UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN
FACULTAD DE INGENIERÍA MECÁNICA Y ELÉCTRICA

TESIS

DISEÑO CON DISPOSITIVOS DE INTERCONEXIÓN DE REDES CISCO PARA UN MEJOR APROVECHAMIENTO DE LA RED LAN

POR

NANCY MARGARITA SÁENZ GARZA

EN OPCIÓN AL GRADO DE MAESTRÍA EN CIENCIAS DE LA INGENIERÍA CON ESPECIALIDAD EN TELECOMUNICACIONES

OCTUBRE, 2016

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FACULTAD DE INGENIERÍA MECÁNICA Y ELÉCTRICA

SUBDIRECCIÓN DE ESTUDIOS DE POSGRADO

TESIS

DISEÑO CON DISPOSITIVOS DE INTERCONEXIÓN DE REDES CISCO PARA UN MEJOR APROVECHAMIENTO DE LA RED LAN

POR
ING. NANCY MARGARITA SÁENZ GARZA

EN OPCIÓN AL GRADO DE MAESTRÍA EN CIENCIAS DE LA INGENIERÍA CON ESPECIALIDAD EN TELECOMUNICACIONES

SAN NICOLÁS DE LOS GARZA, NUEVO LEÓN. OCTUBRE, 2016

UNIVERSIDAD AUTONOMA DE NUEVO LEON

FACULTAD DE INGENIERIA MECANICA Y ELECTRICA

SUBDIRECCIÓN DE ESTUDIOS DE POSGRADO

Los miembros del Comité de Tesis recomendamos que la Tesis "DISEÑO CON DISPOSITIVOS DE RED CISCO PARA UN MEJOR APROVECHAMIENTO DE LA RED LAN" realizada por el alumno(a) "NANCY MARGARITA SAENZ GARZA", con número de matricula 0951031, sea aceptada para su defensa como opción al grado de "MAESTRIA EN CIENCIAS DE LA INGENIERIA CON ESPECIALIDAD EN TELECOMUNICACIONES"

El Comité de Tesis

M.C. Catarino Alor Aguilar
Asesor

M.C. Leopoldo R. Villarreal Jimenez
Revisor

M.C. Rodolfo R. Treviño Martínez
Revisor

Vo. Bo.

Dr. Simón Martínez Martínez
Subdirector de Estudios de Posgrado

San Nicolás de los Garza, Nuevo León, 04 de Noviembre del 2016

Agradecimientos

Quiero agradecer a Dios por permitirme culminar mis estudios de Maestría, a mis padres José Gerardo y María del Carmen, que siempre han tenido para mí todo su amor y apoyo incondicional, gracias por siempre confiar en mí y alentarme a salir adelante.

Gracias a mi esposo Pedro por apoyarme en terminar mi tesis y brindarme su amor, también a nuestra hija Vanessa que es nuestro motor para seguir adelante y la amamos con todo el corazón.

Tabla de Contenido

Resumen

Los dispositivos de interconexión permiten conectar segmentos de una misma red, o redes diferentes. Los dispositivos que se utilizan en una red son: Repetidores, Hub, Bridges, Switch, Routers, Gateways.

Mientras que los Hub, switch y router son elementos básicos necesarios a la hora de crear nuestra red, los bridges y gateways son utilizados sólo en casos muy puntuales. Los gateways se utilizan para comunicar redes de diferentes tipos y los bridges para conectar dos segmentos de una misma red.

Para comunicarse, los dispositivos utilizan un protocolo de comunicación. El más utilizado es el TCP/IP y consta de las siguientes capas: 1) Física, 2) Enlace, 3) Red, 4) Transporte y 5) Aplicación.

Para hacer más eficiente el uso de la red se utiliza un modelo Jerárquico, en Cisco es de la siguiente manera: Capa de Acceso, Capa de Distribución y Capa de Core, en sí definimos funciones dentro de cada capa, ya que las redes grandes pueden ser extremadamente complejas e incluir múltiples protocolos y tecnologías; así, el arreglo nos ayuda a tener un modelo fácilmente entendible de una red y por tanto a decidir una manera apropiada de aplicar una configuración.

Esto con la finalidad de hacer más eficiente la red, evitando saturación, pérdida de información, lentitud y aumentando la productividad.

Introducción

Actualmente la intercomunicación se ha vuelto imprescindible, en la vida diaria nos comunicaciones con aparatos móviles, teléfonos, o a través de una laptop y con una conexión a Internet tenemos la capacidad de poder conectarnos con personas en otras partes del mundo.

Para las empresas Corporativas es de suma importancia estar comunicados, el envío y recepción de documentos, las llamadas telefónicas, sesiones de Tele presencia, consulta de información en Internet, acceso a servidores de aplicaciones centrales, entre otras, son de las muchas actividades que hacen día a día las empresas.

Cuando se maneja un volumen alto de información y de personas interactuando en una organización, es muy relevante el poder tener una infraestructura de Telecomunicaciones tal que permita la comunicación de una forma rápida y confiable.

Por tal motivo, se presenta en esta Tesis los beneficios de usar dispositivos de interconexión Cisco para el mejor desempeño de la red de las empresas y con esto ayudar al personal a hacer más eficiente su trabajo.

Objetivo

Explicar el funcionamiento de los dispositivos de interconexión Cisco y sus beneficios al conectarlos con su modelo jerárquico, en una empresa corporativa.

Justificación

Se presenta el caso de un cliente Corporativo, el cual tiene un manejo muy grande de información y la configuración que tenía en su red con otros dispositivos hacía que presentara lentitud y saturación. Con la implementación del modelo jerárquico Cisco y sus dispositivos de interconexión se obtuvieron el mejor aprovechamiento de la red y la productividad de la empresa aumentó.

Metodología

Primero. Se explicará el funcionamiento de los dispositivos de interconexión Cisco, así como los protocolos de comunicación que maneja.

Segundo. Detallaremos el modelo jerárquico de Cisco para la implementación de red empresariales grandes y las ventajas que presenta con respecto a otros modelos.

Tercero. Se describirá el proceso inicial de solicitud de elaboración de proyecto por parte del cliente hacia el proveedor y los pasos que se deben seguir.

Cuarto. Se presentará un caso de éxito real, de una empresa corporativa de la localidad, la cual tenía dispositivos de red de otro proveedor y un modelo diferente al propuesto, lo cual ocasionaba problemas en la red.

Quinto. Explicaremos los cambios que se hicieron en la red del cliente para lograr su eficiencia, así como los beneficios que obtuvieron.

CAPÍTULO 1. EQUIPOS DE INTERCONEXIÓN CISCO

1.1 Switches y Bridges operan en Enlace Datos

Los bridges y switches de capa 2 trabajan en la capa de Enlace de Datos. En el switch, el frame enviado es tomado por un hardware especializado llamado ASICs (Aplication Specific Integrated Circuits), es por eso que los switches proveen escalabilidad para velocidades de gigabits y baja latencia.

Cuando un bridge recibe un frame, usa la información de la capa de enlace de datos para procesar el frame. En un ambiente "puente transparente" el puente procesa el frame para determinar si necesita ser copiado a otro segmento conectado, este ve cada frame y mira el campo de dirección de origen para determinar en qué segmento la estación de origen reside.

El bridge recuerda esta información usando la tabla de direcciones MAC, llamada estación cache, en esta se lista cada estación final y en que segmento reside. Por ejemplo: Cuando un bridge escucha un frame, este ve la dirección de destino de la capa MAC y usa esta tabla MAC para procesar el frame en alguna de las siguientes formas:

- Si el dispositivo esta en el mismo segmento que el frame que llegó, el bridge bloquea el frame para que no valla a los otros segmentos. Es el filtro por default soportado.
- Si el dispositivo destino está en un segmento diferente, el bridge manda el frame al segmento apropiado.
- Si no se tiene una entrada en la tabla de direcciones MAC para relacionar la dirección destino, como una dirección broadcast, este copia (no envía) el frame a todos los segmentos directamente conectados.

1.2 Switches

Todos los segmentos deben usar la misma implementación de la capa de Enlace de Datos (Ethernet). Si una estación final debe hablar a otra estación de diferente medio, entonces un router tiene que realizar el puente de translación. En un ambiente switcheado un dispositivo por segmento puede mandar frames al mismo tiempo, entonces permite que el camino principal sea compartido.

1.3 Funciones de la Capa de Red

- Define direcciones de origen y destino asociadas con un protocolo específico.
- Define caminos a través de la red.
- Interconecta múltiples enlaces de datos.
- Define como transportar tráfico entre dispositivos que no están localmente juntos.

Hay dos tipos fundamentales de paquetes en la capa de red:

- Paquetes de datos de la capa de red.- Estos paquetes incluyen datos del usuario y la información apropiada de control de las capas superiores.
- Descubrimiento de ruta o actualización de paquetes.- Paquetes actualizados de ruteo incluyen información acerca de cada red en la intrared, el camino para alcanzar cada red y la distancia (definida por una métrica) entre la red de origen y destino.

Las direcciones de la capa de enlace de datos usualmente existen dentro de un espacio de direccionamiento plano, las direcciones de la capa de red son usualmente jerárquicas en las que se define la red y el dispositivo (nodo) asociado con cada red.

La dirección lógica de la capa de red consiste de 2 porciones, una porción de dirección de red y una porción de host:

- La porción de dirección de red identifica el camino usado por el router dentro de la nube de intered.
- La porción de dirección de host se refiere a un dispositivo o a un puerto específico de un dispositivo en una red.

Una dirección de red comúnmente usada es la dirección IP, la cual tiene los siguientes componentes:

- Una dirección de 32 bits, dividida en 4 octetos. Esta dirección identifica una red específica y un host específico en la red, usando TCP/IP
- Una submáscara de subred de 32 bits, igual dividida en 4 octetos. Esta es usada para interpretar la dirección donde los 1s definen la red y los 0s marcan la línea de división entre la red y los componentes de hosts de las direcciones.

El direccionamiento lógico permite redes jerárquicas. Se requiere configuración. La información configurada identifica los caminos para la red. Las tablas de ruteo incluyen lo siguiente:

Dirección de red. Una dirección de red es de un protocolo específico. Si un router soporta más de un protocolo, deberá tener una tabla única de dirección de red por cada protocolo.

INT. Se refiere al camino para alcanzar una dirección dada. El router lista la interface o interfaces a través de los cuales va a enviar los paquetes destinados para una red específica.

Métrica. Se refiere a la distancia para la red destino. Comúnmente la métrica incluye el número de dispositivos de interconexión que un paquete debe cruzar, (cuenta de saltos) el tiempo que le toma desde la dirección de origen a la dirección destino (retardo) o el valor asociado con la velocidad del enlace.

1.4 Routers: Operan en la capa de Red

Son usados para separar segmentos en un único dominio de broadcast y colisión.

- Controlan Broadcast
- Controlan Multicast
- Determinación de la ruta óptima
- Manejo del tráfico.
- Direccionamiento lógico
- Conecta servicios de WAN

Características adicionales.

- No envían frames de broadcast y multicast de capa 2
- Los routers envían paquetes basados en la información del encabezado de capa3.
- Los routers limitan o aseguran el tráfico de la red basado en atributos identificables dentro de cada paquete, este control puede ser aplicado a los paquetes que entran o salen en cualquier interface del router, este control es llamado Lista se Acceso.
- Los routers pueden desempeñar puenteo o ruteo dependiendo de su configuración.
- En redes switcheadas en capa 2 que usan LANs virtuales (VLANs), los routers proveen conectividad entre diferentes VLANs.

- Los routers pueden ser usados para desplegar parámetros de medidas de seguridad y calidad de servicio (QoS) para especificar tipos de tráfico de red.

Usando routers para proveer acceso remoto

- Los routers son usados para conectar locaciones remotas a la oficina principal.
- Soportan una variedad de estándares de conectividad de capa física, que permiten construir redes de área amplia.
- Proveen seguridad y control de acceso necesarios cuando se conectan locaciones remotas.

1.5 Funciones de la Capa de Transporte

- Distingue entre las aplicaciones de las capas superiores.
- Establece conectividad punto a punto entre aplicaciones
- Define control de flujo
- Provee servicios confiables o no confiables para la transferencia de datos.
- Una sesión consiste de una conexión lógica entre las capas pares de transporte en las estaciones finales de origen y destino.

Permite a las estaciones finales ensamblar y desensamblar múltiples segmentos de las capas superiores dentro de la misma ráfaga de datos de la capa de transporte, esto es para asignar identificadores de aplicaciones de las capas superiores. Estos identificadores son referidos como identificadores de puertos. Ejemplo: Telnet 23

Permite a las aplicaciones solicitar transporte de datos confiables entre los sistemas finales de comunicaciones. El transporte confiable usa una relación orientada a la conexión entre los sistemas finales de comunicación para lograr lo siguiente:

- Asegurar que los segmentos a entregar serán regresados con acuse de recibo al que envía.
- Proveer retransmisión de algunos segmentos que no tienen acuse de recibo.
- Poner los segmentos de regreso con su correcta secuencia a el dispositivo destino.
- Provee el control de flujo y evita congestion .

Ejemplo. Cuando los datagramas llegan muy rápido al host o gateway para procesarlos, son almacenados en memoria de buffers temporalmente.

Si los datagramas son parte de una pequeña ráfaga, entonces este almacenamiento en buffers resuelve el problema. Si el tráfico continúa, el host o gateway excede esta memoria y deben descartar datagramas adicionales que lleguen.

En vez de permitir que los datos se pierdan, la función de la capa de transporte es de poder emitir un indicador al dispositivo que envía “no listo”, señal de alto. Cuando el par receptor puede capturar segmentos adicionales, este manda un indicador de transporte “listo”, el cual es como una señal de avance.

