DISEÑO DE CAMBIOS ESTRUCTURALES PARA MEJORAR LA OPERACIÓN DE LA RED LAN QUE CONECTA LOS USUARIOS Y SERVIDORES A NIVEL NACIONAL, BASADO EN UN MODELO DE RED LAN EFICIENTE Y REDUNDANTE, EN LA EMPRESA UNIFIANZA S.A.

Juan Pablo Vaca Penagos

SEMINARIO DE PROFUNDIZACIÓN PARA OPTAR AL TÍTULO

DE INGENIERO DE TELECOMINICACIONES

Asesor: Ing. Janeth Ortiz Aguilar

Profesión: Ingeniera Electrónica

UNIVERSIDAD COOPERATIVA DE COLOMBIA
FACULTAD DE INGENIERÍA
BOGOTÁ

2020

Dedicatoria

Es muy satisfactorio poder culminar con esta etapa cómo estudiante de una carrera profesional, y poder decir “Lo logré”, por eso quiero dar gracias a Dios inicialmente, porque él es la fuerza interior que nos motiva a seguir adelante cada día.

También, quiero agradecer a los integrantes de mi hogar, Mi esposa e hija, quienes me han acompañado durante este proceso largo y duro, brindándome su apoyo incondicional y motivándome a ser mejor cada día y en cada esfuerzo, creo que sin su apoyo no habría sido posible lograrlo.

De igual manera, quiero agradecer a mi madre y hermana, que siempre estuvieron respaldando las decisiones que he tomado, y con sus consejos han logrado sembrar en mi un ser de constante lucha y perseverancia.

Por último, quiero agradecer a todos los docentes y compañeros que estuvieron presentes conmigo durante el desarrollo de las clases y actividades referentes a la carrera, aprendí mucho de todos ustedes y me llevo un gran y amplio conocimiento, Infinitas gracias por todo lo que me brindaron.

Contenido

LISTA DE FIGURAS

LISTA DE TABLAS

1. Direccionamiento IP Inicial

2. Direccionamiento IP Final

RESUMEN

La compañía Unifianza SA manifiesta que tiene problemas continuamente en la operación diaria que afecta su rendimiento, y el problema más crítico esta relacionado con la conectividad de los usuarios a los servicios y aplicaciones más importantes de la red de datos.

Con en este informe, se mostrará la metodología utilizada que replantea la forma inadecuada en la cual opera la red LAN de Unifianza SA; dicha red cuenta con más de 120 Usuarios a nivel nacional y depende en un gran porcentaje de la correcta operación de los dispositivos que intervienen en el tráfico de los datos.

Para la metodología adoptada, se utilizó el modelo de referencia OSI (Open System Interconnection), y paso a paso se irán escalando los temas desde la capa más baja hasta llegar a la capa más alta, mostrando así las falencias en las cuales se tomó el reto y las mejoras propuestas como solución.

Cabe la pena aclarar, que gran parte de la fundamentación teórica fue tomada del seminario de profundización con la academia CISCO, y a pesar de que Cisco pone sobre la mesa herramientas propias de la marca, también existen protocolos y herramientas de uso abierto que logran obtener los mismos resultados.

De esta manera, con una planeación muy rigurosa y con el apoyo de Ingenieros de Sistemas, Telecomunicaciones y Eléctricos, el proyecto se finalizó y mejoró notablemente la operación de la compañía Unifianza SA, obteniendo una mejor respuesta a nivel de tiempo y eficiencia en los procesos que se ejecutan diariamente.

Palabras clave

Subred, Puerta de enlace, Enrutamiento, Túnel VPN, Corta fuegos

ABSTRACT

The company Unifianza SA says that it continuously has problems in its daily operations that affect its performance, and the most critical problem is related to the connectivity of users to the most important services and applications of the data network.

With this report, the methodology used will be shown that rethinks the inadequate way in which the Unifianza SA LAN network operates, which connects more than 120 Users nationwide and depends in a large percentage on the correct operation of the devices involved in data traffic.

For the adopted methodology, the OSI (Open System Interconnection) reference model will be used, and step by step the topics will be scaled from the lowest layer to the highest layer, thus showing the shortcomings in which the analysis was taken. challenge and the improvements with which it was solved.

It is worth clarifying that a large part of the theoretical foundation was taken from the in-depth seminar with the CISCO academy, and despite the fact that Cisco puts its own brand tools on the table, there are also open-use protocols and tools that manage to obtain the same results.

n this way, with very rigorous planning and with the support of Systems, Telecommunications and Electrical Engineers, the project was completed and the operation of the company Unifianza SA significantly improved, obtaining a better response in terms of time and efficiency in the processes that run daily.

Keywords

Subnet, Gateway, Routing, Tunnel VPN, Firewall

CAPITULO I. PLANTEAMIENTO DEL PROBLEMA

1. Planteamiento general

Unifianza SA es una compañía del sector Inmobiliario, que tiene cómo actividad principal afianzar a dueños de bienes raíces cuándo dejan sus inmuebles en modalidad de arrendamiento; esto les permite a los propietarios tener el respaldo que garantiza el pago de los cánones acordados entre arrendatario y arrendador.

De acuerdo, a lo anterior Unifianza SA tiene cobertura con sedes en Bogotá, Medellín, Barranquilla y Pereira, lo que significa que cuenta con una conectividad de túneles de Tipo IPSec desde todas las sedes hacia la sede principal de Bogotá, utilizando la red Pública de Internet.

Actualmente, su operación está funcionando sobre una Red LAN que posee una infraestructura que ha ido creciendo en relación de las necesidades del día a día, contando, con una configuración de servidores, firewalls, switches y dispositivos finales limitadas.

Sin embargo, Unifianza SA tiene problemas de conectividad críticas en la operación de la red, de las cuales se determinaron los siguientes:

- Pérdida de envío y recepción de paquetes entre una sucursal y otra.
- Pérdida de envío y recepción de paquetes entre un host y un algún servidor de la sede principal.
- Inadecuada Organización en la segmentación de las subredes y Vlan´s utilizadas.
- Desconexión temporal (Caídas de Servicio ISP´s), por consecuente, desconexión de túneles entre sedes.
- No existe conectividad por Wifi.
- No existe un adecuado acceso a la vlan de gestión en la sede principal de Bogotá.
- Robotización en el sonido de la voz, pérdida de llamadas.

Es por estos motivos, que es necesario replantear y corregir la operatividad funcional de la red de datos y la forma en la que los usuarios tienen conectividad hacia los servicios que la red debe prestar diariamente.

2. **Justificación**

Cuando una compañía crece, y los procesos de su operación se vuelven día a día más complejos y difíciles, nace la necesidad de centralizar de manera óptima y eficiente la estructura que se encarga de transportar, procesar y almacenar todos los datos que allí se transmiten.

Por lo anterior, aparece la oportunidad de poder aportar la idea de una infraestructura de red que pueda ser:

- Ágil, transportando la información de un sitio a otro de manera rápida y eficiente.
- Segura, garantizando que el acceso a la red únicamente sea para usuarios y personal autorizado.
- Confiable, para que la funcionalidad de la red tenga algún mecanismo de redundancia que le permita estar prestando sus servicios en la mayor parte del tiempo
- Escalable, para que pueda crecer en su número de usuarios y servicios, sin afectar o degradar la operabilidad de los dispositivos de la red.
- Disponible, para que los servicios y el acceso a la información estén accesibles de forma fácil pero segura.

