate), tipo de memoria que trabaja al doble de velocidad en la transferencia de datos.

DHCP, son las siglas en inglés de Protocolo de configuración dinámica de servidores. Es un protocolo de red en el que un servidor provee los parámetros de configuración a las computadoras conectadas a la red informática que los requieran (máscara, puerta de enlace y otros) y también incluye un mecanismo de asignación de direcciones de IP.

Dial Up, servicio que proporciona algún proveedor de acceso a Internet que permite conectarse a través de una línea telefónica y un MODEM.

El DNS (Domain Name System), es un conjunto de protocolos y servicios (base de datos distribuida) que permite a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas.

Duplex, es una transmisión que permite establecer una comunicación en dos sentidos.

DS3 (Digital Signal 3), este termino es usado para referirse a los 45 Mbps de señales digitales fácilmente llevado en un T3 (44,736 Mbps)

DSSS, el espectro ensanchado por secuencia directa (del inglés direct sequence spread spectrum o DSSS), también conocido en comunicaciones móviles como DS-CDMA (acceso múltiple por división de código en secuencia directa), es uno de los métodos de modulación en espectro ensanchado para transmisión de señales digitales sobre ondas radiofónicas que más se utilizan

DWDM(Dense Wavelength Division Multiplexing), una tecnología óptica usada para incrementar el ancho de banda existente en el backbone de fibra óptica.

ECC (Error Checking and Correction), chequeo y corrección de errores.

EPIC (Explicitly Parallel Instruction Computing), procesamiento de instrucciones explícitamente en paralelo.

Ethernet, generalmente las computadoras conectadas a Internet utilizan TCP/IP a través de una red de tipo Ethernet. Lo que caracteriza a una red de área local como Ethernet es el modo en el que las computadoras deciden a quién le toca transferir. Existe una diversidad de cableado que soporta a su vez diferentes velocidades de comunicación (entre dos y cien millones de bits por segundo).

FCC, agencia independiente del gobierno estadounidense responsable de la regulación de las comunicaciones interestatales e internacionales por radio televisión y cable.

FDDI (Fiber distributed data interface), se define como una topología de red local en doble anillo y con soporte físico de fibra óptica.

Fibra Monomodo, estas fibras están caracterizadas por contener un núcleo de pequeñísimo diámetro, pequeño NA, baja atenuación y gran ancho de banda.
FTP, es uno de los diversos protocolos de la red Internet, concretamente significa File Transfer Protocol (Protocolo de Transferencia de Archivos) y es el ideal para transferir datos por la red.

GFP, el dispositivo de una protección del circuito que previene el flujo de corriente eléctrica a tierra si un corto circuito está presente. Normalmente requerido en ambientes húmedos, aire libre.

Gigabit Interface Conversor (GBIC), es un transceiver que convierte corrientes eléctricas a señales ópticas, y señales ópticas a corriente eléctrica. El GBIC es típicamente empleado en fibra óptica y sistemas de Ethernet como una interface para la gestión de redes de gran velocidad. Los datos se transfieren a una velocidad de 1gigabit por segundo (1 Gbps) o más.

GNU, Licencia Publica General. Software desarrollado para distribución sin fines de lucro. El proyecto GNU (GNU es un acrónimo recursivo para "Gnu No es Unix")

comenzó en 1984 para desarrollar un sistema operativo tipo Unix completo, que fuera Software Libre.

Host, ordenador que permite a los usuarios comunicarse con otros sistemas centrales de una red. Los usuarios se comunican utilizando programas de aplicación, tales como correo electrónico, Telnet y FTP.

Hosting, servicio de alojamiento de las páginas web que gestionan empresas especializadas. Las empresas que se dedican a este servicio son como los hoteleros de la red: ofrecen espacio para que otras compañías almacenen cualquier información que quieran que sea accesible por una red, desde sus páginas web hasta la información de su red interna o Intranet.

HSSI, es una interface serial que soporta una tasa de transmisión a 52 Mbps, se usa para conectar routers en redes de área local con redes de área ancha (Wan).

HTTP (HyperText Transmission Protocol), protocolo para transferir archivos o documentos hipertexto a través de la red. Se basa en una arquitectura cliente / servidor.

HTTP daemon, es un programa que corre de fondo en el servidor Web y espera peticiones externas al servidor. El daemon responde las peticiones y sirve los hipertextos y multimedios a través de Internet usando HTTP.