Funciones de confiabilidad de la Capa de Transporte

El transporte confiable de datos requiere el uso de protocolos que soporten servicios orientados a la conexión, como TCP. UDP es un ejemplo de servicio no confiable o sin conexión.

Los servicios orientados a la conexión desempeñan las siguientes tareas: Establecimiento de la conexión, transferencia de datos y desconecta la sesión. Cuando se establece una sesión confiable y es definido un camino a través de la red, entonces este camino es usado por la duración de la transferencia. Los servicios no confiables usan cualquier camino que esté disponible durante una sesión para transmitir los datos.

Primero se establece una sesión, para hacer esto, ambos programas de aplicaciones que envían y reciben información a sus sistemas operativos informan que una conexión será iniciada. El modulo de software de protocolos del SO de las estaciones finales se comunican para enviar mensajes a través de la red para verificar que la transferencia es autorizada y que ambos lados están listos.

Después que la sincronización ha ocurrido, se establece la conexión y la transferencia de información empieza. La estación receptora hace una verificación de datos por medio de un acuse de recibo del datagrama a un intervalo predefinido.

Si la estación receptora notifica a la estación transmisora que un datagrama no fue recibido, la estación que envía retransmitirá los datagramas perdidos.

CAPITULO 2. MODELO JERARQUICO CISCO

2.1 Estructura de la red definida por Jerarquía

Para simplificar el diseño de la red, la implementación y el manejo, Cisco utiliza el modelo jerárquico para describir la red. Para construir apropiadamente una red que pueda ver y direccionar los requerimientos de tráfico del usuario, el modelo jerárquico de 3 capas es organizado de la siguiente manera: Capa de Acceso, Capa de Distribución y Capa de Core

Características de la Capa de Acceso

- Es el punto al cual los usuarios son conectados a la red, por lo cual se refiere a esta capa como "Capa de Escritorio".
- El tráfico de y para los recursos locales es limitado entre los recursos, switches y usuarios finales.
- Múltiples grupos de usuarios y sus recursos están en esta capa.

Características de la Capa de Distribución

- Agregación de direcciones ó grupos de usuarios de la capa de acceso y de entidades remotas como oficinas remotas y usuarios móviles.
- Ruteo de tráfico para proveer acceso departamental o de grupo.
- Definición de dominio de Broadcast/Multicast.
- Translación del medio físico.
- Seguridad.
- Es la capa que provee “conectividad basada en políticas” porque determina sí y como los paquetes pueden acceder al core de la red.
- Determina el camino más rápido para la petición del usuario.

Características de la Capa Core

- El único propósito de la capa de core es de switchear el tráfico lo más rápido posible.

Cuando un usuario requiere tener acceso a los servicios de la empresa, la petición del usuario es procesada en la capa de distribución, entonces esta manda la petición a la capa de core.

2.2 Repaso del modelo OSI

Figura 1 Capas del Modelo OSI

Las 4 capas menores definen el camino o forma en que las estaciones finales establecen conexión con cada otra en la medida en que se intercambian datos. Las 3 capas superiores definen como las aplicaciones dentro de las estaciones finales se comunican con cada otra y con los usuarios finales.

Capas Superiores

- Aplicación.- Es en donde el usuario interactúa con la máquina. Los protocolos de esta capa identifican comunicación del equipo par remoto, determina la disponibilidad de los recursos y sincroniza la comunicación.

- Presentación.- Provee una variedad de funciones de codificación y conversión que son aplicadas a los datos para la capa de aplicación. Un ejemplo de función de codificación es la encriptación.

- Sesión.- Establece, maneja y termina las sesiones de comunicación entre las entidades de la capa de presentación.

2.3 Comunicación entre Capas

Encapsulación de Datos

Cada capa del modelo OSI usa su propio protocolo para comunicarse con su capa par en el dispositivo destino. Para intercambiar información, cada capa usa PDUs (Protocol Data Unit). Los PDUs incluyen información de control y datos del usuario, esta información reside en campos llamados encabezados (headers) y colas (trailers).

Para agregar información de control a un PDU, las capas usan un proceso llamado encapsulación, véase la figura 2. Por ejemplo: La capa de transporte recibe datos de las capas superiores, en esta capa se encapsula información de control del protocolo de transporte en el encabezado del segmento y así se continúa con el proceso hasta llegar a la capa física con la información de control de los protocolos de las capas superiores y la información se manda en bits a través del cable.

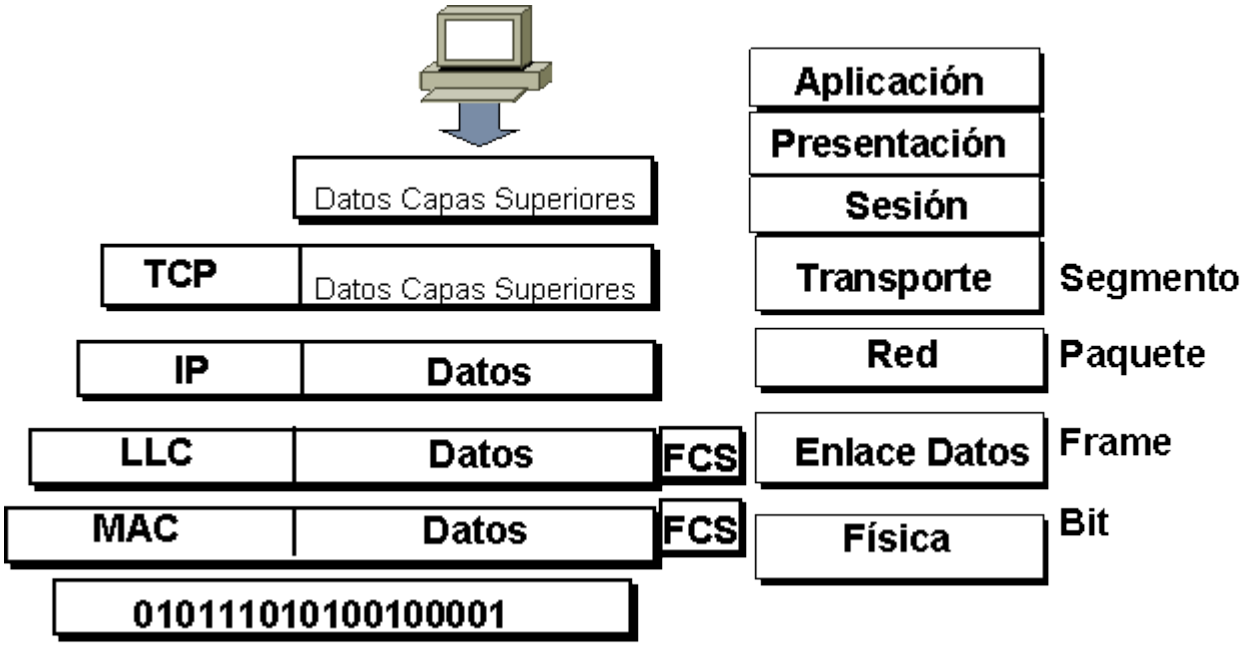

Figura 2. Proceso de Encapsulación de datos

Des-encapsulación de Datos

Cuando el dispositivo remoto recibe una secuencia de bits, estos se pasan a la capa de Enlace de Datos para la manipulación del frame. Cuando la capa de Enlace de Datos recibe el frame, hace lo siguiente:

- Lee la información de control provista por la capa par del dispositivo de origen.
- Extrae la información de control del frame.
- Pasa el frame a la capa siguiente superior siguiendo las instrucciones que aparecen en la porción de control del frame.

Cada capa subsiguiente realiza el mismo proceso llamado des-encapsulación, véase la figura 3.

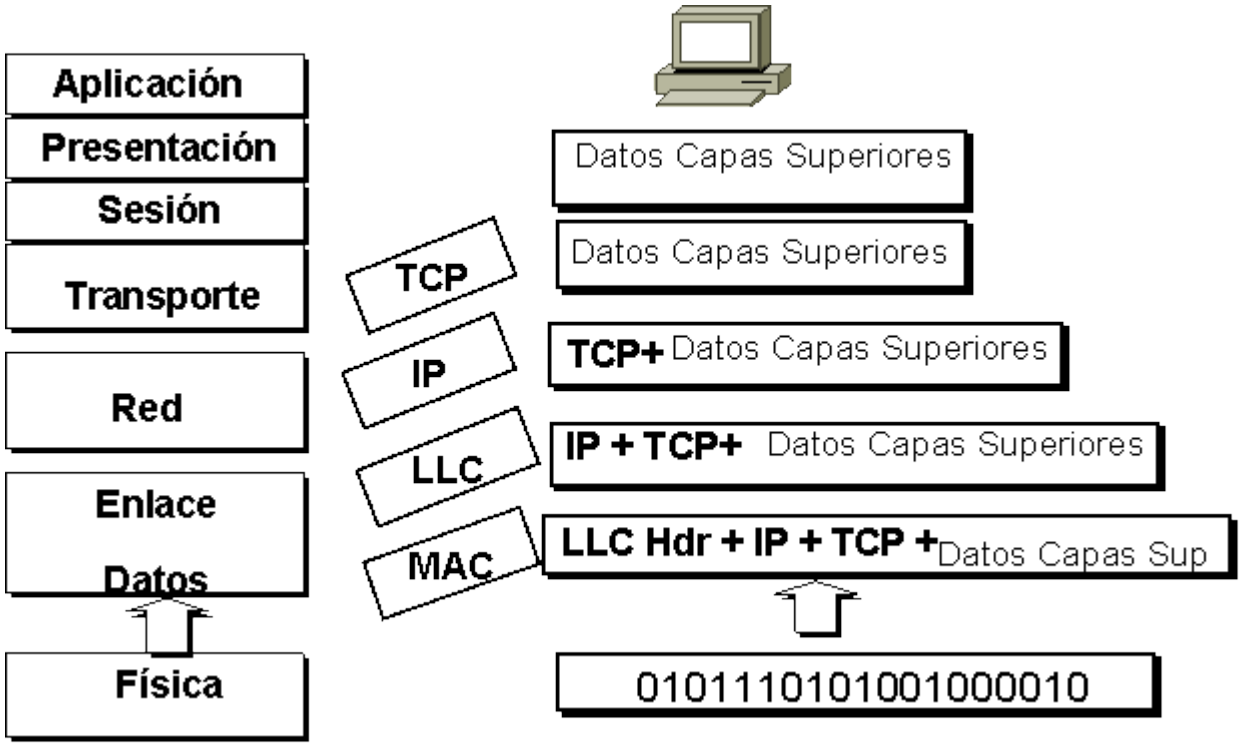

Figura 3. Proceso de Desencapsulación de datos

2.4 Funciones de la capa física

La capa física especifica los requerimientos eléctricos, mecánicos, de procesos y funcionales para la activación, mantenimiento y desactivar el enlace entre los sistemas finales.

Especifica características como voltaje, razón de datos, distancias máximas de transmisión y conectores físicos. Todas las estaciones en un segmento que escuchan todo el tráfico en el cable, están en el mismo dominio de colisión. Una colisión ocurre cuando más de una estación trata de mandar información al mismo tiempo.

Las estaciones que están en el mismo dominio de colisión están también en el mismo dominio de broadcast, todas las estaciones en un segmento oyen los broadcast mandados en el segmento. En resumen, la capa física define: Tipo de medio, conector y señalización.

Ethernet 802.3

La Ethernet y el estándar IEEE802.3 definen una topología bus para una LAN que opera a una señalización banda base a un rango de 10Mbps. Las estaciones se unen al segmento por un cable que corre desde una AUI (Attachment Unit Interface) en la estación hasta un transceiver que es directamente agarrado al cable coaxial Ethernet.

10Base2.- Segmentos de red hasta 185 m en cable coaxial.
10Base5.- Segmentos de red hasta 500 m en cable coaxial.
10BaseT.- Ethernet en par torcido a 10Mbps.

Los hubs operan en la capa Física

Los hubs son dispositivos usados para extender una red Ethernet cableada para permitir a más estaciones comunicarse con otras si éstas están en el mismo segmento. Cuando se usa un hub, la topología cambia de una forma linear donde cada dispositivo se conecta, a una topología estrella. En resumen, en un hub:

- Todos los dispositivos están en el mismo dominio de colisión y broadcast
- Los dispositivos comparten el mismo ancho de banda.

La tecnología Ethernet LAN presentada es CSMA/CD (Carrier Sense Múltiple Access/ Collision Detection). Esto es, estaciones en la LAN CSMA/CD pueden

mandar datos, las estaciones CSMA/CD “escuchan” la red para ver si está en uso, si no lo están, la estación transmite.

Una colisión ocurre cuando dos estaciones escuchan el tráfico de la red y no oyen nada, entonces transmiten simultáneamente. La transmisión se daña y las estaciones tienen que volver a retransmitir la información.

2.5 Funciones de la capa Enlace de Datos

La capa de enlace de datos define como son transportados los datos sobre un medio físico. También define como encapsular tráfico de un protocolo específico en el cual el tráfico que va a diferentes protocolos de las capas superiores pueden usar el mismo “canal” así este sube por la pila de capas. Define:

- Direccionamiento físico del origen y destino.
- Protocolos de capas superiores asociadas con el frame.
- Topologías de la red.
- Secuencia del frame.
- Control de flujo.
- Conexiones orientadas o no a la conexión.

Subcapas de la capa de enlace de datos.

MAC (802.3).- Define como transmitir frames a través del cableado, se encarga del direccionamiento físico asociado a cada dispositivo, definición de la topología de red, disciplina de línea, notificación de error, ordenamiento deliberado de frames y control de flujo (opcional).

