UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

MEJORAMIENTO DE LA DISPONIBILIDAD DE LA RED DE DATOS DE UNA ENTIDAD FINANCIERA

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

EDWIN GIANCARLO VASQUEZ VILLANO

PROMOCIÓN

2010-I

LIMA-PERÚ

2014

MEJORAMIENTO DE LA DISPONIBILIDAD DE LA RED DE DATOS DE UNA ENTIDAD FINANCIERA

A mi Padre Benito Vásquez, quien con su gran sacrificio permitió que sea un profesional. A mi madre María Villano, quien es el empuje diario en mi vida. Una madre abnegada a quien admiro. Sin ellos no sería nada. Finalmente a mi familia completa, para quienes espero ser un ejemplo a seguir.

SUMARIO

El presente informe de suficiencia surge por la necesidad de establecer un mejor diseño redundante y seguro de la red de datos interna de una empresa financiera, utilizando el mismo equipamiento de comunicaciones que le pertenece y garantizando la disponibilidad y fiabilidad de los servicios. Asimismo orientamos el presente trabajo a cumplir algunos requisitos que exige la Norma Técnica Peruana "NTP-ISO/IEC 27001: 2008 Técnicas de seguridad - Sistemas de gestión de seguridad de la información", con la finalidad de que la empresa obtenga esta certificación en un futuro.

El desarrollo del informe incluye la descripción de los equipos de comunicaciones, el diseño físico y lógico propuesto, así como protocolos de redundancia y seguridad propuestos.

Al final del informe se presenta un análisis matemático de la redundancia de la red, así como las conclusiones y recomendaciones.

INDICE

INTRODUCCION

El concepto de empresa dinámica se centra en la necesidad de reforzar la red de datos y crear una red fiable y abierta, capaz de adaptarse al crecimiento de la empresa y a los cambios de sus necesidades de comunicación. Sedebe garantizar la disponibilidad y fiabilidad de la red de datos de una empresa, ya que si esta queda inoperativa, se pierden oportunidades de negocio y se deterioran las condiciones de trabajo de los empleados, obteniendo resultados de efectos negativos para la empresa. Asimismo se debe mejorar la conectividad ya que los usuarios necesitan acceso permanente (24 horas al día y 7 días a la semana) a la red tanto si están en la oficina central, como en una sucursal, en su propio domicilio o de viaje. Estas actividades se incrementan más si se trata de una empresa que pertenece al sector financiero, ya que los usuarios finales realizan transacciones electrónicas en cualquier momento del día.

Asimismo, hoy en día para los administradores de red es muy importante la seguridad de acceso a los equipos de comunicaciones, debemos de proteger la red de datos debido a que se enfrentan a un creciente número de amenazas, como los ataques de virus cada vez más complejos y los intentos de sabotaje cada vez más elaborados de usuarios intrusos, e inclusive usuarios pertenecientes a la empresa misma.

El presente informe abarca principalmente estos dos temas: disponibilidad y seguridad, los cuales vamos a desarrollarlos en una empresa perteneciente al sector financiero nacional, encargada de gestionar, realizar, fiscalizar y auditar las transacciones electrónicas y otras formas de pago electrónico. Esta empresa opera en la ciudad de Lima. Describiremos la plataforma de la red de datos interna que tienen actualmente y posteriormente analizaremos las fallas que presenta. En el centro de datos principal observar hardware principalmente de marca CISCO, lo cual es un estándar exigido a nivel corporativo en todos los países donde opera la empresa.

Por otra parte, el 23 de mayo del 2012 a través de la Resolución Ministerial N° 129-2012-PCM publicada en el diario El Peruano, se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001: 2008 Técnicas de Seguridad - Sistemas de gestión de seguridad de la información" en todas las entidades públicas pertenecientes al Sistema Nacional de Informática. En el sector privado esta norma momentáneamente es opcional, sin embargo este trabajo permitirála adaptación de esta norma en la empresa en un largo plazo.

CAPITULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

El Capítulo I se centra en el planteamiento de ingeniería del problema. Este capítulo se inicia realizando el enunciado de dicho problema, exponiendo luego los objetivos del proyecto y del informe. El capítulo también hace una breve evaluación de la problemática en cuestión (actualmente la red de datos no presenta disponibilidad física y el acceso a los equipos de comunicaciones es vulnerable), finalmente se precisan las limitaciones y una síntesis del trabajo.

1.1Descripción del problema

Actualmente la red de datos interna de la empresa presenta problemas de conectividad, los usuarios eventualmente experimentan lentitud al momento de ingresar a sus aplicaciones internas vía web. En una ocasión el servicio de datos se interrumpió debido a la avería de un componente que forma parte del switch principal. Asimismo la empresa tiene dos oficinas que están ubicadas en el cuarto piso de dos edificios contiguos, y estas oficinas se interconectan utilizando una fibra óptica multimodo, la cual tiene un enlace de redundancia (Figura 1.1), sin embargo la conmutación es manual, y esto trae como consecuencia que ante una falla o rotura en la fibra óptica la oficina N° 2 no tenga servicio de datos hasta que se realicemanualmente el cambio en los equipos de comunicaciones de cada oficina (Todos los servidores y aplicaciones internas principales se encuentran en el centro de datos principal). Estosdos problemasindican que no existe un correcto diseño de redundancia en la red de datos, al que describiremos posteriormente. Otro problema detectado es la plataforma de seguridad para el acceso de los equipos de comunicaciones, ya que no se utilizan protocolos seguros de encriptación ni se cuenta con una política de gestión centralizada de contraseñas de los equipos.Comparten el mismo nombre de usuario los integrantes del equipo de soporte técnico y los administradores de red. Esto puede traer como consecuencia que algún atacante interno o externo capture las credenciales de los equipos y altere el comportamiento normal de la red de datos.

1.2 Objetivos del trabajo

La descripción de la sección anterior permite plantear los siguientes objetivos para el desarrollo del presente informe:

- Describir la situación actual de la red LAN de datos de la empresa, incluyendo los equipos de comunicaciones.

- Analizar la información recogida, indicando aquellos aspectos que deben ser corregidos, mejorados o eliminados, bajo criterios de mejor desempeño y buenas prácticas.
- Proponer mejoras a la red de datos de la empresa, en los parámetros de disponibilidad y redundancia, reutilizando el mismo equipamiento debido a la falta de un presupuesto para la compra o renovación de nuevos equipos de comunicaciones.
- Proponer un mejor sistema de seguridad de acceso administrativo a los equipos de comunicaciones.

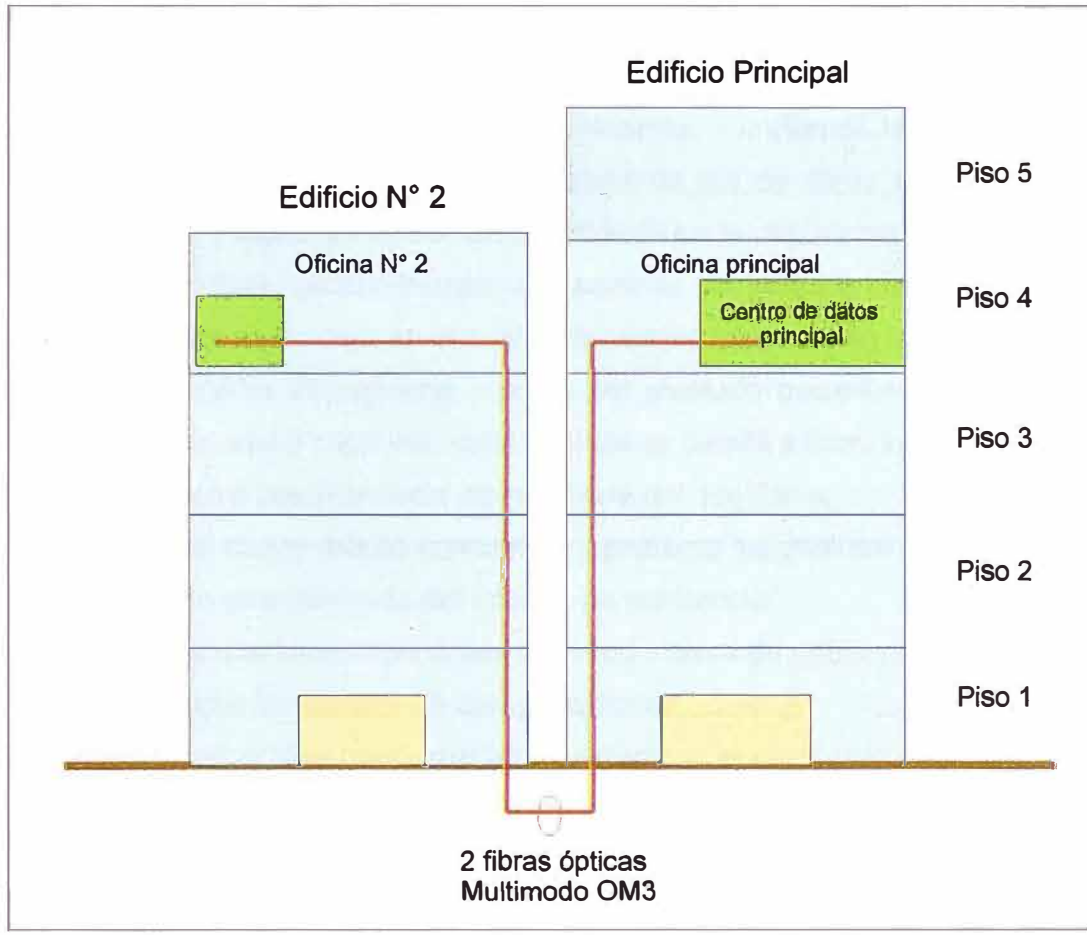

Figura 1.1 Ubicación de las oficinas de la empresa.

1.3 Evaluación del problema

Después de reconocer los problemas existentes en la red de datos, se analizará posibles soluciones de disponibilidad y seguridad, se implementará las mejoras, con el fin de reducir principalmente la caída del servicio de datos, que afecta la continuidad del negocio, lo cual se refleja lo que en genera grandes pérdidas económicas.

1.4 Limitaciones del trabajo

El presente trabajo está limitado al estudio de la red de datos de la empresa, y no abarca las conexiones externas de datos a otros proveedores. Asimismo se hace referencia a la alta disponibilidad de la red de datos aplicable en forma particular a esta empresa, reutilizando el mismo equipamiento existente. No se describe o analiza los servi-

cios a nivel de aplicaciones internas de la propia empresa. Los equipos que se conectan en los enlaces WAN están administrados por otras empresas proveedoras, por lo cual los administradores de red no tienen gestión sobre estos equipos. No ahondaremos en la configuración de los routers marca CISCO que cuenta la empresa, ya que todos son administrados por la empresa Telefónica del Perú. Asimismo no haremos un estudio detallado del servicio de telefonía IP con el que cuenta actualmente, ya que este servicio lo administra y gestiona la empresa Telefónica del Perú.

1.5 Síntesis del trabajo

En el presente trabajo vamos a dar a conocer la arquitectura de alta disponibilidad y redundancia aplicable a la red de datos de la empresa, cumpliendo las buenas prácticas recomendadas por la industria. Vamos a describir la red de datos actual, proponer un mejor diseño físico y lógico y mejorar la redundancia en la red interna. Referente a la seguridad de los equipos, propondremos un esquema centralizado de contraseñas, con niveles y prioridades de acceso, en el cual cada cambio realizado en los equipos quedara grabado en un servidor de registros y podrá ser auditado posteriormente. El presente informe contiene en total 6 capítulos, cada capítulo se detalla a continuación:

- El capítulo I explicael planteamiento de ingeniería del problema.
- El capítulo II es el marco teórico conceptual y presenta los diversos conceptos necesarios para el correcto entendimiento del informe de suficiencia.
- El capítulo III describe los componentes de la red interna de datos y detalla la conexión que existe entre todos los equipos de comunicaciones.
- En el capítulo IV se analiza la información mostrada en el capítulo III, proponiendo mejores esquemas de diseño y recomendando soluciones a los problemas encontrados.
- En el capítulo V se muestra la implementación de las mejoras propuestas.
- Finalmente se presenta las conclusiones del trabajo y las recomendaciones finales.

CAPITULO II
MARCO TEORICO CONCEPTUAL

En este capítulo se exponen las bases teóricas conceptuales más importantes para la comprensión del sistema descrito en el presente informe.

2.1 Antecedentes del problema

Los sistemas de alta redundancia en redes existen desde hace mucho tiempo pero antes sólo estaban al alcance de empresas muy grandes. Con la disminución del precio del hardware y el software en los últimos años, estas tecnologías son asequibles y están disponibles incluso para empresas pequeñas. Por un coste un poco superior, la red de datos de una empresa puede instalarse y configurarse de forma redundante en sus puntos críticos, de tal manera que el fallo de un equipo de red no implique la pérdida del servicio.

Hoy en día se pueden redundar todos los equipos críticos de la red de datos, mediante múltiples conexiones entre los switches, líneas de Internet redundantes con varios routers, etc.

Por otra parte, debido a intentos de intrusión, ataques de hackers, virus, ataques de denegación de servicio y amenazas combinadas a una gran velocidad, es necesario contar con una plataforma de seguridad interna y externa que proteja las contraseñas y archivos de configuración de los equipos de comunicaciones. En el mercado actual tenemos muchos fabricantes que nos ofrecen una gestión centralizada de contraseñas ante posibles ataques, sin embargo la corporación a la que pertenece la empresa utiliza como estándar las soluciones tecnológicas de la marca Cisco.

2.2 Bases teóricas

2.2.1 Arquitectura de alta disponibilidad de la red de datos

En esta sección vamos a describir las diversas tecnologías, protocolos y equipamiento que se utiliza y adapten en la red de datos de la empresa seleccionada. Asimismo vamos a describir las diferentes tecnologías que utilizaremos en el mejoramiento de la red de datos. Los protocolos y estándares que describiremos son propietarios de la marca Cisco, debido a que los administradores de red tienen una amplia experiencia en el manejo de estas tecnologías y a su vez es un estándar que ha adoptado la corporación en los diversos países donde la empresa está presente.

a) Tecnología Cisco stackwise

La empresa Cisco ha desarrollado la tecnología stackwise, la cual es soportada por los switches familia catalyst 3750.Esta tecnología consiste en interconectar los switches 3750 por la parte posterior (Figura 2.1) utilizando un cable de stacking (Figura 2.2).Esta arquitectura de apilamiento ofrece interconexión de 32 Gigabits por segundo y puede unificar hasta nueve switches, permitiéndoles comportarse como una única unidad lógica de convergencia optimizada, facilitando el despliegue de aplicaciones de voz, vídeo y datos. Esta tecnología está orientada principalmente a pequeñas y medianas empresas y ofrece así la posibilidad de aumentar los niveles de eficiencia operativa de las redes LAN permitiéndoles al mismo tiempo adaptarse a las cambiantes necesidades de negocio.

Con stackwise, Cisco ha pretendido aportar la flexibilidad y escalabilidad características de las soluciones apilables con nuevos niveles de disponibilidad por medio de funciones avanzada de recuperación ante fallos tanto de hardware como de software, y servicios unificados, con transmisión distribuida y calidad de servicio. Además, la nueva arquitectura facilita el manejo y la gestión del entorno mediante capacidades de configuración automatizada, y proporciona alto rendimiento y soporte inmediato de protocolo IP versión 6.

Esta tecnología es la que en los próximos capítulos vamos a implementar en la red de datos de la empresa, ya que los switches principales son de este modelo.

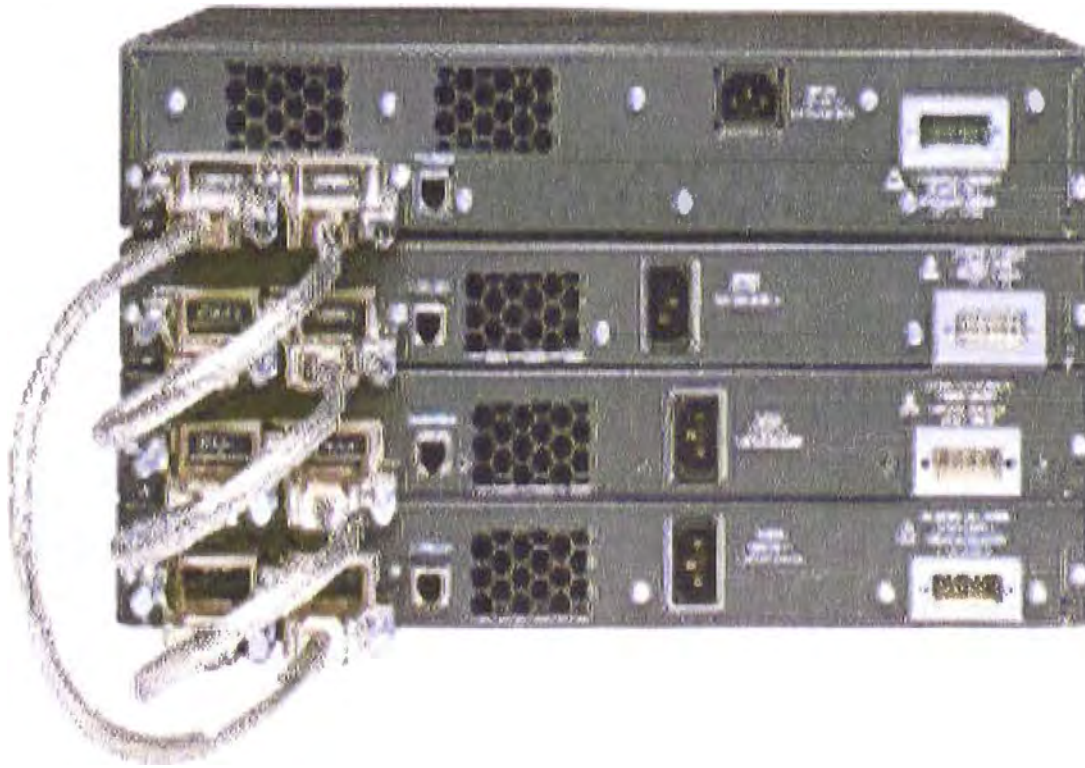

Figura 2.1 Conexión stacking switches Cisco 3750

Figura 2.2 Cable de conexión stackwise

b) Tecnología Cisco flexstack

La tecnología Cisco flexstack ha sido diseñada para los switches Cisco Serie 2960-S, los cuales proveen una verdadera solución de apilamiento entre switches, apilando los switches como una sola unidad lógica. Esta tecnología provee una sola unidad interna de plano de datos, y una sola configuración lógica para un grupo de switches Cisco 2960-S, reduce el costo de mantenimiento de la red porque existen menos equipos que gestionar y la disponibilidad de la red se incrementa al tener un esquema en redundancia. Asimismo con Cisco flexstack se pueden reducir la cantidad de interfaces de interconexión con otros equipos y configurar el protocolo EtherChannel (Figura 2.3), con el cual se pueden agrupar las interfaces en un solo grupo lógico, manteniendo todos los beneficios de este protocolo.

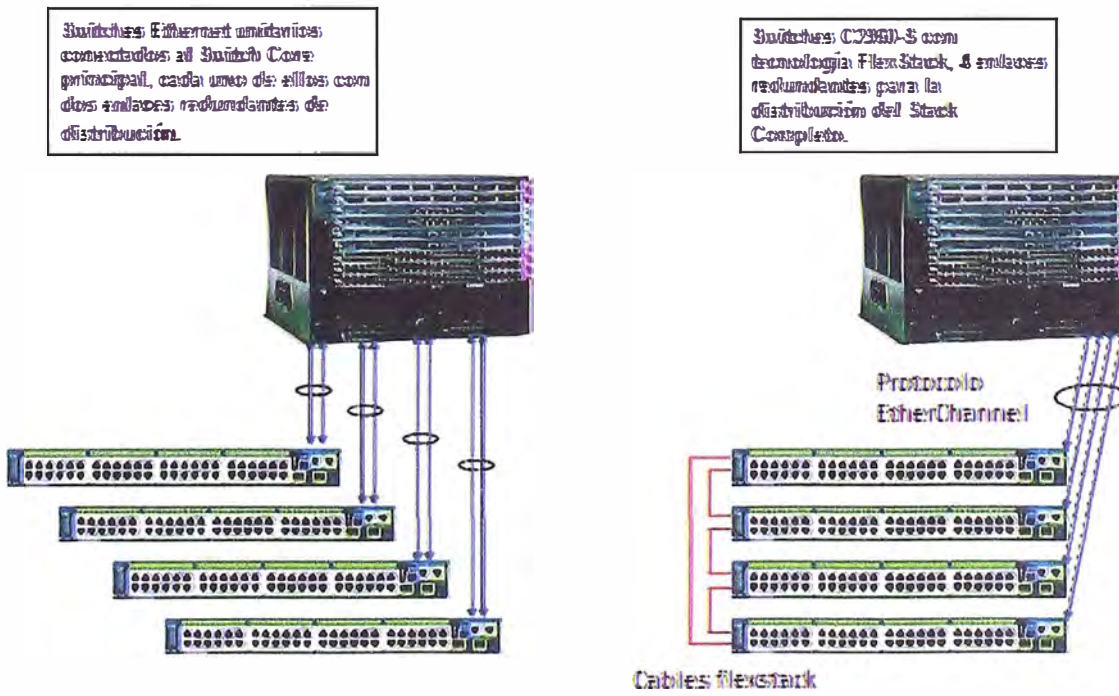

Figura 2.3 Comparación tecnología Cisco flexstack

Otro beneficio es que esta tecnología es escalable al crecimiento de la red: La instalación de un nuevo switch en el grupo apilado de switches es relativamente fácil. Si es necesario el crecimiento de las interfaces en el conjunto de switches, simplemente debemos añadir un nuevo switch unitario del mismo modelo y la configuración del conjunto de switches automáticamente se copia en el nuevo switch.

Flexstack es una tecnología orientada únicamente a los switches Cisco familia catalyst modelo2960-S, y está compuesta de un módulo de hardware que se inserta en la parte posterior del switch (Figura 2.4) y a su vez por el protocolo flexstack.

Figura 2.4 Modulo flexstack

c)Protocolo Spanning-Tree

En una red de datos interna la redundancia se logra teniendo varios enlaces físicos entre los switches, de forma que queden varios caminos para llegar a un mismo destino. El resultado de esto es que la red queda con ciclos o bucles (Figura 2.5).