ICMP (Internet Control Message Protocol), es un protocolo de control usado en el nivel de red. Este protocolo se usa principalmente por los routers de Internet, para informar de sucesos inesperados, errores, etc. También se usa para hacer pruebas sobre la red (local o Internet), por ejemplo enviando un comando de petición de eco (ping) a un ordenador, y esperar que responda.

IEEE, corresponde a las siglas del Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos, una asociación estadounidense dedicada a la estandarización. Es una asociación internacional

sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros de telecomunicaciones, ingenieros electrónicos, Ingenieros en informática.

IEEE 802.3, es el nombre de un comité de estandarización del IEEE y por extensión se denominan así los estándares por el producidos.

ILD, es un semiconductor láser que produce luz debajo de 780 manómetros en el espectro infrarrojo.

IP (Internet Protocol), el protocolo encargado del direccionamiento (identificación del origen y destino).

IPMI , Interface de Dirección de Plataforma inteligente (IPMI) es una especificación que define un juego de interfaces comunes al hardware de la computadora y firmware que se usan para controlar y supervisar el funciones.

IPv4 ,es la versión 4 del Protocolo IP (Internet Protocol). Esta fue la primera versión del protocolo que se implemento extensamente, y forma la base de Internet.

IPX (Internet Packet Exchange). Intercambio de Paquetes entre Redes. Inicialmente protocolo de Novell para el intercambio de información entre aplicaciones en una red Netware.

ISM (Industrial, Scientific, Medical), información que debe transferirse dentro de un tiempo fijo.

ISP (Proveedor de Servicios de Internet), empresa u organización que brinda el servicio de conexión a Internet.

Kernel, en Linux parte principal del sistema operativo. Código fuente del propio sistema.

LAN (Local Area Network). Red de Área Local. Red de datos para dar servicio a un área geográfica máxima de unos pocos kilómetros cuadrados con velocidades de transmisión de hasta 100 Mbps (100 megabits por segundo).

LAT (Transporte del Área local), protocolo usado para la transferencia de datos y para sistemas de host digitales

LED (Diodo emisor de luz (Light Emitting Diode)), piloto luminoso que indica la actividad o funcionamiento de un elemento. (Por ejemplo, el led del módem, de la disquetera, del encendido del PC)

LLC (Control Lógico de Enlaces), consiste en el control de flujo en enlaces lógicos, entre sistemas finales, a través de una red Frame Relay.

LOG, un archivo diario que informa sobre las conexiones a un servidor.

LOS, el momento en el cual una estación receptora terrestre deja de captar las señales de radio procedentes de un satélite.

MAC, en redes de computadoras Media Access Control address cuyo acrónimo es MAC es un identificador físico -un número, único en el mundo, de 48 bits- almacenado en fábrica dentro de una tarjeta de red o una interface usada para asignar globalmente direcciones únicas en algunos modelos OSI (capa 2) y en la capa física del conjunto de protocolos de Internet

MAN (Metropolitan Area Network), que en español significa Red de Área Metropolitana. Es una red de distribución de datos para un área geográfica en el entorno de una ciudad.

MPLS, es un esquema típicamente usado para reforzar una red IP.

Multicast, es un mensaje que se envía simultáneamente a un grupo de nodos específicos en una red.

Multistack o multiprotocolo, cuando un dispositivo de red tiene configurado varios protocolos de comunicación que estén trabajando simultáneamente.

Multicasting, es la forma de transferencia de datos en donde es posible enviar información de un sólo emisor a muchos puntos diferentes (receptores) simultáneamente.

NAP (Network Access Point) Punto de Acceso a la Red. Es una facilidad de intercambio público de red donde los proveedores de acceso a Internet (ISPs: Internet Service Providers) pueden conectarse entre sí. Los NAPs son un componente clave del backbone de Internet porque las conexiones dentro de ellos determinan cuánto tráfico puede rutearse. También son los puntos de mayor congestionamiento de Internet.

NetBios, nivel software originalmente desarrollado por IBM y Sytek para conectar un sistema operativo de red con el hardware específico.

Networking, trabajar en red, trabajar en colaboración a través de una red. Término utilizado para referirse a las redes de telecomunicaciones en general.

Nodos, puntos en los cuales se ubican equipos de procesamiento en una red, ya los cuales están conectados los enlaces de la misma.