LLC (802.2).- Es el responsable de la identificación lógica de los diferentes tipos de protocolos y entonces encapsularlos. La identificación lógica es hecha por un tipo código o un identificador SAP (Service Access Point). Opciones adicionales de

la capa LLC incluyen soporte para conexiones entre aplicaciones corriendo en la LAN, control de flujo de las capas superiores y control de secuencia. Por otros protocolos, esta capa es usada para definir servicios confiables o no confiables.

CAPA MAC 802.3

El frame IEEE 802.3 empieza con un patrón alternado de 1's y 0's llamada preámbulo. El preámbulo le dice a la estación receptora que un frame está llegando. Inmediatamente después del preámbulo están los campos de dirección física de origen y destino, las cuales son referidas a las direcciones de la capa MAC.

La dirección MAC esta expresada en 48 bits como 12 dígitos hexadecimales. Los primeros 6 dígitos hexadecimales de la dirección MAC contienen una identificación de manufactura conocido como OUI. Los últimos 6 dígitos hexadecimales son administrados por cada vendedor y a veces representan el número de la interface serial.

La dirección de origen siempre es unicast, mientras que la dirección destino, puede ser unicast, multicast o broadcast. El campo de 2 bytes seguido de la dirección de origen es el campo de longitud, el cual indica el número de bytes de datos que siguen este campo.

El siguiente campo es el de datos, incluye información de control LLC, información de control de capas superiores y los datos del usuario. El campo siguiente de 4 bytes es el FCS y contiene el valor de CRC (Cyclic Redundancy Check), el cual es creado por el dispositivo que envía y recalculado por el dispositivo que recibe para revisar si hubo algún daño en el frame al transmitirlo. Para revisar la estructura del frame MAC 802.3 véase figura 4.

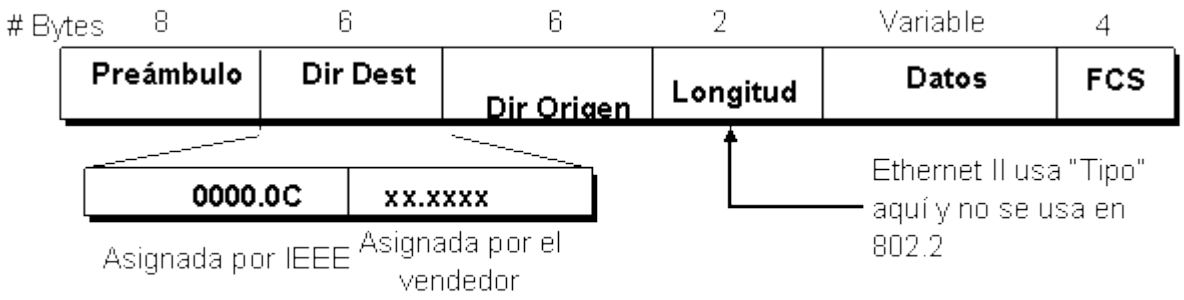

Figura 4. Estructura del frame MAC 802.3

802.2 SNAP Y SAP

Hay dos tipos de frames LLC: SAP y SNAP. En el encabezado LLC, los campos SAP de destino y origen (DSAP y SSAP) son de 1 byte cada uno y actúan como índices a los protocolos de las capas superiores en una estación.

El proceso SAP provee una interface conveniente a las capas de niveles superiores de la capa OSI. Para especificar que el frame usa SNAP, los campos SSAP y DSAP son puestos en AA hexadecimal y el campo de control es puesto en 3. SNAP tiene un campo de tipo código “type” que permite la inclusión del tipo Ether.

Por ejemplo: TCP/IP usa el tipo Ether para diferenciar entre los paquetes ARP y los frames de datos. Para permitir protocolos propietarios en el frame 802.2, la IEEE definió el formato SNAP. En el frame SNAP, los primeros 3 bytes del encabezado SNAP, seguidos del campo de control son el código OUI del vendedor. Seguido del código del vendedor es un campo de 2 bytes conteniendo el “Type” Ether del frame. Un campo de 4 bytres sigue del campo de datos y contiene el valor CRC.

CAPÍTULO 3. SOLICITUD DE PROPUESTA

3.1 Introducción

Al tener una necesidad en una empresa, el departamento de Compras o Abastecimiento lanza una convocatoria a los proveedores calificados para cubrirla, la cual se llama RFP (Request For Proposal), en donde especifican lo siguiente:

- El área que requiere de los servicios o productos
- La problemática actual
- Las necesidades que deben de cubrir
- Las condiciones actuales y próximas futuras a mediano y largo plazo
- Condiciones de seguridad que deberán cumplirse
- Un contrato tipo en el cual se deben de especificar clausulas de cumplimiento del proyecto

3.2 Explicación de las necesidades del cliente

En este caso de estudio las respuestas a las especificaciones del RFP que lanzó el cliente son:

El área de Infraestructura de Redes y Comunicaciones hizo la solicitud formal al departamento de Abastecimiento, a través del documento RFP para que se lo mandara a los proveedores del mercado que pudieran cubrir con sus necesidades y brindaran la mejor propuesta técnica y económica.

La problemática que presentaba el área era que la infraestructura de equipos de interconexión de datos, tanto en el Corporativo como en sus oficinas y sucursales

remotas, que tenía era obsoleta y tenían un modelo plano, sin seccionar la red para una mejor distribución.

Adicional a lo anterior, el cableado estructurado no tenía un correcto acomodo ni la capacidad de transmisión adecuada a las necesidades que estaba teniendo el cliente.

También debían de mejorar su infraestructura de seguridad para hacerla más robusta y menos vulnerable a intrusos que pudieran hacer mal uso si llegaban a entrar a la red.

Las necesidades que el proveedor debía de cubrir con su propuesta era:

1) Diseño de red con dispositivos de interconexión Cisco, que cubriera las demandas de tráfico actual y pudiera soportar crecimiento futuro.
2) Hacer que la interconectividad de los dispositivos fuera con el modelo jerárquico que maneja Cisco para tener un mejor desempeño de la red y por ende un aprovechamiento de los recursos.
3) Reducir el tiempo de respuesta de las peticiones de los usuarios, la mayoría tenía que interactuar con los servidores del corporativo y en ocasiones presentaban lentitud o desconexión de enlace. También se requería que los usuarios de ventas, los cuales utilizaban hand helds, tuvieran siempre disponibilidad a los servidores para hacer solicitudes de venta en tiempo real y no demorar en entrega de facturas a los clientes.
4) Mejorar el medio de transporte entre los dispositivos, implementando cableado de fibra óptica de altas velocidades.
5) Reemplazar los equipos actuales de seguridad con nuevos equipos de la familia de Cisco, además de implementar políticas de seguridad para los empleados y así evitar tanto los intrusos como pérdida de información valiosa del corporativo.

6) De suma importancia que la migración se haga de manera transparente para la operación de la organización, ya que los movimientos son muy delicados por que impactan las operaciones cruciales de la empresa.
7) Contar con una infraestructura escalable, es decir, que en un futuro próximo el cliente esté preparado para el crecimiento de la empresa.

El cliente detalló su infraestructura actual, tanto en el corporativo como en sus oficinas principales, la planta y sus sucursales. Los equipos con los que contaba, las configuraciones, usuarios, demanda de aplicaciones y anchos de banda de los enlaces, necesidades de cada localidad, así como el arreglo físico brindando recorrido y fotografías de su infraestructura.

Lo que el cliente buscaba con este proyecto era:

1) Actualizar su infraestructura de red con equipo de tecnología de punta
2) Mejorar el cableado estructurado existente, teniendo bien identificado cada nodo.
3) Contar con un diseño jerárquico de la red del corporativo para que con la correcta distribución de los equipos, se mejorar la respuesta al tener alta disponibilidad y velocidad en el corporativo para las solicitudes de los usuarios
4) Minimizar tiempos de respuesta a las peticiones de los usuarios
5) Cumplir con las normas internacionales de las mejores prácticas en los modelos de infraestructura de comunicación empresarial.

El cliente solicitó que se cumplieran con las condiciones de seguridad del corporativo, como el proyecto era migrar al Data Center, era de vital importancia que el personal tomara las medidas necesarias de seguridad, tanto de acceso a las instalaciones como de confidencialidad de la información.

Por tal motivo, se diseño un plan de migración en donde se especificaron los pasos a seguir para los cambios, las configuraciones de los equipos, los check list que deberían de cumplir para asegurar los cambios transparentes de la infraestructura, las fechas establecidas para evitar el menor impacto en la operación y los responsables operativos de cada movimiento.

Para poder presentar la propuesta técnica y económica y así dar respuesta al RFP del cliente, se tuvieron que realizar reuniones técnicas para definir específicamente las necesidades y entender perfectamente los cambios que el cliente requería.

Una vez que se presentó la propuesta y se seleccionó al proveedor ganador, se pasó a la etapa de elaboración del Contrato de prestación de servicios, en el cual se deben de establecer las Cláusulas para la elaboración de los servicios y venta de los equipos.

Los abogados de cada parte (cliente y proveedor) mediados por la parte Comercial, deben de llegar a un acuerdo de cada una de las cláusula del contrato, para poder firmarlo y tener el respaldo legal del cumplimiento de lo ahí establecido para la tranquilidad del cliente, ya que la inversión económica y el impacto en las operaciones cruciales de la empresa son de importancia significativa.

3.3 Procedimiento de la respuesta al RFP

Ya que el cliente cuenta con la respuesta al RFP lanzado de optimización de su infraestructura de red LAN por parte del proveedor, los pasos a seguir son:

- Firma del contrato de prestación de servicios
- Elaboración de las órdenes de compras, en las cuales describen a detalle los equipos, sus características, cantidades, precios unitarios y totales, así como los datos de facturación.

- Las órdenes de servicio son recibidas por el proveedor, el cual realiza internamente los movimientos para compra de los equipos al fabricante (en este caso Cisco) y asigna las fechas de entrega de los equipos al cliente.
- Teniendo las fechas de entrega de los equipos con el cliente, se procede a la elaboración de un Plan de Migración con una grafica de Gantt, el administrador del proyecto le expone al cliente cuales son los pasos a seguir para la implementación exitosa de la migración y cumplir con los requerimientos.
- Contando físicamente con los equipos, el proveedor comienza con la fase de pre configuración para prepararlos al momento de hacer el reemplazo físico en los sitios. En este paso se le brinda al cliente la calendarización de las migraciones, se asignan responsables de ambas partes para comprobara el éxito de los cambios.
- Todos los cambios se hacen basados en el diseño que el departamento de Consultoría sugirió en la respuesta técnica al RFP.
- Al término de los cambios de equipos y configuraciones se elaboran cartas de aceptación por parte del cliente en donde expresa que está de acuerdo con los cambios de equipamiento y ha revisado que las aplicaciones funcionen correctamente validando con un check list que deben cumplir.
- El proveedor emite las facturas en respuesta a las órdenes de compra que el cliente emitió, las cuales deben de coincidir en cuanto a montos totales y razones sociales.
- El ciclo se completa cuando el cliente hace el pago del proyecto al proveedor y se entrega al cliente las configuraciones de todos sus equipos.

CAPITULO 4. CASO DE ESTUDIO

4.1 Objetivo del proyecto

El objetivo de este caso de estudio es proponer al Cliente un diseño, alineado a las mejores prácticas de Cisco y otros estándares de calidad mundial, para la implementación de una solución de comunicaciones que permita al Cliente optimizar la utilización de sus recursos informáticos y alcanzar una reducción de gastos operativos.

Para ello se propone la implementación de un modelo jerárquico y redundante de red que proporcione mayor disponibilidad y desempeño de los diferentes servicios de datos, voz y video, de forma local y hacia los sitios remotos.

La solución propuesta comprende las siguientes tecnologías:

1. Red LAN (Switches L2/L3) Corporativo del cliente y sitios remotos
2. Seguridad (Firewall ASA 5550)
3. Infraestructura auxiliar y cableado UTP y Fibras Ópticas MDF é IDF´s

4.2 Antecedente del Proyecto

La red actual del Cliente está compuesta por los siguientes sitios:

- 1 Corporativo Monterrey
- 1 Planta
- 2 Oficinas (Guadalajara, México)
- 67 Sucursales a nivel nacional

La red LAN actual del Cliente, en sus diferentes sitios, está constituida en una plataforma marca 3COM, integrando una red plana que no cuenta con un protocolo de ruteo dinámico. En el nodo corporativo el ruteo es manejado de forma estática en los firewalls y core switches.

El nodo corporativo Monterrey cuenta con un MDF principal en donde se alojan los servicios principales y el centro de datos, y donde se concentran los 17 IDF de la planta a través de uplinks de fibra óptica multimodo con conectores tipo SC a 1GB de velocidad.

4.3 Descripción del Diseño

Bloques de Servicios

El diseño de la red LAN Corporativa del Cliente en Monterrey está basada en un modelo conceptual jerárquico de 3 capas lógicas, Core, Distribución y Acceso, colapsando Core y Distribución en una sola plataforma de alto desempeño para el ahorro de recursos.

Capa de Core/Distribución

En la capa de Core se realiza únicamente la conmutación de la información del usuario y aplicativa, en esta capa no se procesa información. La capa de Distribución es la capa intermedia de la red LAN que interconecta a la Capa de Acceso con la Capa de Core, y se encarga de realizar la búsqueda de las mejores rutas.

En la capa colapsada de Core/Distribución es donde se tiene la mayor demanda de tráfico, por lo que se implementará sobre equipos Switches LAN de grandes capacidades de procesamiento y velocidad en su backplane. Dichos equipos se conectarán mediante puertos 10GB y 1GB hacia las zonas de acceso. Esta capa cuenta con redundancia en equipo de Core y en fuente de energía.

