DISEÑO RED LAN SEDE PSECO

Miguel Angel Rubiano Perilla

Ingeniería de Telecomunicaciones

Pedro Enrique Guerrero

INSTITUTO TECNOLÓGICO METROPOLITANO

28/09/2015

RESUMEN

El despliegue de servicios de red corporativos a generado diferentes modelos de servicio con una amplia cantidad de variables según la criticidad de las aplicaciones en las redes donde se brinda escalabilidad, adaptabilidad y facilidad de administración.

El comportamiento del mercado de los Contact Center, su alta rotación de personal, servicios críticos de voz para la atención de llamadas y volúmenes de tráfico determinan condiciones exclusivas de networking y switching, mediante el análisis de dichos requerimientos y bajo el modelo metodológico de diseño de redes de Cisco hemos logrado dimensionar los equipos y modelos de configuración necesarios para el diseño de la red LAN en la sede PSeco de Allus basados en la estructura jerárquica de la red y el modelo OSI.

El análisis de las aplicaciones, servicios y alta disponibilidad fijaron las condiciones de red para las diferentes capas de la topología de red, En el Core se definió un modelo de alta disponibilidad con 2 enlaces hacia el data center bajo infraestructuras diferentes, en la capa de distribución se brindará la alta disponibilidad a través de una estrella en malla con conexión a los 2 Switchs Core, en la capa de acceso se inicia la aplicación de políticas de QoS para el tráfico de voz política que se implementará durante las diferentes capas del modelo.

El diseño de las políticas de seguridad PCI-DSS se define a través de las listas de control de acceso que se implementan en los Switchs Core limitando el acceso a recursos de red.

Bajo estas premisas se definió el modelo de diseño y topología de red cumpliendo con los requerimientos exigidos por Allus para sus clientes, esperamos que la sede PSeco sea implementada bajo los estándares de calidad propuestos que garantizarán un servicio de red óptimo a los clientes de Allus.

Dentro del plan de mejoras se tiene proyectado sugerir el cambio de configuración de vlan por puerto a vlan por MAC para disminuir costos operativos por los traslados y facilitar los procesos administrativos de la red.

RECONOCIMIENTOS

Dedico este trabajo de grado a mis familiares y amigos los cuales me han brindado un apoyo incondicional durante toda mi vida, quiero dar una dedicatoria especial a mi hijo Alejandro Rubiano quien con su amor y cariño me motivan para trabajar, superarme y cumplir mis sueños día tras día.

Un capítulo especial de esta dedicatoria es para mí asesor de trabajo de grado, los docentes y personal del ITM centro de sabiduría y generador de conocimiento los cuales durante mi vida universitaria me brindaron las herramientas para mi crecimiento moral, ético e intelectual.

ACRÓNIMOS

***ACD** tiempo de conexión de los asesores la cual es la base de facturación a los clientes*

***ACL** Access Control List*

***CPU** Central Processing Unit*

***DHCP** Dynamic Host Configuration Protocol*

***DWDM** Dense Wavelength Division Multiplexing*

***EIGRP** Enhanced Interior Gateway Routing Protocol*

***HSRP** Hot Standby Router Protocol*

***IP** Internet Protocol*

***L2L** LAN to LAN*

***LAN** Local Area Network*

***OSI** Open System Interconnection*

***OSPF** Open Shortest Path First*

***PCI-DSS** Payment Card Industry Data Security Standard*

***SNMP** Simple Network Management Protocol*

***TCP** Transmission Control Protocol*

***VLAN** Virtual LAN*

***WAN** Wide Area Network*

PDIOO Modelo de diseño de red de Cisco

TABLA DE CONTENIDO

INTRODUCCIÓN

Las compañías de contact center ofrecen tercerización de servicios y procesos a los clientes corporativos entre ellos servicios de back office, soluciones de almacenamiento, telemarketing, soporte técnico y se especializan en mejorar las interacciones de las compañías con los clientes finales, constantemente se presentan a licitaciones donde cada licitante esgrime sus mejores razones financieras, técnicas y de experticia en el negocio para que le sea adjudicado el contrato.