Con las anteriores definiciones, y de manera conjunta acudiendo a parámetros basados en la investigación de conceptos dados por academias expertas en el tema de las redes y servidores, se llegó a un acuerdo para replantear y mejorar las condiciones operativas actuales de la red de Datos de Unifianza SA.

Adicional a esto, la compañía manifiesta que realizará una inyección significativa de capital para agregar unos nuevos servicios que deben estar ubicados en un lugar seguro y con prestaciones de redundancia muy altas, y anuncia el cambio en la forma cómo va a operar la aplicación más importante de la compañía, haciéndose así cada vez más relevante la necesidad de mejorar la conectividad de la red de datos que conecta la compañía.

3. Objetivos

3.1 Objetivo General

Diseñar cambios estructurales a nivel físico y lógico, para mejorar la operación de la Red LAN que conecta los usuarios y servidores a nivel nacional, basado en un modelo de red LAN eficiente y redundante en la empresa Unifianza SA.

3.2 Objetivos Específicos

- Identificar la ubicación de dispositivos o periféricos de comunicación de la red nuevos y existentes para proporcionar las mejoras que se van a obtener con las nuevas medidas adoptadas en la topología.

- Analizar el conjunto de subredes y Vlan´s que actúan en la capa de acceso de la red LAN de acuerdo con la ubicación geográfica de la sede.

- Rediseñar la interconexión remota contratando un nuevo servicio (ISP) para aplicar redundancia a nivel crítico en la lógica de servidores de la red LAN entre las sedes.

Capítulo II. DISEÑO INGENIERIL

En este capítulo, se conocerán los detalles sobre los cuales se presenta la problemática que afecta la red LAN de Uifianza SA, la forma detallada (topología actual) en la que opera la red y las medidas adoptadas para mejorar y corregir los inconvenientes.

Cabe aclarar, que el funcionamiento de una red LAN hace parte de la integración de muchos elementos y dispositivos cómo lo son el cableado estructurado, dispositivos finales, dispositivos intermedios, dispositivos de enrutamiento, aplicaciones, etc. Esto hace que el campo de acción y las decisiones tomadas a nivel técnico estén sumergidas en un mundo de posibilidades muy grande.

Inicialmente, se realizó un levantamiento de información en sitio, para lo cual es necesario estar presente en cada una de las sedes que hacen parte del funcionamiento de la red LAN, y se identifican problemáticas del siguiente tipo:

- Dispositivos finales cómo teléfonos y computadores que no pueden acceder a la red.
- Pérdida de llamadas o robotización de la voz.
- No hay entrega de direcciones IP por parte del servicio DHCP.
- Duplicidad de direccionamiento IP.
- Pérdida de conectividad entre sedes, por caídas temporales del servicio (ISP)
- Saturación en los canales de datos (ISP) por congestión en los túneles creados entre sedes.
- Bajo rendimiento en las aplicaciones (la aplicación más importante, funciona actualmente sobre un servicio de RDP entre un servidor y los usuarios o clientes)
- Impresoras compartidas conectadas localmente a computadores, que dejan de estar en disponibilidad si el equipo host se apaga o entra en suspensión.
- No hay acceso a redes wifi para el personal que debe moverse entre todas las sedes, de esta manera no puede conectar sus dispositivos móviles ni computadores portátiles.

Adicional a las problemáticas anteriores, se detecta que la sede ubicada en Bogotá es la más crítica para la operación diaria, debido a que esta sede aloja los servidores de controlador de dominio, aplicación y voz; es decir que, al perder la conexión hacia esta sede desde una sede remota, los usuarios perderán su autenticación por el servidor de controlador de dominio, acceso a la aplicación de la operación y entrada o salida de llamadas.

Es por lo anterior, que Unifianza SA, solicita que se realice un análisis de las condiciones actuales y manifiesta que el departamento de sistemas planea realizar un cambio radical en la forma como funciona la capa de aplicación, para que durante el diseño de la nueva topología se tenga en cuenta la inclusión de unos nuevos servidores de aplicación basados en un entorno WEB, para que progresivamente de acuerdo al desarrollo y avance del software, se retiren los servicios RDP del anterior servidor, esto acompañado de un ambiente de pruebas para estar seguros de los cambios en el desarrollo antes de lanzarlo a producción.

Los servidores mencionados anteriormente, no deberán estar ubicados en la sede principal de Bogotá, y por solicitud del departamento de sistemas, la decisión tomada es llevarlos a un centro de datos de alto nivel, que tenga la capacidad de prestar redundancia a nivel eléctrico y seguridad en el acceso físico.

Ya con una información clara del estado de la red, se muestra la topología actual de la compañía Unifianza SA, **(Figura 1.1)** con la cual ha venido creciendo la compañía en los 16 años que lleva de fundada, y las tablas con el direccionamiento IP encontrado en cada una de las sedes.

- Tabla 1.1 (Sede Bogotá)
- Tabla 1.2 (Bodega Archivo)
- Tabla 1.3 (Sede Medellín Poblado)
- Tabla 1.4 (Sede Medellín Laureles)
- Tabla 1.5 (Sede Barranquilla)
- Tabla 1.6 (Sede Pereira)

Con en la información recolectada, y el enfoque de las mejoras que se deben realizar para solventar los problemas actuales, se inicia el rediseño para la topología de red y

las medidas tomadas para mejorar las condiciones operativas de la red LAN de Unifianza SA.

Se realiza el nuevo diseño para la red LAN, teniendo en cuenta aspectos que van desde la capa más baja, hasta la más alta del modelo de referencia OSI, iniciando por la capa de física de la red, en la cual se sugiere a Unifianza S.A, que se valide el estado y la categoría del cableado actualmente instalado desde los patch panel de los centros de cableado hasta el face plate que conecta al usuario o teléfono.

Para este caso, los dispositivos finales y switches de acceso funcionan sobre el estándar **Gigabit Ethernet 802.3z de la IEEE**, por lo que se hace necesario según la teoría, verificar que el cableado existente cumpla las características mínimas para operar sobre este ancho de banda. (UTP Cat6 ANSI/TIA/EIA-568-B), adicional a esto, en caso de cumplir con las características mencionadas, es importantísimo que se someta todo el cableado a una certificación realizada con equipos de verificación que logren determinar si la forma en la que están instalados los cables cumplen con los requerimientos técnicos exigidos por la norma **ANSI/TIA/EIA-568-B,** la cual contempla aspectos importantes como lo son:

- No se permiten puentes, derivaciones o empalmes a lo largo de todo el trayecto del cableado.
- Se debe considerar su proximidad con el cableado eléctrico que genera altos niveles de interferencia electromagnética (motores, elevadores, transformadores etc.) y cuyas limitaciones se encuentran en el estándar ANSI/EIA/TIA 569.
- La máxima longitud permitida independientemente del tipo de medio de TX utilizado es 100 metros = 90 m + 3m usuario + 7 m patchpannel.

De acuerdo con lo anterior, para cubrir todos los aspectos de la capa física, se debe determinar por medio de un estudio de cobertura, cuál debe ser la ubicación adecuada de los puntos de acceso que van a prestar el servicio de WIFI en todas las sedes, y a

nivel de equipos, éstos deben contar con el estándar de la IEEE 802.1n, que logra operar en las bandas de los 2.4 y 5 GHz con anchos de banda de hasta 600 Mbps.