Se cuenta en el Core colapsado con equipos redundantes y modulares, es decir, se incluyen dos equipos, uno espejo del otro. Cada uno de ellos cuenta con supervisora simple y fuente de poder redundante, en una arquitectura robusta de alta disponibilidad.

No se considera doble tarjeta supervisora en los switches de core/distribución, ya que la arquitectura redundante en esta capa permite que un switch asuma el control de todo el tráfico de la red en caso de falla fatal en alguno de ellos. Sin embargo, si se considera doble fuente de poder en cada uno de estos switches, para proveer un grado mas alto de disponibilidad.

Capa de Acceso

La capa de Acceso de la red LAN está dividida en 4 bloques de servicio como se indica a continuación:

- ✓ Bloque de Usuarios (IDFs)
- ✓ Bloque de Wireless LAN
- ✓ Bloque de Telefonía IP
- ✓ Bloque de Enterprise Edge
- ✓ Bloque de Data Center

Cada una de estas capas se conectará hacia la capa de Core/Distribución mediante un par de enlaces redundantes de Uplink, a través de un tendido de cableado estructurado, ya sea en fibra a 10GB o 1GB, o con cobre categoría 6 como mínimo.

Cada enlace de Uplink estará configurado como troncal 802.1Q para el traspaso de VLANS desde los bloques de acceso hacia la capa de core/distribución. Se utilizará la funcionalidad de PVST (Per VLAN Spanning Tree) de Cisco para realizar la distribución de VLANS entre cada par redundante de Uplinks con objeto de balancear el tráfico entre los dos Uplinks.

La figura 5 muestra el diseño conceptual propuesto para la red del Cliente, con los diferentes bloques de servicios propuestos.

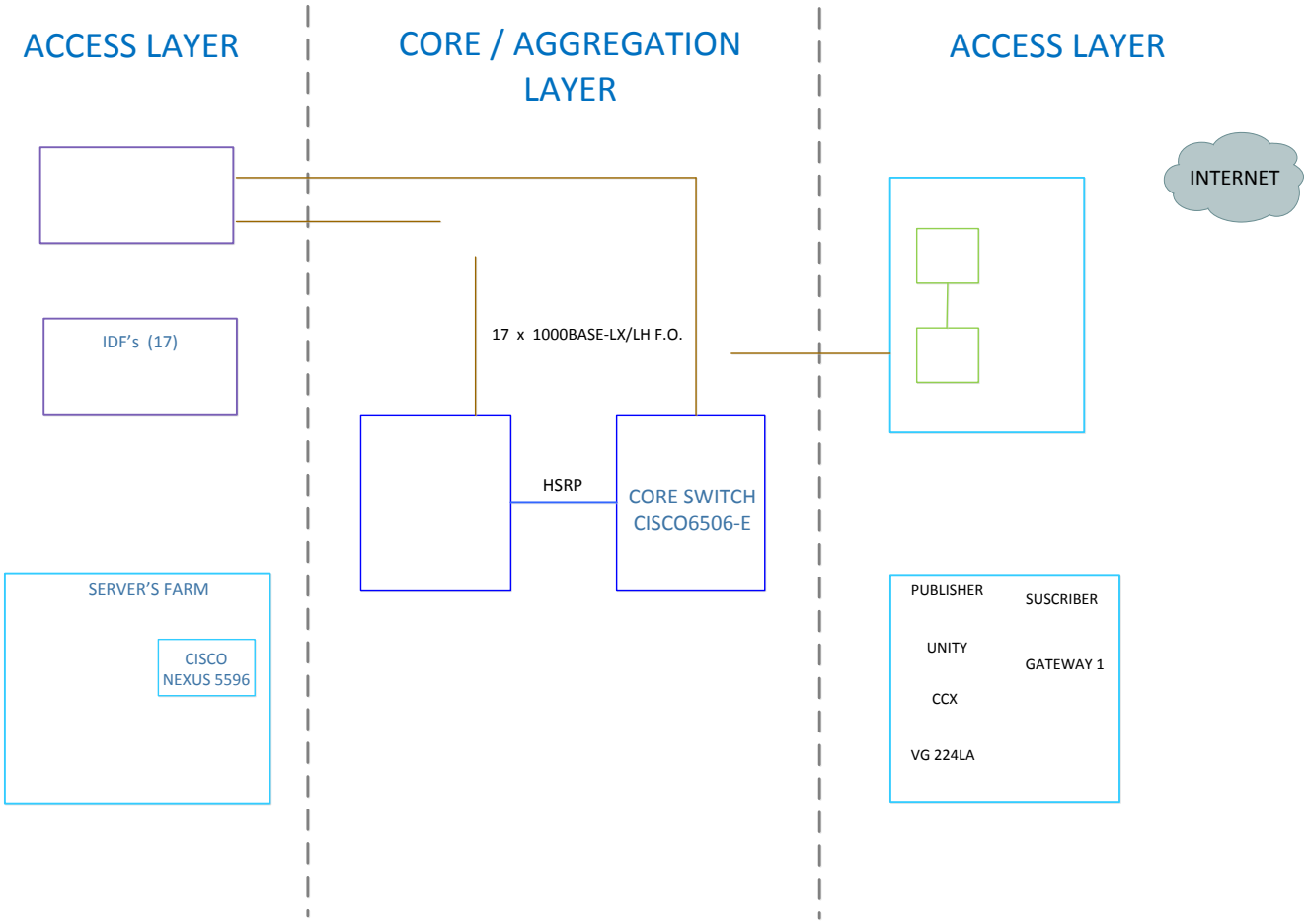

Figura 5. Diseño Conceptual de la red LAN del Cliente

4.4 Bloque de usuarios (IDFs)

El bloque de usuarios está conformado por 17 IDFs distribuidos a lo largo de la planta del Cliente en Monterrey. Cada IDF estará conformado por una plataforma de switcheo de Capa 2 (LAN Base) a 1GB con capacidad PoE.

Aquí se establecerán las conexiones de los usuarios y servicios a la red, como son equipos de cómputo, impresoras, cámaras de video, Access points, impresoras, etc.

Todos estos usuarios y servicios obtienen acceso a la red LAN conectándose a la Capa de Acceso mediante cableado estructurado en cobre categoría 6 hacia el cuarto de comunicaciones (IDF), en donde finalmente, a través de un patch cord UTP se conecta a un puerto RJ-45 Fast Ethernet 100 Mbps de un equipo standalone, es decir, un equipo con puertos fijos, los cuales pueden ser de 24 ó 48 puertos 10/100 con capacidad PoE 802.1f.

La conexión de cada IDF hacia la capa de core/distribución se realiza mediante un par de enlaces de Uplink en Fibra Óptica mono modo LX/LH con velocidad de 1Gbps.

4.5 Bloque de Wireless LAN

El bloque de Wireless LAN permite el acceso de los usuarios inalámbricos hacia la red LAN del Cliente, a través de los dispositivos Access Point distribuidos en toda la planta.

Mediante la tecnología LWAPP (Lightweight Access Point Protocol) se establecen túneles de capa 2 o capa 3 desde cada AP hacia un dispositivo controlador WLC (Wireless LAN Controller), el cual establece la conectividad de los AP hacia la red LAN.

El bloque de Wireless LAN está constituido por uno o varios dispositivos WLC que se conectan hacia la capa de Core/Distribución mediante enlaces redundantes de Uplink. Estos enlaces se consideran a 1GB sobre cableado UTP RJ45 cat 6.

4.6 Bloque de Telefonía IP

El bloque de Telefonía IP comprende la infraestructura utilizada para proporcionar los servicios de telefonía IP a la red del cliente, la cual comprende dispositivos tales como servidores de telefonía y gateways.

Toda esta infraestructura estará implementada en un bloque dedicado de servicios de la red LAN interconectados entre sí a través de una plataforma de switcheo de Capa 2 (LAN Base) a 100 Mbps con puertos Fast Ethernet RJ-45.

El bloque de Telefonía IP se conecta hacia la capa de Core/Distribución mediante enlaces redundantes de Uplink. Estos enlaces se consideran a 1GB sobre cableado UTP RJ45 categoría 6.

4.7 Bloque de Enterprise Edge

El bloque de Enterprise Edge concentra las comunicaciones del Corporativo del Cliente hacia otras redes, tanto internas como externas. La incorporación de estas redes se realiza a través de una plataforma de seguridad conformada por un par de dispositivos Firewall en configuración de alta disponibilidad HA (High Abailavility) en modo activo / hot stand by.

En el modo de operación HA activo / stand by, los dispositivos Firewalls son configurados como un par failover, el cual sincroniza continuamente el estado de las conexiones de red. En caso de una falla del equipo activo, las sesiones de red son transferidas automáticamente al equipo de respaldo (stand by) el cual continúa con la labor de filtrado de tráfico, con completa trasparencia para los usuarios.

En la plataforma de Enterprise Edge se terminan las conexiones VPN de los usuarios móviles, así como el acceso de navegación hacia Internet de los usuarios de la red, constituyendo una frontera de seguridad para las conexiones hacia el exterior de la red.

De igual manera, también se provee acceso seguro hacia otras redes, locales y remotas, que requieren conectividad hacia la red corporativa del Cliente, como es el caso de la red WAN MPLS, por medio de la cual las oficinas remotas y sucursales pueden accesar los servicios informáticos del Corporativo del Cliente, así como conexiones internacionales con diferentes proveedores.

4.8 Bloque Data Center

El bloque de Data Center constituye una plataforma de acceso para la granja de servidores, donde se concentran los diferentes servidores que soportan las aplicaciones corporativas del Cliente. La plataforma de switcheo utilizada proporciona conectividad a 1 Gbps con puertos 1000Base-T en cobre categoría 6, con capacidad de conmutación en capas 2 y 3.

Se cuenta con dos switches de acceso de alto desempeño, donde se distribuirán las conexiones de los servidores, procurando un balanceo de carga entre los dos dispositivos. Estos equipos cuentan con capacidad para el crecimiento a futuro de ancho de banda a 10GB hacia los servidores.

La conectividad hacia la capa de Core/Distribución se lleva a cabo mediante enlaces Uplink redundantes de 20 Gbps, conformados cada uno de ellos por dos enlaces de 10 Gbps en modo de agregación de ancho de banda (Etherchannel).

4.7 Capa de Core/Distribución

La capa de Core/Distribución está conformada por un par de switches modulares de alto desempeño en modo de redundancia para proveer una alta disponibilidad.

Todas las conexiones hacia los diferentes bloques de la capa de acceso se hacen mediante troncales Uplink redundantes, ya sea en cobre o en fibra, a 1 o 10 Mbps.

La plataforma de Core/Distribución constituye el núcleo de la red, por lo que el diseño propuesto cuenta con la capacidad necesaria y suficiente para cubrir las necesidades actuales de ancho de banda de la red, así como con capacidad de crecimiento para responder a las necesidades futuras del cliente.

CAPÍTULO 5. SOLUCIÓN RED LAN

5.1 Bloque de Core/Distribución

Antecedentes

Actualmente se encuentra en operación en el MDF del sito de Monterrey 5 equipos 3COM 5500G-E en stack apilados sin esquema de CORE redundante físico, referencia Fig 6.

También se encuentra la interconexión hacia los diferentes IDF´s, plantas de Canadá, doméstico y oficinas es través de uplinks de Fibra Óptica Multimodo con conectores ó jumpers tipo SC a 1GB de velocidad sin redundancia.

Figura 6. Situación actual 3COM 5500G-E en Stack

Premisas de Diseño

La propuesta de diseño de la infraestructura LAN se rige bajo un modelo conceptual de 3 capas (Core, Distribución y Acceso).

Se requiere implementar un backbone redundante (doble equipamiento) que proporcione alta disponibilidad de los servicios, permitiendo la continuidad de la operación ante la pérdida de conectividad u operatividad en alguno de los equipos. Se considera la utilización del protocolo propietario de Cisco HSRP (Hot Stanby Routing Protocol).

Se considera un par de equipos Cisco Catalyst WS-C6506-E para el Core de la LAN en modo activo/activo de forma redundante. Cada una de los chasises cuenta con doble fuente de poder de corriente alterna.

Se propone un modelo jerárquico de red, definiendo bloques de servicio para la separación física o lógica de diferentes funciones o aplicaciones de red, como son:

- Bloque de Usuarios (IDFs)
- Bloque de Wireless LAN
- Bloque de Telefonía IP
- Bloque de Enterprise Edge o Seguridad (Wan, MPLS, Internet)
- Bloque de Data Center

Cada uno de estos bloques tendrá una separación física mediante una capa de acceso implementada sobre una plataforma de switcheo con enlaces redundantes de Uplink hacia el Core.

De esta manera el bloque de Data Center se implementará sobre una plataforma de switches Nexus 5596 en modo redundante, con objeto de independizar

físicamente la zona de servidores aplicativos del resto de la infraestructura de red. Se utilizarán enlaces de Uplink a 10 Gbps.

Para el bloque de IDFs se utilizará una plataforma de switcheo en capa 2 sobre switches Catalyst 2960S, conectados cada uno hacia el Core mediante un par de enlaces de Uplink en fibra a 1 Gbps.

El resto de los bloques (Enterprise Edge, Wireless LAN y ToIP) se implementarán también mediante una plataforma en capa 2 con enlaces de Uplink en cobre a 1 Gbps.

Propuesta Switch Core

En la figura 7 se muestra la familia de switches 6500 Series con doble fuente

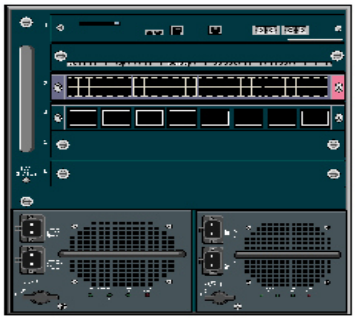

Figura 7. Chassis Catalyst 6506

Bloque Core 6506-E

De acuerdo al diseño, se considera dos equipos cisco SW-6506-E para la implementación de la capa de Core/Distribución. Estos switches cumplen con los estándares de capa 3 y 2 del modelo OSI y cuenta con protocolos IP de enrutamiento como OSPF, además de otros estándares como IPv4 o IPv6.