Anteriormente después de asignada la licitación se disponía de tiempos razonables para la implementación de los servicios de telecomunicaciones para la atención de los nuevos clientes, con la baja rotación de los clientes en los diferentes contact center el mercado presentaba una relativa estabilidad lo que permitía que se diera esa situación, hoy en día se tienen una nueva dinámica y reto para los contact center es que estas implementaciones se den de una manera rápida bajo las premisas de la eficiencia y eficacia.

Los contact center actualmente tiene alta rotación de personal para las campañas cortas de los clientes, eso implica la implementación de sedes satélites con altos costos de arrendamiento y sus respectivos enlaces de telecomunicaciones.

Para brindar una solución ágil a estos nuevos retos Allus construirá la sede PSeco y bajo los siguientes objetivos esperamos la implementación de la misma.

OBJETIVOS

Objetivo general

Diseñar la red LAN para la sede PSeco de Allus que permita a los usuarios tener acceso a las aplicaciones de los diferentes clientes corporativos.

Objetivos específicos

Determinar el modelo de conectividad de los enlaces contra la sede Berrio donde está ubicado el data center y el esquema de continuidad a través de un anillo L2L.

Diseñar la topología de red para la sede PSeco y sus dispositivos de networking y Switching.

Determinar las políticas de PCI para garantizar la integridad de la información en la red.

Registrar los equipos de red para el monitoreo en la herramienta CACTI y PRTG.

La fusión de los conceptos del marco teórico, los requerimientos de tráfico y políticas de servicio en la red brindaron las bases de conocimiento para el diseño de la red y definen los esquemas de continuidad de servicio en los enlaces L2L por medio de fibras en tecnologías de acceso diferentes con rutas diversas para alta disponibilidad y conmutación automática

en la red de transmisión, 2 switchs core principal y backup en la sede PSeco y el data center Berrio.

A nivel de la capa de distribución es necesario garantizar la alta disponibilidad de la red con conexiones redundantes hacia los switchs Core y en la capa de acceso estará permitido el acceso a los recursos de red, es la interfaz de comunicación de los usuarios con los servicios y aplicaciones alojadas en los servidores, a través de las políticas de QoS para la voz como servicio core del negocio para la atención de llamadas determinaron la prioridad más alta de tráfico en las políticas de QoS y seguridad por medio de PCI-DSS exigencia de Allus y los clientes corporativos para el diseño e implementación del servicio.

El monitoreo se efectuará a través de las herramientas CACTI y PRTG las cuales brindan información del estado de conectividad de los equipos y los enlaces bajo el protocolo SNMP.

Los resultados obtenidos durante la elaboración de la tesis y en particular en la metodología de diseño de Cisco PPDIOO evidenciaron la criticidad de los servicios de voz, la política de QoS a implementar para garantizar la prioridad en la red son aspectos fundamentales del servicio, el monitoreo se constituye en una herramienta fundamental para garantizar la estabilidad de la red y poder detectar de una manera proactiva los incidentes sin esperar el reporte de falla de la operación, la generación de tickets, evaluar las causas de la afectación y los planes acción para evitar nuevamente incidentes por la misma causa.

Como acción futura se recomienda a Allus cambiar el esquema de asignación de vlans por puerto a Vlan por MAC, los movimientos frecuentes de las operaciones entre sedes, crecimientos de clientes, cierre de campañas, las políticas de antivirus y asignación de licencias de telefonía para las plataformas Avaya y Nortel las cuales se asocian a la MAC de los equipos es más expedita que la configuración actualmente implementada, adicionalmente los beneficios que se obtienen en la reducción de costos de nomina por concepto de horas extras del personal técnico e ingenieros que realizan y acompañan estas actividades que frecuentemente se realizan en la noche y los fines de semana.

MARCO TEÓRICO

Las medianas y grandes compañías hoy en día necesitan modelos de redes que garanticen que el trafico sensible y crítico para las operaciones este priorizado en la red ,que los enlaces no se saturen, también se requiere garantizar la seguridad de la información estos son solo algunos de los conceptos que se deben tener en cuenta al momento de diseñar e implementar redes LAN entre ellos se debe tener claro conceptos como el modelo OSI, las capas de la arquitectura de red, Direccionamiento IP, vlans, ACL, políticas de seguridad basadas en PCI, Protocolos de enrutamiento, topologías de red, trafico entre otras para poder realizar el dimensionamiento adecuado de una red.