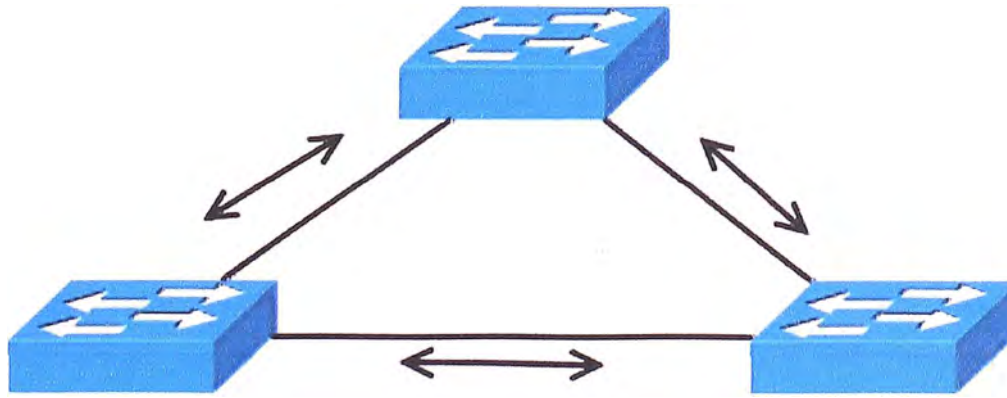

Figura 2.5 Red de switches redundantes.

Si bien la red anterior es redundante, los bucles que se forman son altamente perjudiciales para la misma debido a que producen una serie de problemas que acabaránpordejar la red congestionada y por consiguiente inutilizable. Dentro de dichos problemas podemos encontrarnos con:

-**Tormentas de broadcast:** los broadcast en la red son reenviados una y otra vez y permanecen circulando en la misma sin fin, dado que en ethernet no existe un campo de TTL. Lógicamente, al no eliminarse la situación se agrava con cada nuevo broadcast.

- **Múltiples copias de una trama:** con la redundancia es muy probable que un computador reciba una trama repetida, dado que la misma podría llegar por dos enlaces diferentes.

- **Tabla MAC inconsistente:** una trama que proviene de una MAC en particular podría llegar desde enlaces diferentes.

- **Bucles recursivos:** un bucle puede generar un nuevo bucle y estos crecen de forma exponencial. En una situación así la red quedará inutilizable en pocos segundos.

Ante la necesidad de tener una red LAN redundante y dinámica libre de los problemas mencionados es necesario la existencia de un protocolo que sea capaz de resolver estas cuestiones. Es aquí donde entra en acción el Protocolo de Spanning-Tree (STP).

El protocolo Spanning-Tree se usa en redes conmutadas para crear una topología lógica sin bucles a partir de una topología física con bucles. Los enlaces, puertos y switches que no forman parte de la topología activa sin bucles no envían tramas de datos. El protocolo Spanning-Tree es una herramienta poderosa que otorga a los administradores de red la seguridad de contar con una topología redundante sin que exista el riesgo de que se produzcan problemas provocados por los bucles de conmutación.

d) Protocolo Etherchannel

Cuando existen dos enlaces entre dos switches una alternativa es utilizar el protocolo Etherchannel. Esta tecnología lo que hace es combinar dos o más interfaces como si fueran una sola, agregando el ancho de banda a ese único canal lógico. El protocolo Etherchannel provee también redundancia, dado que si uno de los links se cae, el enlace sigue funcionando perfectamente, con un ancho de banda reducido. La ventaja entonces en comparación con el protocolo Spanning-Tree es que Etherchannel hace uso activo de todos los enlaces, en contraste con STP que de un conjunto utilizaría sólo uno.

Cuando tenemos muchos servidores que salen por un único enlace troncal, puede que el tráfico colapse el enlace. Una de las soluciones más prácticas es el uso del protocolo Etherchannel, cuyo esquema se muestra en la Figura 2.6.De esta manera sumamos la velocidad de los puertos que agregamos al enlace lógico

2.2.2 Definición de VLAN

Una VLAN (acrónimo de Virtual LAN) es una subred IP separada de manera lógica, y permite que redes IP y subredes múltiples existan en la misma red conmutada, y son útiles para reducir el tamaño del broadcast y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (como departamentos para una em-

presa, oficina, universidades, etc.) que no deberían intercambiar datos usando la red local.

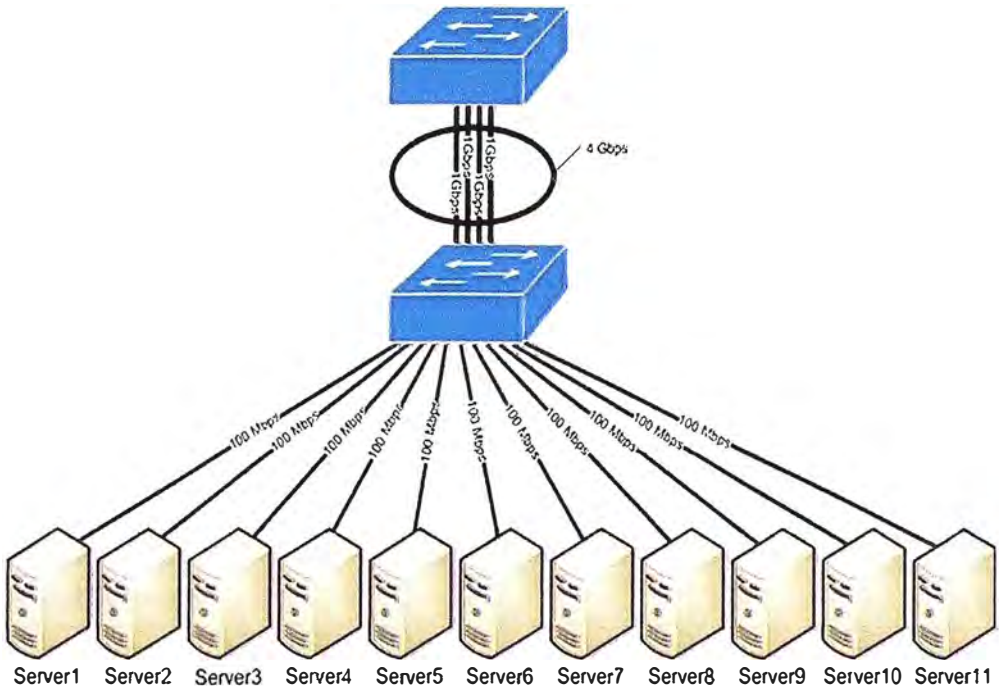

Figura 2.6 Uso del protocolo Etherchannel

Cada computadora de una VLAN debe tener una dirección IP y una máscara de subred correspondiente a dicha subred. Mediante la línea de comandos un switch, pueden crearse las VLAN y a cada puerto se le debe asignar la VLAN por la cual va a trabajar.

No es obligatorio el uso de VLAN en las redes conmutadas, pero existen ventajas reales para utilizarlas como seguridad, reducción de costo, mejor rendimiento, reducción de los tamaño de broadcast y mejora la administración de la red. El acceso a las VLAN está dividido en un rango normal o un rango extendido, las VLAN de rango normal se utilizan en redes de pequeñas y medianas empresas, se identifican por un ID de VLAN entre el 1 y 1005 y las de rango extendido posibilita a los proveedores de servicios que amplíen sus infraestructuras a una cantidad de clientes mayor y se identifican mediante un ID de VLAN entre 1006 y 4094.

2.3 Descripción de la plataforma de seguridad

Proteger el tráfico de datos que circula por la red de datos son aspectos críticos de la seguridad de una empresa, siendo esto mucho más crítico al tratarse de una empresa financiera.

Los métodos de protección de los equipos de comunicaciones son tareas esenciales que no debe de ser pasado por alto por los administradores de red. Se trata de la aplicación de métodos de probada eficacia para proteger el acceso administrativo a los routers o switches, utilizando los comandos de Cisco IOS. Algunos de estos métodos consisten en garantizar el acceso administrativo, incluyendo el mantenimiento de contraseñas, con-

figurar las características mejoradas de acceso virtuales, implementación del protocolo SSH (Secure Shell) y el Protocolo AAA (Autenticación, autorización y contabilización). Debido a que no todo el personal de tecnología de la información debe tener el mismo nivel de acceso a los dispositivos de la infraestructura, la creación de usuarios por niveles de acceso es de mucha importancia en una red de datos.

2.3.1 Seguridad de los equipos de comunicaciones

El acceso administrativo de los equipos de comunicaciones es siempre requerido para propósitos de gestión de la red de datos. Si una persona no autorizada llega a tener acceso a estos equipos, puede alterar los parámetros de enrutamiento, deshabilitar algunas funciones, y descubrir o ganar acceso a otros equipos de la red. Algunas de las tareas que están envueltas dentro de la seguridad del acceso administrativo a los equipos son:

- Restringir el acceso al dispositivo, las interfaces que no se estén utilizando deshabilitarlas administrativamente.
- Realizar periódicamente una auditoria de todas las cuentas de usuarios permitidos, incluyendo los comandos que se han ejecutado, el equipo afectado y la fecha exacta.
- Autenticar el acceso, asegurándonos que el acceso se concede sólo a los usuarios autenticados por grupos y servicios. Asimismo limitar el número de intentos de conexión fallidos y el tiempo entre inicios de sesión.
- Mostrar un aviso legal al momento de iniciar sesión en un equipo de comunicaciones, desarrollado en conjunto con el asesor legal de la empresa.

Algunos de los equipos de comunicaciones necesitan ser accedidos remotamente. El acceso remoto se da normalmente permitiendo los protocolos Telnet, Secure Shell (SSH), HTTP, HTTPS o SNMP. Algunos equipos envían la data, incluyendo los usuarios y contraseñas en texto simple no encriptado. Si un usuario no autorizado puede capturar esta información, va a poder capturar las credenciales de los equipos y tener acceso a los equipos de comunicaciones. Es por esta razón, que debemos de tomar las siguientes precauciones:

- Encriptar todo el tráfico entre la computadora del administrador y los equipos de comunicaciones. Por ejemplo en vez de utilizar el protocolo Telnet o HTTP, debemos usar el protocolo SSH y HTTPS, los cuales son encriptados.
- Establecer una VLAN de gestión dedicado para el acceso remoto a los equipos de comunicaciones. El acceso a esta VLAN debe solo estar autorizado para las computadoras del personal que ingresa a los equipos de comunicaciones, y si es posible realizar la conexión a una interface dedicada del switch o router (Gestión fuera de banda), con la finalidad de proteger el acceso no autorizado de otros usuarios.

- Permitir solo la conexión SSH de las computadoras de los administradores de red hacia los equipos de comunicaciones de red de datos interna.

2.3.2 Configuración de contraseñas seguras

Los usuarios que atacan una red de datos pueden desplegar diversos métodos para descubrir las credenciales de administración de un equipo de comunicaciones. Su principal arma puede ser utilizar información personal de los usuarios, o realizar una captura de paquetes de datos que contiene archivos de configuración en texto sin encriptar. Los atacantes pueden utilizar herramientas tales como "L0phtCrack" o "Cain& Abel" para intentar ataques de fuerza bruta y descubrir las contraseñas (Figura 2.7).

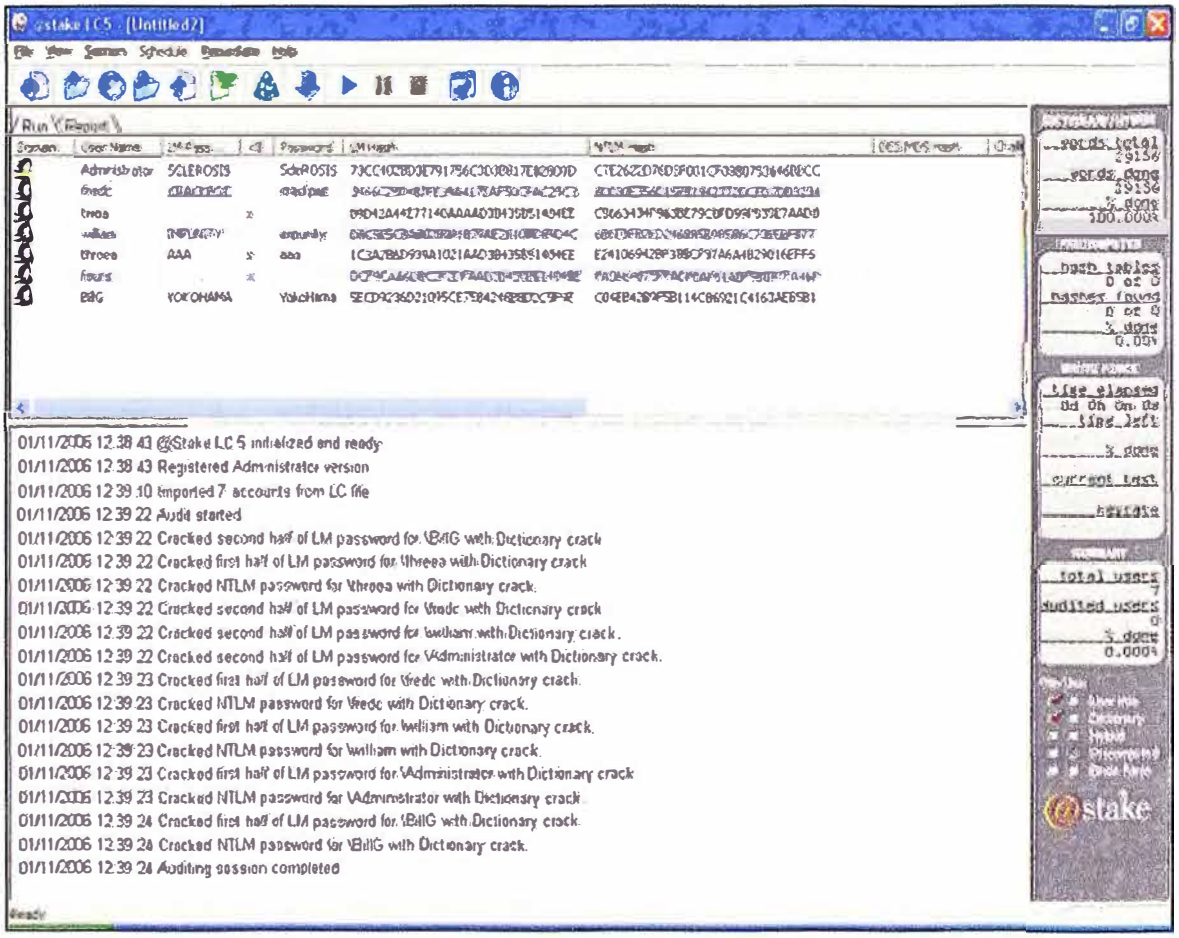

Figura 2.7 Descubrimiento de contraseñas por ataque de fuerza bruta

Para proteger efectivamente las credenciales de los equipos de comunicaciones, debemos de seguir las siguientes pautas, las cuales hacen mucho más difícil su descubrimiento o captura utilizando software que craquean contraseñas:

- Utilice una contraseña que contenga mínimo 10 o más caracteres. Mientras más caracteres contenga mucho mejor.
- Utilice contraseñas complejas. Incluya combinaciones de letras mayúsculas y minúsculas, números, símbolos y espacios, con lo finalidad de hacer mas difícil la desencriptacion de las contraseñas.

- Evite contraseñas basadas en palabras del diccionario, letras o secuencia de números, nombres de mascotas, cumpleaños, etc.
- Cambiar la contraseña frecuentemente, esto limita bastante el accionar del atacante ya que la contraseña expira cada cierto tiempo.
- Deshabilitar sesiones remotas no utilizadas luego de un periodo de tiempo. Por defecto una sesión iniciada en un switch Cisco permanece activa durante 10 minutos después de la última actividad realizada. Si un administrador de red está ausente del terminal y con la sesión activa, puede ser víctima que un atacante tome control de su terminal y ganar acceso no autorizado. Es recomendable que estos tiempos de sesión activa sean reconfigurados a dos o tres minutos máximo.

A continuación se muestra ejemplos de contraseñas fáciles de descifrar (Tabla 2.1) y aquellas que son más difíciles para los atacantes (Tabla 2.2).

Tabla 2.1 Contraseñas fáciles de recordar

Contraseña simple	Explicación
cisco123	Combinación simple de letras y números.
Smith	Nombre de Persona.
Toyota	Marca de Auto
Jose1967	Nombre de persona y fecha de nacimiento

Tabla 2.2 Contraseñas difíciles de recordar

Contraseña Fuerte	Explicación
B678/)&.12Df	Combinación de caracteres alfanuméricos y símbolos.
C2@h u´sp7.-	Combinación de caracteres alfanuméricos, símbolos e incluye un espacio.

2.3.3 Seguridad mejorada para acceso administrativo remoto

Con la finalidad de evitar que algún usuario no autorizado gane acceso a los equipos de comunicaciones utilizando ataques de denegación de servicio o de fuerza bruta, es recomendable habilitar en los equipos de comunicaciones parámetros que detecten cuando el equipo está siendo víctima de un ataque y bloquear el acceso administrativo remoto como medida preventiva. Para esto, el fabricante Cisco recomienda configurar los parámetros mejorados que dan una mayor seguridad al Sistema Operativo IOS de los dispositivos cuando crean una conexión virtual utilizando SSH, y los cuales debe de cumplir los siguientes parámetros:

- Configurar un tiempo de retraso entre intentos consecutivos de acceso al equipo.
- Deshabilitar la consola de acceso remoto cuando se sospecha de un ataque de denegación de servicios o de fuerza bruta.
- Generar unos mensajes de advertencia que se almacenen en un sistema externo al dispositivo para alertar a los administradores.

Estos procedimientos generalmente no aplican para las conexiones realizadas por consola, ya que el cuarto de comunicaciones donde se encuentran los equipos físicos instalados tiene todas las medidas de seguridad requeridas y solo tiene acceso personal autorizado.

2.4 Protocolo Secure Shell (SSH)

SSH es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remoto tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

SSH está diseñado para reemplazar los métodos más viejos y menos seguros para registrarse remotamente en otro sistema, tales como Telnet. El cliente transmite su información de autenticación al servidor usando una encriptación robusta de 128 bits. Todos los datos enviados y recibidos durante la sesión se transfieren por medio de encriptación de 128 bits, lo cual los hacen imposible de descifrar y leer.

2.5 Protocolo AAA

En seguridad informática, el acrónimo AAA corresponde a un tipo de protocolo que realizan tres funciones: Autenticación, Autorización y Contabilización. La expresión AAA se refiere a una familia de protocolos que ofrecen los tres servicios citados. Esto garantiza el control de quién se conecta a la red y qué están autorizados a hacer los usuarios conectados, al tiempo que permite mantener una pista de auditoría de la actividad de los usuarios. Cisco provee dos métodos comunes de implementación de servicio AAA

- Autenticación Local AAA, donde se utiliza la base de datos local para autenticaciones. Este método almacena los usuarios y contraseñas localmente en los equipos Cisco, y los usuarios se autentican contra la base local. Este método es ideal para redes pequeñas.
- Autenticación AAA basada en servidor, en el cual se utiliza un servidor externo y se despliega el protocolo RADIUS o TACACS+. Ejemplos de servidores externos puede incluir Cisco Secure Access, Cisco Secure ACS SolutionEngine o Cisco Secure ACS Express.

TACACS+ es un protocolo propietario de Cisco de autenticación remota que se usa para gestionar el acceso (proporciona servicios separados de autenticación, autorización y registro) a servidores y dispositivos de comunicaciones. Su funcionamiento se visualiza en la Figura 2.8.

Pasos:

1. El cliente establece una conexión con el router.
2. El router solicita al usuario el usuario y contraseña.

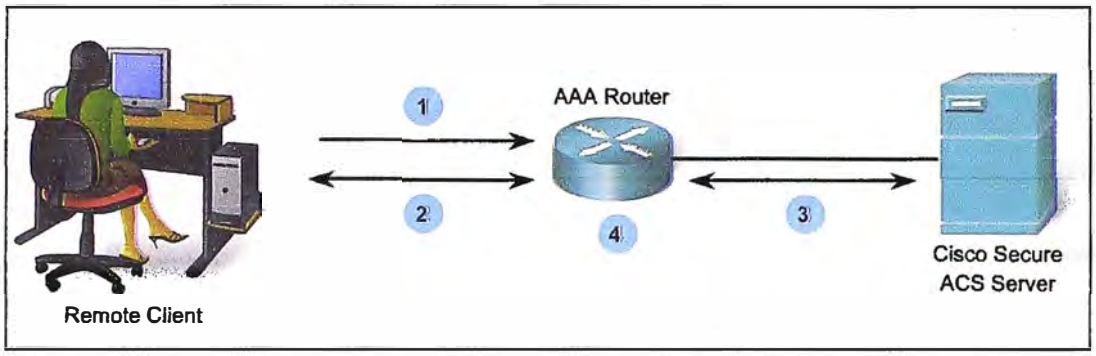

Figura 2.8 Funcionamiento del protocolo TACACS+

3. El router autentica el usuario y contraseña utilizando un servidor externo AAA.

4. El cliente es autorizado en ingresar al equipo o a la red basado en la información del servidor externo AAA.

2.6 Equipamiento de la red de datos

A continuación se presentan las características principales de los equipos que forman parte de la red LAN de datos de la empresa:

a) Switch Cisco WS-C3750G-24TS

- Switch de 24 puertos Ethernet 10/100/1000, con 2 o 4 interfaces de fibra óptica SFP 1Gbps (Figura 2.9).
- Switch estándar de capa 2 y 3 del modelo OSI, el cual tiene funciones de enrutamiento estático y dinámico.
-Soporta el protocolo enrutamiento RIP básico y rutas estáticas, pero se puede realizar una actualización de sistema operativo del switch para que soporte otros protocolos dinámicos de enrutamiento.
- Soporta tecnología Cisco stackwise, con velocidad de interconexión de hasta 32 gigabits por segundo y una arquitectura de apilamiento optimizada para gigabit ethernet.
- Esta tecnología está diseñada para responder a la adición, eliminación y redistribución de switches apilables, manteniendo al mismo tiempo un rendimiento constante. La tecnología Cisco stackwise puede unir hasta 09 Switches en una unidad lógica, usando un cable de apilamiento.
- Gestión del conjunto de switches apilados con una única dirección IP, el cual otorga la capacidad de gestionar como un único objeto y con una única dirección IP hasta 9 switches de esta familia, esta característica es soportada para actividades de detección de falla, creación y modificación de VLANS, seguridad de red, y los controles de calidad de servicio.

b) Switch Cisco WS-C3750-48PS

- Switch Cisco Catalyst de 48 puertos Ethernet 10/100 integrado con Protocolo Estándar POE+ y adicionalmente 4 Puertos SFP Gigabit Ethernet (Figura 2.10)

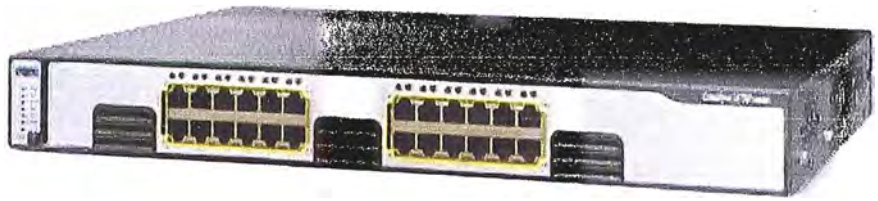

Figura 2.9 Switch Cisco 3750G-24TS

- Soporta el protocolo enrutamiento RIP básico y rutas estáticas, pero se puede realizar una actualización de sistema operativo del switch para que soporte otros protocolos dinámicos de enrutamiento.
- Soporta tecnología Cisco stackwise, con velocidad de interconexión de hasta 32 gigabits por segundo y una arquitectura de apilamiento optimizada para gigabit ethernet. Esta tecnología está diseñada para responder a la adición, eliminación y redistribución de switches apilables, manteniendo al mismo tiempo un rendimiento constante. La tecnología Cisco stackwise puede unir hasta 09 Switches en una unidad lógica, usando un cable de apilamiento.
- Gestión del conjunto de switches apilados con una única dirección IP, el cual otorga la capacidad de gestionar como un único objeto y con una única dirección IP hasta 9 switches de esta familia, esta característica es soportada para actividades de detección de falla, creación y modificación de VLANS, seguridad de red, y los controles de calidad de servicio.