La configuración actual tiene la capacidad de recibir a los 17 IDF´s en SFP de fibra LX/LH a una velocidad de 1Gbps con conexiones redundante. Esto con la finalidad de tener alta disponibilidad y minimizar la afectación de los usuarios en caso de falla.

Al ser un equipo modular, cuenta con la capacidad de tener tarjetas con puertos en cobre. Para este caso se equipó con una tarjeta de puertos 10/100/1000 para la interconexión de los diferentes bloques de acceso con Uplinks en cobre.

Adicionalmente se propuso una tarjeta con 8 puertos Ethernet a 10 Gbps con la finalidad de proporcionar interconexión hacia el bloque de servidores, ya que el flujo de trafico mas alto está en el área de los servidores, por lo que con esta conexión tiene las facilidad de mantener alta disponibilidad y el manejo del trafico en altas velocidades; quedan dos slot libres para crecimiento futuro.

Para soportar los diferentes bloques, cuenta con un backplane de 720 Gbps. Soporta un desempeño mínimo de 400 Mpps (paquetes de 64 bytes). Este Core soporta hasta 192 de 1 Gbps o 32 Gbps de 10 en trocales de interconexión. Con este desempeño en la supervisora se puede soportar la operación actual (trafico IDF, WAN, LAN, Voz, Internet, video vigilancia, Wlan, bloque de servidores) así como un crecimiento futuro, siendo esta una de las premisas de diseño por la que se recomienda este equipo. Opcionalmente tiene la funcionalidad de tener dos supervisoras (incluida solo una) la cual tiene convergencia de 1 a 3 milisegundos para restablecer la red.

Ambas supervisoras (Core 1 y Core 2) incluyen 2 puertos 10Gbps para interconexión entre ellas con la finalidad de tener alta disponibilidad en ambos switches Core.

Adicionalmente, los switches de Core/Distribución propuestos cuentan con las siguientes capacidades técnicas:

- Fuentes de alimentación AC redundantes de 6,000 Watts. Cada fuente de poder tiene la capacidad de proveer de energía a todo el chasis y los módulos requeridos en el equipo.
- Todos los módulos son hot-swap.
- El equipo tiene una arquitectura non-blocking.
- Manejo de enrutamiento y bridging multiprotocol.
- Modulos de switcheo (Switch Fabric Modules) de 32 a 256Gbps
- Manejo de multimedia
- Manejo de protocolos RIP I y RIP II, OSPF y soporte de BGP4.
- Manejo de VoIP, VoFR, BRE, Easy VPN,
- Manejo de 4000 VLAN's, y un mínimo de 30000 direcciones MAC.
- Alto rendimiento en capa 3 (Supervisor Engine 720: up to 400 mpps)

Cada uno de los equipos propuestos para la capa de Core / Distribución cuenta con las siguientes características técnicas:

- 1 Chasis Cat6506-E
- 1 Supervisoras 720
- 48 puertos Gigabit Ethernet 10/100/1000 Base-T RJ45
- 17 puertos Gigabit Ethernet 1000 BASE-LX/LH en fibra
- 10 puertos 10 Gigabit 10GBase-SR
- 2 fuentes de poder 6000W AC cada una
- IOS: ENTERPRISE SERVICES versión 12.2(33)SXJ

Administración Centralizada

El diseño básico de un Sistema Cisco Catalyst 6500 Virtual Switching Series 1440 permite la gestión centralizada de todos los recursos de red y dispositivos, incluidos los protocolos de Capa 3 (OSPF, EIGRP, BGP, y así sucesivamente) y protocolos de capa 2 (Spanning Tree Protocol, Protocolo de detección de vínculos unidireccionales [UDLD], control de flujo, LACP, y así sucesivamente). Un motor

de supervisora sencillo en el sistema de conmutación de Cisco Virtual es elegido como el punto central de gestión para todo el sistema.

Direcciones MAC del router

Las direcciones MAC del router se asignan a las interfaces de capa 3 (interfaces físicas o VLAN). Se utilizan principalmente para hacer frente a la capa de 2 campos de la interfaz para las comunicaciones, pero también son fundamentales para el dispositivo para realizar una búsqueda de nivel 3, nivel 3 de búsquedas se inician sólo si la dirección MAC de destino de la trama es igual a la MAC del router de la interface.

En un Cisco Catalyst 6500 independiente, la dirección MAC del router se deriva de la MAC electrónica programable y borrable memoria de sólo lectura (EEPROM) que está incrustada en cada chasis Catalyst 6500 de Cisco. En un entorno de Cisco Virtual Switching System, ya que dos chasis físicos forman el dispositivo lógico, único, las direcciones MAC del router deben ser coherentes en ambos chasis físicos. Por lo tanto, la asignación de la dirección MAC del router varía en un entorno de Cisco Virtual Switching System.

Enlace Virtual de Switch

El Cisco Catalyst 6500 Serie Virtual Switching System 1440 se compone inicialmente de dos chasis de Cisco Catalyst 6500. Con el fin de unir los dos chasis en un único nodo lógico de señalización, de control especial y la información debe ser intercambiada entre los dos chasis en forma oportuna. Para facilitar este intercambio de información, es necesario un vínculo especial con la transferencia de datos y de control de tráfico entre el chasis de pares. Este enlace se conoce como el enlace de conmutador virtual (VSL).

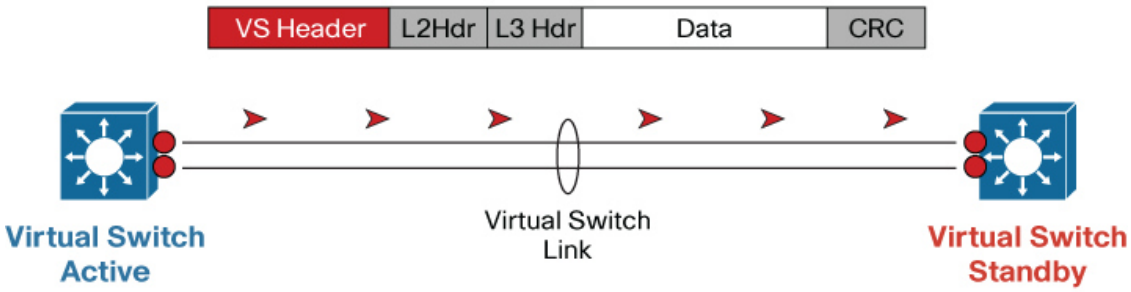

Figura 8. Encabezado Switch Virtual

El VSL es tanto la tecnología que permite el sistema de conmutación de Cisco Virtual y es un eslabón fundamental del sistema. Internamente Cisco Catalyst 6500 controla información que normalmente se mantiene en el chasis y ahora se debe cambiar a través de la VSL al switch peer, que se extiende del plano posterior entre los dos interruptores.

Comunicación Control-Plana

El VSL es crucial para ambos CPUs en cada supervisora para comunicarse entre sí. También se utiliza para determinar qué conmutador virtual se convierte en el conmutador virtual activo y que se convierte en el switch virtual de espera. Debido a que esta determinación afecta el comportamiento de cada interruptor, los papeles deben ser negociados en los primeros momentos del ciclo de arranque del chasis. Como resultado, el sistema debe llevar a los VSL y sus puertos asociados en línea antes de inicializar el resto del sistema.

La comunicación entre los dos chasis se facilita con la mensajería interna que se envía a través de la VSL. Debido a que la VSL se implementa como una interfaz de Cisco EtherChannel, es resistente a un solo enlace de falla. Sin embargo, siendo realistas tan sólo un link de la VSL es elegido como el vínculo de control en un momento dado debido a que el algoritmo de control de la interfaz de Cisco EtherChannel se basa en la fuente y las direcciones MAC de destino, que siempre son los mismos para cada CPU.

Requerimientos de Hardware en Cisco Catalyst 6500 Series Virtual Switching System 1440

Se requiere hardware especifico para que el Sistema Cisco Virtual Switching este activo; eso existe en la forma de la supervisora y el sistema de forwarding, los módulos VSL, y los módulos que puedan existir en un Sistema Cisco Virtual Switching.

La tabla 1 muestra el layout o configuración de los equipos Cat6506-E propuestos como switches de Core/Distribución.

NÚMERO DE PARTE	DESCRIPCIÓN	CANTIDAD
WS-C6506-E	Catalyst 6500 Enhanced 6-slot chassis,12RU,no PS,no Fan Tray	1
SV33AES-12233SXJ	Cisco CAT6000-VSS720 IOS ADVANCED ENTERPRISE SERVICES	1
VS-S720-10G-3C	Cat 6500 Supervisor 720 with 2 ports 10GbE and MSFC3 PFC3C	1
CF-ADAPTER-SP	SP adapter for SUP720 and SUP720-10G	1
MEM-C6K-CPTFL512M=	Catalyst 6500 Sup720/Sup32 Compact Flash Mem 512MB	1
WS-X6724-SFP	Catalyst 6500 24-port GigE Mod: fabric-enabled (Req. SFPs)	1
GLC-LH-SM	GE SFP, LC connector LH transceiver	17
WS-X6748-GE-TX	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	1
WS-X6708-10G-3C	C6K 8 port 10 Gigabit Ethernet module with DFC3C (req. X2)	1
X2-10GB-SR	10GBASE-SR X2 Module	6
WS-C6506-E-FAN	Catalyst 6506 FAN TRAY for ISBU	1
WS-CAC-6000W	Cat6500 6000W AC Power Supply	2
CAB-AC-2500W-US1	Power Cord, 250Vac 16A, straight blade NEMA 6-20 plug, US	4
Included: VS-F6K-	Catalyst 6500 Multilayer Switch Feature Card (MSFC) III	1

MSFC3		
Included: VS-F6K-PFC3C	Catalyst 6500 Sup 720-10G Policy Feature Card 3C	1
Included: VS-S720-10G	Catalyst 6500 Supervisor 720 with 2 10GbE ports	1
Included: MEM-C6K-CPTFL1GB	Catalyst 6500 Compact Flash Memory 1GB	1
Included: BF-S720-64MB-RP	Bootflash for SUP720-64MB-RP	1
Included: MEM-XCEF720-256M	Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	1
Included: WS-F6700-CFC	Catalyst 6500 Central Fwd Card for WS-X67xx modules	1
Included: MEM-XCEF720-256M	Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	1
Included: WS-F6700-CFC	Catalyst 6500 Central Fwd Card for WS-X67xx modules	1
Included: WS-F6700-DFC3C	Catalyst 6500 Dist Fwd Card for WS-X67xx modules	1
Included: WS-X6708-10GE	Cat6500 8 port 10 Gigabit Ethernet module (req. DFC and X2)	1

Tabla 1 Configuración Switches de Core

Los equipos propuestos para el Core o backbone de la red, cumplen con las siguientes características mínimas solicitadas:

REQUERIMIENTO	CUMPLE
1. Performance is fully distributed, highly scalable	SI
2. Full Layer 2 & Layer 3 switching	SI
3. IPv4 unicast & Multicast forwarding	SI
4. Security ACLs & QoS/policing	SI
5. Flexible NetFlow/NetFlow accounting	SI
6. Redundant Power Supplies and Supervisor modules	SI

7. Dynamic port security, DHCP snooping,	SI
8. Dynamic ARP inspection, IP source guard	SI
9. QoS	SI
10. Tiered Access Control	SI
11. Anti-Spoofing Filtering	SI
12. 802.1X	SI
12. EnergyWise	SI

Tabla 2 Matriz de Cumplimiento de Requerimientos

5.2 Bloque de Data Center

Antecedentes

El Data Center del cliente está constituido por 52 servidores aplicativos, los cuales se encuentran conectados a la red LAN a través de puertos del backbone 3COM. No existe una capa de distribución/acceso que permita una separación física del Data Center del backbone de la red.

Premisas de Diseño

Se requiere implementar conectividad para 52 servidores aplicativos que constituyen el Data Center del Cliente, con requerimientos de puertos Gigabit en cobre y crecimiento posible a futuro del 10% en la cantidad de servidores.

Se considera que los servidores aplicativos cuentan, en algunos casos, con más de un puerto de red para conexión hacia red LAN, en modo de Link Aggregation para la suma de ancho de banda. No se considera que se utilicen puertos adicionales en los servidores para redundancia.

Esta condición causa que los 52 servidores físicos ocupen aproximadamente 90 puertos Ethernet en los switches de red LAN.

La arquitectura propuesta para el Data Center considera un par de switches de acceso para la conexión de los servidores aplicativos. Se realizará un balanceo de

cargas entre los switches de acceso, distribuyendo los servidores equitativamente entre ambos switches, de tal manera que el tráfico hacia la capa Core/Distribución quede balanceada entre los enlaces de Uplink.

Propuesta Switch Distribución Servidores

Para la solución de Data Center (servidores) se selecciono la familia de Equipos Nexus 5596, ideal para interconexión de servidores, utilizando conectores de tipo SFP a 1 Gbps en cobre RJ45 (1000BASE-T SFP) para recibir los enlaces de acceso de los servidores, con los cuales cubre la capacidad de tener hasta 96 puertos fijos por tarjeta (2 slots) y dos módulos de expansión en 2 UR.

La conectividad actual con conectores SFP de 1 Gbps en cobre puede ser reemplazada, a futuro, con conectores SFP a 10 Gbps, para recibir conexiones de servidores a 10G.