MODELO OSI

El modelo OSI (Open System Interconnection) es un esquema de lineal de 7 capas, cada capa provee servicios particulares en la red y maneja una relación directa con las capas adyacentes.

7	APLICACIÓN
6	PRESENTACION
5	SESION

4	TRANSPORTE
3	RED
2	ENLACE
1	FISICA

Ilustración 1 (Elaboración propia)

El modelo OSI está basado en protocolos, las 4 capas más bajas Transporte, red, enlace de datos y física definen el modelo de comunicación de las capas superiores.

La capa Física es el nivel más bajo del modelo de OSI o la primera capa, incluye los medios de comunicación de redes físicas, tales como un cable o conector de acoplamiento. El protocolo de capa física y la tensión generada con el fin de enviar y recibir señales y transportar datos. La capa física proporciona la activación, mantenimiento, una estrecha comunicación entre el punto final de propiedades mecánicas, propiedades eléctricas y las características del proceso.

(Yadong Li, Wenqiang Cui, Danlan Li, & Rui Zhang, 2011a)

La capa Enlace de datos es la segunda capa, controla la comunicación entre la capa de red y la capa física, algunos dispositivos conectados como los switchs decodifican la trama para enviar la información al destino correcto así trabaja la capa de enlace.

La función principal de la capa de enlace de datos es volver la transferencia de datos que es poco fiable en la capa física a fiable en la capa de enlace de datos, a fin de garantizar la transmisión recibida desde la capa de red.

El frame se utiliza para mover la estructura de datos de paquete, que incluye no sólo los datos en bruto, sino también el origen y la mac de destino, los errores de información, sus parámetros característicos incluyen : la dirección física, la topología de red, mecanismo de detección de errores, la clasificación de transmisión de tramas de datos y control.

(Yadong Li, Wenqiang Cui, Danlan Li, & Rui Zhang, 2011b)

La capa de red tiene en cuenta la prioridad de transmisión, nivel de congestión de la red, la calidad de servicio y enrutamiento por un enlace, la transferencia de datos se realiza de una manera inteligente basada en el esquema de direccionamiento o protocolos de enrutamiento, la función principal de la capa de red es completar la transmisión de paquetes entre los host, los protocolos de capa de red son : EIGRP, RIP, OSPF, IP, IPX

(Yadong Li, Wenqiang Cui, Danlan Li, & Rui Zhang, 2011c)

La capa de transporte es la capa más importante del modelo OSI, la capa de sesión y la capa de transporte determinan los servicios para los usuarios, la mejor conexión es la cual donde no se presentan errores en el transporte de los datos, la capa de transporte de conformidad con el tamaño máximo de la red puede manejar paquetes grandes que obligarán a la división. Los protocolos de la capa de transporte TCP / IP del TCP. La función principal de la capa de transporte es garantizar la comunicación de datos confiable entre diferentes usuarios, incluyendo el protocolo de recuperación de errores.

(Yadong Li et al., 2011b)

La capa de sesión es responsable de que los dos host de la red establezcan y mantengan la comunicación. Define cómo iniciar, controlar y poner fin a una sesión, incluyendo el número de horas de control y gestión de dos vías con el fin de completar sólo una parte de un mensaje continuo puede informar a la aplicación y termina las sesiones entre entidades de la capas de presentación.

(Yadong Li et al., 2011b)

Capa de presentación, las capas de aplicación y de red son las traductoras entre la red de datos y puede ser entendido de acuerdo con el formato de los programas; Este formato también es utilizado por la red debido a los diferentes tipos y define una serie de códigos y la conversión de código para asegurar los datos de origen y destino. La función principal

de la capa de presentación es encriptar y desencriptar los datos. Esta capa asegura que la información será recibida entre aplicaciones de los sistemas.

(Yadong Li et al., 2011c)

La capa de aplicación es la capa de más alto nivel orientada al usuario, las aplicaciones de software en la red a través de un diálogo directo con los usuarios, establece la comunicación entre sí, identifica los recursos disponibles y la sincronización, es la capa de aplicación para el sistema operativo es la interfaz de comunicación entre usuario y computadora. Los protocolos determinan la sincronización de comunicaciones algunos de estos protocolos son telnet, SMTP, FTP, HTTP, POP3.