Para la capa de acceso, se comprobó que los switches actuales tienen funcionalidades que operan en la capa 2 del modelo de referencia OSI, por lo cual, se debe adoptar en su configuración la seguridad de acceso sobre los puertos con el método de apagado, esto cuándo el equipo detecte que algún dispositivo no conocido en su tabla MAC intente conectarse a la red. Adicional a esto, se establece la forma en la cual deben crearse las VLan que van a operar en cada sede, de acuerdo con las necesidades y requerimientos solicitados, se determinó que deben configurarse bajo el estándar 802.1Q de la IEEE, básicamente para poder transportar todas las Vlan creadas por un mismo medio físico.

Los ID de Vlan para cada sede son las siguientes:

- Servidores ubicados en el centro de Datos de Alto Nivel (Triara):

  - Vlan 10 Producción y Gestión.
  - Vlan 20 Pruebas.

- Sede principal Bogotá.

  - Vlan 10 Servidores y Gestión
  - Vlan 92 Voz
  - Vlan 11 Usuarios
  - Vlan 12 Invitados

- Bodega Archivo Bogotá

  - Vlan 11 Usuarios y Gestión
  - Vlan 12 Invitados
  - Vlan 23 Voz

- Sede Medellín (Poblado)

  - Vlan 11 Usuarios y Gestión

- Vlan 12 Invitados
- Vlan 23 Voz

- Sede Medellín (Laureles)

  - Vlan 11 Usuarios y Gestión
  - Vlan 12 Invitados
  - Vlan 23 Voz
- Sede Barranquilla

  - Vlan 11 Usuarios y Gestión
  - Vlan 12 Invitados
  - Vlan 23 Voz

- Sede Pereira

  - Vlan 11 Usuarios y Gestión
  - Vlan 12 Invitados
  - Vlan 23 Voz

Ya entrando en un tema más complejo, se determinó cual va a ser la operación a nivel de capa 3 del Modelo de referencia OSI, y en este apartado intervienen tres puntos importantes que son:

- Tipo de direccionamiento IP
- Direccionamiento IP Asignado
- Enrutamiento de capa 3

Tipo de direccionamiento IP: el tipo de direccionamiento a utilizar está directamente asociado a la cantidad de usuarios o direcciones que se deben entregar en cada subred, y de acuerdo a la revisión realizada y la información suministrada por el departamento de sistemas de la compañía, la sede más grande cuenta con la conexión de aproximadamente 70 Usuarios y dispositivos, motivo por el cual no es

necesario pensar en un esquema de direccionamiento tan grande como IPv6, se considera que una subred con máscara de red de 254 usuarios para la administración de las subredes es suficiente, teniendo en cuenta que puede haber un crecimiento a futuro.

Direccionamiento IP Asignado: El direccionamiento IP va de la mano con las Vlan sugeridas, es decir que se deben crear 17 subredes y quedarán distribuidas de la manera que estipulan las siguientes tablas:

- Tabla 2.1 (Sede Bogotá)
- Tabla 2.2 (Servidores Triara)
- Tabla 2.3 (Bodega Archivo)
- Tabla 2.4 (Sede Medellín Poblado)
- Tabla 2.5 (Sede Medellín Laureles)
- Tabla 2.6 (Sede Barranquilla)
- Tabla 2.7 (Sede Pereira)

Enrutamiento de capa 3: en este tema determinante, hay que tener en cuenta que la operación de la compañía se basaba en el uso de túneles de tipo **IPSec** entre las sedes Remotas y la sede Principal en Bogotá, para ello, es indispensable contar con un proveedor de servicios de internet (ISP) en cada sede, ya que éste tipo de Túnel es capaz de operar en la red pública de Internet a un costo bajo, pero con un reúso en la red de Internet muy alto, bajando así el rendimiento de las conexiones entre sedes, adicional a esto, la falta de una segunda opción cómo alternativa de enrutamiento en caso de fallas en el **ISP.**

Es por lo anterior, que se recomienda en la nueva topología contar con una segunda alternativa de enrutamiento que sea capaz de llevar los datos de manera segura, confiable y dedicada entre las sedes, y se opta por un servicio de tipo **MPLS (Multiprotocol Label Switching)**, la cual es capaz de transportar cualquier tipo de protocolo y ofrece la posibilidad de dar Calidad de servicio para priorizar el tráfico de voz.

Cabe la pena aclarar, que esta tecnología MPLS, inicialmente opera en la capa de enlace de Datos, pero debe ser enrutada desde la capa de Red.

Contando con las dos alternativas de enrutamiento, Se puede decidir cuál va a ser el camino para paquetes que transporten información referente a datos o voz utilizando el recurso de las **rutas estáticas**, ya que la topología aún no es muy grande y se puede administrar de manera manual, y adicional a esto, el recurso de **rutas estáticas flotantes**, para que sean las rutas que van a respaldar la principal en caso de que exista alguna falla en la ruta estática principal.

Teniendo claridad en lo anterior, se muestra la nueva topología de red diseñada para la operación de la red LAN de Unifianza SA. **(Figura 2.1)**

Después de conocer gráficamente la forma en la cual se planea que opere la Red LAN de Unifianza SA, se analiza la capa de transporte dónde básicamente se definen los protocolos sobre los cuales se van a mover segmentos o datagramas (Datagrama es la Unidad de datos del protocolo en la capa de transporte) aunque basados en la información entregada por los ingenieros encargados del desarrollo de software, éstos serán de tipo **TCP,** sin embargo, también se van a mover datos de tipo **UDP** como lo son la voz, la cual contará con prioridad **(QoS)** ya que en caso de errores, esta no será retransmitida.

Es casi seguro que la mayoría de las aplicaciones van a utilizar el protocolo TCP de la capa de transporte, debido a que es un protocolo orientado a la conexión y va a garantizar la entrega de los datagramas.

- SIP (UDP)
- DNS (TCP o UDP)
- DHCP (UDP)
- SMTP (TCP)
- IMAP (TCP)
- FTP (TCP)
- SMB (TCP)

- HTTP (TCP)
- HTTPS (TCP)

Y por último, se sabe que la capa de aplicación está muy ligada a la capa de transporte, también que la aplicación core nueva (Aplicación más importante de la organización) va a funcionar sobre el protocolo HTTPS, reemplazando el protocolo RDP sobre el cuál funciona la aplicación actual, de esta manera, se puede realizar un monitoreo del tráfico de la red y saber cuál va a ser su comportamiento, éste monitoreo de la red será realizado por medio del protocolo SNMP, el cual permite saber en tiempo real cuál es el comportamiento de los dispositivos que se vinculen a su revisión.

TABLAS

Tabla 1.1

Direccionamiento IP Inicial Sede Bogotá

Dispositivo	ID-Vlan	Subred	Nombre Vlan	Dirección IP	Máscara
FIREWALL - GATEWAY SERVIDORES	10	192.168.200.0	Servidores	192.168.200.1	255.255.255.0
SERVIDOR DE CONTROLADOR DE DOMINIO	10	192.168.200.0	Servidores	192.168.200.3	255.255.255.0
SERVIDOR DE APLICACIÓN RDP	10	192.168.200.0	Servidores	192.168.200.4	255.255.255.0
SERVIDOR WSUS	10	192.168.200.0	Servidores	192.168.200.5	255.255.255.0
SERVIDOR DE VOZ	10	192.168.200.0	Servidores	192.168.200.7	255.255.255.0
FIREWALL - GATEWAY VOZ	87	192.168.1.0	Voz	192.168.1.0	255.255.255.0
RANGO DHCP TELEFÓNOS	87	192.168.1.0	Voz	192.168.1.10 - 192.168.1.254	255.255.255.0
FIREWALL - GATEWAY CONTABILIDAD	20	172.24.10.0	Contabilidad	172.24.10.1	255.255.255.0
RANGO DHCP USUARIOS	20	172.24.10.0	Contabilidad	172.24.10.1 - 172.24.10.254	255.255.255.0
FIREWALL - GATEWAY CARTERA	30	10.0.1.0	Cartera	10.0.1.1	255.255.255.0
RANGO DHCP USUARIOS	30	10.0.1.0	Cartera	10.0.1.10 - 10.0.1.254	255.255.255.0
FIREWALL - GATEWAY AFILIACIONES	40	192.168.100.0	Afiliaciones	192.168.100.1	255.255.255.0
RANGO DHCP USUARIOS	40	192.168.100.0	Afiliaciones	192.168.100.10 - 192.168.100.254	255.255.255.0