El Cisco Nexus 5596UP ofrece hasta 192 terabits por segundo de rendimiento para soportar los 50 servidores actuales incluyendo los diferentes servicios virtuales, mas crecimiento futuro por cada 48 puertos ofrece 960-Gbps de throughput

El equipo está diseñado para tener tiempos de respuesta constantes así como latencia muy baja con protocolos como high-performance computing (HPC) para data center, y replica de servicios entre ellos.

El equipo Nexus 5000 tiene las siguientes capacidades:

- Alta densidad
- Alto rendimiento
- Equipo Modular

Características sobresalientes:

- Nexus es la plataforma líder en Centros de Datos
- Protección de la Inversión mediante Next Generation Technology
- Inversión a largo plazo
- Escalabilidad 10 G (conectores SPF)
- Evolución a corto plazo 40GbE & 100GbE
- Sistema de Tbps (1,92 terabits)
- Arquitectura Flexible con crecimiento en 10Gbps o FCoE
- Soporta Trafico de tipo SAN o almacenaje
- Conexión en cobre para 10Gbps en categoría 6 (Cat6a) para servidores
- Facilidad de extensión de equipos
- Módulos Hot-swappable
- MAC address table entries: 32,000

Capa 2

- Puertos capa 2 y enlaces VLAN
- Encapsulación IEEE 802.1Q VLAN
- Soporta hasta 4096 VLANs
- Rapido Per-VLAN Spanning Tree Plus (PVRST+) (IEEE 802.1w compatible)
- Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s): 64 instances
- Spanning Tree PortFast
- Spanning Tree root guard
- Spanning Tree Bridge Assurance
- Tecnología Cisco EtherChannel (hasta 16 ports por EtherChannel)
- Tecnología Cisco vPC
- Configuración sincronización vPC
- Link Aggregation Control Protocol (LACP): IEEE 802.3ad
- Advanced PortChannel hashing based on Layer 2, 3, y 4 information

- Frames grandes en todos los puertos (hasta 9216 bytes)
- Pause frames (IEEE 802.3x)
- Control de tormentas (unicast, multicast, and broadcast)
- VLANs privadas
- VLAN privadas sobre troncales
- VLANs privadas sobre vPC y EtherChannels

Cada uno de los equipos propuestos para la capa de acceso en el Data Center cuenta con las siguientes características técnicas:

- 1 Chasis Nexus C5596
- 62 puertos Gigabit Ethernet 10/100/1000 Base-T RJ45
- 6 puertos 10 Gigabit 10GBase-SR
- 2 fuentes de poder
- IOS: NEXUS BASE versión 5.0.3N21

La tabla 3 muestra la el layout o configuración de los equipos Nexus5596 propuestos como switches de acceso en el Data Center.

NÚMERO DE PARTE	DESCRIPCIÓN	CANTIDAD
N5K-C5596UP-FA	Nexus 5596UP 2RU Chassis, 2PS, 4 Fans, 48 Fixed 10GE Ports	1
CAB-N5K6A-NA	Power Cord, 210/220V 30A North America	2
GLC-T	1000BASE-T SFP	46
N55-M160L3	Nexus 5596 Layer 3 Expansion Module	1
N55-M16P	Nexus 5500 Module 16p 10GE Ethernet/FCoE	1
GLC-T	1000BASE-T SFP	16
N55-M16P	Nexus 5500 Module 16p 10GE Ethernet/FCoE	1
SFP-10G-SR	10GBASE-SR SFP Module	6
N5KUK9-503N2.1	Nexus 5000 Base OS Software Rel 5.0(3)N2(1)	1
N55-LAN1K9	Layer 3 License for Nexus 5500 Platform	1
Included: N55-BAS1K9	Layer 3 Base License for Nexus 5500 Platform	1

Included: N55-PAC-1100W	Nexus 5500 PS, 1100W, Front to Back Airflow	2
Included: N5596-ACC-KIT	Nexus 5596 Chassis Accessory Kit	1
Included: N5596UP-FAN	Nexus 5596UP Fan Module	4

Tabla 3 Configuración Switches de Data Center

Interconexión del bloque de Data Center hacia la Capa de Core / Distribución

La propuesta está compuesta de 2 equipos para el bloque de Core (6506-E) los cuales están interconectados a través de conexiones a 10Gbps entre las supervisoras (720Gbps) para alto rendimiento los cuales soportan todos los bloques, hacia el Bloque de servidores están los Equipos Nexus 5596 los cuales a puertos SFP se podrán conectar a 1Gbps de velocidad, y tiene la capacidad de tener SFP a 10Gbps o a través de cableado cat 6.

Para la interconexión con el Core esta por una tarjeta 10Gbps de forma cruzada la cual también se recibe en el nexus a 10Gbps quedando con un rendimiento alto, alta disponibilidad, y redundante de esta manera se puede recibir a los servidores de manera que también tiene crecimiento a futuro por tener escalabilidad entre el core y el bloque de servidores.

La figura 9 muestra el detalle de la interconexión del bloque de Data Center hacia la plataforma de Core/Distribución.

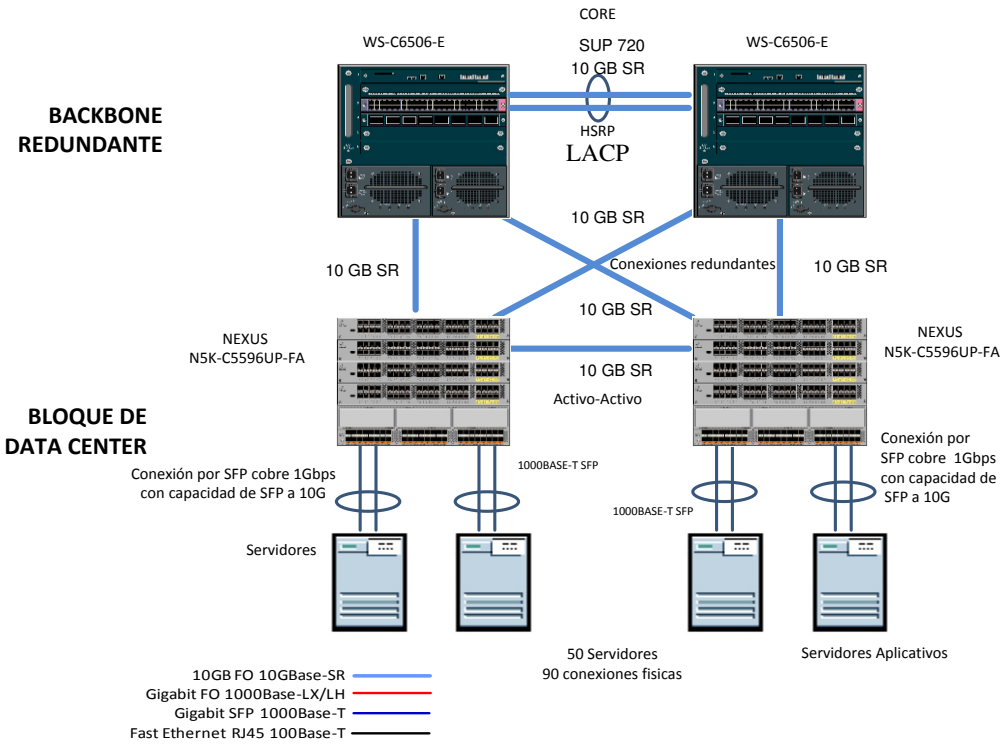

Figura 9.Bloques de Core/Distribución y Data Center

5.3 IDF's Monterrey

Antecedentes

Como antecedente es necesario remplazar los equipos 3COM con tecnología de tipo Cisco con funcionalidades más robustas para servicios IP y su gama de servicios flexibles, ya que esto deberá mejorar la disponibilidad de la red LAN hacia los usuarios.

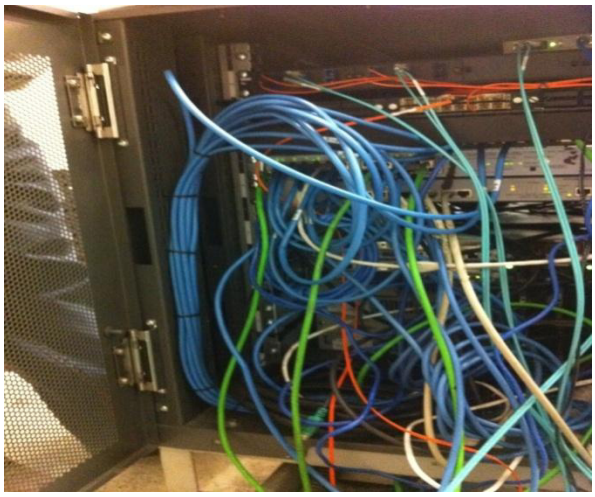

Figura 10. Situación actual IDFs

Premisas de Diseño IDFs MTY

Se requiere que todos los puertos de usuario (IDF) sean a Gigabit 10/100/1000 con PoE para tener la facilidad de conectar dispositivos IP que requieran energía para dar servicio ya sea de datos, voz o video vigilancia.

Cada IDF contará con dos enlaces de Uplink en fibra, hacia cada uno de los switches de backbone respectivamente. Se considera un total de 17 IDF en todo el Corporativo del cliente.

Se utilizarán switches de capa 2 conectados por medio de puertos troncales hacia los switches de backbone, por donde se distribuirán las VLANs que sean requeridas. La funcionalidad de PVST (Per VLAN Spanning Tree) de Cisco permitirá balancear el tráfico de las VLANs entre los 2 enlaces troncales de Uplink, permitiendo hacer un uso más eficiente de los recursos de ancho de banda disponibles.

Se utilizarán switches Cisco Catalyst 2960S que son equipos capa 2 que soportan voz, video, datos y acceso seguro; ofrecen una administración escalable conforme cambian las necesidades de su negocio.

Para los IDF con requerimientos de hasta 24 puertos se utilizará un switch Cat2960S de 24 puertos 10/100/1000 PoE, mientras que los que requieren de 25 a 48 puertos se utilizará un switch Cat2960S de 48 puertos 10/100/1000 PoE.

Para los IDF con requerimientos mayores a 48 puertos, se utilizarán pilas de switches Cat2960-S de 24 y/o 48 puertos 10/100/1000 PoE para cubrir los requerimientos específicos de cada IDF.

Para el cálculo de la cantidad de puertos requeridos por IDF se consideró la cantidad actual utilizada de puertos, mas los puertos requeridos para cámaras y un crecimiento futuro del 10%.

Propuesta IDFs

Los IDF se implementarán mediante switches capa 2, de 24 y 48 puertos 10/100/1000 RJ45 (1000BASE-T) con capacidad de apilamiento, marca Cisco de la serie Catalyst 2960S.

Funcionalidades de los equipos:

- Inteligencia: Da prioridad al tráfico de voz o al intercambio de datos para ajustar la entrega de información hacia los usuarios
- Seguridad mejorada: Proteger la información importante, mantener a los usuarios no autorizados alejados de la red y conseguir un funcionamiento ininterrumpido través de Port security
- Soporte para comunicaciones de datos, inalámbricas y voz que le permite instalar una única red para todas sus necesidades de comunicación.

- Función Power over Ethernet que le permite implementar fácilmente nuevas funciones como comunicaciones por voz e inalámbricas sin necesidad de realizar nuevas conexiones.
- Opción de Fast Ethernet (transferencia de datos de 100 megabits por segundo) o Gigabit Ethernet (transferencia de datos de 1000 megabits por segundo), Varias configuraciones de modelo con la capacidad de conectar escritorios, servidores, teléfonos IP, puntos de acceso inalámbrico, cámaras de TV de circuito cerrado u otros dispositivos de red.
- Capacidad de configurar LAN virtuales de forma que los empleados estén conectados a través de funciones de organización, equipos de proyecto o aplicaciones en lugar de por criterios físicos o geográficos.
- Seguridad integrada

Figura 11. WS-C2960S-24PSL y WS-C2960S-48FPS-L

5.4 IDF's de Sucursales

Antecedentes

Además de la sede de Monterrey, la red del cliente incluye 63 sitios remotos, consta de 3 oficinas (Guadalajara, México Central y México Sur), una planta en Jalisco y 59 sucursales en todo el país.

La actual plataforma de red LAN en sitios remotos se despliega sobre la tecnología de 3Com. La mayoría de los sitios remotos están equipados con un solo switch 3Com 4226T, que proporciona conectividad a todos los usuarios en el sitio, sin embargo, hay algunos sitios donde se ha implementado una configuración de switch de múltiples, dependiendo del número de usuarios o de su distribución en el instalaciones.

Actualmente se tienen aproximadamente 63 sitios o IDF´s remotos distribuidos en diferentes zonas geográficas de la República Mexicana las cuales cuentan con un nodo conectado por enlace tipo MPLS hacia la nube del carrier los cuales tienen comunicación constante y comparten información con su nodo central ubicado en Monterrey.