(Yadong Li et al., 2011c)

Estructura de red

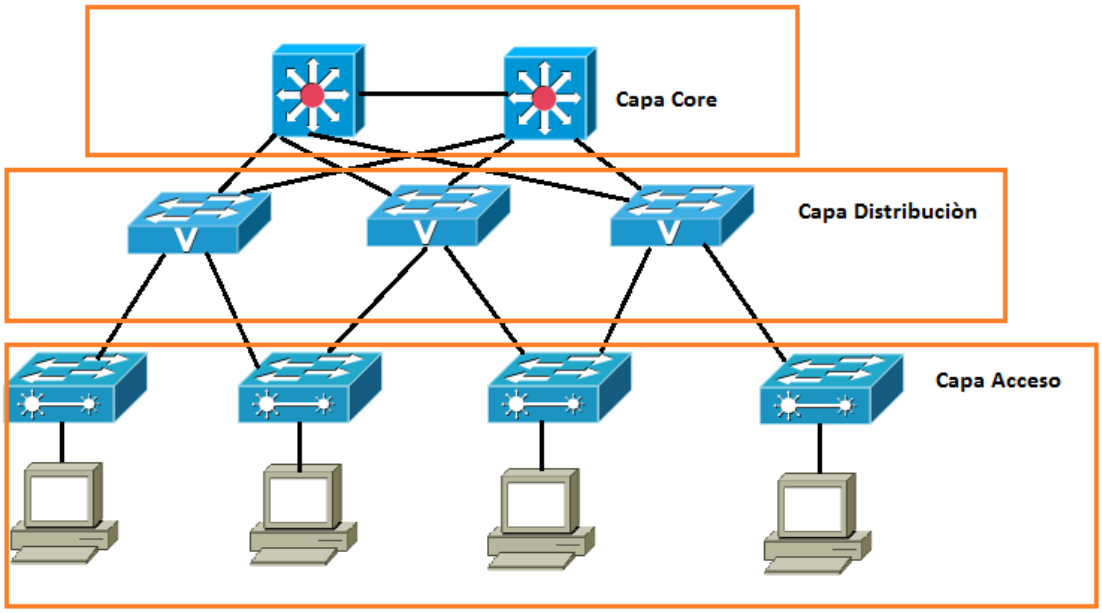


***Figura 1*. Estructura de** red**. (Elaboración propia a partir de iconos Cisco)**

La figura 1 muestra la estructura de red con las capas core, distribución y acceso

La capa de acceso de red es el punto en el cual los usuarios finales son conectados a la red. El tráfico hacia y desde los recursos locales están vinculados directamente entre los recursos de red, switchs y usuarios finales.

La capa de distribución marca el punto entre la capa de acceso y el core, manipula paquetes mediante ruteo, filtrado y acceso WAN. La capa de distribución proporciona conectividad basada en políticas, porque determina como pueden acceder al core o al

backbone. Determina el camino más rápido para una petición de usuario, una vez que la capa de distribución decide la trayectoria se envía la petición a la capa core.

La capa core o backbone tiene como función switchear el tráfico rápidamente. El tráfico que cursa son los servicios de usuarios (e-mail, acceso a internet, videoconferencia).

(«Educarchile», s. f.)

Las VLANs ofrecen beneficios significativos en términos de eficiencia y uso de ancho de banda con ellas de disminuye el trafico de broadcast, flexibilidad, rendimiento y seguridad. Las VLANs Segmentan lógicamente la red en diferentes dominios de difusión, las vlans son subredes lógicas independientes que se encuentran bajo una misma red física, para que los paquetes solamente se conmuten entre los puertos designados para la misma VLAN proporcionan seguridad de la información al tratarse de redes independientes, este enfoque también mejorar la escalabilidad particularmente en LAN.

(Rajaravivarma, 1997)

Los Switchs son uno de los componentes de las comunicaciones de VLAN ellos son la puerta de entrada para el final de la estación y las comunicaciones en toda la empresa los enfoques más comunes para la agrupación lógica de VLANs se agrupa en funciones

administrativas, el filtrado de paquetes es una técnica que examina el campo de identificación del paquete o Tag de la VLAN en la trama definida por el administrador del Switch para cada paquete.