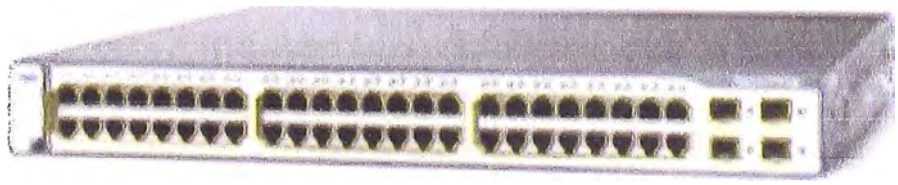

Figura 2.10 Switch Cisco WS-3750-48PS

c) Switch Cisco WS-C3560G-24TS

- Switch Cisco catalyst de 24 interfaces ethernet 10/100/1000 y 4 puertos SFP gigabit Ethernet (Figura 2.11)
- Switch de capa 2 y 3 del modelo OSI, el cual soporta protocolo enrutamiento RIP básico y rutas estáticas, se puede realizar una actualización al sistema operativo del switch para que soporte otros protocolos dinámicos de enrutamiento.
- El sistema operativo del switch soporta características avanzadas de calidad de servicio, velocidad de intercambio de paquetes en cada puerto y listas de control de acceso (ACL), configuración de Vlan, protocolo Spanning Tree, protocolos propietarios de Cisco, Protocolo seguro SSH, protocolo VTP y características especiales de un switch de capa 3.

- Soporta tecnología Cisco energywise, el cual promueve un uso eficiente de la energía eléctrica, reduciendo los costos de energía eléctrica en el centro de datos donde está instalado el equipo.

Figura 2.11 Switch Cisco WS-C3560G-24TS

d) Switch Cisco WS-C2960S-24TD

- Switch Cisco catalyst de 24 interfaces ethernet 10/100/1000 y 2 interfaces de fibra óptica de 10 Gigabit Ethernet (Figura 2.12)
- Soporta la tecnología Cisco flexstack con una velocidad de conmutación de 20 gigabits por segundo.
- Permite administrar a los switches que están dentro del stack como una sola unidad de gestión, utilizando una única dirección IP, reduciendo las horas hombre en la configuración de los equipos.
- Excelente equipo de borde, con amplia variedad de características que se pueden desplegar para una operación más fácil del equipo.

Figura 2.12 Switch Cisco WS-C2960S-24TD

e) Switch Cisco WS-C2960S-24PD

- Switch Cisco catalyst de 24 interfaces gigabit ethernet con soporte del protocolo POE+, el cual hace que cada interface soporte una potencia de 30Watts por interface y es utilizado para conectar dispositivos de comunicaciones (teléfonos IP, antenas inalámbricas). También cuenta con dos interfaces de 10 Gigabit Ethernet.
- Soporta tecnología Cisco flexstack con una velocidad de conmutación de 20 gigabits por segundo, el cual permite administrar a los switches apilados como una sola unidad de gestión, utilizando una única dirección IP, reduciendo las horas hombre en la configuración de los equipos.
- Excelente equipo de borde, con amplia variedad de características que se pueden desplegar para una operación más fácil del equipo.

f)Cisco Secure Access Control (ACS)

El equipo Cisco ACS (control de acceso seguro) es un dispositivo que soporta los protocolos de autenticación Radius y Tacacs+, los cuales entre sus múltiples funciones per-

miten centralizar los usuarios y contraseñas de los diversos administradores de los equipos de comunicaciones, así como establecer privilegios y roles entre los distintos usuarios. Este esquema tiene como ventaja mejorar el control de los usuarios que acceden a los dispositivos, estableciendo políticas de acceso, horarios de acceso, tiempo de caducidad de contraseña, etc.

Actualmente la empresa cuenta con este equipo en su almacén (Figura 2.13), el cual no está en producción y tiene su licencia valida. Este equipo fue adquirido en el año 2010, pero no se ha puesto en producción por falta de personal capacitado. Como parte de desarrollo del presente proyecto, se va a recomendar la instalación y configuración de este equipo, para obtener una gestión centralizada de las contraseñas de los usuarios que acceden a los equipos de comunicaciones.

Figura 2.13 Equipo Cisco ACS

2.7 Análisis matemático de la disponibilidad de la red

Por el año 1990 algunas empresa globales recién empezaban a ofrecer servicios vía correo electrónico ya que las páginas web casi no eran tan comunes para los usuarios, en cambio hoy en día estos servicios han evolucionado de tal manera que ya existen las compras online, diariamente se envían millones de correos electrónicos en el mundo, se realizan transferencia bancarias, entre otros diversos servicios que se pueden realizar vía web, por lo que los servicios de comunicaciones se han convertido indispensables en nuestras vidas, y principalmente las empresas financieras dependen de este recurso. Cuando decimos que nuestra red es confiable, queremos decir que nuestra red de datos funciona todo el tiempo.

En esta sección, vamos a brindar los conceptos básicos para el cálculo de la disponibilidad de una red de comunicaciones. Existen dos métodos para calcular la disponibilidad de una red, el primero se llama el Método del Porcentaje (el cual utilizaremos en este estudio), y el segundo se llama el Método defecto por millón. En ambos métodos se define los siguientes conceptos:

- MTBF (tiempo promedio entre fallas), es el tiempo promedio de falla del equipo, depende principalmente de los componentes internos, microprocesadores, chips, fuente de po-

der, etc. Es un valor que lo proporciona los fabricantes de los equipos de comunicaciones en las especificaciones técnicas del equipo.

- MTTR (tiempo promedio en reparar), es el tiempo promedio de reemplazar o reparar un equipo. Normalmente se considera como el tiempo de atención que se demora el soporte técnico del fabricante en resolver el problema. Depende de varios factores, por ejemplo si es que la empresa tiene personal capacitado, el tipo de contrato que se tiene con el fabricante, la experiencia de los administradores de red, la complejidad de la red, etc.

2.7.1 Determinación de la disponibilidad de un componente

Para calcular la disponibilidad de la red de datos de la empresa, primero debemos de calcular la disponibilidad de cada componente de la red. En este caso, nos vamos a enfocar en los switches de la red de datos, que es el "corazón" de la red por donde fluyen todos los servicios (Aplicaciones, voz sobre IP, transacciones, datos de usuario, gestión de equipos).La disponibilidad de un componente se define por la ecuación 2.1

$$A = \frac{MTBF}{MTTR + MTBF} \quad \textbf{(2.1)}$$

Dónde:

A: Disponibilidad del componente

MTBF: Tiempo promedio entre fallas

MTTR: Tiempo promedio en reparar

Tabla 2.3 Calculo de la disponibilidad de los componentes de la red de datos

N°	MODELO	HOSTNAME	MTBF	MTTR	Disponibilidad (A)
1	WS-C3750-48PS	SW_CORE	166,408	28	0.99983
2	WS-C3750G-24TS	SW_CORE	188,574	28	0.99985
3	WS-C3750G-24TS	SW_CORE	188,574	28	0.99985
4	WS-C3750-48PS	SW_CORE	166,408	28	0.99983
5	WS-C3750-48PS	SW_CORE	166,408	28	0.99983
6	WS-C3750-48PS	SW_CORE	166,408	28	0.99983
7	WS-C3750-48PS	SW_CORE	166,408	28	0.99983
8	WS-C3560G-24TS	VNSW-A01	230,700	28	0.99987
9	WS-C3560G-24TS	VNSW-A02	230,700	28	0.99987
10	WS-C2960S-24TD	VNSW-A06	332,958	28	0.99991
11	WS-C2960S-24PD	VNSW-C01	237,016	28	0.99988
12	WS-C2960S-24PD	VNSW-C02	237,016	28	0.99988
13	WS-C2960S-24PD	VNSW-C03	237,016	28	0.99988
14	WS-C3560G-24TS	VNSW-R01	230,700	28	0.99987
15	WS-C3560G-24TS	VNSW-SV1	230,700	28	0.99987
16	WS-C2960S-24TD	VNSW-A07	332,958	28	0.99991

En la Tabla 2.3 se muestran los valores MTBF extraídos de la página web del fabricante Cisco, los valores MTTR (valor promedio que hemos calculado nosotros) y el valor de la disponibilidad de cada uno de los componentes de la red.

Observación:

- Los valores MTBF y MTTR están expresados en horas.
- La empresa tiene contratado un tiempo de respuesta de 24 horas con el fabricante. Se está considerando que los administradores de red de la empresa se demoran un promedio de 4 horas en reemplazar el equipo, sumando estos dos valores nos proporciona el valor MTTR que se muestra en la Tabla 2.3.

2.7.2 Determinación de la disponibilidad de múltiples componentes

Para calcular la disponibilidad de múltiples componentes, debemos utilizar dos ecuaciones más: topología en serie y topología en paralelo.

- Topología en serie: En este tipo de topología (Figura 2.14), el flujo de datos se da en una dirección, por consecuencia cada equipo es crítico.

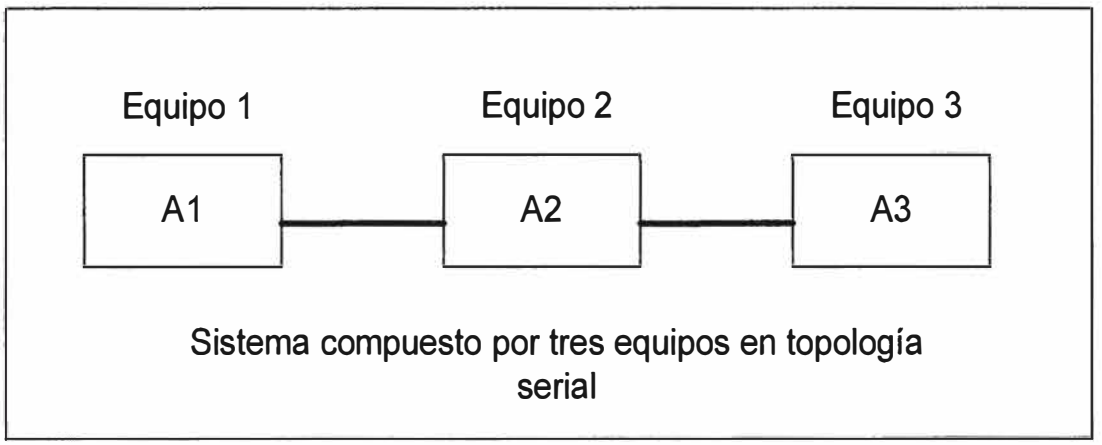

Figura 2.14 Topología en serie

La disponibilidad total (A_t) es el producto de las disponibilidades de cada equipo, tal y como se muestra en la ecuación 2.2

$$A_t = A1 * A2 * A3 \quad \textbf{(2.2)}$$

Dónde:

A_t: Disponibilidad total

A1: Disponibilidad equipo 1

A2: Disponibilidad equipo 2

A3: Disponibilidad equipo 3

- Topología enparalelo: En este diseño tenemos caminos redundantes (Figura 2.15), en donde si un equipo intermedio se avería, el sistema puede conmutar e ir por otro camino. Esta tendencia se da principalmente para los equipos críticos de la red, por ejemplo los

servidores principales. Suponiendo que la conmutación en estos equipos funciona correctamente, el cálculo de la disponibilidad total se muestra en la ecuación 2.3

$$A_t = 1 - (1 - A1) * (1 - A2) * (1 - A3) \quad (2.3)$$

Dónde el significado de A_t, A1, A2 y A3 son las mismas que para la topología en serie.

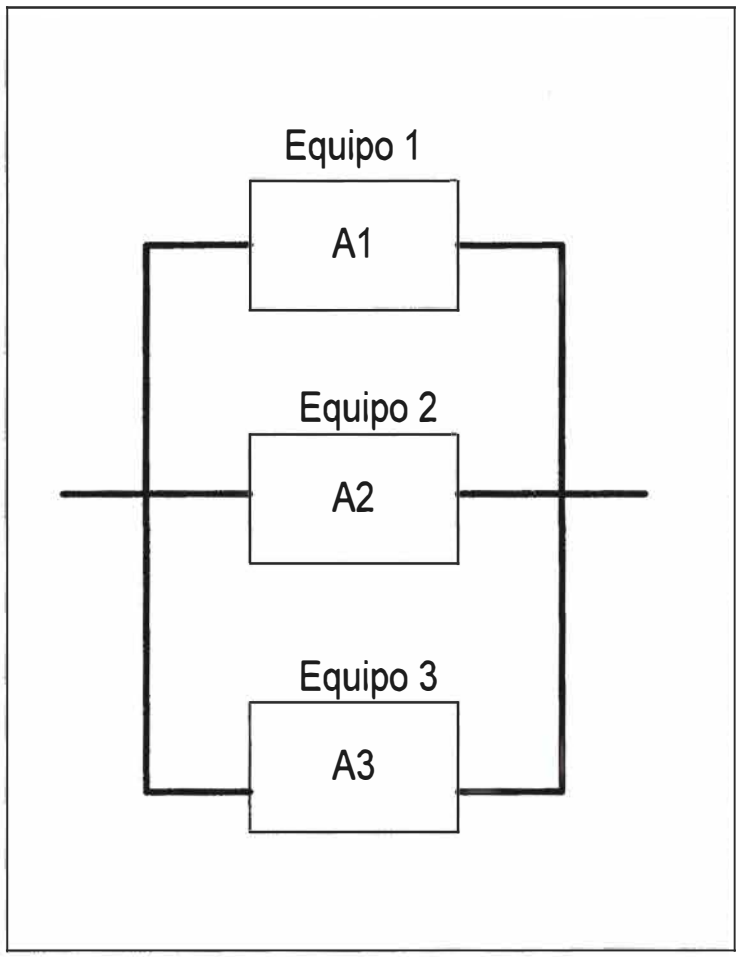

Figura 2.15 Topología en paralelo

Las redes reales son una mixtura de topologías en serie y paralelo. Si los componentes están combinados en serie, la disponibilidad total es mucho menor que los componentes propios. Sin embargo si estos equipos están combinados en paralelo, la disponibilidad del sistema puede ser mayor que la disponibilidad de cada uno de los componentes.

CAPITULO III
DESCRIPCION DE LA REDDE DATOS

En este capítulo vamos a describir los equipos que forman parte de la red de datos de la empresa, así como los diagramas de red de interconexión entre ellos.

3.1 Inventario de equipos

El presente estudio se basa principalmente en el estado actual de la red de datos, el cual está conformado por switches marca Cisco en su gran mayoría y dos switches marca 3COM. En la Tabla 3.1se detallan los equipos que forman parte de la red de comunicaciones y el status de cada uno de ellos. Tener presente que los equipos marca 3COM que actualmente utilizan los tienen con la configuración por default, es decir todas sus interfaces y su dirección IP de gestión están en la VLAN 1.

3.2 Descripción del switch core

El núcleo de la red de datos de la empresa está conformado por 7 switches marca Cisco, los cuales están conectados en cascada, utilizando la tecnología Cisco stackwise. Este conjunto de equipos lo llamaremos en adelante como. Los modelos exactos de los equipos, así como el número de interfaces que poseen se detallan en la Tabla 3.2. Notamos que actualmente existen varias deficiencias en el diseño del apilamiento de estos 7 switches, las cuales las vamos a describir en el capítulo IV.

3.3Diagramas de interconexión

Debido a que la red de comunicaciones de la empresa tiene una cantidad considerable de equipos, hemos elaborado como parte del informe de suficiencia diagramas de interconexión, para comprender detalladamente la conexión física y lógica que existe entre ellos y analizar posteriormente las deficiencias que tienen. Luego propondremos un mejor diseño en la red de datos. Los diagramas que hemos elaborado son:

- Diagrama de conexión con el firewall.
- Diagrama de conexión de los switches.
- Diagrama de conexión de los routers.

Tabla 3 1 Inventario de equipos de comunicaciones

N°	Modelo	Marca	Nombre del switch	IP de gestión
1	WS-C3750-48PS-S	CISCO	SW_CORE	172.16.0.1
2	WS-C3750G-24T-S	CISCO	SW_CORE	172.16.0.1
3	WS-C3750G-24T-S	CISCO	SW_CORE	172.16.0.1

4	WS-C3750-48PS-S	CISCO	SW_CORE	172.16.0.1
5	WS-C3750-48PS-S	CISCO	SW_CORE	172.16.0.1
6	WS-C3750-48PS-S	CISCO	SW_CORE	172.16.0.1
7	WS-C3750-48PS-S	CISCO	SW_CORE	172.16.0.1
8	WS-C3560G-24TS-S	CISCO	VNSW-A01	172.40.0.201
9	WS-C3560G-24TS-S	CISCO	VNSW-A02	172.40.0.202
10	WS-C2960S-24TD-L	CISCO	VNSW-A06	172.40.0.206
11	WS-C2960S-24PD-L	CISCO	VNSW-C01	172.40.0.212
12	WS-C2960S-24PD-L	CISCO	VNSW-C02	172.40.0.214
13	WS-C2960S-24PD-L	CISCO	VNSW-C03	172.40.0.216
14	WS-C3560G-24TS	CISCO	VNSW-R01	No está en producción.
15	WS-C3560G-24TS	CISCO	VNSW-SV1	No está en producción.
16	WS-C2960S-24TD-L	CISCO	VNSW-A07	No está en producción.
17	CSACSE-1113-K9	CISCO	VNACS01	No está en producción.
18	4400SE	3COM	VNSW_3C01	172.16.0.223
19	4400SE	3COM	VNSW_3C05	172.16.0.219

Tabla 3.2 Componentes del switch principal

N°	Modelo	Número de interfaces
1	WS-C3750G-24T	24 puertos 10/100/100 y 4 puertos SFP.
2	WS-C3750G-24T	24 puertos 10/100/100 y 4 puertos SFP.
3	WS-C3750G-48PS	48 puertos 10/100/1000 y 4 puertos SFP.
4	WS-C3750G-48PS	48 puertos 10/100/1000 y 4 puertos SFP.
5	WS-C3750G-48PS	48 puertos 10/100/1000 y 4 puertos SFP.
6	WS-C3750G-48PS	48 puertos 10/100/1000 y 4 puertos SFP.
7	WS-C3750G-48PS	48 puertos 10/100/1000 y 4 puertos SFP.

3.3.1Conexión física con el firewall

Actualmente la empresa tienes dos firewall Juniper modelo SRX240 configurados en clúster activo-pasivo. Por decisión del área de seguridad corporativa de la empresa, los firewall no estánconectados directamente al, sino a otros dos switches dedicados, los cuales son los switches de nombre VNSW_A01 (172.40.0.201) y VNSW_A02 (172.40.0.202). Las conexiones entre los firewall y los switches se detallan en las siguientes Tablas 3.3 y 3.4. En la Figura B1[1] se muestra el diagrama de conexión entre el clúster de los Firewalls Juniper y los equipos switches VNSW_A01 y VNSW_A02.

[1] Hace referencia a figura del Anexo B.