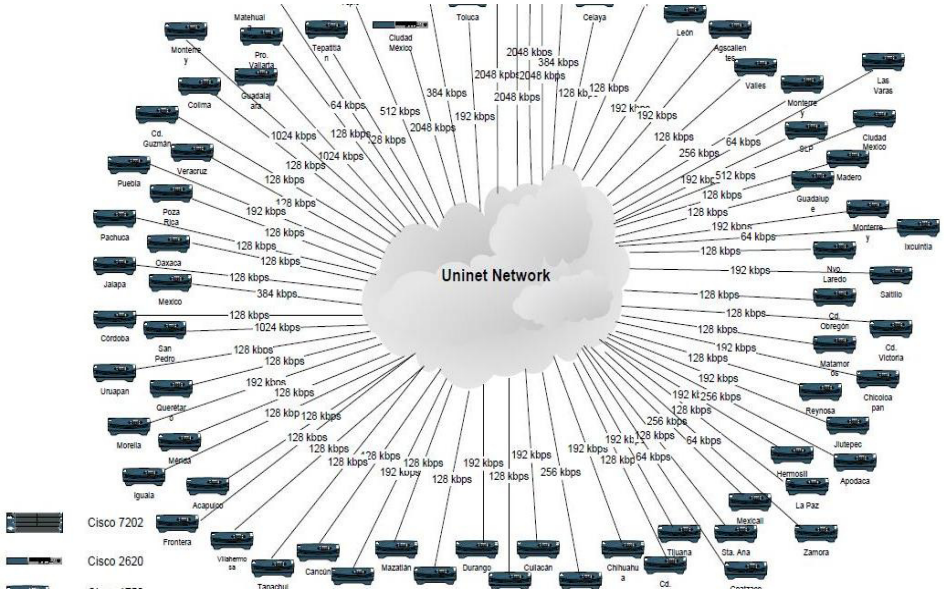

Figura 12. Nodos Remotos cliente

Premisas de Diseño

El Cliente ha solicitado, para todos sus sitios remotos, la sustitución de sus equipos de conmutación de 3Com para una nueva plataforma, impulsada por la marca Cisco, para ofrecer más robustos y capacidades de los servicios IP más flexibles, buscando con esta actualización mejorar la disponibilidad de la red LAN a los usuarios. De acuerdo al requerimiento hecho por el Cliente, la actualización de la infraestructura LAN es requerida para todos los sitios remotos.

La información proporcionada por las mejores técnicas disponibles en el documento de solicitud de propuestas, así como en diferentes archivos y gráficos, se ha tenido en cuenta para calcular el número de puertos y el equipo necesario para cada sitio.

Basado en toda la información disponible, se han definido los siguientes diseños:

1. Se cuenta con 5 sitios críticos remotos, donde las aplicaciones de telefonía están en uso y donde hay switches capaces de soportar PoE, se deben tener consideración con puertos Gigabit 10/100/1000 Mbps RJ45. El resto de los sitios remotos deben ser equipados sin PoE puertos Gigabit Ethernet 10/100/1000 Mbps RJ45.

2. Todos los switches en la propuesta deben tener capacidad para stacking.

3. En sitios sin puertos PoE son requeridos Cisco Catalyst 2960s.Un switch Cisco Catalyst 2960S-24TS-S de 24 puertos serán desplegados en los sitios remotos donde no mas de 24 puertos se necesitan, mientras que un switch Cisco Catalyst 2960S-48TS-S de 48 puertos serán desplegados en sitios que requieran hasta 48 puertos.

4. Para los cinco principales sitios remotos. Se utilizaran Cisco Catalyst 3750X swiches, con capacidad de conmutación en las capas 2 y 3, puertos Gigabit RJ-45, que proporcionan una alta disponibilidad y escalabilidad, alto desempeño y características innovadoras para la gestión de la energía eficiente, como Cisco EneryWise y Cisco StackPower.

Como fue requerido por el Cliente, uno o dos switches Cisco Catalyst 3750X-48PF-S 48-10/100/1000 PoE serán desplegados en cada una de las oficinas principales. Ademas, 2 o 3 swicthes Catalyst 2960S-48FPS-L deberan ser incluidos a fin de llenar las necesidades de puertos físicos por cada sitio.

Propuesta IDF's Depots

Los sitios principales serán implementados en switches de capa 3, 48 10/100/1000 RJ45 ports (1000BASE-T) PoE Cisco Catalyst 3750X Series.

Cisco Catalyst 3750-X Series Características primarias**:**

- 24 y 48 10/100/1000 PoE+, non-PoE models,12 y 24 GE SFP modelos de Puerto.
- Cuatro uplinks opcionales con modulo de red en puertos GE o 10GE.
- PoE+ con 30W de energía en todos los puertos en 1 unidad de rack(RU).
- Redundancia dual, suministro de energía modular y ventiladores
- Media Access Control Security (MACsec) encripcion de hardware.
- Flexible NetFlow y switch-to-switch hardware encryption con el uplink Service Module.
- Open Shortest Path First (OSPF) para acceso ruteado en imagen de IP.
- Enrutamiento IPv4 y IPv6, enrutamiento multicast, calidad de servicio avanzada (QoS) y funciones de seguridad en el hardware.
- Garantía limitada de por vida a el siguiente día hábil y remplazo de hardware avanzado y 90 días de acceso a el soporte TAC de cisco.

- Mejora Cisco con el EnergyWise para la optimización de los costos operativos mediante la medición de consumo real de energía de los dispositivos PoE, los informes y reducir el consumo energeticoa través de la red.
- Puertos USB tipo A y tipo B para almacenamiento y consola respectivamente y un puerto out-of-band de administración.

Configuraciones de switch

Todos los modelos de switch se pueden configurar con cuatro módulos de red opcional. El + PoE y sin PoE switch están disponibles con Base LAN o teléfono IP Base. El feature de IP services está disponible como una actualización en el momento que se ordena o por medio de una licencia en un momento posterior. Los modelos GE SFP switch están disponibles con IP o servicios IP.

Cisco Catalyst 3750-X Series Software

Ademas para los features de IP Base y IP Services, el Cisco Catalyst 3750-X y 3560-X vienen con un nuevo feature de Base LAN. Los tres features disponibles con el Cisco Catalyst 3750-X y 3560-X switch son:

- Base LAN: Servicios Inteligentes Mejorados.
- Base IP: Servicios de empresa de base.
- IP Services: Servicios de empresa.

La característica de Base de LAN ofrece mejores servicios de inteligencia que incluye una completa comprensión de capa 2, con un máximo a 255 VLANs. La característica Base

Los Cisco Catalyst 3750-X con característica de base LAN pueden configurarse como stack con otro Cisco Catalyst 3750-X. Un conjunto de stacks de base LAN con base IP o servicios IP no es soportado.

Operación eficiente de switch

Cisco Catalyst 3750-X y X-3560 Series Switches, diseñados y desarrollados por Cisco, proporcionan ahorro de energía óptima, las operaciones de baja energía, y la capacidad de consumo de energía.

El Cisco Catalyst 3750-X y los puertos 3560-X son capaces administrar ahorro de energía para que los puertos no utilizados pueden entrar en un estado de menor utilización.

StackPower permite a los clientes simplemente agregar una fuente de alimentación adicional en cualquier switch del stack y proporciona redundancia de alimentación ya sea por cualquiera de los miembros del stack, o simplemente añadir más poder a la pila de stack.

Fuentes de Alimentación Redundantes Dual

El equipo Cisco Catalyst 3750-X soporta fuente de poder redundante, el switch contiene una fuente de poder de default, si una fuente de poder es instalada, esta debería de estar ubicada en la bay 1 de el switch. La figura 13 nos muestra las fuentes que deben de ser redundantes.

Figura 13.Fuente de Poder CAB-3KX-AC

Switch WS-C2960S 48FPS-L

Para sitios remotos no primarios, con requerimientos no solamente puertos 10/100 PoE, el cisco Catalyst 2960 son usados como equipos de capa 2 para soportar voz, video, datos y acceso seguro, ofrece una administración escalable como las necesidades de negocio lo requieran.

El Cisco Catalyst 2960-S y Switches de la serie 2960 son los líderes de capa 2, proporcionando una mayor facilidad de uso, las operaciones de negocios de alta seguridad, mejora de la sustenibilidad, y una experiencia de red sin fronteras.

Las características del Cisco Catalyst 2960-S se muestran a continuación:

- 10 y 1 puerto Gigabit Ethernet de enlace ascendente con flexibilidad pequeño más Form-Factor Pluggable (SFP +), proporcionando la continuidad del negocio y la rápida transición a 10 Gigabit Ethernet.
- 24 o 48 puertos de Gigabit Ethernet en PC de escritorio.
- Cisco FlexStack módulo de apilamiento de 20 Gbps de rendimiento, lo que permite facilidad de manejo con una sola configuración y actualización de switch simplificado
- PoE+ con arriba de 30 W por Puerto que permite soportar versiones anteriores de PoE+.
- USB storage para respaldo de archivos, distribución y simplificar operaciones.
- Una amplia gama de funciones de software para proporcionar facilidad de uso, las operaciones de negocios de alta seguridad, la sustenibilidad, y una experiencia de red sin fronteras.

Power over Ethernet Plus PoE+

Además de PoE 802.3af, el Cisco Catalyst 2960-S Series Switches soporta PoE + (IEEE 802.3 estándar), que proporciona hasta 30 vatios de energía por puerto.

El Cisco Catalyst 2960-S y los switches 2960 Series puede ofrecer un menor costo total de propiedad para los despliegues que incorporan los teléfonos IP de Cisco, Cisco Aironet LAN inalámbrica (WLAN), o cualquier IEEE 802.3af dispositivo final. PoE elimina la necesidad de energía de la pared a cada dispositivo habilitado para PoE y elimina el costo de cableado adicional y circuitos eléctricos que de otro modo sería necesario en el teléfono IP y el despliegue de WLAN.

CAPÍTULO 6. SOLUCIÓN DE SEGURIDAD

6.1 Antecedentes

El objetivo de este capítulo en lo correspondiente a seguridad es diseñar e implementar un diseño acorde a las mejores prácticas de Seguridad para el Cliente, realizar la migración de forma trasparente y sin afectaciones de los servicios de Seguridad Perimetral y Redes Privadas Virtuales.

A si mismo se requiere incorporar un servidor de Autenticación, Autorización y Contabilización de acuerdo al manejo de roles dentro de la organización.

De manera general, el diseño propuesto involucra en su totalidad equipos del fabricante Cisco Systems. El alcance, abarca el suministro, la instalación física, configuración y puesta a punto de la infraestructura de seguridad propuesta y descrita de este documento.

6.2 Premisas de diseño

Los principales requerimientos expresados por el cliente, acerca de su necesidad relacionada con seguridad son las siguientes:

Conexiones seguras vía VPN

- Solución de VPN basada en un dispositivo de hardware
- Capacidad de realizar VPN's de forma remota y site to site
- Se requiere que el equipo se encuentre en Alta Disponibilidad
- Protocolo a utilizar para la realización de VPN IPsec y SSL
- Conectividad con Desktops, LapTops y VPN´s Host to Host (firewalls) mediante la solución vía VPN.

Firewall´s

- Sugerir el mejor esquema en el módulo de seguridad del Enterprise edge utilizando los Firewalls ASA5520 con los que cuenta el Cliente y reemplazando los Firewalls Checkpoint existentes.
- Capacidad de soportar 2000 usuarios, 1500 con acceso a Internet y 50 servidores físicos.
- Se requiere que el equipo se encuentre en Alta Disponibilidad.

Control de Acceso (Identificación y Autenticación de usuarios)

- Solución que controle el acceso de usuarios autorizados y proteja de accesos no autorizados.
- Capacidad de importar información de usuarios de directorios activos y/o LDAP, para un perfilamiento de usuarios más ágil.
- Capacidad de autenticar por RADIUS o TACACS+
- Capacidad de registrar la actividad de los usuarios en base al concepto AAA (autenticación, Autorización y Accounting)
- Solución basada en appliance de propósito específico

6.3 Propuesta de Seguridad

Conexiones Seguras vía VPN y Firewall

La razón por la cual se recomienda el Firewall ASA550 es por su máxima capacidad de conexiones, la integración de VPNs y su número de interfaces físicas.

La solución está basada en el equipo ASA-5550. Este equipo es una solución de propósito específico que contiene para éste proyecto características de seguridad FIREWALL, Terminador de Túneles VPN de IPSec y SSL provee una defensa basada en características de seguridad a nivel de red y capa aplicativa, así como control de acceso a usuarios permitidos.

El equipo NO integra funcionalidades de Prevención de Intrusos. Provee un máximo de túneles IPsec de 5000 y un máximo de túneles SSL de 5000. Este equipo esta dimensionado para soportar un máximo de 2500 usuarios sin sobrepasar el 80 % de su capacidad.

El Cisco ASA 5550 está previsto para funcionar en alta disponibilidad Activo/Pasivo, con esto se garantiza la continuidad de la protección de servicios.

El número de interfaces que cuenta el equipo son 8 10/100/1000 y la cantidad máxima de interfaces Virtuales (VLAN) es de 250.

Resumen de rendimiento	
Capacidad máxima de procesamiento (Mbps) del firewall	1200
Capacidad máxima de procesamiento (Mbps) de VPN 3DES/AES	425
Cantidad máxima de sesiones de usuario de VPN de sitio a sitio y de acceso remoto	5000
Cantidad máxima de sesiones de usuario de VPN SSL1	5000
Cantidad máxima de conexiones	650.000
Cantidad máxima de conexiones/segundo	28.000
Paquetes por segundo (64 bytes)	600.000

Tabla 4 Capacidades Cisco ASA5550

Control de Acceso (Identificación y Autenticación de Usuarios)

La solución que controlará el acceso de usuarios autorizados y protegerá de accesos no autorizados, está basada en un appliance del fabricante Cisco Systems modelo CSACS-1120. Soporta diferentes escenarios de acceso, incluyendo wireless LAN, 802.1x alambrica, y accesos remotos.

Este dispositivo está diseñado únicamente para tal función y está constituido con un sistema operativo endurecido, que tiene las ventajas de no depender de actualización o parches frecuentes como lo haría un sistema operativo genérico.

Para un deployment rápido, tiene la capacidad de importar la información de usuarios de directorios activos y/o LDAP y/o ODBA, para un perfilamiento de usuarios más ágil.

Soporta la capacidad de autenticar por RADIUS o TACACS+, pero no ambos al mismo tiempo. Capacidad de registrar la actividad de los usuarios en base al concepto AAA (autenticación, autorización y accounting). Dicha información puede ser explotada para elaborar reportes sobre cada usuario que haya accesado o cada intento fallido.