Fuente: Elaboración propia

Tabla 1.2

Direccionamiento IP Inicial Bodega Archivo Bogotá

Dispositivo	ID-Vlan	Subred	Nombre Vlan	Dirección IP	Máscara
FIREWALL - USUARIOS	1	10.1.1.0	Usuarios	10.1.1.1	255.255.255.0
RANGO DHCP USUARIOS y TELÉFONOS	1	10.1.1.0	Usuarios	10.1.1.10 - 10.1.1.254	255.255.255.0

Fuente: Elaboración propia

Tabla 1.3

Direccionamiento IP Inicial Sede Medellín Poblado

Dispositivo	ID-Vlan	Subred	Nombre Vlan	Dirección IP	Máscara
FIREWALL - USUARIOS	1	172.24.200.0	Usuarios	172.24.200.1	255.255.255.0
RANGO DHCP USUARIOS	1	172.24.200.0	Usuarios	172.24.200.10 - 172.24.200.254	255.255.255.0

Fuente: Elaboración propia

Tabla 1.4

Direccionamiento IP Inicial Sede Medellín Laureles

Dispositivo	ID-Vlan	Subred	Nombre Vlan	Dirección IP	Máscara
FIREWALL - USUARIOS	1	172.24.300.0	Usuarios	172.24.300.1	255.255.255.0
RANGO DHCP USUARIOS	1	172.24.300.0	Usauarios	172.24.300.10 - 172.24.300.254	255.255.255.0

Fuente: Elaboración propia

Tabla 1.5

Direccionamiento IP Inicial Sede Barranquilla

Dispositivo	ID-Vlan	Subred	Nombre Vlan	Dirección IP	Máscara
FIREWALL - USUARIOS	1	10.1.2.0	Usuarios	10.1.2.1	255.255.255.0
RANGO DHCP USUARIOS	1	10.1.2.0	Usuarios	10.1.2.10 - 10.1.2.254	255.255.255.0

Fuente: Elaboración propia

Tabla 1.6

Direccionamiento IP Inicial Sede Pereira

Dispositivo	ID-Vlan	Subred	Nombre Vlan	Dirección IP	Máscara
FIREWALL - USUARIOS	1	192.168.300.0	Usuarios	192.168.300.1	255.255.255.0
RANGO DHCP USUARIOS	1	192.168.300.0	Usuarios	192.168.300.10 - 192.168.300.254	255.255.255.0

Fuente: Elaboración propia

Tabla 2.1

Direccionamiento IP Final Sede Bogotá

Dispositivo	ID-Vlan	Subred	Nombre Vlan	Dirección IP	Máscara
FIREWALL	10	172.17.50.0	Servidores y Gestion	172.17.50.1	255.255.255.192
SERVIDOR WSUS	10	172.17.50.0	Servidores y Gestion	172.17.50.2	255.255.255.192
SERVIDOR CONTROLADOR DE DOMINIO	10	172.17.50.0	Servidores y Gestion	172.17.50.3	255.255.255.192
SERVIDOR APLICACIÓN RDP	10	172.17.50.0	Servidores y Gestion	172.17.50.4	255.255.255.192
SERVIDOR DE VOZ	10	172.17.50.0	Servidores y Gestion	172.17.50.5	255.255.255.192
GATEWAY MPLS	10	172.17.50.0	Servidores y Gestion	172.17.50.9	255.255.255.192
SWITCH_1	10	172.17.50.0	Servidores y Gestion	172.17.50.10	255.255.255.192
SWITCH_2	10	172.17.50.0	Servidores y Gestion	172.17.50.11	255.255.255.192
SWITCH_3	10	172.17.50.0	Servidores y Gestion	172.17.50.12	255.255.255.192
SWITCH_4	10	172.17.50.0	Servidores y Gestion	172.17.50.13	255.255.255.192
FIREWALL	92	172.17.50.129	Voz	172.17.50.129	255.255.255.128
SERVIDOR DE VOZ	92	172.17.50.129	Voz	172.17.50.130	255.255.255.128
RANGO DHCP TELEFÓNOS	92	172.17.50.129	Voz	172.17.50.135-172.17.50.254	255.255.255.128
FIREWALL	11	172.17.51.0	Usuarios	172.17.51.1	255.255.255.0
IMPRESORA_1	11	172.17.51.0	Usuarios	172.17.51.2	255.255.255.0
IMPRESORA_2	11	172.17.51.0	Usuarios	172.17.51.3	255.255.255.0
IMPRESORA_1	11	172.17.51.0	Usuarios	172.17.51.4	255.255.255.0
IMPRESORA_1	11	172.17.51.0	Usuarios	172.17.51.5	255.255.255.0
ACCESS POINT_1	11	172.17.51.0	Usuarios	172.17.51.6	255.255.255.0
ACCESS POINT_2	11	172.17.51.0	Usuarios	172.17.51.7	255.255.255.0
RANGO DHCP USUARIOS	11	172.17.51.0	Usuarios	172.17.51.100-172.17.51.254	255.255.255.0
FIREWALL	12	172.17.50.64	Invitados	172.17.50.65	255.255.255.192
RANGO DHCP INVITADOS	12	172.17.50.64	Invitados	172..17.50.70-172.17.50.126	255.255.255.192

Fuente: Elaboración propia.

Tabla 2.2

Direccionamiento IP Servidores Triara

Dispositivo	ID-Vlan	Subred	Nombre Vlan	Dirección IP	Máscara
FIREWALL	10	10.0.0.0	Producción y Gestión	10.0.0.1	255.255.255.0
NAS	10	10.0.0.0	Producción y Gestión	10.0.0.3	255.255.255.0
SERVIDOR CONTROLADOR DE DOMINIO	10	10.0.0.0	Producción y Gestión	10.0.0.11	255.255.255.0
SERVIDOR BASE DE DATOS SQL	10	10.0.0.0	Producción y Gestión	10.0.0.12	255.255.255.0
SERVIDOR APLICACIÓN WEB	10	10.0.0.0	Producción y Gestión	10.0.0.13	255.255.255.0
SERVIDOR MONITOREO SNMP	10	10.0.0.0	Producción y Gestión	10.0.0.14	255.255.255.0
SERVIDOR BACKUPS	10	10.0.0.0	Producción y Gestión	10.0.0.15	255.255.255.0
SERVIDOR ANTIVIRUS	10	10.0.0.0	Producción y Gestión	10.0.0.16	255.255.255.0
FIREWALL	20	10.0.1.0	Pruebas	10.0.1.1	255.255.255.128
SERVIDOR APLICACIÓN WEB PRUEBAS	20	10.0.1.0	Pruebas	10.0.1.3	255.255.255.128
SERVIDOR BASE DE DATOS SQL PRUEBAS	20	10.0.1.0	Pruebas	10.0.1.4	255.255.255.128

Fuente: Elaboración propia.