Tabla 3.3 Descripción switch VNSW-A01 y el firewall Juniper

SWITCH VNSW_A01 (172.40.0.201)	FIREWALL 1 (ACTIVO)	
INTERFACE	INTERFACE	TRAFICO PASANTE
GI0/2	GE-0/0/1	VLAN 1,7, 8, 9
GI0/3	GE-0/0/2	VLAN 400
GI0/5	GE-0/0/3	VLAN 220, 240, 260, 270, 280
GI0/6	GE-0/0/4	VLAN 160, 60
GI0/7	GE-0/0/5	VLAN 320 , 340
GI0/9	GE-0/0/6	VLAN 120, 20
GI0/10	GE-0/0/7	VLAN 10, 140
GI0/11	GE-0/0/8	VLAN 990

Tabla 3.4 Descripción switch VNSW-A01 y el firewall Juniper

SWITCH VNSW_A01 (172.40.0.202)	FIREWALL 2 (PASIVO)	
INTERFACE	INTERFACE	TRAFICO PASANTE
GI0/2	GE-0/0/1	VLAN 1,7, 8, 9
GI0/3	GE-0/0/2	VLAN 400
GI0/5	GE-0/0/3	VLAN 220, 240, 260, 270, 280
GI0/6	GE-0/0/4	VLAN 160, 60
GI0/7	GE-0/0/5	VLAN 320 , 340
GI0/9	GE-0/0/6	VLAN 120, 20
GI0/10	GE-0/0/7	VLAN 10, 140
GI0/11	GE-0/0/8	VLAN 990

3.3.2Conexión física de los switches

En esta sección detallaremos la configuración de los interfaces troncales de los switches Cisco. El diagrama de Interconexión de los Switches de core, distribución y acceso se muestra en la Figura B2.

a) Conexión entre elswitch core y el switch VNSW_A01

Esta conexión está formada por 5 enlaces troncales, los cuales están configurados para que pasen únicamente ciertas VLANS (Tabla 3.5).

b) Conexión entre elswitch core y el switch VNSW_A02

Esta conexión está formada por 5 enlaces troncales, los cuales están configurados para que pase únicamente ciertas VLANS (Tabla 3.6)

c) Conexión entre el switch core y el switch VNSW_A06

Esta conexión está formada por 1 enlace troncal de 100 Mbps de ancho de banda, el cual está configurado para el transporte de las VLAN 1, 10, 20, 120, y 400.

d) Conexión entre el switch VNSW_A01 y el switch VNSW_A02

Esta conexión está formada por un único enlace troncal físico de 1Gbps de ancho de banda, el cual está configurado de forma que pasen únicamente las VLANS 980 y 990 (Sincronización del firewall Juniper).

e) Conexión entre el switch VNSW_A06 y el switch VNSW_C01

El equipo VNSW_A06 se encuentra ubicado físicamente en el centro de datos principal (edificio N° 1) y el equipo VNSW_C01 se encuentra ubicado en el edificio N° 2. La conexión entre ellos esta formada por un único enlace troncal físico, el cual está configurado para que pasen únicamente las VLANS1, 10, 20,120, y 400. Físicamente es una fibra óptica multimodo OM3 de 10Gbps que se tiende entre los dos edificios contiguos. Esta fibra óptica tiene un enlace de redundancia, con las mismas características, el cual no se encuentra conectado y ante alguna averia se realiza una conmutación manual.

f) Conexión entre el switch VNSW_C01 y el switch VNSW_C03

Esta conexión está formada por un único enlace troncal físico, el cual está configurado para que pasen únicamente las VLANS 10, 20, 120, y 400.

g)Conexión física de los routers y equipos de voz IP

En la FiguraB3[2] se muestra la conexión física que existe entre el switch core, los routers y los equipos de telefonía IP de la red de datos de la empresa. Asimismo se muestra detalladamente las interfaces de interconexión entre ellos.

Tabla 3.5 Enlaces troncales SW_CORE y VNSW_A01

N° Enlace	Interfaz SW_CORE	Interfaz VNSW_A01	ID VLAN
1	Gi 1/0/8	Gi 0/14	1,7, 8, 9
2	Gi 1/0/9	Gi 0/17	220, 240, 260, 270, 280
3	Gi 1/0/10	Gi 0/18	60, 160, 320, 340, 380, 400
4	Gi 1/0/12	Gi 0/19	20, 120
5	Gi 1/0/11	Gi 0/20	10, 140

Tabla 3.6 Enlaces Troncales SW_CORE y VNSW_A02

N° Enlace	Interfaz SW_CORE	Interfaz VNSW_A01	ID VLAN
1	Gi 2/0/8	Gi 0/14	1, 7, 8, 9
2	Gi 2/0/9	Gi 0/17	220, 240, 260, 270, 280
3	Gi 2/0/10	Gi 0/18	60, 160, 320, 340, 380
4	Gi 2/0/12	Gi 0/19	20, 120
5	Gi 2/0/11	Gi 0/20	10, 140

[2] Hace referencia a figura del anexoB.

3.4 Direccionamiento lógico

Las VLANS creadas y el direccionamiento IPde cada subred que tiene la empresa se muestra en la Tabla 3.7.Como se puede observar, no existe un segmento de red dedicado para la gestión de los equipos de comunicaciones. En el siguiente capítulo analizaremos con mayor detalle este problema y propondremos una subred independiente para la gestión de los equipos de comunicaciones, así como un direccionamiento IP exclusivo para los administradores de red. Esto último nos va a ayudar a filtrar las computadoras que pueden tener acceso remoto a los equipos, utilizando las listas de control de acceso. Asimismo se observa que la dirección IP de la puerta de enlace de cada VLAN está definida en el clúster de los firewall Juniper, por lo que concluimosque el enrutamiento en la red de datos interna lo realiza los firewall.

Tabla 3.7 Direccionamiento IP y VLANS existentes

ID Vlan	Nombre	Subred	Mascara	Puerta de enlace
1	Default	172.16.0.0	255.255.0.0	172.16.254.254
7	HGM	192.168.2.0	255.255.255.0	192.168.2.2
8	ALIGNET	192.168.14.0	255.255.255.240	192.168.14.2
9	TDP	192.168.1.0	255.255.255.0	192.168.1.4
10	DATOS	172.17.0.0	255.255.254.0	172.17.0.251
20	VOICE	172.18.0.0	255.255.254.0	172.18.0.1
50	INTERNET	200.60.106.96	255.255.255.240	200.60.106.110
60	VOIP-PROVINCIAS	172.18.7.0	255.255.255.0	172.18.7.250
120	ESTACIONES	172.17.4.0	255.255.254.0	172.17.5.250
140	SERVIDORES_PCI	172.17.3.0	255.255.255.0	172.17.3.250
160	PROVINCIAS	172.17.7.0	255.255.255.0	172.17.7.250
220	DMZ_CORREO	172.16.10.0	255.255.255.240	172.16.10.1
240	DMZ_VPN	172.16.40.0	255.255.255.0	172.16.40.250
260	DMZ_PROXY	172.16.60.0	255.255.255.0	172.16.60.250
270	DMZ_IEA	172.16.70.0	255.255.255.0	172.16.70.250
280	DMZ_FTS	172.16.80.0	255.255.255.0	172.16.40.250
400	DATOS_2	172.40.0.0	255.255.255.0	172.40.0.254

CAPITULO IV
ANALISIS DE DISPONIBILIDAD Y SEGURIDAD

En este capítulo vamos a analizar la red de datos de la empresa, tanto a nivel de redundancia como de seguridad, y vamos a proponer un mejor diseño en la red de datos. Vamos a utilizar la información del capítulo III, así como los diagramas y tablas elaborados.

4.1 Análisis del switch core

Como se mencionó en el capítulo anterior, el principal de la empresa está conformado por 07 switches Cisco conectados en cascada, los cuales presentan dos problemas que pueden afectar considerablemente a la operación diaria de la empresa.

a) Problema de elección del switch master

Los equipos pertenecientes al están interconectados entre sí (Figura 4.1). Se observa que existen 02 problemas en la configuración y despliegue del stack. La elección del switch máster varía de forma no controlada, no siguiendo el orden de la prioridad configurada. El switch master debe de ser el equipo más potente dentro del conjunto de switches, ya que en el recae todas las funcionalidades del stack completo. Se recomienda que se establezca mediante prioridades la elección del switch master, y que este no esté oscilando ya que puede alterar el comportamiento normal del stack entero. Para conocer que switch del stack está asumiendo el rol de master, ejecutamos el comando "show switch" en el modo privilegiado del switch core. Para efecto de medir si la elección se lleva correctamente, realizamos la medición en dos fechas distintas (Figura 4.2 y 4.3),observando que la elección del switch master cambia, lo cual es un comportamiento no recomendable, ya que todos los switches que forman el stack están operativos y no han presentado alguna avería. Asimismo la elección del switch master no está cambiando de acuerdo a la prioridad pre-configurada, lo cual es incorrecto. Al analizar detalladamente el problema, observamos que existe un error en la versión actual del sistema operativo, por lo que requiere realizar una actualización del sistema operativo Cisco IOS a todos los switches que forman el stack completo. Este error puede traer como consecuencia que en algún momento el stack elija como switch master a cualquier otro switch que no tenga las condiciones adecuadas para funcionar como equipo principal o que esta elección suceda en un momento de alto uso de la red de datos de la empresa, generando lentitud o pérdida de servicio durante esta elección.

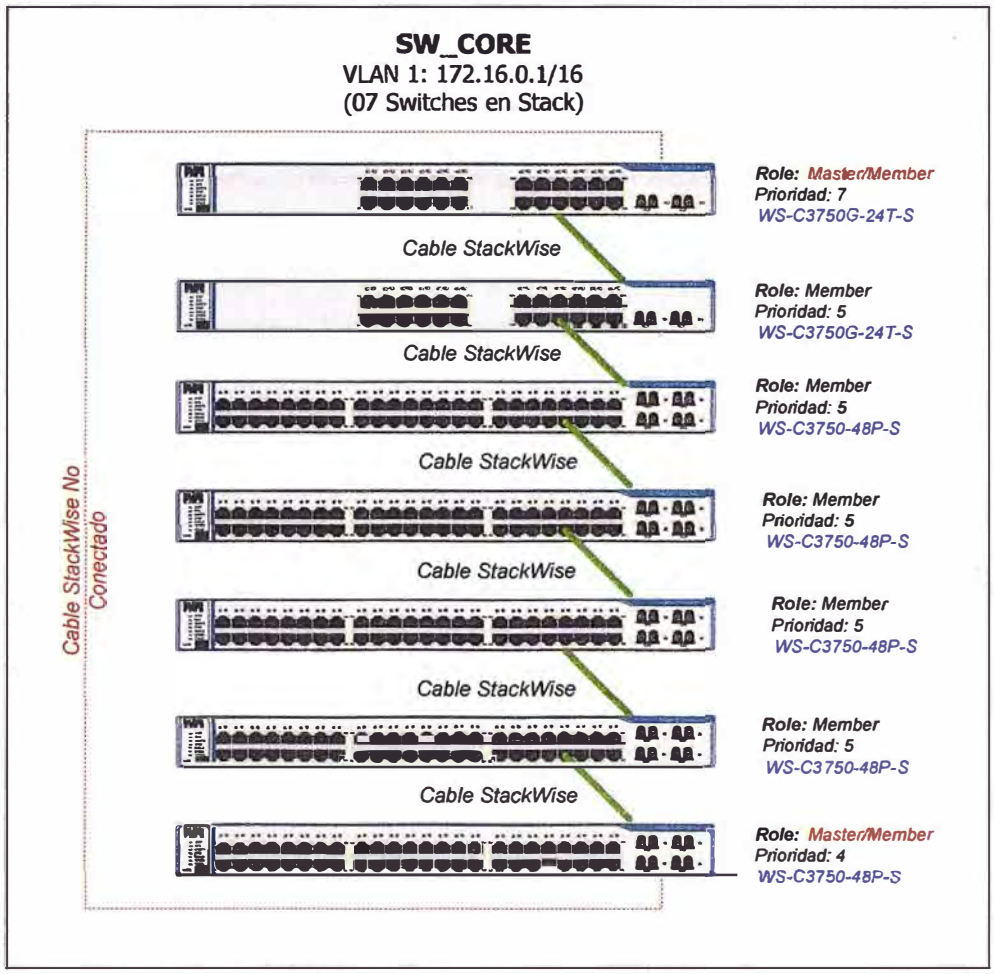

Figura 4.1 Diagrama delstack en el switch core

```
SW_CORE# show switch
Switch       Role         Mac Address       Priority    Status
*1           Master       001a.e395.cf00    7           Ready
2            Member       001a.e395.f400    6           Ready
3            Member       001c.0e18.0e80    5           Ready
4            Member       001b.909e.d000    3           Ready
5            Member       001c.0e18.1b80    1           Ready
6            Member       001b.90b1.c600    2           Ready
7            Member       001b.90b1.4e80    4           Ready
```

Figura 4.2 Salida del comando "show switch" – Fecha 01

```
SW_CORE# show switch
Switch       Role         Mac Address       Priority    Status
1            Member       001a.e395.cf00    7           Ready
2            Member       001a.e395.f400    6           Ready
3            Member       001c.0e18.0e80    5           Ready
4            Member       001b.909e.d000    3           Ready
5            Member       001c.0e18.1b80    1           Ready
6            Member       001b.90b1.c600    2           Ready
*7           Master       001b.90b1.4e80    4           Ready
```

Figura 4.3 Salida del comando "show switch" – Fecha 02

Como se puede observar en las Figuras 4.2 y 4.3, la elección del switch master cambia de prioridad 7 a prioridad 4, lo cual es incorrecto. Para evitar este comportamiento, se recomienda lo siguiente:

- Definir en términos de CPU, memoria RAM y procesamiento que switches deberían ser elegidos como switch master principal y de backup.
- Actualizar el sistema operativo de todos los switches miembros del stack.
- Reconfigurar las prioridades y las políticas de elección del switch master en todos los switches que forman del switch core.
- Simular una caída del switch master y verificar que el switch con la segunda prioridad más alta asume como switch principal, este tipo de conmutación debe de ser automático.

4.1.2 Switch core no redundante

Para verificar si todas las conexiones físicas del switch core están correctas, se ejecutó el comando "show switchstack-ports" (Figura 4.4).

```
SW CORE# show switch stack-ports
Switch      Port 1      Port 2
1           ok          Down
2           ok          ok
3           ok          ok
4           ok          ok
5           ok          ok
6           ok          ok
7           Down        ok
```

Figura 4.4 Salida del comando show switch stack-ports

Como se observa, hay 02 interfaces que están en estado caído (down), y esto significa que no se están interconectando los switches N° 1 y N° 7 (Figura 4.1) a través de un cable stackwise, lo cual trae como consecuencia:

- Falta de redundancia en el switch core, es decir los equipos miembros de stack están apilados de forma serial, siendo critico este diseño.
- Utilización del 50% de la velocidad de conmutación disponible entre los equipos que forman parte del switch core.

En el siguiente capítulo solucionamos este problema segmentando el switch core y conectando el cable stacking.

4.1.3 Número de switches miembros

Si bien la tecnología Cisco stackwise puede soportar hasta el apilamiento de 9 switches, en este caso particular se recomienda independizar el switch core en 2 conjuntos diferentes de switches modelo 3750, con la finalidad de independizar las funcionalidades de core y acceso. Esto traerá como beneficio que los equipos tengan una menor carga de tráfico de datos, por lo que consumirán menos memoria RAM y CPU, teniendo una mayor

velocidad al momento de procesar y conmutar los datos. Asimismo este nuevo diseño haría más fácil y rápido el proceso de resolución de problemas ante cualquier incidencia que se presente en cualquiera de los switches.

4.2 Análisis de redundancia

En esta sección vamos a mostrar las deficiencias de redundancia física y lógica que existen actualmente en la red de datos de la empresa.

4.2.1 Redundancia física

En la Tabla 4.1 se muestran los equipos que poseen enlaces físicos redundantes y su nivel de impacto en la red datos. Como se puede observar, los switches Cisco no presentan redundancia a nivel físico, por lo que se recomienda lo siguiente.

- Conectar un cable stacking en el, para cerrar la topología en anillo del stack.
- Configurar los 5 enlaces troncales que conectan el switch VNSW_A01 y el switch core como un único enlace lógico etherchannel, así aseguramos tener 5 enlaces troncales en redundancia y con un mayor ancho de banda.
-Configurar los 5 enlaces troncales que conectan el switch VNSW_A02 y el switch core como un único enlace lógico etherchannel, así aseguramos tener 5 enlaces troncales en redundancia y con un mayor ancho de banda.
- Configurar el mayor número de enlaces redundantes entre los equipos de comunicaciones, y configurar correctamente el protocolo Spanning-Tree y etherchannel a fin de tener una red de datos con caminos redundantes.

4.2.2 Redundancia a nivel lógico

Luego de revisar la existencia de enlaces físicos redundantes en la sección anterior, pasamos a revisar los protocolos de redundancia a nivel lógico: Spanning-Tree y Etherchannel.

a) Protocolo Spanning-Tree (STP)

Este protocoloestáhabilitado en los switches de la red. Los valores de las prioridades configuradas de los switches se muestran en la Tabla 4.2. Se observa que los valores de las prioridades inicialmente estuvieron bien configurados, pero conforme se fueron añadiendo nuevos switches a la topología se ha ido generando un desorden en el árbol Spanning-Tree, ya que no configuraron un valor de prioridad correcto. Esto trae como consecuencia que al momento de conectar involuntariamente dos equipos en un bucle, se tenga un comportamiento no ordenado ni controlado del protocolo, afectando negativamente la operación de la red de datos de la empresa. Es por esto, que de acuerdo a lo observado, se recomienda lo siguiente:

- Reconfigurar y uniformizar los valores de las prioridades por VLANs en los switches marca Cisco.

- Reorganizar una nueva topología de Spanning-Tree incluyendo switch raíz principal y switch raíz de respaldo, en donde se considere un balanceo por el número de VLANs.
- Deshabilitar la configuración de "portfast" en los enlaces troncales de interconexión de los switches, ya que esta característica evita la negociación del protocolo STP en los enlaces troncales que interconectan los switches.

Tabla 4.1 Disponibilidad de enlaces redundantes por equipo

N°	HOSTNAME	DISPONIBILIDAD DE ENLACE	CRITICIDAD	COMENTARIOS
1	SW_CORE	NO	ALTA	No existe redundancia en el Stack
2	SW_CORE	NO	ALTA	No existe redundancia en el Stack
3	SW_CORE	NO	ALTA	No existe redundancia en el Stack
4	SW_CORE	NO	ALTA	No existe redundancia en el Stack
5	SW_CORE	NO	ALTA	No existe redundancia en el Stack
6	SW_CORE	NO	ALTA	No existe redundancia en el Stack
7	SW_CORE	NO	ALTA	No existe redundancia en el Stack
8	VNSW_A01	NO	ALTA	Cada enlace que se conecta al transporta ciertas VLANS.
9	VNSW_A02	NO	ALTA	Cada enlace que se conecta al transporta ciertas VLANS.
10	VNSW_A06	NO	ALTA	No existe redundancia en el enlace troncal.
11	VNSW_C01	NO	ALTA	No existe redundancia en el enlace troncal.
12	VNSW_C02	SI	ALTA	No existe redundancia en el enlace troncal.
13	VNSW_C03	NO	ALTA	No existe redundancia en el enlace troncal.

b) Protocolo Etherchannel

Es de suma importancia desplegar este protocolo y combinarlo de manera correcta con el protocolo Spanning-Tree, para hacer de la red de datos altamente redundante. Actualmente no está implementado este protocolo en la red de datos. En el siguiente capítulo se muestra el esquema de redundancia propuesto como solución.

4.3 Análisis de seguridad

4.3.1 Protocolos de acceso remoto

Como parte del levantamiento de información del presente proyecto, hemos observado que el acceso remoto a los equipos de comunicaciones es a través del protocolo inseguro Telnet. Asimismo en todos los switches Cisco se tiene habilitado por defecto el protocolo HTTP, el cual también es un protocolo inseguro. La Tabla 4.3 muestra la relación de equipos y el método de acceso remoto a cada uno de ellos.

Tabla 4.2 Prioridades del protocolo STP

N° Vlan	Switch Raiz	Prioridad
Vlan 7	SW_CORE	32775
Vlan 8	SW_CORE	32776
Vlan 9	SW_CORE	32777
Vlan 10	VNSW-A01	24586
Vlan 20	VNSW-A01	24596
Vlan 50	SW_CORE	32818
Vlan 60	VNSW-A01	24636
Vlan 110	SW_CORE	32878
Vlan 120	VNSW-A01	24696
Vlan 140	VNSW-A01	24716
Vlan 160	VNSW-A01	24736
Vlan 220	VNSW-A01	24796
Vlan 240	VNSW-A01	24816
Vlan 260	VNSW-A01	24836
Vlan 270	VNSW-A01	24846
Vlan 280	VNSW-A01	24856
Vlan 320	VNSW-A01	24896
Vlan 340	VNSW-A01	24916
Vlan 380	VNSW-A01	24956
Vlan 400	VNSW-A01	24976
Vlan 980	VNSW-A01	33748
Vlan 990	VNSW-A01	33758

Tabla 4.3 Protocolos de acceso remoto utilizados

N°	Nombre del Switch	Dirección IP de gestión	Protocolo utilizado	Riesgo
1	SW_CORE	172.16.0.1	TELNET, HTTP	Alto
2	SW_CORE	172.16.0.1	TELNET, HTTP	Alto
3	SW_CORE	172.16.0.1	TELNET, HTTP	Alto
4	SW_CORE	172.16.0.1	TELNET, HTTP	Alto
5	SW_CORE	172.16.0.1	TELNET, HTTP	Alto
6	SW_CORE	172.16.0.1	TELNET, HTTP	Alto
7	SW_CORE	172.16.0.1	TELNET, HTTP	Alto
8	VNSW-A01	172.40.0.201	TELNET, HTTP	Alto
9	VNSW-A02	172.40.0.202	TELNET, HTTP	Alto
10	VNSW-A06	172.40.0.206	TELNET, HTTP	Alto
11	VNSW-C01	172.40.0.212	TELNET, HTTP	Alto
12	VNSW-C02	172.40.0.214	TELNET, HTTP	Alto
13	VNSW-C03	172.40.0.216	TELNET, HTTP	Alto
14	VNSW-R01	No está en producción.	TELNET, HTTP	Alto
15	VNSW-S01	No está en producción.	TELNET, HTTP	Alto

Como parte de las mejoras planteadas en esta sección, se recomienda deshabilitar el protocolo Telnet en todos los dispositivos de comunicaciones, y habilitar el protocolo seguro encriptado SSH. Para esto tenemos que revisar la versión del sistema operativo de los switches, el cual se muestra en la Tabla 4.4.

Tabla 4.4 Soporte protocolo SSH y HTTPS

Nombre del switch	Nombre IOS	Soporta SSH/HTTPS	Observación	Riesgo
SW_CORE	c3750-ipbase-mz.122-25.SEE3	No	Actualizar el Cisco IOS	Alto
VNSW-A01	c3560-ipbase-mz.122-35.SE5	No	Actualizar el Cisco IOS	Alto
VNSW-A02	c3560-ipbase-mz.122-35.SE5	No	Actualizar el Cisco IOS	Alto
VNSW-A06	c2960s-ipbase-mz.122-53.SE2	No	Actualizar el Cisco IOS	Alto
VNSW-A06	c2960s-ipbase-mz.122-53.SE2	No	Actualizar el Cisco IOS	Alto
VNSW-C01	c2960s-ipbase-mz.122-53.SE2	No	Actualizar el Cisco IOS	Alto
VNSW-C02	c2960s-ipbase-mz.122-53.SE2	No	Actualizar el Cisco IOS	Alto
VNSW-C03	c2960s-ipbase-mz.122-53.SE2	No	Actualizar el Cisco IOS	Alto
VNSW-R01	c3560-ipbase-mz.122-35.SE5	No	Actualizar el Cisco IOS	Alto
VNSW-S01	c3560-ipbase-mz.122-35.SE5	No	Actualizar el Cisco IOS	Alto

En la Tabla 4.4 se observa que todos los switches no soportan el protocolo seguro SSH ni HTTPS, por lo que es necesario actualizar la versión del sistema operativo. En el siguiente capítulo documentaremos el procedimiento a seguir.