Tiene la capacidad de interactuar a futuro con soluciones de NAC (enforzamiento de políticas de seguridad del Cliente, antes de permitir el acceso completo a recursos de la red). Capacidad de soportar esquema de alta disponibilidad a futuro. La Tabla 5 muestra las características físicas de servidor AAA CISCO CSACS.

CSACS 1120	
Component Specifications	
CPU	3.4 GHz Intel Pentium 4, 800 MHz FSB, 2 MB cache
System memory	1GB
Hard disk drive	160 GB SATA
Media	CD/DVD combo
I/O ports	RS232 Serial Port, 3 USB 2.0 (1 front, 2 rear)
Physical dimensions	(1RU) ● 429 (W) x 508 (D) x 42 (H) mm
Rated input power	345W

Tabla 5 Características se servidor AAA CISCO CSACS

Descripción del Escenario Funcional

El diseño del equipo ASA5550 que es el dispositivo que tendrá la funcionalidad de Firewall Perimetral y concentrador de Túneles se propone un diseño en Alta Disponibilidad.

La configuración del equipo ASA failover requiere 2 equipos de seguridad idénticos conectados uno al otro a través de un cable dedicado. El diseño de equipo ASA5550 se implementara en HA Activo-Pasivo y funcionara la alta

disponibilidad en caso de falla del equipo Activo el segundo equipo tomara el control del tráfico.

El funcionamiento de las conexiones será por medio de VLAN´s interconectadas a través de 2 puertos troncales hacia el Firewall. Una conexión será de enlaces Externos y otra conexión de enlaces Internos.

El firewall aplicara las políticas de seguridad, una vez filtradas las conexiones y autenticadas para el caso de las VPN se conectara hacia el switch core quien será el encargado de distribuir las direcciones hacia los servicios.

El servidor AAA se propone que esté conectado en la Granja de servidores para realizar la función de control de la gestión y política de acceso de los recursos de la Red.

Flujo de Tráfico de Seguridad

A continuación se describe el flujo de tráfico a través de la solución de seguridad propuesta sobre plataforma Cisco ASA5550:

1.-Usuario desde acceso remoto VPN´s

- Acceso a internet publico
- El usuario accesa por IPSec o SSL (medios seguros) por medio de Internet
- El router de Internet del cliente recibe la conexión y la entrega a un Switch de acceso.
- El switch de acceso recibe la conexión a través de una Vlan y lo canaliza por medio de un puerto troncal hacia el Firewall ASA 5550.
- El firewall ASA550 autentica al usuario y aplica las políticas. Si la política no lo permite accesar, la conexión queda bloqueada.
- Una vez permitida la conexión, lo canaliza al switch Core quien es el encargado de direccionar los servicios solicitados.

2.-Usuario desde Acceso MPLS

- Acceso a MPLS
- El router MPLS del cliente recibe la conexión y la entrega al Switch de acceso.
- El switch de acceso recibe la conexión a través de una Vlan y canaliza la conexión a través de un puerto troncal hacia el Firewall ASA 5550.
- El firewall ASA550 recibe la VLAN a través de su interface Externa y una vez recibida se encarga de aplicar las políticas. Si la política no lo permite accesar, la conexión queda bloqueada.
- Si la política lo permite lo canaliza por medio de su interface Interna hacia el Switch Core, siendo este último encargado en direccionar los servicios.

3.-Usuario desde Redes Externas

- Acceso a Redes Externas
- El switch de acceso recibe la conexión a través de una Vlan y canaliza la conexión a través de un puerto troncal hacia el Firewall ASA550.
- El firewall ASA550 recibe la VLAN a través de su interface Externa y una vez recibida se encarga de aplicar las políticas. Si la política no lo permite, la conexión queda bloqueada.
- Si la política lo permite lo canaliza por medio de su interface Interna del Firewall ASA550 hacia el Switch Core, siendo este último encargado en direccionar los servicios.

4.-Usuario desde Redes Internas

- Acceso a Redes Internas
- El Switch de acceso recibe la conexión a través de una Vlan y canaliza la conexión a través de un puerto troncal hacia el Firewall ASA550.
- El firewall ASA550 recibe la VLAN a través de su interface Externa y una vez recibida se encarga de aplicar las políticas. Si la política no lo permite entrar, la conexión queda bloqueada.

- Si la política lo permite lo canaliza por medio de su interface Interna del Firewall ASA5550 hacia el Switch Core, siendo este último encargado en direccionar los servicios.

Figura 14 Flujo de Tráfico

Reforzamiento de la Red LAN y WAN

El Carrier debe de tener procedimientos establecidos que otorgan servicios para robustecer la seguridad a nivel LAN y WLAN basados en las mejores practicas de Seguridad.

WLAN.

Se sugiere realizar un Site Survey cuya finalidad es:

- Determinar el lugar óptimo de emplazamiento de los Puntos de Acceso Inalámbrico
- Detectar las "zonas oscuras", es decir zonas de mucho ruido, detectar los obstáculos, que influirán en la calidad de la red. Estos deberán ser tenidos en cuenta al diseñar esa red específica.
- Asegurar una cobertura adecuada a todos los usuarios

Pasos a Seguir en la Realización de un Site Survey:

1.- Conseguir un plano del sitio

2.- Recorrer físicamente las instalaciones. Obstáculos y fuentes de interferencias como peceras, micro-ondas, grandes masas de metal, etc no figuran en los planos. Deben ser indicadas en los planos.

3.- Determinar la ubicación preliminar de cada Punto de Acceso

4.- Testear las ubicaciones preliminares y comprobar que se alcanzan las coberturas y rendimientos esperados

5.- Evaluar la re-ubicación de los Puntos de Acceso para alcanzar mejores coberturas y rendimientos

6.- Evaluar la posibilidad de añadir o quitar Access Point rediseñando las celdas previstas

7.- Identificar fuentes de energía y conexiones de red para los Puntos de Acceso. Quizás no estén muy disponibles y haya que realizar ciertas obras para acercar los cables.

8.- Documentar la ubicación final de Access Point, enchufes y cableados.

Assessment de la seguridad en Wireless

El propósito y objetivo de la auditoría de seguridad inalámbrica será determinar si la red inalámbrica (802.11) de la red se ha implementado adecuadamente para proporcionar un nivel razonable de seguridad de conformidad con las políticas y directrices de la empresa y de acuerdo a las mejores prácticas.

Procedimiento de Assessment de seguridad WLAN:

Descubrimiento del Perímetro

1.- Identificación de WAP autorizado

2.- Identificación de los WAP (rogue) no autorizados

Descubrimiento del Perímetro Interno

1.- Confirmación de WAP (identificados durante el descubrimiento del perímetro) desde el interior de las instalaciones del cliente.

2.- Identificación y análisis de la configuración de WAP (es decir, emisión SSID, SSID por defecto).

3.- Identificación y análisis de cifrado utilizado en WAP (es decir: la existencia de la codificación, el tipo de encriptación).

4.- Análisis de señal para identificar fugas fuera de los puntos de acceso (no cliente) que son accesibles desde el interior de las instalaciones del cliente.

5.- Análisis de la seguridad física de WAP autorizado.

A continuación se anexa un listado de las mejores prácticas de seguridad en WIRELESS:

1. Utilice el cifrado WPA/WPA2. Evite el uso de cifrar por medio de WEP de WiFi. Use WiFi Protected Access (WPA) o WPA2 con autenticación 802.1x, si es posible. Si es posible utilice un Pre-Shared Key (PSK), use una contraseña fuerte (también conocido como WPA con clave compartida) que es por lo menos ocho caracteres de longitud y es una combinación de alfanuméricos y caracteres especiales.

2. Cambiar la contraseña por defecto y el SSID (caracteres y una combinación de caracteres alfanuméricos) para evitar que usuarios no autorizados accedan a su punto de acceso WiFi. Use un SSID que es simple, pero que no revela la identidad o información sensible acerca de su organización.

3. Mantenga su firmware AP actualizado. Cada vez que una vulnerabilidad en el software de AP es descubierto, los vendedores suelen lanzar un parche para solucionar el problema. Asegúrese de actualizar su punto de acceso con la última versión del software.

4. Habilitar la seguridad para los accesos invitados WiFi. Se debe tener un sistema para autenticar a los usuarios antes de darles acceso a la red (guest). Si el acceso de invitados es más abierta WiFi, se debe utilizar la capa superior de seguridad, tales como Secure Socket Layer (SSL) utilizado en HTTPS para autenticar usuarios de forma segura y evitar la fuga de las credenciales.

5. Fomentar las mejores prácticas de seguridad del punto final. Mantenimiento de su software de controlador WiFi actualizado, utilizando una red privada virtual (VPN) a través de un punto de acceso WiFi, para evitar la conexión a redes WiFi que no son de confianza, limpiar regularmente la "Lista de preferencia de redes", desactivar el modo ad-hoc de conexión, y apague su WiFi cuando no esté en uso.

6. Llevar a cabo auditorías de seguridad Wi-Fi con regularidad. Exploración del espacio aéreo en los alrededores de sus instalaciones para evitar las lagunas en su postura de seguridad Wi-Fi y de cumplimiento normativo, y en detectar la presencia de dispositivos no autorizados y la actividad de sus locales.

7. Considere el uso de un WIPS de monitorización 24x7 y una protección completa.

Un sistema de prevención de intrusión inalámbrica (WIPS) proporciona una protección completa contra todo tipo de amenazas inalámbricas incluyendo dispositivos no administrados (por ejemplo, Rogue AP). WIPS también puede ser reutilizado como una solución rentable para la realización de auditorías de seguridad Wi-Fi para la regulación de cumplimiento.

LAN

A continuación se presenta un listado basado en las Mejores prácticas de seguridad en la red LAN

1.-Crear Políticas de Seguridad para la empresa, documentarlas y hacerlas públicas y obligatorias para los empleados. Debemos fomentar la conciencia y la formación en seguridad corporativa.

2.-Entrenar a los usuarios en mejores prácticas de seguridad, y ponerlos al tanto sobre las tácticas de ingeniería social y otros ataques.

3.-Aplicar Parches de manera rutinaria a Sistemas Operativos y Aplicaciones.

4.-Deshabilitar en todos los servidores y host los servicios y puertos no necesarios.

5.-Exigir a nuestro usuarios passwords seguros (largos, que no tengan nada que ver con familiares, mascotas o fechas, que combinen números letras, mayúsculas y minúsculas…). Además deben habilitarse la actualización periódica de contraseñas.

6.-Proteger con controles de acceso los sitios físicos donde tengamos servidores y equipo de red.

7.-Hacer copias de respaldo periódicas de la información importante y verificar la integridad de los respaldos periódicamente.

8.-Usar siempre encriptación de datos para información sensible de la empresa.

9.-Implementar equipo y software de seguridad para proteger la red y los servidores (Firewall, IPS's, Antivirus). Instalar en todos los host de la empresa un agente Antivirus recomendablemente Firewal, e IPS personal.

10.-Se debe tener un plan de continuidad y recuperación de desastres (DRP). Elaborar un mapa de riesgos.

11.-Es recomendable tener en toda empresa un comité de seguridad y un equipo que le de seguimiento a las contingencias.

El Carrier debe cumplir con las mejores prácticas de seguridad de los equipos propuestos, las cuales son:

Mejores Practicas	Cumple
STP Sec	si
Routing Security	si
VLANs ACL	si
ACL,Mgmt channel	si
PVLAN	si
Syslog	si
DHCP Snooping	si
DAI	si
Port Security	si
CoPP/Store Ctl	si
broadcast control	si
Segurity in Console, Aux,VTY	si
Enable Flood Attack Prevention	si
ICMP	si
Banner	si
Administrative Interfaces	si
RADIUS or TACACS	si
Enable Network Time Protocol	si
Syslog logging	si
Network Time Protocol	si
Anti-spoofing	si

Tabla 6. Mejores Prácticas de seguridad

CONCLUSIONES

Con la realización de este proyecto se logró la satisfacción del cliente en la renovación de su infraestructura de red LAN, teniendo importantes cambios en la operación diaria de la compañía, dentro de las cuales destacan:

- Reducción en los tiempos de respuesta de las solicitudes hechas hacia los servidores corporativos.
- Mayor velocidad en el procesamiento de información.
- Menor pérdida de paquetes de datos, mejoró notablemente la transmisión de video llamadas así como de llamadas hechas a través de la red con voz sobre IP.
- Se consolidó el proyecto de Tele presencia con una calidad sorprendente por la optimización que se hizo en sus dispositivos LAN y el modelo jerárquico de sus capas hasta llegar al CORE.
- Con la documentación de toda su infraestructura LAN, la configuración de sus equipos y etiquetado de cada puerto, el cliente logró una certificación nacional de calidad en su infraestructura.
- Mejoró la apariencia física de los cableados y equipamiento de red LAN del cliente.
- Se cuenta con un proveedor que conoce la infraestructura LAN del cliente, lo cual le permite hacer modificaciones para mejoras a futuro.
- El cliente cuenta con tecnología de punta en sus comunicaciones, las cuales son de vital importancia para el negocio.

En resumen, el cliente quedó muy satisfecho con la realización de este proyecto, el precio pagado por esta mejora tecnológica le trajo muchos beneficios a los empleados que se traducen en aumento en su productividad, logrando con esto un pronto retorno de la inversión.

BIBLIOGRAFIA

El presente trabajo se hizo basado en la teoría del libro:

CCNA ICND1 (CCNA Guía de exámenes) Fondo Profesional Computing

Así como en un proyecto empresarial que se realizó a un cliente del sector Industria y de experiencia propia.

Índice de Figuras y Tablas

Figuras

Tablas