Tabla 2.3

Direccionamiento IP Final Bodega Archivo Bogotá

Dispositivo	ID-Vlan	Subred	Nombre Vlan	Dirección IP	Máscara
FIREWALL	11	172.17.56.0	Usuarios y Gestión	172.17.56.1	255.255.255.192
SWITCH_1	11	172.17.56.0	Usuarios y Gestión	172.17.56.2	255.255.255.192
IMPRESORA_1	11	172.17.56.0	Usuarios y Gestión	172.17.56.3	255.255.255.192
ACCESS POINT_1	11	172.17.56.0	Usuarios y Gestión	172.17.56.4	255.255.255.192
GATEWAY MPLS	11	172.17.56.0	Usuarios y Gestión	172.17.56.9	255.255.255.192
RANGO DHCP USUARIOS	11	172.17.56.0	Usuarios y Gestión	172.17.56.10-172.17.56.62	255.255.255.192
FIREWALL	23	172.17.56.64	Voz	172.17.56.65	255.255.255.192
RANGO DHCP USUARIOS	23	172.17.56.64	Voz	172.17.56.70-172.17.56.125	255.255.255.192
FIREWALL	12	172.17.56.128	Invitados	172.17.56.129	255.255.255.224
RANGO DHCP USUARIOS	12	172.17.56.128	Invitados	172.17.56.35-172.17.56.157	255.255.255.224

Fuente: Elaboración propia.

Tabla 2.4

Direccionamiento IP Final sede Medellín Poblado

Dispositivo	ID-Vlan	Subred	Nombre Vlan	Dirección IP	Máscara
FIREWALL	11	172.17.52.0	Usuarios	172.17.52.1	255.255.255.192
SWITCH_1	11	172.17.52.0	Usuarios	172.17.52.2	255.255.255.192
IMPRESORA_1	11	172.17.52.0	Usuarios	172.17.52.3	255.255.255.192
ACCESS POINT_1	11	172.17.52.0	Usuarios	172.17.52.4	255.255.255.192
GATEWAY MPLS	11	172.17.52.0	Usuarios	172.17.52.9	255.255.255.192
RANGO DHCP USUARIOS	11	172.17.52.0	Usuarios	172.17.52.10 - 172.17.52.62	255.255.255.192
FIREWALL	23	172.17.52.64	Voz	172.17.56.65	255.255.255.192
RANGO DHCP USUARIOS	23	172.17.52.64	Voz	172.17.56.70-172.17.56.125	255.255.255.192
FIREWALL	12	172.17.52.128	Invitados	172.17.52.129	255.255.255.224
RANGO DHCP USUARIOS	12	172.17.52.128	Invitados	172.17.52.35-172.17.52.157	255.255.255.224

Fuente: Elaboración propia.

Tabla 2.5

Direccionamiento IP Final sede Medellín Laureles

Dispositivo	ID-Vlan	Subred	Nombre Vlan	Dirección IP	Máscara
FIREWALL	11	172.17.54.0	Usuarios y Gestión	172.17.54.1	255.255.255.192
SWITCH_1	11	172.17.54.0	Usuarios y Gestión	172.17.54.2	255.255.255.192
IMPRESORA_1	11	172.17.54.0	Usuarios y Gestión	172.17.54.3	255.255.255.192
ACCESS POINT_1	11	172.17.54.0	Usuarios y Gestión	172.17.54.4	255.255.255.192
GATEWAY MPLS	11	172.17.54.0	Usuarios y Gestión	172.17.54.9	255.255.255.192
RANGO DHCP USUARIOS	11	172.17.54.0	Usuarios y Gestión	172.17.54.10 - 172.17.54.62	255.255.255.192
FIREWALL	23	172.17.54.64	Voz	172.17.54.65	255.255.255.192
RANGO DHCP USUARIOS	23	172.17.54.64	Voz	172.17.54.70-172.17.54.125	255.255.255.192
FIREWALL	12	172.17.54.128	Invitados	172.17.54.129	255.255.255.224
RANGO DHCP USUARIOS	12	172.17.54.128	Invitados	172.17.54.35-172.17.54.157	255.255.255.224

Fuente: Elaboración propia.

Tabla 2.6

Direccionamiento IP Final Sede Barranquilla

Dispositivo	ID-Vlan	Subred	Nombre Vlan	Dirección IP	Máscara
FIREWALL	11	172.17.53.0	Usuarios y gestión	172.17.53.1	255.255.255.192
SWITCH_1	11	172.17.53.0	Usuarios y gestión	172.17.53.2	255.255.255.192
IMPRESORA_1	11	172.17.53.0	Usuarios y gestión	172.17.53.3	255.255.255.192
ACCESS POINT_1	11	172.17.53.0	Usuarios y gestión	172.17.53.4	255.255.255.192
GATEWAY MPLS	11	172.17.53.0	Usuarios y gestión	172.17.53.9	255.255.255.192
RANGO DHCP USUARIOS	11	172.17.53.0	Usuarios y gestión	172.17.53.10 - 172.17.53.62	255.255.255.192
FIREWALL	23	172.17.53.64	Voz	172.17.53.65	255.255.255.192
RANGO DHCP USUARIOS	23	172.17.53.64	Voz	172.17.53.70-172.17.53.125	255.255.255.192
FIREWALL	12	172.17.53.128	Invitados	172.17.53.129	255.255.255.224
RANGO DHCP USUARIOS	12	172.17.53.128	Invitados	172.17.53.35-172.17.53.157	255.255.255.224

Fuente: Elaboración propia.

Tabla 2.7

Direccionamiento IP Final Sede Pereira

Dispositivo	ID-Vlan	Subred	Nombre Vlan	Dirección IP	Máscara
FIREWALL	11	172.17.55.0	Usuarios y gestión	172.17.55.1	255.255.255.192
SWITCH_1	11	172.17.55.0	Usuarios y gestión	172.17.55.2	255.255.255.192
IMPRESORA_1	11	172.17.55.0	Usuarios y gestión	172.17.55.3	255.255.255.192
ACCESS POINT_1	11	172.17.55.0	Usuarios y gestión	172.17.55.4	255.255.255.192
GATEWAY MPLS	11	172.17.55.0	Usuarios y gestión	172.17.55.9	255.255.255.192
RANGO DHCP USUARIOS	11	172.17.55.0	Usuarios y gestión	172.17.55.10 - 172.17.55.62	255.255.255.192
FIREWALL	23	172.17.55.64	Voz	172.17.55.65	255.255.255.192
RANGO DHCP USUARIOS	23	172.17.55.64	Voz	172.17.55.70-172.17.55.125	255.255.255.192
FIREWALL	12	172.17.55.128	Invitados	172.17.55.129	255.255.255.224
RANGO DHCP USUARIOS	12	172.17.55.128	Invitados	172.17.55.35-172.17.55.157	255.255.255.224

Fuente: Elaboración propia.

Capítulo III. MARCO TEÓRICO

En el proceso de configuración y rediseño de la red LAN se tuvo en cuenta la teoría de las redes a nivel de las capas OSI como se presenta a continuación:

MODELO DE REFERENCIA OSI

A comienzos de los años 80 los productores tecnológicos más relevantes del momento se unieron para centralizar diferencias y unir la mayor información acerca de cómo lograr integrar sus productos no compatibles entres si y únicos para cada uno de ellos. Como conclusión de esta unión, nace el modelo de referencia OSI, que continua con los parámetros convencionales de hardware y software haciendo posible la integración multifabricante. modelo OSI (Modelo abierto de internetwork, no confundir con ISO) separa a la red en distintas capas con la intención de que cada fabricante trabaje puntualmente en su campo sin la necesidad de depender de otras. Un desarrollador inventa una aplicación puntual sin importarle cuáles serán los medios por los que se transportaran los datos, contrariamente un técnico de comunicaciones entregará comunicación sin importarle qué tipo de datos transporta. En su totalidad el modelo OSI se forma de siete capas bien definidas que son: APLICACIÓN, PRESENTACIÓN, SESIÓN, TRANSPORTE, RED, ENLACE DE DATOS Y FÍSICA.