4.3.2 VLAN de gestión

Como se puede observar en la Figura B2[3], las direcciones IP de gestión de los equipos de comunicaciones están en la VLAN 1 o en la VLAN 400. Estas dos VLANs utilizan los usuarios internos para acceder a las aplicaciones internas y navegación hacia internet, no son VLANS dedicadas a la gestión de los equipos de comunicaciones.

El no tener una VLAN dedicada a la gestión de los equipos implica un riesgo de seguridad, ya que algún usuario no autorizado puede infiltrarse en la red y capturar los datos o contraseñas utilizando un software que captura paquetes. Por tal motivo se recomienda crear una VLAN de gestión dedicado única y exclusivamente para la gestión de los switches y otros equipos de comunicaciones, y donde puedan acceder únicamente los administradores de red y usuarios que administren los equipos, realizando un filtrado de direcciones IP utilizando listas de control de acceso. Asimismo, como buena práctica de diseño se recomienda dejar de utilizar la VLAN 1, ya que este segmento de red es el más propenso a recibir ataques de fuerza bruta o de denegación de servicios.

[3] Hace referencia a figura del Anexo B.

4.3.3 Gestión de contraseñas de acceso remoto

Como parte del levantamiento de información para la parte de seguridad, hemos solicitado a los administradores de red las credenciales que ellos utilizan, y los métodos de autenticación, con la finalidad de analizar la información recogida y proponer un mejoramiento en la plataforma de seguridad de contraseñas.

Con respecto a las credenciales de acceso, se observa que todos los usuarios ingresan de forma remota a los equipos utilizando una mismacredencial, no existen usuarios personalizados y categorizados por niveles de acceso. Por este motivo se recomienda crear usuarios personalizados y categorizarlos por niveles, por ejemplo para los usuarios administradores utilizar el máximo nivel permitido (nivel 15), y a los usuarios de soporte técnico crearle usuarios de lectura (nivel 5), con la finalidad de tener un mejor control de acceso a los equipos, y posteriormente auditar los cambios que se realicen.

Asimismo la contraseña utilizada actualmente es relativamente fácil de hackear utilizando software de hacking, ya que contiene 6 caracteres y es una combinación de letras y números. Se recomienda incrementar la dificultad de las contraseñas utilizando las siguientes premisas:

- Longitud mínima de 10 caracteres.
- La contraseña debe de tener una expiración automática de 90 días calendarios.
- Utilizar símbolos alfanuméricos, mayúsculas y espacios, con la finalidad de dificultar su identidad.

Para la ejecución de estas premisas, se recomienda la instalación del equipo Cisco ACS 1113, el cual la empresa lo tiene guardado en el almacén. Luego implementar el protocolo TACACS+ e integrar este equipo con los switches, para tener un gestor centralizado de contraseñas, ya que las contraseñas son creadas de forma local en el mismo equipo, lo cual dificulta tener un control sobre las políticas de creación de contraseñas.

Finalmente se observa que en los switches no existe una política de seguridad ante ataques de fuerza bruta, por lo que la red de datos está siendo muy vulnerable en caso suceda este tipo de ataque. Esto traería como consecuencia el mal funcionamiento del equipo o en el peor de los casos, la caída del servicio de red de datos de la empresa. Para mitigar estas consecuencias, se recomienda configurar un tiempo de retraso entre intentos consecutivos de acceso al equipo, así como deshabilitar la consola de acceso remoto cuando se sospecha de un ataque de denegación de servicios. Asimismo se aconseja generar un registro por cada ingreso al equipo y almacenarlo en un servidor externo de registros.

CAPITULO V
IMPLEMENTACION DE LASMEJORAS

En este capítulo vamos a detallar las actividades realizadas en la empresa. Estas actividades tienen como finalidad incrementar la disponibilidad de la red de datos de la empresa y aumentar los niveles de seguridad de acceso a los equipos de comunicaciones.

5.1 División del switch core

Con el fin de independizar las funciones de core y acceso, se procedió a dividir el conjunto de switches Cisco modelo 3750 en dosgrupos de switches apilados independientemente.En las Tablas 5.1 y 5.2 se muestranla relación de switches que pertenecen a cada nuevo grupo:

Tabla 5.1 Grupo de switches N° 1

GRUPO 01 - SWITCH CORE			
N°	**Modelo**	**Marca**	**Nombre del grupo**
1	WS-C3750G-24T-S	CISCO	SW_CORE
2	WS-C3750G-24T-S	CISCO	SW_CORE

Tabla 5.2 Grupo de switches N° 2

GRUPO 02 - SWITCH ACCESO			
N°	**Modelo**	**Marca**	**Nombre del grupo**
1	WS-C3750-48PS-S	CISCO	VNSW_ACC1
2	WS-C3750-48PS-S	CISCO	VNSW_ACC1
3	WS-C3750-48PS-S	CISCO	VNSW_ACC1
4	WS-C3750-48PS-S	CISCO	VNSW_ACC1

Los switches del grupo N°2 se unen alos switches del grupo N°1 utilizando cuatro enlaces gigabit ethernet, los cuales están unidos lógicamente utilizando el protocolo etherchannel. La relación de interfaces conectadas se muestra en la Tabla 5.3.

Tabla 5.3 Interfaces de conexión

	GRUPO N° 2	**GRUPO N° 1**
Nro. de Interface	**Interfaces**	**Interfaces**
1	Gi 1/0/24	Gi 1/0/23
2	Gi 2/0/24	Gi 1/0/24
3	Gi 3/0/24	Gi 2/0/23
4	Gi 4/0/24	Gi 2/0/24

En las Figuras 5.1 y 5.2 se muestran los nuevosgrupos de switches formados, así como los valores de las prioridades configuradas. En las figuras del anexo B se muestra los diagramas finales de interconexión de todos los equipos luego de realizado los cambios.

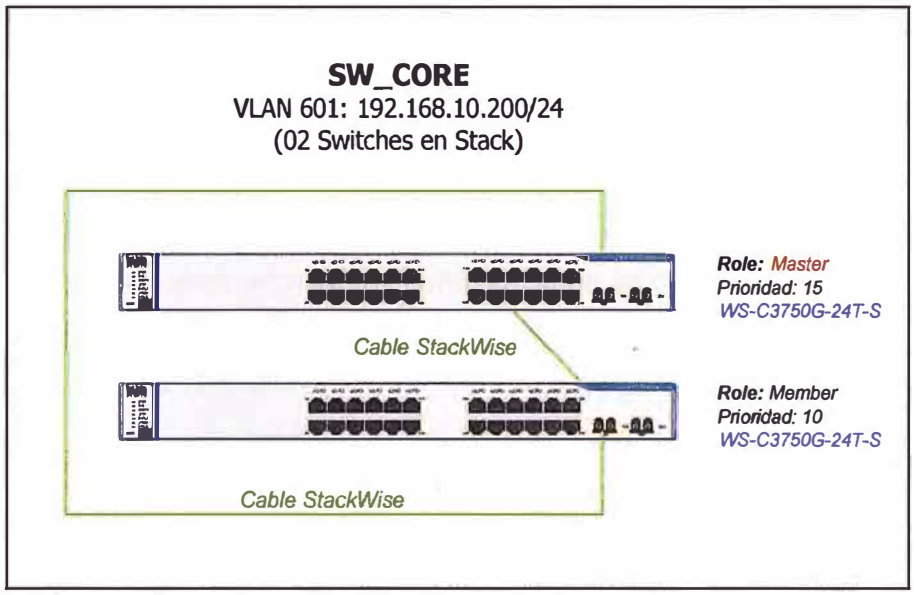

Figura 5.1 Grupo N°1 de switches formados

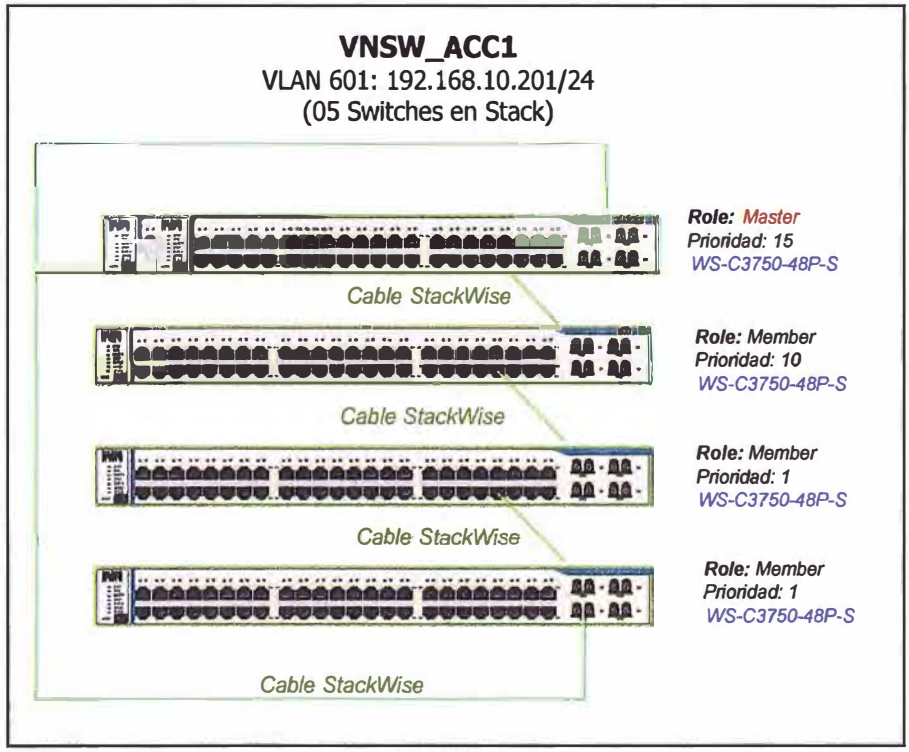

Figura 5.2 Grupo N°2 de switches formados

5.2 Cierre del anillo topológico del nuevo switch core

Se procedió a conectar un cable stackwise en el grupo de switches N°1 recientemente formado, cerrando el anillo topológico del mismo. El cable stackwise conecta el switch N°1 y el switch N° 2 (Figura 5.1).

5.3 Reconfiguración de las prioridades de los nuevos switches apilados

Con la finalidad de tener un proceso controlado en la elección del switch, se procedió a configurar las prioridades de los switches de cada grupo formado en la sección 5.1. Con estos valores forzamos que se elija al switch con la más alta prioridad como switch mas-

ter, y en caso que esté presente una avería, el equipo con la segunda prioridad más alta será elegido como switch master.

5.4 Rediseño de la red LAN

Con la finalidad de darle redundancia a la red de datos, hemos redistribuido los switches y routers de acuerdo a la Figura B4[4].De manera similar hemos rediseñado las conexiones a los routers, centralizando las conexiones en un nuevo switch Cisco de nombre VNSW_R01, el cual no estaba siendo utilizado. En la Tabla 5.4 se muestran los nuevos equipos switches Cisco instalados y su función respectiva:

Tabla 5.4 Nuevos switches instalados

Item	Hostname	Función	Observación
1	VNSW_R01	Switch de Distribución	Todos los routers se centralizan en este equipo
2	VNSW_S01	Switch de Distribución	Todos los servidores se centralizan en este equipo
3	VNSW_A07	Switch deDistribución	Se ha instaladocomorespaldo al Switch VNSW_A06, y se ha conectado la fibra óptica de backup que poseía el cliente.
4	VNSW_C04	Switch de Acceso	Switch de 48 puertos para los usuarios finales

Se han utilizado todos los equipos Cisco que son propiedad de la empresa, con el fin de estandarizar la red de datos, retirando los switches 3COM. Esto debido a que la empresa tiene como planes futuros desplegar herramientas de monitoreo y gestión propietarias del fabricante, y estas no son compatibles con equipos de otras marcas.

5.5 Actualización del sistema operativo Cisco IOS

Como parte del proceso de optimización de la red de datos, se realizó la actualización del sistema operativo Cisco IOS de todos losswitches listados en la Tabla 3.1. Se procedió a instalar la última versión disponible del fabricante, la cual es 12.2-55-SE4. Este software tiene las siguientes características:

- Soluciona los bugs detectados de las versiones anteriores, principalmente los relacionados al proceso de elección del switch master en un conjunto de switches apilados.
- Soporta funcionalidades avanzadas de capa 2 y capa 3, así como todos los protocolos de enrutamiento dinámico interno (RIP, OSPF, EIGRP, BGP)
- Soporta los protocolos encriptados SSH y HTTPS, así como el protocolo TACACS+.
- Soporta la integración con el software CiscoWorks LMS 4.2, el cual es un software propietario de monitoreo y gestión.

En el Anexo C se muestra el procedimiento particularseguido para la actualización del sistema operativo del switch core, teniendo como referencia que para los demás equipos el procedimiento es similar. En la Tabla 5.5 se muestra la relación de los equipos actualizados.

---

[4] Hace referencia a figura del Anexo B.

Tabla 5.5 Relación de switches actualizados

Item	Switch	Versión Anterior	Versión Actual
1	SW_CORE	12.2(25)SE3 IPBASE-M	12.2(55)SE4 IPSERVICES-K9
2	VNSW_A01	12.2(35)SE5 IPBASE-M	12.2(55)SE4 IPSERVICES-K9
3	VNSW_A02	12.2(35)SE5 IPBASE-M	12.2(55)SE4 IPSERVICES-K9
4	VNSW_A06	12.2(53)SE5 IPBASE-M	12.2(55)SE4 IPSERVICES-K9
5	VNSW_A07	12.2(53)SE5 IPBASE-M	12.2(55)SE4 IPSERVICES-K9
6	VNSW_C01	12.2(53)SE5 IPBASE-M	12.2(55)SE4 IPSERVICES-K9
7	VNSW_C02	12.2(53)SE5 IPBASE-M	12.2(55)SE4 IPSERVICES-K9
8	VNSW_C03	12.2(53)SE5 IPBASE-M	12.2(55)SE4 IPSERVICES-K9
9	VNSW_R01	12.2(25)SE3 IPBASE-M	12.2(55)SE4 IPSERVICES-K9
10	VNSW_S01	12.2(25)SE3 IPBASE-M	12.2(55)SE4 IPSERVICES-K9

En las Figuras 5.3 y 5.4 se muestran imágenes de la versión del IOS antes y después del proceso de actualización del switchcore.

```
SW_CORE# show version
Cisco IOS Software,C3750 Software,(C3750-IPBASE-M), Version
12.2(25)SEE3 RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c)1986-2004 by Cisco Systems, Inc.
Compiled Thu 11-Mar-04 19:57 by eaarmas
ROM: System Bootstrap, Version 12.2(8r) [cmong 8r], RELEASE SOFTWARE
(fc1)
System returned to ROM by power-on
```

Figura 5.3 Versión del IOS antes de la actualización

```
SW_C◆RE# show version
Cisco IOS Software,C3750 Software,(C3750-IPSERVICESK9-M), Version
12.2(55)SEE4 RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Thu 11-Mar-04 19:57 by eaarmas
ROM: System Bootstrap, Version 12.2(8r) [cmong 8r], RELEASE SOFTWARE
(fc1)
System returned to ROM by power-on
```

Figura 5.4 Versión del IOS después de la actualización

5.6Creación de una vlan de gestión

Tal y como se recomendó en el capítulo anterior, se procedió a crear una nueva VLAN de gestión para los equipos de comunicaciones. Los datos de esta VLAN son:

- ID vlan : 601
- Nombre : gestión
- Subred : 192.168.10.0
- Mascara : 255.255.255.0

- Puerta de enlace : 192.168.10.1 (Creado en el Switch Core)

A cada uno de los equipos de comunicaciones se le ha asignado una nueva dirección IP perteneciente a esta VLAN, las cuales se muestran en la Tabla 5.6.

Tabla 5 6 Direcciones IP de gestión de los equipos

Item	Nombre del switch	Vlan de Gestión	IP Gestión	Máscara
1	SW_CORE	601	192.168.10.200	255.255.255.0
2	VNSW_ACC1	601	192.168.10.201	255.255.255.0
3	VNSW-A01	601	192.168.10.202	255.255.255.0
4	VNSW-A02	601	192.168.10.203	255.255.255.0
5	VNSW-A06	601	192.168.10.204	255.255.255.0
6	VNSW-A07	601	192.168.10.211	255.255.255.0
6	VNSW-C01	601	192.168.10.205	255.255.255.0
7	VNSW-C02	601	192.168.10.206	255.255.255.0
8	VNSW-C03	601	192.168.10.207	255.255.255.0
9	VNSW-C04	601	192.168.10.208	255.255.255.0
10	VNSW-R01	601	192.168.10.210	255.255.255.0
11	VNSW-S01	601	192.168.10.209	255.255.255.0

Las otras direcciones IP de los switches fueron deshabilitadas, únicamente se podrán gestionar los equipos con las direcciones IP de la Tabla 5.6. En el anexo B se puede observar el diagrama topológico final con las nuevas direcciones IP asignadas a cada equipo. Se recomienda que esta vlan este bloqueada en el firewall perimetral para que no tenga ninguna conexión hacia el exterior, esto como una medida de seguridad preventiva para que ningún usuario externo pueda ingresar o capturar tráfico de los equipos. Se ha considerado que el rango de direcciones IP disponibles soporte un gran crecimiento futuro, en el caso que la empresa adquiera más equipos de comunicaciones. Se recomienda que los nuevos equipos que se vayan añadiendo en el futuro se configuren su dirección IP en esta subred.

5.7 Creación de una vlan de administración

Como parte del rediseño de la red de datos e incrementando la seguridad, se procedió a crear una VLAN exclusivamente para los administradores de red y personal de soporte técnico que tiene acceso a los equipos de comunicaciones. Los datos técnicos de esta VLAN son:

- ID vlan : 602
- Nombre : Admin_Red
- Subred : 192.168.11.0
- Máscara : 255.255.255.0
- Puerta de enlace : 192.168.11.1

La asignación de direcciones IP en cada computadora es de manera estática, ya que es recomendable no utilizar un servidor DHCP para esta subred porque pueden falsificar

una solicitud y el servidorles puede asignar una dirección IP valida. Se ha considerado que el rango de direcciones IP disponibles soporte un gran crecimiento futuro. En la Tabla 5.7 detallamos las direcciones IP asignadas a cada una de las computadoras del personal del área de sistemas.

Tabla 5.7 Direcciones IP asignadas al personal de sistemas

Ítem	Puesto	Dirección IP	Mascara	Gateway
1	Jefe	192.168.11.30	255.255.255.0	192.168.11.1
2	Administrador 1	192.168.11.31	255.255.255.0	192.168.11.1
3	Administrador 2	192.168.11.32	255.255.255.0	192.168.11.1
4	Administrador 3	192.168.11.33	255.255.255.0	192.168.11.1
5	Soporte 1	192.168.11.34	255.255.255.0	192.168.11.1
6	Soporte 2	192.168.11.35	255.255.255.0	192.168.11.1

Esta VLAN se ha propagado por todos los switches, y estápermitida en el Firewall para que tengan navegación externa. Para permitir que las direcciones IP de las computadoras del personal que accede a los switches sean las únicas permitidas, debemos de configuraruna lista de control de acceso en los switches Cisco (Figura 5.5)

```
(config)#access-list 10 permit host 192.168.11.30
(config)#access-list 10 permit host 192.168.11.31
(config)#access-list 10 permit host 192.168.11.32
(config)#access-list 10 permit host 192.168.11.33
(config)#access-list 10 permit host 192.168.11.34
(config)#access-list 10 permit host 192.168.11.35
(config)#line vty 0 15
(config-line)#access-group 1 in
```

Figura 5.5 Comandos Cisco IOS – Lista de control de acceso

Como se puede observar, para realizar el filtro de direcciones IP hemos creado una lista de control de acceso estándar (ACL) en donde permitimos solo las direcciones IP válidas. Las demás direcciones IP del rango seleccionado serán denegadas por la sentencia implícitaque existe en un ACL.

5.8 Optimización de la configuración de los enlaces troncales

En esta parte del proyecto se procedió a estandarizar la configuración de los enlaces troncales que conectan los switches Cisco luego del rediseño que se ha aplicado a la red de datos. Los cambios efectuados a los enlaces troncales se detallan a continuación:

a) Conexión entre el switch SW_CORE y el switch VNSW_A01

- Se estandarizó las configuraciones en ambos extremos de los enlaces troncales.
- Se configuro la vlan nativa 601 en el enlace troncal.
- Se conectaron únicamente 4 enlaces troncales de los 5 existentes, y unieron lógicamente a través del protocolo Etherchannel.

b) Conexión entre el switch SW_CORE y el switch VNSW_A02

- Se estandarizó las configuraciones en ambos extremos de los enlaces troncales.
- Se configuro la vlan nativa 601 en el enlace troncal.
- Se conectaron únicamente 4 enlaces troncales de los 5 existentes, y unieron lógicamente a través del protocolo Etherchannel.

c) Conexión entre el switch SW_CORE y el switchVNSW_A06

- Se estandarizó las configuraciones en ambos extremos de los enlaces troncales.
- Se configuro la vlan nativa 601 en el enlace troncal.
- Se eliminaron los parámetros de STP, DHCP de la configuración del enlace trocal.

d) Conexión entre el switch VNSW_A01 y el switch VNSW_A02

- Se eliminó el enlace troncal entre estos dos equipos, ahora el tráfico de sincronización de los firewalls circula a través del Switch Core.

e) Conexión entre el switch VNSW_A06 y el switch VNSW_C01

- Ya no existe una conexión directa entre estos dos equipos.

f) Conexión entre el switch VNSW_C01 y el switch VNSW_C02

- Se estandarizó las configuraciones en ambos extremos de los enlaces troncales.
- Se configuro la vlan Nativa 601 en el enlace troncal.
- Se eliminaron los parámetros de STP, DHCP de la configuración del enlace troncal.