OSI, modelo para la interconexión de sistemas abiertos (Open Systems Interconnection). Es un modelo teórico de conexión de sistemas, estructurado en 7 capas (física, enlace, red, transporte, sesión, presentación y aplicación).

Open Shortest Path First (frecuentemente abreviado OSPF), es un protocolo de encaminamiento basado en el algoritmo Enlace Estado (LSA - Link State

Algorithm), el cual proporciona ciertas ventajas frente a RIP. Las características de OSPF incluyen ruteo a menor costo, ruteo multiruta y balanceo de carga.

OTDR (Optical Time Domain Reflectometer), equipos usados para probar instalaciones de fibra óptica.

Patch Panel, un tablero de puertos de la red usualmente dentro de un armario de telecomunicaciones que conectan líneas entrantes y salientes de una Lan a otra comunicación electrónica o sistema eléctrico.

PCI-X, forma abreviada en que también es conocido el bus PCI Express usado en computadoras u ordenadores.

PHY, define parámetros como proporciones de los datos, método de la modulación, los parámetros de la señalización, sincronización del transmitter/receiver, etc.

Ping (Packet Internet Groper),es una utilidad que comprueba el estado de la conexión con uno o varios hosts remotos. El comando ping utiliza los paquetes de solicitud de eco (protocolo ICMP) y de respuesta de eco para determinar si un sistema IP específico es accesible en una red.

PoE (Power over Ethernet), es una tecnología que permite la alimentación eléctrica de dispositivos de red a través de un cable UTP / STP en una red ethernet.

RARP son las siglas en inglés de Reverse Address Resolution Protocol (Protocolo de resolución de direcciones inverso).

Red, conjunto de computadoras y elementos que permite una comunicación entre sí y forman parte de un mismo ambiente.

RFC (Acrónimo de Request for Comments, 'Solicitud de comentarios'). Los RFC discuten todos los aspectos de las comunicaciones informáticas, pero atendiendo especialmente a estándares y protocolos.

RIP son las siglas de Routing Information Protocol (Protocolo de información de encaminamiento). Es un protocolo utilizado por los routers para intercambiar información acerca de la red.

RMON (Remote MONitor), es la especificación para recoger información SNMP de un dispositivo dócil de la red RMON.

Router, (enrutador o encaminador) es un dispositivo hardware o software de interconexión de redes de ordenadores / computadoras que opera en la capa 3 (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando como base la información de la capa de red.

Rx, abreviatura de Recepción o Recibiendo.

SAP, en un punto de acceso al servicio.

SCPC (Single Channel Per Carrier), un sistema de comunicaciones en el que cada circuito tiene su propia frecuencia del portador dentro de un transponder.

SCSI , Sigla de Small Computer System Interface (Interfaz de sistema para pequeñas computadoras). SCSI es una interfaz estándar para conectar una amplia variedad de dispositivos a la computadora. Los dispositivos SCSI más populares son las unidades de disco, aunque también es común encontrar unidades de cinta y scaners.

Semiduplex, se utiliza este término para describir transmisiones de datos que pueden ocurrir en dos direcciones en el mismo enlace de comunicaciones, en una sola dirección a un tiempo.

Simple Network Management Protocol (SNMP), o protocolo simple de gestión de redes, es aquel que permite la gestión remota de dispositivos de red, tales como switches, routers y servidores.

SNAP, función que permite unir en uno solo, dos nodos que se encuentran dentro de un radio predefinido.

Sniffer, programa que monitorea y analiza el tráfico de una red para detectar problemas. Su objetivo es mantener la eficiencia del tráfico de datos. Pero también puede ser usado ilegítimamente para capturar datos en una red.

SSH, es el nombre de un protocolo y del programa que lo implementa. Este protocolo sirve para acceder a máquinas a través de una red, de forma similar a como se hacía con telnet. La diferencia principal es que SSH usa técnicas de cifrado para que ningún atacante pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión.

Switch (en castellano "conmutador"), es un dispositivo de interconexión de redes de ordenadores / computadoras que opera en la capa 2(nivel de enlace de datos) del modelo OSI.

Synchronous Optical Network (SONET), es un estándar para el transporte de telecomunicaciones en redes de fibra óptica.

T1, canal portador cuya velocidad de transmisión es 1.544 Mbps. El canal portador T1 maneja 24 canales de voz o datos de 64 Kbps cada uno, más un canal de 8 Kbps para portar señales de control.

TCP (Transmission Control Protocol), es uno de los protocolos de comunicaciones sobre los que se basa Internet. Posibilita una comunicación libre de errores entre ordenadores en Internet.