Todas estas capas dan servicio a la capa inmediatamente superior, teniendo en cuenta que la capa de aplicación es la única que no lo hace ya que al ser la final capa, su servicio está relacionada únicamente con el usuario. Así mismo, estas siete capas del host origen se comunican en igual jerarquía con su similar en el host de destino. Las primeras cuatro capas en orden ascendente también se conocen como capas de medios (o capas de flujo de datos), por el contrario, las tres últimas capas se llaman de Host.

Figura 1.
De “Ernesto Ariganello” por Alfaomega Grupo Editor, Redes Cisco, p. 2. Derechos de autor enero 2009.

DIRECCIONAMIENTO IP

Para establecer la comunicación entre dos dispositivos, es indispensable poder identificarlos claramente. Una dirección IP es una secuencia lógica de unos y ceros con 32 bits. Para hacer más entendible el direccionamiento, una dirección IP se escribe en forma de cuatro números decimales separados por puntos. La notación decimal punteada es un modelo más simple de entender que el método binario de unos y ceros. Esta notación decimal punteada también evita que se establezcan una importante cantidad de errores por transposición, que sí sucedería si sólo se utilizaran números binarios. El uso de decimales separados por puntos ayuda a comprender mejor los patrones numéricos.

Una dirección IP consta de dos partes. Una parte identifica la red y la segunda identifica el sistema o host en particular de esa red. Esta clase de dirección recibe el nombre de dirección jerárquica porque contiene distintos niveles. Una dirección IP mezcla estos dos identificadores en un único número. Este número debe ser exclusivo, porque las direcciones repetidas no permiten el enrutamiento. La primera parte identifica la dirección de la red del sistema. La segunda parte, la del host, identifica qué máquina en articular la red. Las direcciones IP se clasifican en

clases para separar las redes de tamaño pequeño, mediano y grande. Las direcciones con Clase A se asignan a las redes de mayor tamaño. Las direcciones con Clase B se utilizan para las redes de tamaño medio y las de Clase C para redes pequeñas. Dentro de cada rango existen direcciones privadas para uso interno que no son visibles en Internet. Las direcciones de clase D son de uso multicast y las de clase E, experimentales.

SUBREDES

Las redes se pueden separar en redes más pequeñas, para un mejor aprovechamiento de la misma, que se nombran subredes; además, de contar con esta flexibilidad, la separación en subredes permite que el administrador de la red brinde protección de broadcast y seguridad de bajo nivel en la LAN. La separación en subredes, adicionalmente, entrega seguridad ya que el acceso a las otras subredes está disponible únicamente a través de los servicios de un enrutador. Las clases de direcciones IP disponen de 256 a 16,8 millones de Hosts dependiendo de su clase.

El proceso de creación de subredes inicia solicitando "prestado" al rango de host la cantidad de bits que se requieren para el número de subredes implementadas. Se debe tener particular cuidado en esta acción de pedir prestado debido a que deben quedar mínimo dos bits del rango de host. La máxima cantidad de bits disponibles para este propósito depende del tipo de clase:

Clase A cantidad disponible 22 bits
Clase B cantidad disponible 14 bits
Clase C cantidad disponible 6 bits

INTRODUCCIÓN A LAS VLAN

Las VLAN (Redes Virtuales) dan seguridad, segmentación, flexibilidad, permiten hacer agrupaciones de usuarios de un mismo dominio de broadcast con independencia de su ubicación fisica en la red. Utilizando la tecnología VLAN se

logran agrupar lógicamente puertos del switch y los usuarios conectados a ellos en grupos de trabajo con interés común.

Uniendo la electrónica y los medios existentes es posible unir usuarios lógicamente con toda la independencia de su ubicación física incluso a través de una Red WAN. Las VLAN pueden ser creadas en un solo switch o bien estar presentes en varios de ellos. Las VLAN pueden extenderse a muchos switch por medio de enlaces troncales que permiten transportar tráfico de múltiples VLANS.

El rendimiento de una red se ve mejorado enormemente al no propagarse las difusiones de un segmento a otro incrementando también los niveles de seguridad. Para que las vlans logren comunicarse son indispensables los servicios de enrutadores que pueden implementar el uso de ACL para mantener el margen de seguridad necesario.

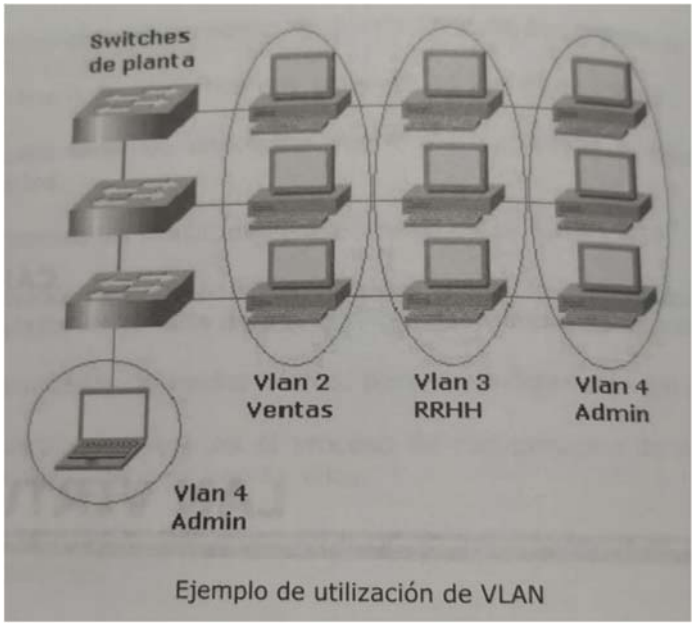


Figura 2.
De “Ernesto Ariganello” por Alfaomega Grupo Editor, Redes Cisco, p. 182. Derechos de autor enero 2009.

RUTAS ESTÁTICAS

Las rutas estáticas se definen administrativamente y brindan rutas puntuales que han de seguir los paquetes para ir de un puerto de origen hasta un puerto de destino. Se establece un control riguroso del enrutamiento de acuerdo a los parámetros del administrador.

Las rutas estáticas por defecto (default) establecen una puerta de enlace (gateway) de último recurso, a la que el enrutador debe enviar un paquete destinado a una red que no figura en su tabla de enrutamiento, es decir, que no conoce.
Las rutas estáticas se utilizan normalmente en enrutamientos desde una red hasta una red de conexión única, debido a que no existe más que un camino de entrada y salida en una red de conexión única, evitando de esta manera la sobrecarga de tráfico que genera un protocolo de enrutamiento.

Una ruta estática se programa para lograr conectar con un enlace de datos Que no esté directamente conectado al router. Para interconectar un extremo a otro, es necesario configurar la ruta estática en ambas direcciones. Las rutas estáticas permiten la creación manual de la tabla de enrutamiento.