5.9 Conexión de enlaces físicos redundantes

Con la finalidad de aumentar la disponibilidad de la red de datos ante la avería de algún equipo intermedio o de algún enlace físico, se procedió a conectar enlaces físicos redundantes entre los equipos de comunicaciones. Los enlaces físicos nuevos conectados son:

- Conexión entre el switchcore y el switch de distribución VNSW_A07
- Conexión entre los switches de distribución VNSW_A06 y VNSW_A07
- Conexión entre el switch de distribución VNSW_A07 y el switch de acceso VNSW_C01
- Conexión entre el switch de distribución VNSW_A06 y el switch de acceso VNSW_C02
- Conexión entre los switches de acceso VNSW_C01 y VNSW_C04
- Conexión entre los switches de acceso VNSW_C03 y VNSW_C04
- Conexión entre los switches de acceso VNSW_C02 y VNSW_C03

En la Figura B6[5] se muestra el rediseño que se ha efectuado a la red de datos, y se observa todos los enlaces redundantes nuevos que se han conectado, así como los números del protocolo PortChannel configurado. Esta redundancia funciona libre de bucles debido a que el protocolo Spanning-Tree se ha reconfigurado correctamente, tal y como se indica en la sección posterior. Se ha diseñado la red de datos de la manera más

[5] Hace referencia a figura del Anexo B.

redundante posible utilizando el mismo equipamiento, y pasando a producción los switches Cisco que estaban guardados en el almacén de la empresa. Todos los nuevos enlaces conectados son configurados como enlaces troncales y permiten todas las VLANS desplegadas en la empresa.

5.10 Implementación del protocolo STP

De acuerdo a la sección anterior, debido a que se han conectado enlaces redundantes entre los switches, es necesario reconfigurar correctamente el protocolo Spanning-Tree en todos los switches para evitar que se generen bucles, y a la vez tener una elección controlada del switch raíz principal y switch raíz de respaldo. En el presente proyecto hemos combinado eficientemente el uso del protocolo Spanning-Tree y el protocolo Etherchannel para darle una doble redundancia a los enlaces que conectan los switches. En la Tabla5.8 se detalla los valores de las prioridades configuradas en los switches, mientras que en la Tabla5.9 se muestra la elección de los Switches principal y de respaldo por cada vlan. Asimismo en el Anexo E se muestra la configuración del protocolo Spanning-Tree en los switches.

Tabla 5.8 Prioridades de los switches

Ítem	Equipo	Vlan	Prioridad	Función
1	SW_CORE	1-602	4096	Switch Raíz
2	VNSW 0A01	1-602	32768	-
3	VNSW_A02	1-602	32768	-
4	VNSW_A06	1-602	8192	Switch Raíz de Backup
4	VNSW_A07	1-602	12288	-
5	VNSW_C01	1-602	16384	-
6	VNSW_C02	1-602	20480	-
7	VNSW_C03	1-602	24576	-
8	VNSW_R01	1-602	32768	-
9	VNSW_SRV1	1-602	32768	-
10	VNSW_ACC1	1-602	32768	-
11	VNSW C04	1-602	28672	-

5.11 Configuración del protocolo Etherchannel

Se ha procedido a configurar el protocolo Etherchannel en los enlaces troncales que conectan los switches, con la finalidad de aumentar la disponibilidad de los enlaces y el ancho de banda disponible entre ellos. En la Tabla 5.10 se resume los enlaces Etherchannel creados y el número de PortChannel asignado, así como los equipos involucrados. Como se puede observar, el ancho de banda disponible en la conexión de los equipos ha aumentado considerablemente con la implementación de este protocolo. Esto nos ayuda a que no se genere un cuello de botella en el tráfico de datos, y a su vez soporte

las futuras aplicaciones que circulen por la infraestructura del cliente y requieran gran ancho de banda disponible.

Tabla 5.9 Elección del switch principal y de respaldo

N° Vlan	Switch raíz principal	Switch raíz de respaldo
7	SW_CORE	VNSW_A06
8	SW_CORE	VNSW_A06
9	SW_CORE	VNSW_A06
10	SW_CORE	VNSW_A06
20	SW_CORE	VNSW_A06
50	SW_CORE	VNSW_A06
60	SW_CORE	VNSW_A06
120	SW_CORE	VNSW_A06
140	SW_CORE	VNSW_A06
160	SW_CORE	VNSW_A06
220	SW_CORE	VNSW_A06
240	SW_CORE	VNSW_A06
260	SW_CORE	VNSW_A06
270	SW_CORE	VNSW_A06
280	SW_CORE	VNSW_A06
400	SW_CORE	VNSW_A06
601	SW_CORE	VNSW_A06
602	SW_CORE	VNSW_A06

Tabla 5.10 Protocolo Etherchannel

Equipo 1	Equipo 2	Numero de Interfaces involucradas	Nro. Port-channel	Velocidad del enlace
SW_CORE	VNSW_ACC1	4	23	4 Gbps
SW_CORE	VNSW_A01	4	21	4 Gbps
SW_CORE	VNSW_A02	4	22	4 Gbps
SW_CORE	VNSW_A06	2	30	2 Gbps
SW_CORE	VNSW_A07	2	31	2 Gbps
VNSW_A06	VNSW_A07	2	32	2 Gbps
SW_CORE	VNSW_R01	2	26	2 Gbps
SW_CORE	VNSW_S01	2	27	2 Gbps
VNSW_C01	VNSW_C02	2	25	2 Gbps

5.12 Implementación del protocolo SSH

Como parte de las mejoras de seguridad para el acceso remoto, se procedió a deshabilitar el protocolo telnet y habilitar el protocolo SSH en los todos los switches de la red de comunicaciones (Figura 5.6). Como se puede observar, estamos escogiendo una llave de encriptación de 1024 bits y el algoritmo de encriptación RSA, el cual es elegido como estándar en la industria.

```
(config)#ip domain name visaperu.pe
(config)#crypto key generate rsa general-keys modulus 1024
(config)#linevty 0 15
(config-line)#login local
(config-line)#transport input ssh
(config-line)#exit
```

Figura 5.6 Comandos del protocolo SSH

5.13 Configuración de parámetros de tiempo de espera

Con la finalidad de evitar los ataques automatizados a los switches Cisco, se procedió a implementar un mecanismo de tiempo de espera en todos los switches. Este mecanismo lo hemos configurado de acuerdoa los siguientes parámetros:

- Número de intentos consecutivos : 3
- Tiempo máximo de espera : 60 segundos
- Tiempo de bloqueo : 120 segundos.

La configuración que se realiza en cada switch se muestra en la Figura 5.7.

```
(config)#configure terminal
(config)#login block-for 120 attempts 3 within 60
(config)#login delay 3
(config)#login on-failure log every 1
(config)#login on-success log every 1
```

Figura 5.7 Comandos configurados en los switches

Con esta herramienta configurada en todos los switches Cisco, estamos protegiendo los dispositivos de ataques automatizados, bloqueando durante 60 segundos cualquier conexión luego de 3 intentos fallidos.

5.14 Configuración de equipo Cisco ACS

El equipo Cisco ACS (Secure Access Control) es un dispositivo que soporta los protocolos de autenticación Radius y Tacacs+, los cuales entre sus múltiples funciones permiten centralizar los usuarios y contraseñas de los diversos administradores de los equipos, así como establecer privilegios entre los distintos usuarios. Este esquema tiene como ventaja mejorar el control de los usuarios que acceden a los dispositivos, estableciendo políticas de acceso, horarios de acceso, tiempo de caducidad de contraseña, etc.

Durante la ejecución de este proyecto, se procedió a instalar un equipo Cisco ACS modelo 1113, el cual fue comprado por la empresa en el año 2010 y se encontraba guardado en el almacén de la empresa. Este nuevo equipo ACS se configuró con los siguientes parámetros:

- Nombre del equipo : VNACS01

- Dirección IP : 192.168.10.220
- Máscara : 255.255.255.0
- Puerta de enlace : 192.168.10.1
- NTP : 172.40.0.250
- DNS : 172.17.0.220, 172.17.4.210

Adicionalmente se realizaron las siguientes actividades en el equipo:

- Se habilito el protocolo SSH y HTTPS, para la gestión del equipo en forma remota.
- Se integró el certificado digital del equipo ACS con el servidor emisor de certificados del dominio del cliente.
- Integración del equipo ACS con el directorio activo del dominio, instalando un agente en un servidor Windows Server 2003. Con esta integración el cliente puede gestionar los usuarios y contraseñas a través del directorio activo.
- Creación de grupos de usuarios para el acceso remoto a los equipos. Los grupos que se definieron son:

- Grupo soporte técnico, con nivel de privilegio 5, los usuarios que pertenecen a este grupo tienen acceso solo de lectura.
- Grupo administradores, con nivel de privilegio 15, los usuarios que pertenecen a este grupo tienen acceso de lectura y escritura.
- Configuración de políticas de seguridad para las contraseñas de los grupos de soporte técnico y administradores.

Para ingresar vía web al equipo, ingresamos a la siguiente dirección: https://192.168.10.220:2002 (Figura 5.8).

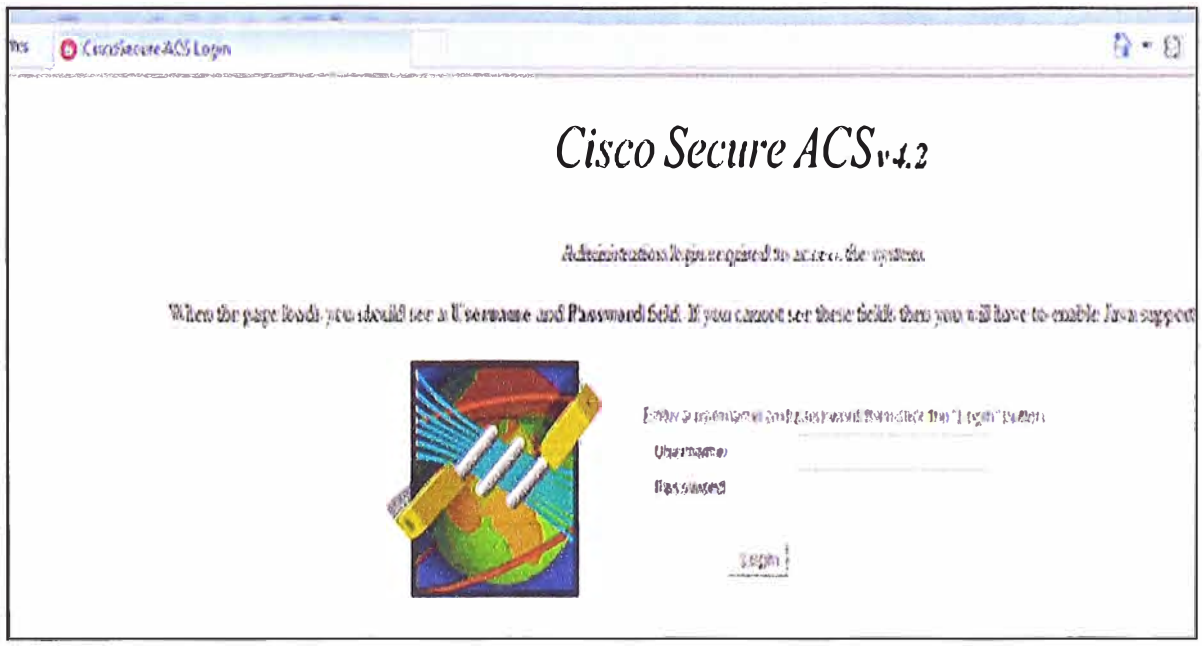

Figura 5.8 Página principal del equipo Cisco ACS

Adicionalmente tenemos que configurar ahora todos los switches con el protocolo TACACS+. Este procedimiento se muestra en el Anexo D.

5.15 Calculo de la disponibilidad de la red

Para calcular la disponibilidad de la red, primero vamos a calcular el valor de la disponibilidad del nuevo switch core formado. Este es un conjunto de dos switches 3750G conectados en cascada. De acuerdo a la Tabla 2.3, la disponibilidad de cada switch es 0.99985.

Tabla 5.11 Cálculo de disponibilidad por segmentos

Item	Segmento	Tipo de topología	Equipos involucrados	Disponibilidad (%)	Tiempo de no disponibilidad (minutos)
1	Usuario A - Usuario C	Serie	A1= VNSW_ACC1*SW_CORE*VNSW_C01*VNSW_C04	99.96	210.384
2	Usuario A - Usuario B	Serie	A2= VNSW_ACC1*SW_CORE*VNSW_C02*VNSW_C03	99.965	184.086
3	Usuario A - Servidor	Serie	A3= VNSW_ACC1*SW_CORE*VNSW_S01	99.985	78.894
4	Usuario B - Servidor	Serie	A4= VNSW_C03*VNSW_C02*VNSW_A06*SW_CORE*VNSW_S01	99.953	247.2012
5	Usuario C - Servidor	Serie	A5= VNSW_C04*VNSW_C01*VNSW_A07*SW_CORE*VNSW_S01	99.948	273.4992
6	Usuario A - Router	Serie	A6= VNSW_ACC1*SW_CORE*VNSW_R01	99.985	78.894
7	Usuario B - Router	Serie	A7= VNSW_C03*VNSW_C02*VNSW_A06*SW_CORE*VNSW_R01	99.953	247.2012
8	Usuario C - Router	Serie	A8= VNSW_C04*VNSW_C01*VNSW_A07*SW_CORE*VNSW_R01	99.948	273.4992

Para calcular la disponibilidad del switch core, aplicamos la ecuación 2.3 porque son equipos que están en paralelo:

$$A_{STACK} = 1 - (1 - 0.99985) * (1 - 0.99985)$$

$$A_{STACK} = 0.99999$$

De igual forma calculamos la disponibilidad para el segundo conjunto de switches, que tiene como nombre VNSW_ACC1. Este conjunto está formado por 4 Switches 3750, donde cada switch tiene una disponibilidad de 0.99983. Luego, utilizandola ecuación 2.3 tenemos la disponibilidad total A_2:

$$A_2 = 1 - (1 - 0.99983)^5$$

$$A_2 = 0.99999$$

Observación: Se eleva a la potencia quinta ya que son 5 equipos en paralelo.

Teniendo ya estos valores calculados, procedemos a elaborar el diagrama de los switches de la red, el cual se muestra en la Figura B7[6]. El cálculo de la disponibilidad de la red se hace por segmentos, el cual se detalla en la Tabla 5.11.

Como se puede observar, los valores de disponibilidad de los segmentos que se mencionan fluctúan entre los valores de 99.948% y 99.985%, generando tiempos de no disponibilidad del servicio de 78 y 273 minutos respectivamente por año. Estos valores se consideran aceptables, teniendo en cuenta que hemos utilizado el mismo equipamiento que tenía inicialmente la empresa.

[6] Hace referencia a figura del Anexo B.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Al cerrar el anillo topológico del nuevo switch core, hemos asegurado en tener dos equipos en redundancia y así evitar la caída del servicio de datos ante alguna avería de algún switch del stack.
2. Luego de los cambios realizados a nivel físico y lógico, la red de datos presenta una mayor redundancia ante alguna avería de algún switch intermedio o de algún enlace físico. Con el nuevo diseño, existe disponibilidad de servicio de la red de datos, teniendo valores que fluctúan entre 99.948% y 99.985%, generando tiempos de no disponibilidad del servicio de 78 y 273 minutos respectivamente por año. Estos valores son aceptables, considerando los equipos disponibles con los que se cuenta.
3. Al configurar correctamente el protocolo Spanning-Tree estamos evitando que se generen tormentas broadcast y alteren el funcionamiento normal de los switches. Asimismo el uso del protocolo Etherchannel en la red de comunicaciones aumenta la disponibilidad de la red de datos y el ancho de banda disponible.
4. Con la conexión de la fibra óptica multimodo de redundancia que tiene el cliente, estamos dando disponibilidad al servicio de datos de la oficina N° 2, ante alguna averia de la fibra óptica actual. Ahora utilizando el protocolo Spanning-Tree la conmutacion es automatica e instantánea.
5. El nivel de criticidad de la disponibilidad de la red ha disminuido considerablemente con todos los cambios físicos y lógicos realizados, ya que con la implementación del protocolo Spanning-Tree en los switches, la red de datos tiene enlaces redundandes entre los equipos de comunicaciones sin generar tormentas de broadcasts de capa 2. Asimismo con la implementación del protocolo Etherchannel, ahora todos los equipos tienen una interconexión troncalde uno o más enlaces, el cual aumenta la redundancia en la conexion y aumenta el ancho de banda disponible entre los equipos. Esto se puede apreciar observando las Figuras B2 y B4[7].
6. Los switches Cisco tienen instalado la última versión disponible del sistema operativo Cisco IOS, el cual soluciona los errores detectados en versiones anteriores e incrementa los servicios de seguridad disponibles.

---

[7] Hace referencia a las figuras del anexo B.

7. Los equipos de comunicaciones utilizan los protocolos seguros y encriptados: SSH y HTTPS.

8. Con la implementación del protocolo TACACS+, la gestión de los usuarios es centralizada y registrada en el servidor. Cualquier cambio efectuado por algún administrador va a quedar almacenado en el servidor Cisco ACS, para luego poder realizar una auditoria si fuese necesario.

10. Se han configurado los switches con parámetros de bloqueo ante algún ataque de denegación de servicios o de fuerza bruta, bloqueando el acceso durante 120 segundos en caso se detecte un ataque.

11. Solo las computadoras de los administradores y soporte técnico pueden gestionar los equipos de comunicaciones, previniendo así cualquier intento de ataque externo.

12. Los usuarios de soporte técnico tienen acceso solo de lectura a los switches, mientras que los administradores tienen acceso de lectura y escritura.

Recomendaciones

1. Desconectar las interfaces que no están siendo utilizados en los switches, colocarlos en estado deshabilitado y asignarlos a una VLAN inutilizable.

2. Configurar los protocolos desplegados en este documento (STP; TACACS+, SSH, etc.) a nuevos equipos que se vayan añadiendo a la red de datos.

3. Implementar protocolos propietarios (VTP, RSTP+, CDP) en la red de datos.

4. Implementar un software de monitoreo de equipos vía SNMP.

5. Revisar periódicamente los consumos de procesamiento y memoria RAM de los equipos de comunicaciones y validar que estén dentro de los parámetros permitidos.

6. Adquirir un switch conlas mismas características al switch VNSW_R01, como medida de respaldo a este equipo y conectarlo en cascada.

7. Adquirir un equipo UPS de energía redundante, para tener un respaldo de energía si es que se corta la electricidad en el edificio.

8. Con la finalidad de mejorar los tiempos de no disponibilidad en la red de datos, se recomienda reemplazar los equipos actuales por un switch modular, el cual tiene un valor MTBF mayor y hace que aumente el porcentaje de disponibilidad. Estos equipos poseen tarjetas supervisoras redundantes, fuentes de poder redundantes, etc.,

9. Realizar un mantenimiento preventivo a los equipos cada 6 meses, extrayéndoles el polvo interno y externo, ya que puede averiar las tarjetas internas de los equipos de comunicaciones.

10. Realizar una capacitación al personal de sistemas de la empresa, en donde se indique los cambios realizados a la red de datos.