TDD (Time Division Duplex), es una designación en el que se usan timeslots diferentes para los canales Tx y Rx. Cada punto de acceso usa un solo único espectro de frecuencia para transmitir y recibir en momentos diferentes.

TDMA son las siglas de Time Division Multiple Access (ANSI-136 o IS-136).Tecnología que distribuye las unidades de información en alternantes slots de tiempo proveyendo acceso múltiple a un reducido número de frecuencias. TDMA es una tecnología inalámbrica de segunda generación que brinda servicios de alta calidad de voz y datos.

Telnet, es el protocolo estándar de Internet que permite la conexión a un terminal remoto.

TFTP son las siglas de Trivial File Transfer Protocol (Protocolo de transferencia de archivos trivial). Protocolo en Internet para la carga remota de ficheros en equipos embebidos.

Token Ring, arquitectura de red desarrollada por IBM con topología lógica en anillo. Cumple el estándar IEEE 802.5.

Topología, disposición física de los nodos de una red. Por ejemplo, es posible que se encuentren formando un bus, una estrella, un anillo, etc.

Trama, conjunto de bits que forman un bloque de datos básico. Generalmente, una trama contiene su propia información de control, en la que se incluye la dirección del dispositivo al que está siendo enviado. Desde uno de los componentes de equipo de red, los cuadros pueden ser unidestinados (enviados a un solo dispositivo), multidestinados (enviados a dispositivos múltiples) o difundidos (enviados a todos los dispositivos).

Transceiver, es un dispositivo que tiene un transmisor y receptor que se combinan en una unidad. Técnicamente el transceiver debe combinar una cantidad significante del transmisor y receptor que manejan circuitería.

Tx, abreviatura de Transmisión o Transmitiendo

UDP, acrónimo de User Datagram Protocol (Protocolo de datagrama a nivel de usuario), perteneciente a la familia de protocolos TCP/IP. Este protocolo no es tan fiable como TCP, pues se limita a recoger el mensaje y enviar el paquete por la red. Para garantizar el éxito de la transferencia, UDP hace que la máquina de destino envía un mensaje de vuelta. Si no es así, el mensaje se envía de nuevo.

Ultima Milla (Local Loop), es el vinculo físico entre el proveedor del servicio de telecomunicaciones y el usuario final.

U-NII , Unlicensed National Information Infrastructure. Espectro de frecuencias en 5.8-GHz.

Unicast, protocolos o dispositivos que pueden transmitir paquetes de una dirección IP a otra directamente.

Uptime, es el tiempo en que un computador esta en forma operacional.

Virtual Private Network. (Red Privada Virtual -RPV-), tecnología que permite la transmisión de información privada sobre redes de uso público de manera segura, utilizando conexiones virtuales.

VLAN es el acrónimo de Virtual Local Area Network o Virtual LAN. Grupo de dispositivos en una o más LANs que son configurados (utilizando software de administración) de tal manera que se pueden comunicar como si ellos estuvieran conectados al mismo cable, cuando en realidad están localizados en un segmento diferente de LAN. Esto es porque VLANs están basadas en las conexiones lógicas en lugar de las físicas y es por eso que son extremadamente flexibles.

VSAT son las siglas de Terminal de Apertura Muy Pequeña (del inglés, Very Small Aperture Terminal). Se trata de un terminal de comunicaciones, que

intactúa con satelites de órbita_geoestacionaria para comunicarse con sus afines. Son bastante económicos, por lo que se consideran la solución a los problemas de comunicación en zonas aisladas, donde no suele llegar el cableado de las ciudades.

WAN, Wide Area Network o Red de Area Amplia. Es una red de computadoras que puede estar localizada en un área geográfica muy extensa y puede contener varios miles de computadoras interconectadas por medio de canales de comunicación de alta velocidad. Utilizadas por organizaciones muy grandes.

WEP, acrónimo de Wired Equivalency Privacy es un sistema de cifrado incluido en el estándar 802.11 como protocolo para redes Wireless que permite encriptar la información que se transmite. Proporciona encriptación a nivel 2. Está basado en el algoritmo de encriptación RC4, y utiliza claves de 64bits, de 128bits o de 256 bits.

WIRELESS (Conexión inalámbrica), conexión entre distintos ordenadores o variados dispositivos compatibles utilizando ondas de radio en vez de medios físicos.