INTRODUCCIÓN A VPN

Una VPN (Red Privada Virtual) se emplea normalmente para conectar dos redes privadas a través de la red pública de datos. Sin embargo, puede tener muchas aplicaciones más. Un túnel es básicamente una forma de encapsular un protocolo en otro. La presencia de protocolos no enrutables hace que la implementación de las VPN sea imprescindible para enviar el tráfico que utiliza este tipo de protocolos. Incluso para otros tipos de protocolos enrutables donde la dificultad de enrutamiento es elevada, se hace más simple cuando este se envía por un túnel.

Otra razón importante para la implementación de túneles es evitar los problemas que dan los protocolos de enrutamiento en redes demasiado grandes debido a que

en muchas ocasiones su arquitectura no coincide en tipos de protocolos o entre áreas.

Seguridad en las VPN

IPSEC (Protocolo de Internet Seguro) es un grupo de protocolos y algoritmos de seguridad creados para la protección del tráfico de red para trabajar con IPV4 e IPV6 de modo natural o modo túnel que soporta una gran diversidad de autenticaciones y encriptaciones. El principio básico de operación de IPSEC es la independencia algorítmica que le ayudan a efectuar cambios de algoritmos si alguien descubre un fallo crítico o si existe otro más eficaz.

IPSEC está creado para entregar seguridad sobre la capa de red IP, por lo cual, puede ser utilizado eficientemente sobre protocolos como TCP, UDP, ICMP y otros. Esto es muy importante porque significa que es posible usar IPSEC con protocolos o aplicaciones inseguras logrando un excelente nivel de seguridad global

FUNCIONAMIENTO Y DISPOSITIVOS WLAN

Una red inalámbrica puede estar conformada de tan sólo dos dispositivos. Los nodos pueden ser simples estaciones de trabajo de escritorio o portátiles. Creados con adaptadores de red inalámbricos, es posible establecer una red del tipo "ad-hoc" comparable a una red cableada par a par o punto a punto. Ambos dispositivos operan como servidores y clientes en este entorno. Aunque proporciona conectividad, la seguridad no es la mejor, al igual que la tasa de transferencia.
Para solucionar posibles inconvenientes de compatibilidad y mejorar operatividad, comúnmente se instala un punto de acceso (AP) para que realice el papel de hub principal dentro de la infraestructura de la WLAN, El AP se conecta por medio de cable a la LAN tradicional con la finalidad de brindar acceso a Internet y conectividad a la red cableada. Los AP están dotados de antenas y brindan conectividad Inalámbrica a un área específica que se conoce como celda.

Según la construcción estructural del lugar donde se instaló el AP y del tamaño y ganancia de las antenas, el tamaño de la celda puede cambiar sustancialmente . Para entregar servicio de acceso inalámbrico a áreas más extensas, es posible instalar varios puntos de acceso con cierto nivel de superposición. Esta superposición permite moverse de una celda a otra (roaming). Esta característica es muy similar a los servicios que brindan las empresas de teléfonos móviles. La superposición, en redes con varios puntos de acceso, es esencial para lograr mover los dispositivos dentro de la WLAN.

De manera similar, el propósito de mejorar las redes y los dispositivos que actúan en los procesos de transmisión de la información y la comunicación permiten realizar un control del ancho de banda, las direcciones IP, los dispositivos o terminales de entrada-salida dando eficiencia y eficacia en la red (Castillo, 2019).

Es así como, varias investigaciones están orientadas al fortalecimiento e implementación de ancho de banda, velocidad en la transmisión y nuevos protocolos de red que acortar el tiempo de transmisión de los datos de manera segura y transparente para los usuarios finales (Pérez, 2007).

A su vez, García (García, 2019) propone que diseñar y rediseñar las redes LAN y WAN es una actividad en constante mejoramiento que permitirá realizar de manera robusta el escalamiento y flexibilidad en los procesos de actualización y compra de dispositivos para la seguridad y protección de la red.

Capitulo IV. RESULTADOS Y DISCUSIÓN

- Se llego al acuerdo de organizar la numeración de las Vlan y Subredes que actúan en todas las sedes, con un tamaño más acorde a la cantidad de usuarios y dispositivos conectados.
- Se realizó un direccionamiento IP que anteriormente se encontraba difícil de comprender, con los cambios realizados va a ser más fácil identificar problemas y sitios con un direccionamiento más organizado.
- Se contemplo en el nuevo diseño la contratación de un nuevo servicio ISP, con la finalidad de tener un camino alternativo en caso de fallas de alguno de los dos, hubo desacuerdos en cuanto a la tecnología que se debía contratar, ya que existía la idea de que se contratara un proveedor diferente al existente con un servicio de Internet dedicado de iguales características al actual. Se decidió finalmente que debía ser un servicio en el cual los datos viajaran sobre una red privada y no pública.
- Se integró a la nueva topología de Red la sede de Servidores que deberá ser ubicada en el centro de datos de alto nivel Triara (Data center de alto nivel administrado por el ISP Claro, ubicado en el sector de Siberia-Cundinamarca). Esta contara con un ambiente de producción y pruebas para que los desarrolladores puedan realizar prácticas antes de lanzar su desarrollo a producción.
- El diseño de la nueva topología de red contempló que se deben instalar equipos de tipo Access Point e impresoras de Red para brindar facilidad a los usuarios que se desplazan entre las distintas sedes, y para los usuarios que requieren impresión de documentos sin tener que depender de computadores encendidos.
- Básicamente, se mejorarán los siguientes aspectos del funcionamiento actual en la red LAN de Unifianza SA:

- Los Dispositivos finales cómo teléfonos y computadores no van a perder conectividad e la red de datos.
- No habrá Pérdidas de llamadas o robotización sobre la red de voz.
- Entrega oportuna del servicio de direccionamiento IP (DHCP)
- Al contar con un servicio automatizado de direccionameinto IP, no se deben volver a presentar problemas de duplicidad en la red.
- Teniendo dos alternativas de enrutamiento en cada sede, y con el uso de rutas estáticas y rutas estáticas flotantes, el inconveniente de la pérdida de conectividad entre sedes será solucionado.
- La Saturación en los canales de datos (ISP) será solucionada, debido a que se enrutará en tráfico de tal manera que las cargas sean balanceadas entre los dos ISP.
- Al pasar la aplicación core que funciona actualmente sobre el protocolo RDP, al protocolo HTTPS, la saturación de la red bajará y el rendimiento mejorará notablemente.

CONCLUSIONES

Basado en una teoría bien fundamentada, con objetivos claros se realizó el diseño de la red LAN para la compañía Unifianza SA, aprendiendo que cada escenario siempre va a ser diferente y las solicitudes del cliente hacen que cada situación sea un reto distinto.

Se realizó un direccionamiento IP más organizado y coherente de acuerdo con la ubicación y servicios de cada sede, creando grupos de Vlan’s que van a permitir tener control del tráfico entrante y saliente en cada subred.

La inclusión de los nuevos servicios (MPLS) con un ISP, mejoraron la redundancia a nivel de rutas entre las sedes para poder garantizar que siempre va a haber conectividad entre ellas, y la centralización de los servicios en un lugar de alta disponibilidad (Servidores) hicieron que los accesos a los servicios que brinda la red sean más rápidos y confiables.

Se ubicaron de manera eficiente los dispositivos de red en cada sede, y los usuarios manifiestan que la forma en la que operan es más cómoda y accesible a la anterior, resaltando que anteriormente no disponían de servicios cómo acceso vía wifi o impresoras conectadas en red; además, una de las mejoras más notable es que no se han presentado a la fecha caídas totales en los servicios HTTPS de los servidores ubicados en Triara, es decir, que la redundancia a nivel de enrutamiento funciona adecuadamente.