ANEXO A
GLOSARIO DE TERMINOS

Siglas	Ingles	Significado en Español
LAN	Local Area Network	Red de área local
WAN	Wide Area Network	Red de área ancha
DOS	Denial Of Service	Denegación de servicio
TTL	Time To Live	Tiempo de vida
MAC	Media Access Control	Control de acceso al medio
STP	SpanningTreeProtocol	Protocolo Spanning-Tree
ACS	Access Control Server	Control de acceso al servidor
AAA	Authentication, authorization, and accounting	Autenticación, autorización y contabilización
SNMP	Simple Network Management Protocol	Protocolo simple de gestión de red
VLAN	Virtual Local Area Networks	Red de área local virtual
FTP	File Transfer Protocol	Protocolo de transferencia de archivos
TACACS	Terminal Access Controller Access-Control System	Sistema de control de acceso mediante control del acceso desde terminales
OSI	Open SystemsInterconnection	Sistema de interconexión abierto
MTBF	Mean time betweenfailures	Tiempo promedio entre fallas
MTTR	Mean time torepair	Tiempo promedio para reparar

ANEXO B
DIAGRAMAS TOPOLOGICOS

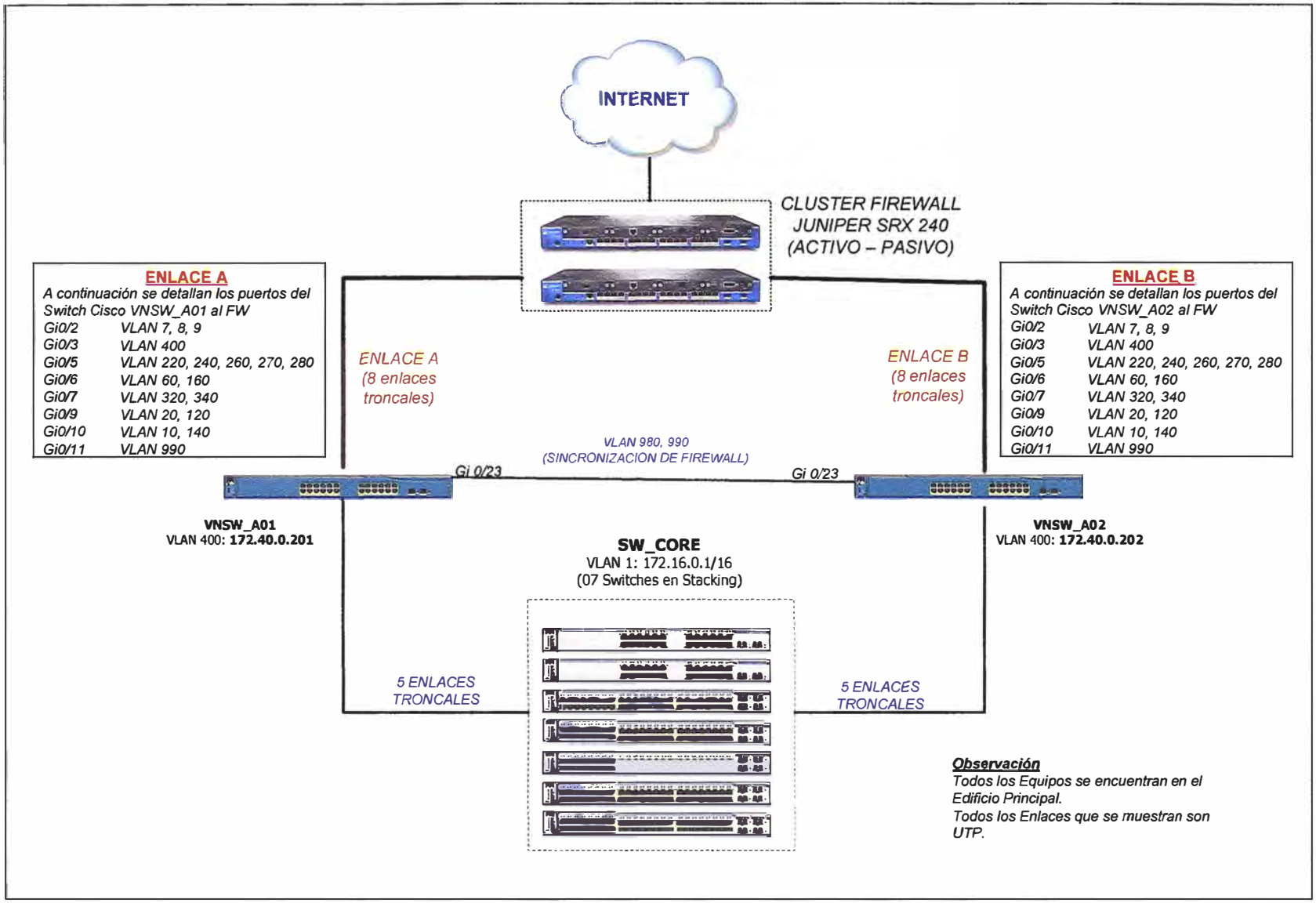

Figura B1 Diagrama de conexión de los Firewall Juniper

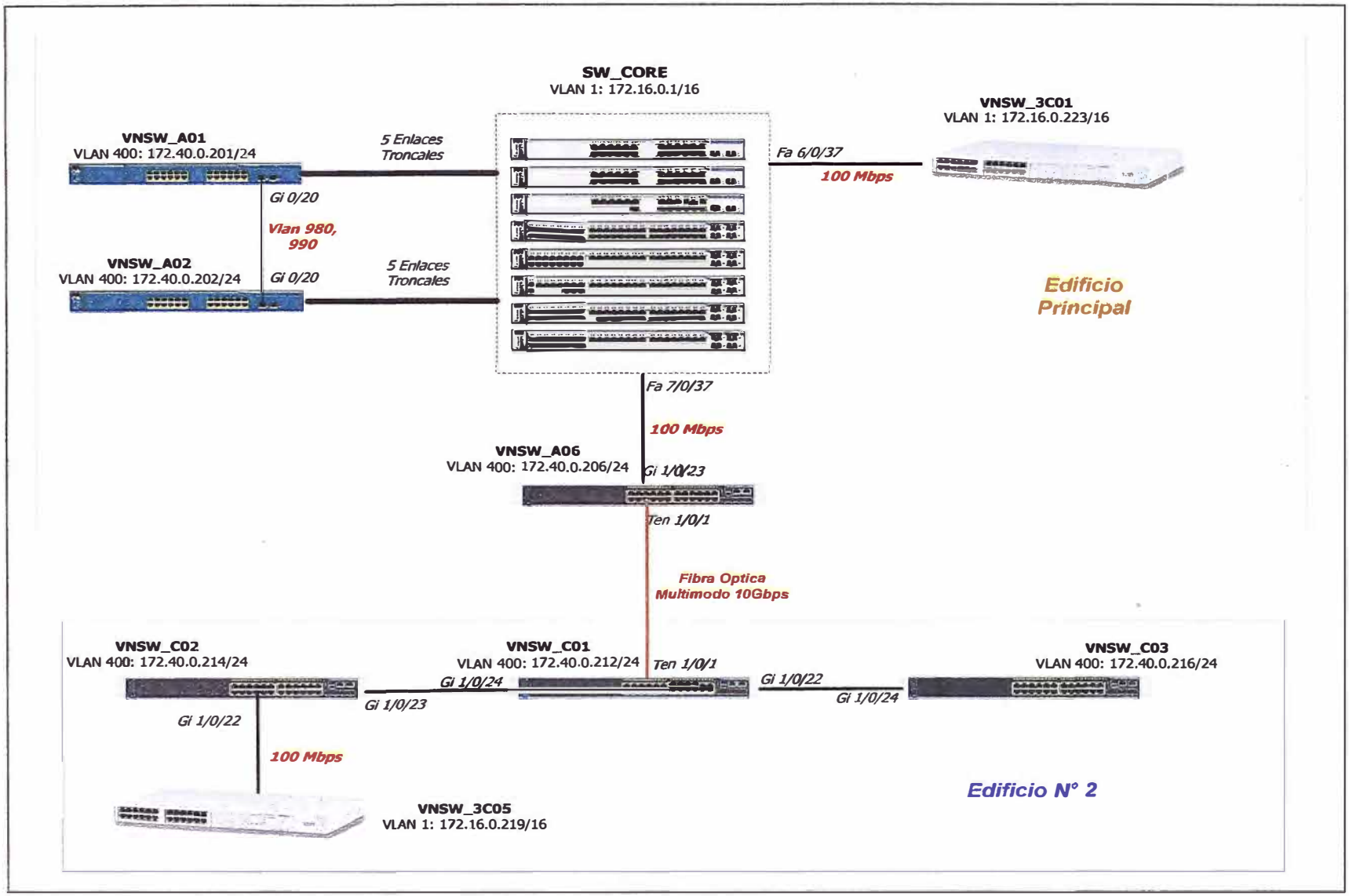

Figura B2 Diagrama de conexión de los switches antes de realizar los cambios

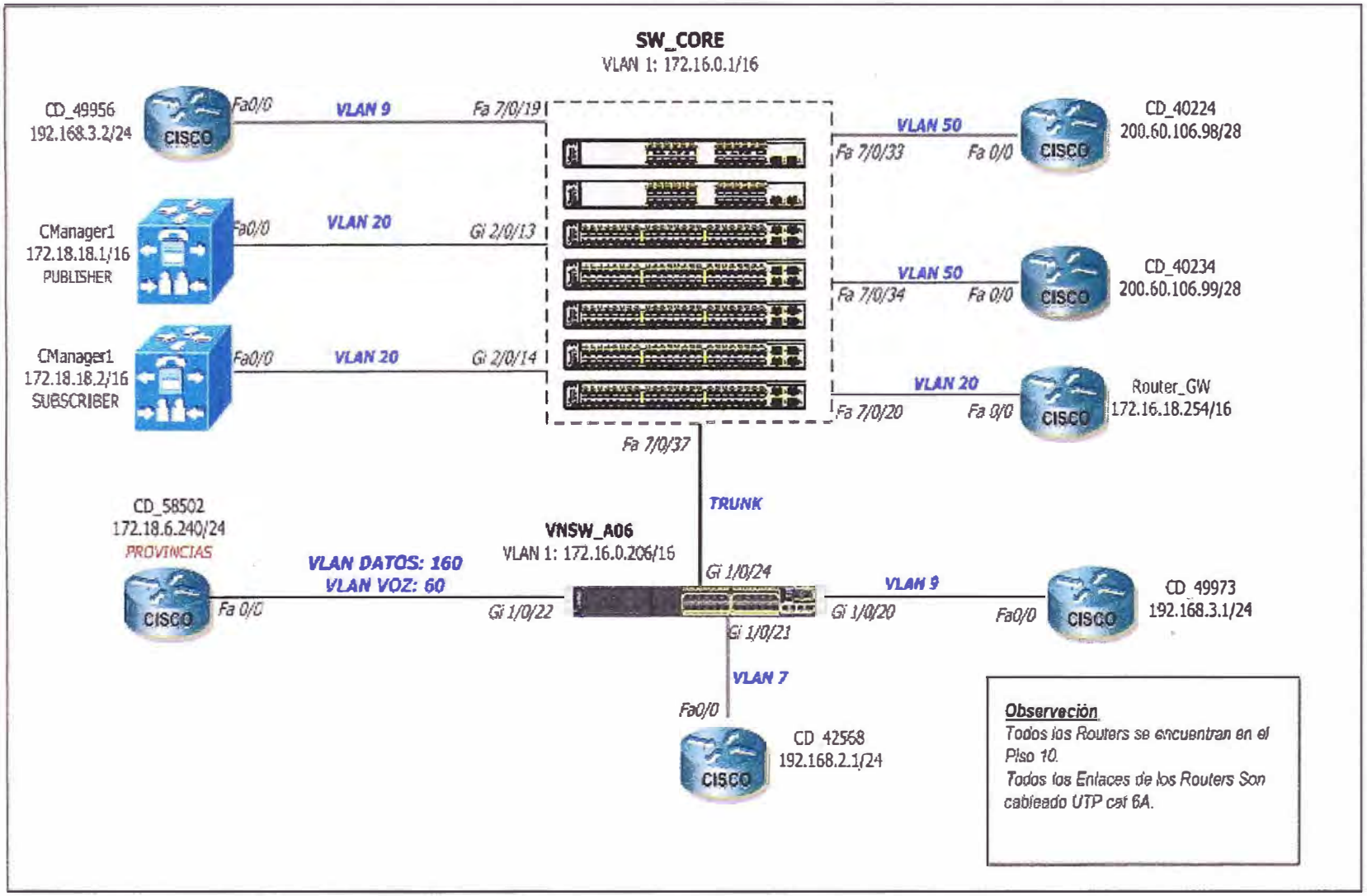

Figura B3 Diagrama de conexión de los routers antes de realizar los cambios

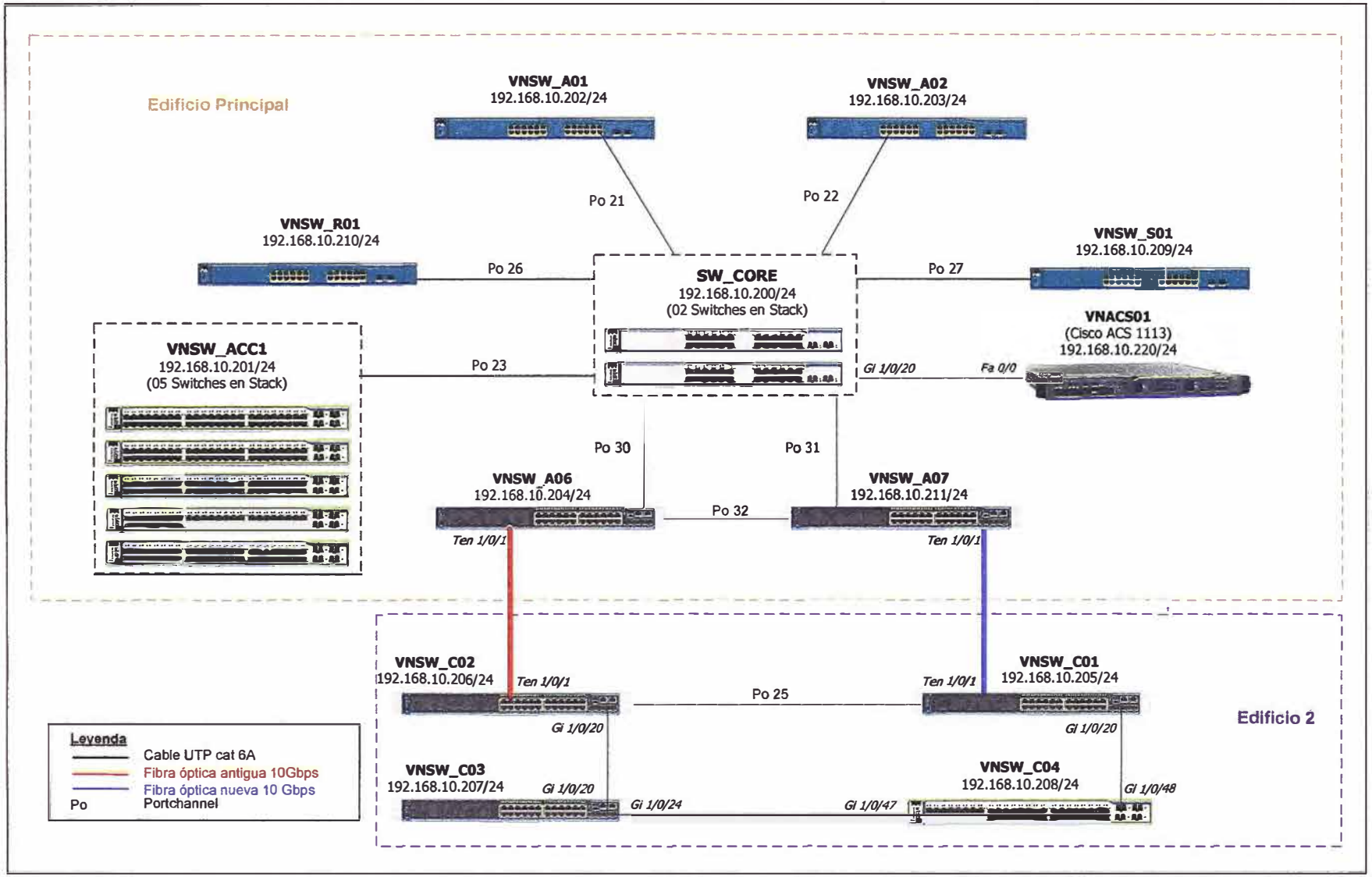

Figura B4 Diagrama de red final después de realizar los cambios.

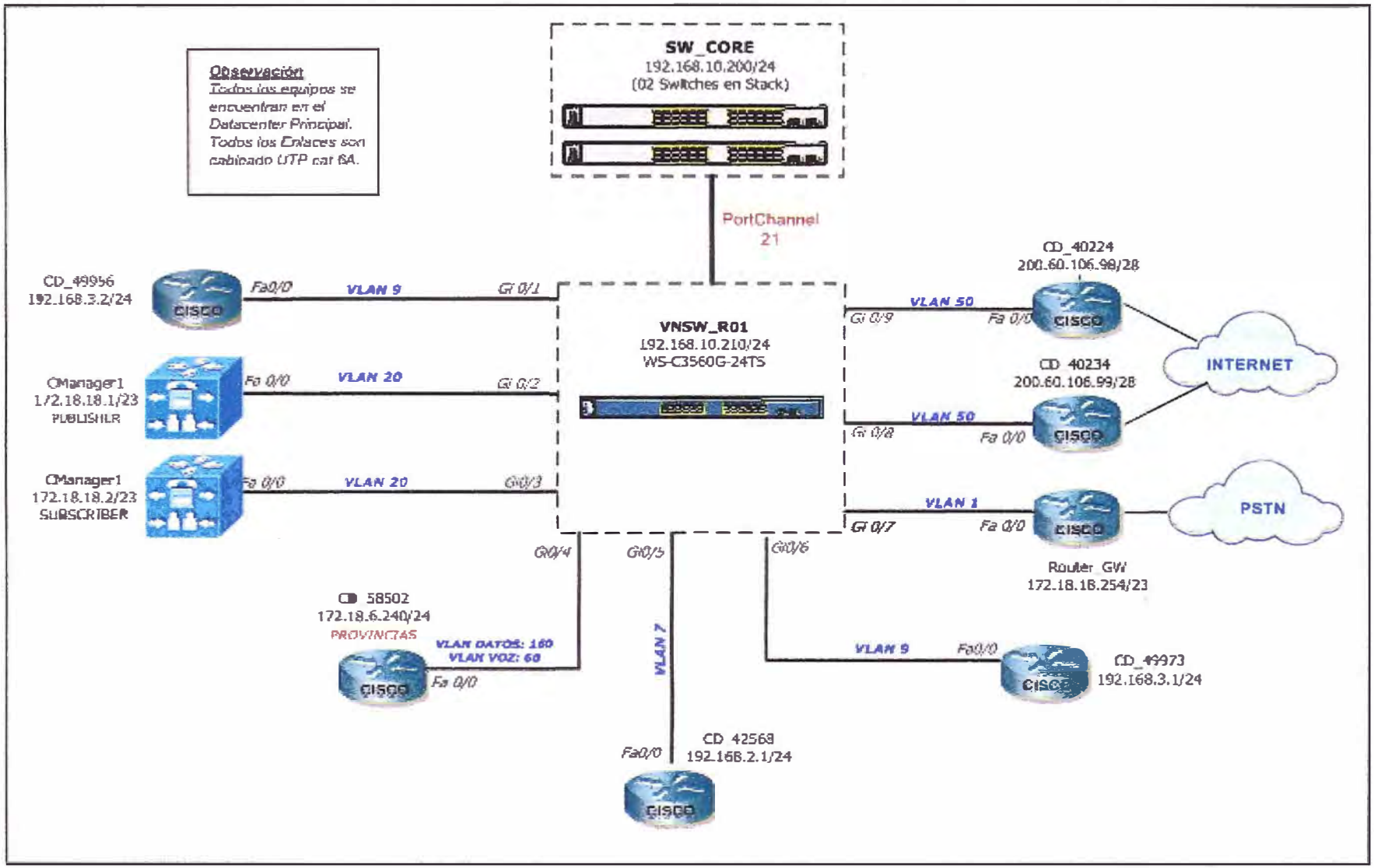

Figura B5 Diagrama de red propuesto para los routers

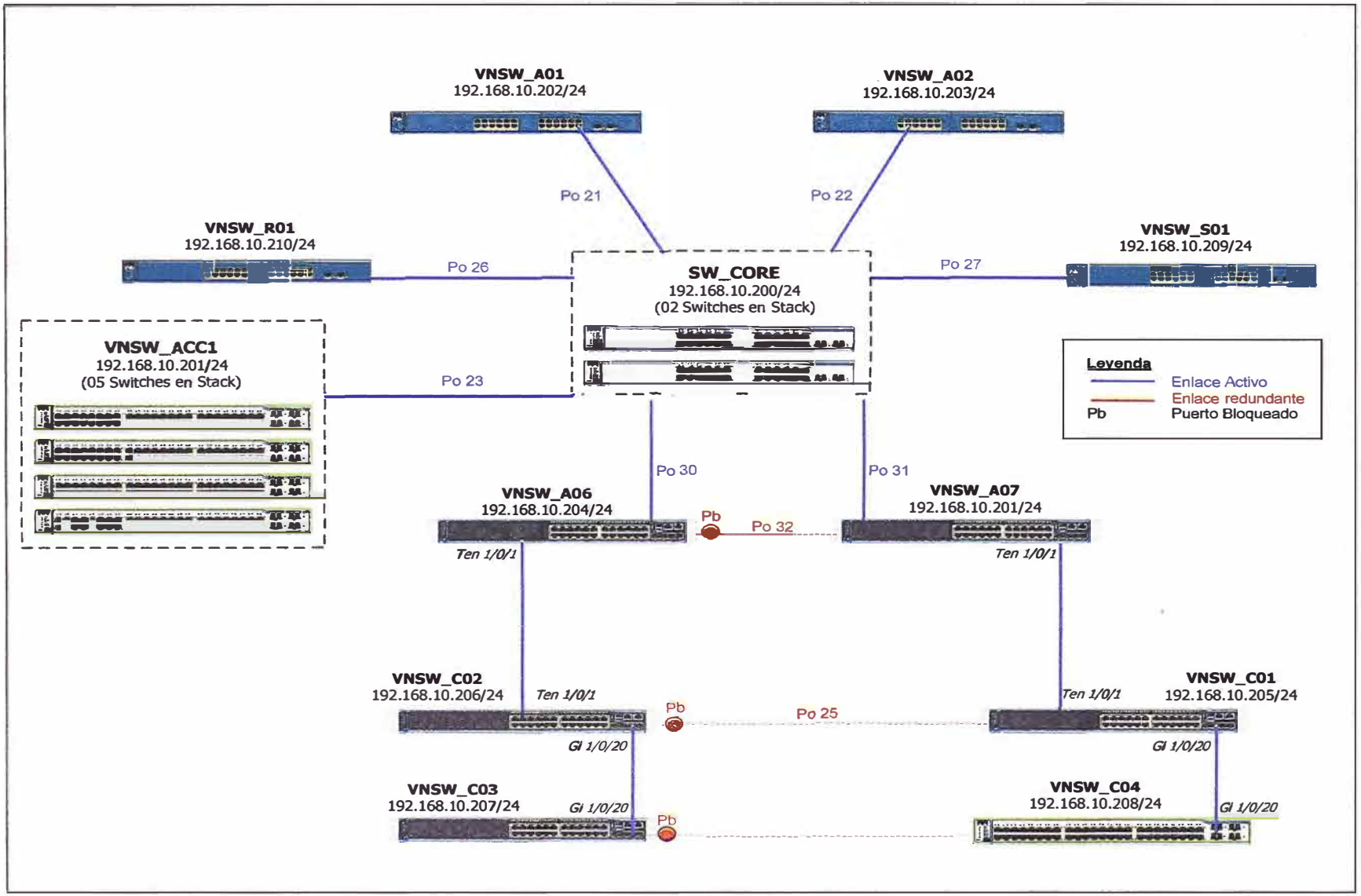

Figura B6 DespliegueProtocoloSpanning-Tree y Etherchannel

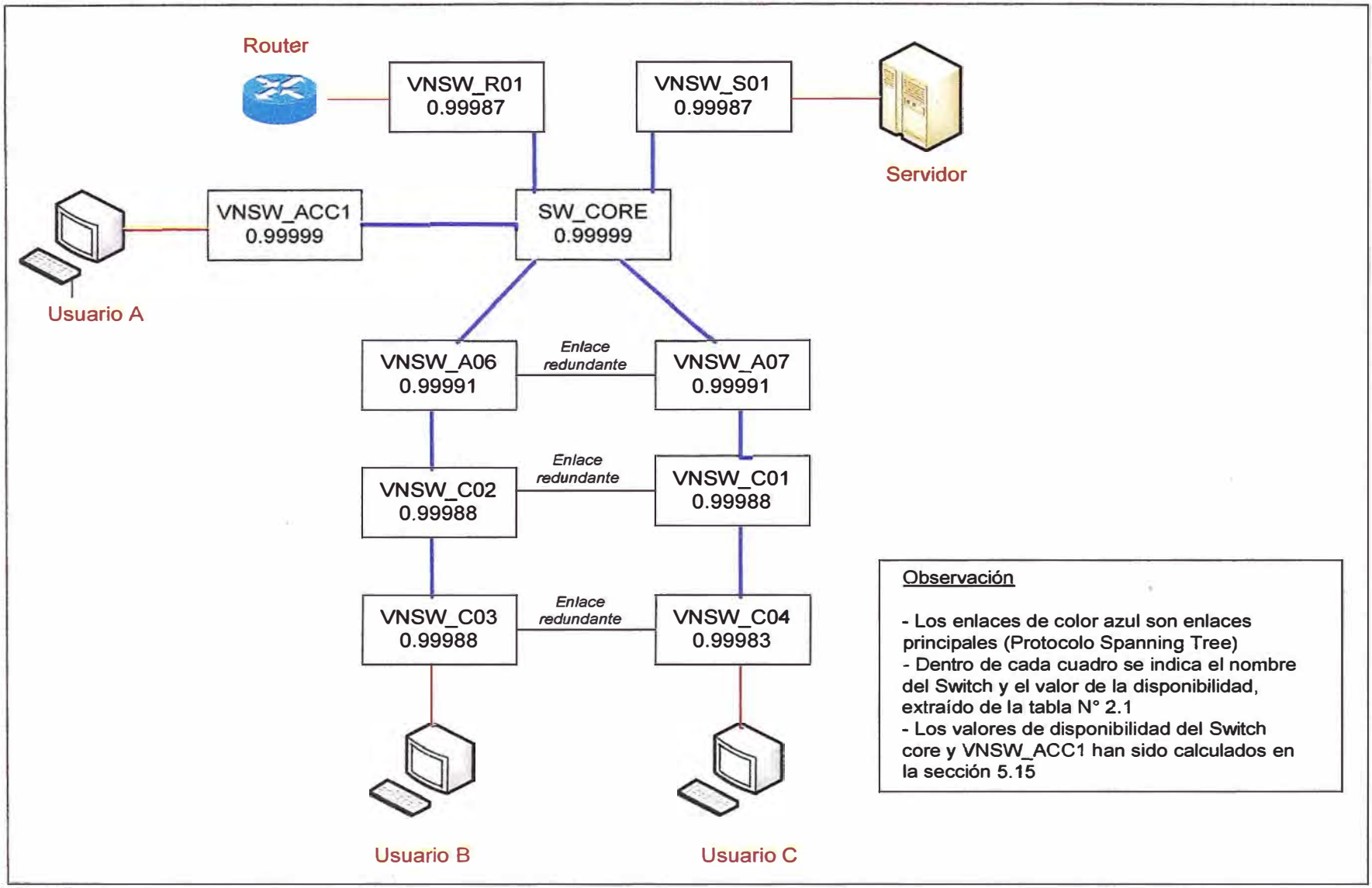

Figura B7 Análisis de disponibilidad de los switches Cisco

ANEXO C
PROCEDIMIENTO ACTUALIZACION IOS SWITCH CORE

1. Descargar la última versión de IOS disponible de la página web del Fabricante. La última versión estable para los Switches 3750 es la 122-55-SE4. Vamos a proceder a instalar el IOS IP Services, el cual contiene soporte capa2 y capa3. El nombre del archivo que vamos a instalar es c3750-ipserviceslmk9-tar.122-55.SE4.tar, el cual tiene funciones HTML para administrar el switch en entorno Web.