REFERENCIAS BIBLIOGRÁFICAS

Barzola Moran, T. L. (2020). DISEÑO DE UNA RED LAN PARA MEJORAR LA TRANSFERENCIA DE INFORMACIÓN EN LAS OFICINAS DE LA COOPERATIVA DE TRANSPORTE DE PASAJEROS EN TAXIS POLICENTRO, EN LA CIUDAD DE GUAYAQUIL, EN EL AÑO 2018 (Bachelor's thesis, Instituto Superior Tecnológico Bolivariano de Tecnología.).

Castillo Porturas, A. N. (2019). Implementación de redes virtuales utilizando Vlan para reducir el tamaño del dominio de difusión de la red en el Inabib.

Delgado Gomez, B. S., & Torres Maldonado, J. C. (2019). Diseño de la Red LAN de ESC Administraciones en la Sede de Bogota.

Garcia Ramos, H. S., & Moreno Suarez, J. (2019). Rediseñar la red LAN y WAN basado en el protocolo VXLAN para mejorar la comunicación de todas las sedes de la compañía CRC, en la ciudad de Bogotá.

Herrera, O., & Briseth, A. (2020). Diseño de una red LAN para las sedes de Lavaseco Exito con sistema de videovigilancia.

Moreno Duarte, S. L. (2020). Análisis de Vulnerabilidades de la Red LAN del gobierno Autónomo Descentralizado de la Parroquia Pimocha (Bachelor's thesis, Babahoyo, UTB-FAFI 2020).

Pérez, S. C., Facchini, H. A., & Mercado, G. (2007). Análisis y Determinación de Patrones de Tráfico de Protocolos en redes LAN. In IX Workshop de Investigadores en Ciencias de la Computación.

Redes Cisco – Guía de estudio para la certificación CCNA – Ernesto Ariganello. Telecomunicaciones – Tecnologías, Redes y Servicios – José Manuel Huidobro Moya

Rodriguez Muñoz, J. A. (2020). Diseño de una red Lan para la empresa la Florida Inversiones cadena hotelera.

Rosas Beltran, I. D. (2020). Rediseño de la red LAN basado en la aplicación del estándar de redes CISCO 802.1 para asegurar la mejora en el rendimiento y la disponibilidad de toda la red de Constructora Bolívar SA en la sede Bogotá.

Sotelo Palacios, A. A. (2019). Propuesta de implementación del protocolo Netflow y la calidad de servicio para mejorar el rendimiento de la Red Lan en una sede de la SUNARP.

Glosario

Subred

La división en subredes es el concepto de dividir la red en porciones más pequeñas llamadas subredes. Esto se hace tomando prestados bits de la parte del host de la dirección IP, lo que permite un uso más eficiente de la dirección de red.

Gateway

El Gateway o puerta de enlace solo se usa cuando un host desea enviar un paquete a un dispositivo en otra red. La dirección de la puerta de enlace es generalmente la dirección de la interfaz de un router conectado a la red local del host. La dirección IP del dispositivo host y la dirección de la interfaz del router deben estar en la misma red o subred.

Routing

Para transferir un paquete a otras redes, debe procesarlo un router. La función del router es seleccionar la mejor ruta y dirigir los paquetes al host de destino en un proceso que se denomina “routing”. Un paquete puede cruzar muchos dispositivos intermediarios antes de llegar al host de destino. Se denomina “salto” a cada router que cruza un paquete antes de alcanzar el host de destino.

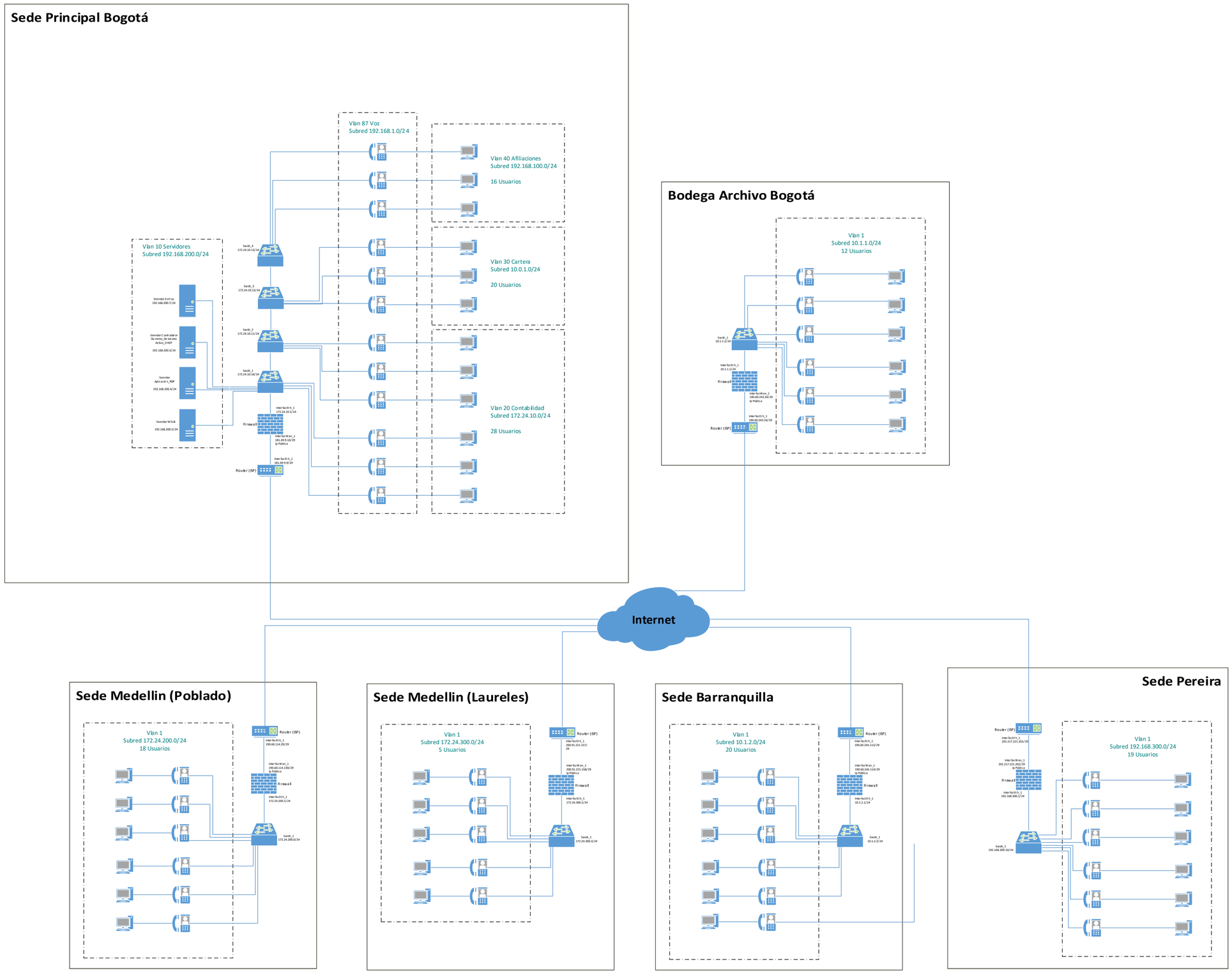
Túnel VPN

Un túnel VPN es una conexión virtual que se enruta a través de Internet desde la red privada de una organización hasta el sitio remoto o el host del empleado. La información de una red privada se transporta de manera segura a través de la red pública para formar una red virtual.

Firewall

Un firewall es un dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad.

TOPOLOGÍA DE RED INICIAL



TOPOLOGÍA DE RED FINAL