2. Configurar una pc que tenga conectividad al switch core.

3. Ingresar vía Web al, y luego ir a la opción Maintenance/Software Upgrade,tal y como se muestra en la figura C1

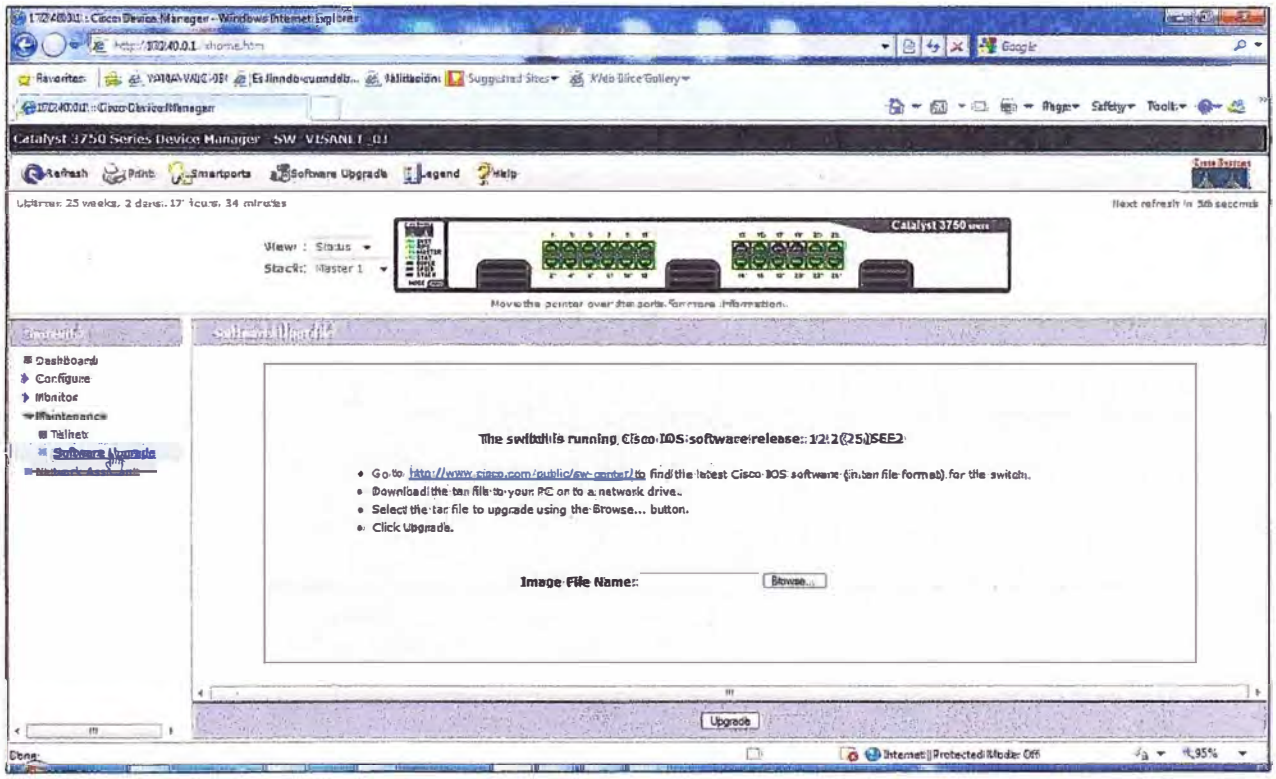

Figura C1 Actualización del switch core

4. Hacer clic en BROWSE, seleccionar el archivo c3750-ipserviceslmk9-tar.122-55.SE4.tar ubicado en el disco duro de nuestra PC y luego hacer click en UPGRADE.Esperar unos 15 minutos para que se complete este proceso, ya que el archivo se debe de copiar en todos los switches del stack y luego descomprimir en la memoria flash de cada uno de los switches.Automáticamente el stack se va a reiniciar y luego va a encender con el nuevo sistema operativo Cisco IOS actualizado.

Verificación del nuevo IOS 122-55.SE4

Para verificar la nueva versión actualizada de los switches, debemos de conectarnos vía consola al equipo y aplicar el siguiente comando:

```
Show switch detail
```

Este comando verifica que todos los Switches estén operativos y funcionando correctamente:

```
3750#show switch detail
                                                    Current
Switch#  Role      Mac Address     Priority     State
-----------------------------------------------------------
 1       Slave     000c.30ae.4f00     9         Ready
*2       Master    000d.bd5c.1680    15         Ready

         Stack Port Status             Neighbors
Switch#  Port 1     Port 2           Port 1   Port 2
-----------------------------------------------------------
  1        Ok         Ok                2        2
  2        Ok         Ok                1        1
```

Show versión

Verifica la versión del sistema operativo del switch:

```
3750#show version
Cisco Internetwork Operating System Software
IOS (tm) C3750 Software (C3750-I5-M), Version 12.2(55)SE4, RELEASE SOFT-
WARE (fc1)
The password-recovery mechanism is enabled.
512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:0D:BD:5C:16:80
Motherboard assembly number     : 73-8307-06
Power supply part number        : 341-0048-01
Motherboard serial number       : CAT073205SU
Power supply serial number      : DTH073004US
Model revision number           : A0
Motherboard revision number     : A0
Model number                    : WS-C3750G-12S-E
System serial number            : CAT0732R0JU
Top Assembly Part Number        : 800-23419-01
Top Assembly Revision Number    : A0
Hardware Board Revision Number  : 0x06
Switch   Ports  Model              SW Version        SW Image
------   -----  -----              ----------        ----------
  1   28     WS-C3750G-24TS     12.2(20)SE       C3750-I5-M
* 2   12     WS-C3750G-12S      12.2(20)SE      C3750-I5-M
```

ANEXO D
CONFIGURACIÓN DEL PROTOCOLO TACACS+

1. Conectarse al switchy eliminar los usuarios activos, dejando únicamente un usuario de privilegio 15, el cual va a funcionar cuando el equipo Cisco ACS este inoperativo.
2. Creamos el usuario genérico nivel 15 de de usuario administrator

```
Username administrator privilege 15 secret ******
```

Este usuario se va utilizar únicamente cuando el servidor TACACS+ este fuera de línea. Mientras el servidor TACACS+ este operativo, no se puede utilizar estas credenciales para ingresar al equipo por ningún modo (consola, telnet o SSH) ya que se encuentra deshabilitado.

3. Configurar los siguientes comandos en todos los switches Cisco:

```
aaa new-model
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting connection default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
tacacs-server host 192.168.10.220
tacacs-server directed-request
tacacs-serverkey ***********
```

4.Ingresar al servidor Cisco ACS y añadir todos los switches en su base de datos, utilizando una contraseña compartida entre el switch y el servidor cisco ACS.
5. Crear grupos de usuarios en el servidor ACS, con lo cual podemos diferenciar los niveles de administración en los switches, por ejemplo podemos crear los siguientes grupos: administradores (Nivel 15), monitores (nivel 5), usuario (nivel 1), etc.
6. Crear usuarios personalizados, los cuales van a estar asociados a un grupo específico definido en el punto 5.
7. Realizar pruebas de funcionamiento.

ANEXO E
CONFIGURACIÓN DEL PROTOCOLO SPANNING-TREE

La configuración del protocolo Spanning-Tree en los switches es la siguiente:

1. Switch SW_CORE

```
spanning-tree mode rapid-pvst
spanning-treeetherchannel guard misconfig
spanning-tree extend system-id
spanning-treevlan2-900  priority 4096
```

2. Switch VNSW_A01

```
spanning-tree mode rapid-pvst
spanning-treeetherchannel guard misconfig
spanning-tree extend system-id
spanning-treevlan2-900  priority 32768
```

3. Switch VNSW_A02

```
spanning-tree mode rapid-pvst
spanning-treeetherchannel guard misconfig
spanning-tree extend system-id
spanning-treevlan2-900  priority 32768
```

4. Switch VNSW_A06

```
spanning-tree mode rapid-pvst
spanning-treeetherchannel guard misconfig
spanning-tree extend system-id
spanning-treevlan2-900  priority 8192
```

5. Switch VNSW_A07

```
spanning-tree mode rapid-pvst
spanning-treeetherchannel guard misconfig
spanning-tree extend system-id
spanning-treevlan2-900  priority 12288
```

6. Switch VNSW_C01

```
spanning-tree mode rapid-pvst
spanning-treeetherchannel guard misconfig
spanning-tree extend system-id
spanning-treevlan2-900  priority 16384
```

7. Switch VNSW_C02

```
spanning-tree mode rapid-pvst
spanning-treeetherchannel guard misconfig
spanning-tree extend system-id
spanning-treevlan2-900  priority 20480
```

8. Switch VNSW_C03

```
spanning-tree mode rapid-pvst
spanning-treeetherchannel guard misconfig
```

```
spanning-tree extend system-id
spanning-treevlan2-900  priority 24576
```

9. Switch VNSW_SRV1

```
spanning-tree mode rapid-pvst
spanning-treeetherchannel guard misconfig
spanning-tree extend system-id
spanning-treevlan2-900  priority 32768
```

10. Switch VNSW_R01

```
spanning-tree mode rapid-pvst
spanning-treeetherchannel guard misconfig
spanning-tree extend system-id
spanning-treevlan2-900  priority 32768
```

11. Switch VNSW_ACC1

```
spanning-tree mode rapid-pvst
spanning-treeetherchannel guard misconfig
spanning-tree extend system-id
spanning-treevlan2-900  priority 32768
```

12. Switch VNSW_C04

```
spanning-tree mode rapid-pvst
spanning-treeetherchannel guard misconfig
spanning-tree extend system-id
spanning-treevlan2-900  priority 28672
```

ANEXO F

NORMA TECNICA PERUANA NTP-ISO/IEC 27001:2008

La Norma Técnica Peruana NTP-ISO/IEC 27001:2008 fue elaborada por el Comité Técnico Permanente de Codificación e Intercambio Electrónico de Datos (EDI) durante los meses de Mayo y Octubre del año 2008, utilizando como antecedente la ISO/IEC 27001:2005 InformationTechnology Security techniques– Informationsecuritymanagementsystems – Requirements.

Esta norma fue publicada por INDECOPI el 11 de Enero del 2009 y reemplaza a la norma NTP 821.101:2005 EDI. Sistema de gestión de seguridad de la información. La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada de acuerdo a las Guías Peruanas GP 001:1995 y GP 002:1995.

Esta Norma Técnica Peruana de seguridad de la información ha sido preparada con el fin de ofrecer un modelo para estableces, implementar, operar, monitorear, mantener y mejorar un efectivo Sistema de Gestión de seguridad de la información (ISMS: Information Security Management System). La adopción de un ISMS debe ser una decisión estratégica para una organización. El diseño e implementación del ISMS de una organización está influenciado por las necesidades y objetivos del negocio, requisitos de seguridad, procesos, tamaño y estructura de la Organización. Esta Norma Técnica Peruana puede usarse en el ámbito interno y externo de las organizaciones.

Es intención de la empresa certificarse en esta norma, con la finalidad de brindar seguridad y confiabilidad a sus clientes. Este es un proyecto que se está programando luego de la implementación de este trabajo, y para esto la empresa debe cumplir con una serie de requisitos que implica tanto a la Gerencia General de la Empresa, como al área de seguridad y red de datos. Los ítems que hemos abordado en este trabajo se detallan en las siguientes tablas, las cuales son un resumen de los requisitos para pasar el proceso de Certificación, y han sido extraídas del anexo A de la Norma Técnica Peruana, la cual se puede adquirir en las oficinas de INDECOPI.

Tabla F.1 Gestión de seguridad de redes

A.10.6 Gestión de seguridad de redes Objetivo de Control: Asegurar la salvaguarda de información en las redes y protección de la infraestructura de soporte.			
A.10.6.1	Controles de red	Control Se implementara un conjunto de controles para lograr y mantener la seguridad en las redes y mantener la seguridad de los sistemas y aplicaciones usuarios de la red, incluyendo la información de transito	Observación Para cumplir este item estamos creando una VLAN de gestión de equipos para que solo el personal autorizado pueda acceder. Así también hemos reforzado las políticas de contraseñas e implementación del protocolo TACACS en los equipos. Se sugiere también el uso del protocolo Port-Security.
A.10.6.2	Seguridad de los Servicios de red	Control Se deben identificar e incluir en cualquier acuerdo de servicio de red los aspectos de seguridad, niveles de servicio y requisitos de gestión, así estos servicios sean provistos interna o externamente.	Observación Para la seguridad de la gestión de los equipos de comunicaciones, se ha creado una VLAN de gestión de equipos, la cual solo tiene acceso personal autorizado. Se sugiere la implementación del protocolo port-security en los switches.

Tabla F.2 Gestión de monitoreo

A.10.10 Monitoreo Objetivo de Control: Detectar actividades de procesamiento de información no autorizadas			
A.10.10.1	Registro de auditoria	Control Se deben producir y guardar por un periodo acordado, los registros de auditoria que registran las actividades de los usuarios, excepciones y eventos de seguridad, con el fin de asistir investigaciones futuras y el monitoreo de control de acceso.	Observación Para cumplir este item, se está instalando el equipo ACS, detallado en la sección 5.14 del presente documento.
A.10.10.4	Registros de administrador y operador	Control Las actividades del administrador y operador deben ser registradas.	Observación Para cumplir este item, se está instalando el equipo ACS, detallado en la sección 5.14 del presente documento.
A.10.10.6	Sincronización de reloj	Control Los relojes de todos los sistemas relevantes de procesamiento de información dentro de la organización deben estar sincronizados con una fuente de tiempo actual acordado.	Observación Se recomienda la instalación de un servidor NTP (Protocolo de tiempo de red) en la red interna del cliente y sincronizar todos los equipos con este equipo. Los equipos mencionados en este trabajo soportan el protocolo NTP.

Tabla F.3 Requisitos para el control de acceso

A.11 Requisito de negocio para el control de accesos Objetivo de Control: Controlar los accesos de información			
A.11.1.1	Políticas de control de acceso	Control Se debe establecer, documentar y revisar una política de control de accesos, basado en requisitos de acceso y seguridad del negocio.	Observación Para cumplir este item, se está instalando el equipo ACS, detallado en la sección 5.14 del presente documento.
A.11.2.2	Gestión de privilegios	Control Se registrara y controlara la asignación y uso de privilegios.	Observación Para cumplir este item, se está instalando el equipo Cisco ACS. En este equipo se puede definir privilegios para los usuarios, así como integrarlo con los controladores de dominio.
A.11.2.3	Gestión de contraseñas de usuario	Control Se controlara la asignación de contraseñas a través de un proceso de gestión formal.	Observación Como parte del cumplimiento de este item, podemos mencionar que el equipo ACS instalado tiene políticas de contraseñas que hemos configurado. Se recomienda hacer lo mismo en los servidores controladores de dominio.
A.11.3.1	Uso de contraseñas	Control Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.	Observación Como parte del cumplimiento de este item, podemos mencionar que el equipo ACS instalado tiene políticas de contraseñas que hemos configurado. Se recomienda hacer lo mismo en los servidores controladores de dominio.

Tabla F4 Control de acceso a los sistemas operativos

A.11.5 Control de acceso al sistema operativo Objetivo de Control: Prevenir accesos no autorizados a los sistemas operativos.			
A.11.5.1	Procedimientos seguro de conexión	Control Se usura un proceso de registro de conexión (login) seguro para acceder a los servicios de información.	Observación Con la implementación del protocolo SSH en los equipos de comunicaciones se cumple este requisito. Todos los equipos de Networking solicitan un usuario (login) y password.
A.11.5.2	Identificación y autenticación del usuario	Control Todos los usuarios tienen un identificador propio y exclusivo para sus actividades y debe elegirse una técnica de autenticación adecuada para sustentar la identidad del usuario.	Observación Para cumplir este ítem, se está instalando el equipo ACS, detallado en la sección 5.14 del presente documento. En el equipo ACS se definen los usuarios que acceden a los equipos de comunicaciones.
A.11.5.3	Sistema de gestión de contraseñas	Control Sistema de gestión de contraseñas proveerán medios efectivos e interactivos, cuyo objetivo es asegurar contraseñas de calidad.	Observación Como parte del cumplimiento de este ítem, podemos mencionar que el equipo ACS instalado tiene políticas de contraseñas que hemos configurado.
A.11.5.5	Desconexiónautomática de terminales	Control Las sesiones inactivas deben cerrarse luego de un periodo definido de inactividad.	Observación Se ha configurado en los equipos de comunicaciones parámetros de tiempo de espera. Se recomienda extender este procedimiento en los demás equipos y servidores de la empresa.
A.11.5.6	Limitación de tiempo de conexión	Control Se usara restricciones de tiempo de conexión para ofrecer seguridad adicional para las aplicaciones de alto riesgo	Observación Se ha configurado en los equipos de comunicaciones parámetros de tiempo de espera. En esta secciónтambién se explica la configuración de los tiempos de conexión y de bloqueo.
A.11.6.2	Aislamiento de sistemas sensibles	Control Los sistemas sensibles tendrán un ambiente de computo dedicado (aislado).	Observación Se ha configurado la VLAN de gestión en la red LAN del cliente, para aislar la gestión de los equipos de comunicaciones. Esta VLAN es bloqueada en el firewall para que no tenga acceso externo y así evitar intrusiones. Asimismo solo pueden acceder los administradores de red y usuarios de soporte técnico.

BIBLIOGRAFÍA

[1] INDECOPI, Página institucional http://www.indecopi.gob.pe

[2] Norma Técnica Peruana NTP 821.101:2005, INDECOPI, Página institucional http://www.indecopi.gob.pe/NTP

[3] Digital Communications: Fundamentals &Applications, Pearson Education, 2009.

[4] Cisco CCNA Switching, Official Cert Guide, Wendell Ondom, 2013.

[5] Cisco CNP SWITCH 642-813 Official Certification Guide, David Hucaby,2013.

[6] Cisco, "Datasheet Switch Catalyst 2960" Cisco Technologies.

[7] Cisco, "Datasheet Switch Catalyst 3560", Cisco Technologies.

[8] Comunicaciones y redes de computadoras, Prentice Hall, 2001

[9] Routing, Flow, and Capacity Design in Communication and Computer Networks, Morgan Kaufmann, 2004.

[10] Cisco, "Implementing AAA using Cisco ACS and Tacacs+", Pickenfield Publishing, 2013.

[11] Cisco CCNP Routing and Switching Oficial Certification, David Hucaby and Kevin Wallace, 2011.

[12] Cisco CCNP Switch 642-813, Oficial Certification Guide, David Hucaby, 2011.

[13] Cisco CCNP Tshoot 642-832, Oficial Certification Guide, Kevin Wallace, 2011.

[14] Computer Networking: A top Down Approach (6ta Edicion), James F. Kurose and Keith W. Ross, 2012.

[15] Principles of Information Security (4ta Edicion), Michael E. Whitman and Herbert J. Mattord, 2011.

[16] CISCO, Pagina web http://www.cisco.com

[17] Applied Information Security, Randy J Boyle, July 26, 2009.

[18] Networking Essentials (3rd Edition), Jeffrey S. Beasley and Piyasat Nilkaew , 2012.

[19] A Practical Guide to Advanced Networking (3rd Edition) Jeffrey S. Beasley, 2013.