(Rajaravivarma, 1997)

Si un host se mueve de un SW a otro es muy probable que su dirección IP cambie por una IP no valida y el administrador de la red deberá configurar el puerto con la vlan adecuada

La comunicación entre las vlans se proporciona a través de un dispositivo de enrutamiento capa 3 para optimizar los servicios de las vlans lo ideal es troncalizar los puertos que tienen conectividad al router o switch multicapa con el switch capa 2.

Hay varias formas de crear una VLAN:

VLAN basada en puerto: es la forma más simple de VLAN. En este modelo de VLAN la agrupación de puertos de conmutación se realiza en el switch.

VLAN basada en MAC: La dirección MAC de origen se encuentra asociada a una VLAN este enfoque resuelve algunos de las limitaciones de las vlans basadas en puertos.

VLANS basadas en puerto: La VLAN permiten que una subred se difunda a través de un número de puerto esto proporciona una buena flexibilidad y es más fácil de manejar que las VLAN basadas en MAC.

Las VLAN Basadas en políticas: Son más flexibles, asignan a los dispositivos VLAN utilizando políticas establecidas en la red de gestión, que se aplica a todos los switchs.

(Rajaravivarma, 1997)

Estructura de Vlans

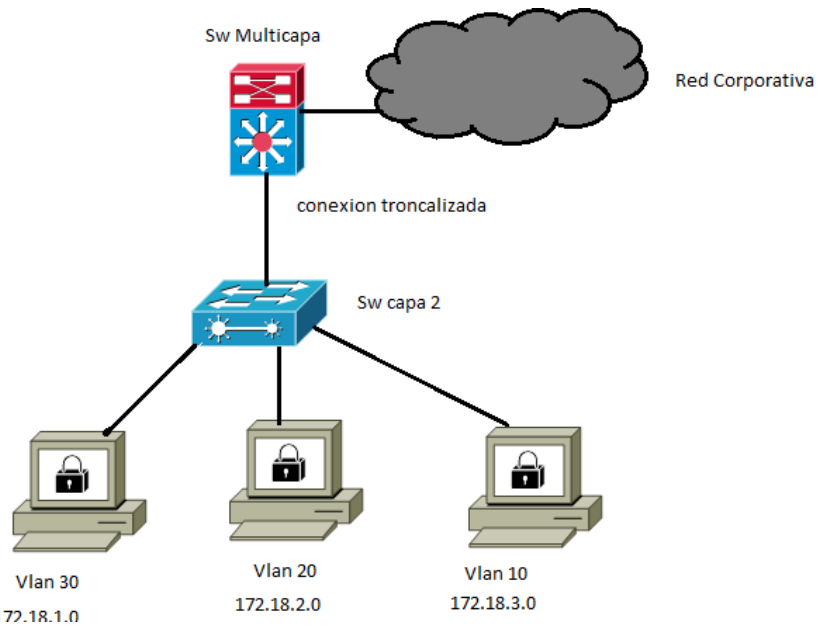


Figura 1. **Estructura de Vlans. Elaboración propia a partir de íconos Cisco**

Figura 2. La imagen muestra el modelo de conexión para las diferentes vlans

PCI-DSS

Visa y Mastercard han emitido un compendio de normas para garantizar la seguridad e integridad de la información de los usuarios conocida como el estándar PCI-DSS las normas buscan garantizar que no se presenten fugas en la información de los clientes. La seguridad digital está definida como las medidas de privacidad digital implementadas para evitar los accesos no autorizados a las computadoras, bases de datos y sitios web mediante la aplicación de políticas, directivas, mecanismos de seguridad, constante evaluación de riesgos y huecos de seguridad para evitar ataques y filtración de la información critica de los clientes.

(Talib, Khelifi, & Ugurlu, 2012)

Para PCI versión 3.0

Requerimientos:

Construir y Mantener una red segura	Instalar y Mantener un Firewall
	No emplear parametros de seguridad y usuarios del sistema por defecto
Proteger los datos de las tarjetas	Proteger los datos almacenados en las tarjetas
	Cifrar la transmision de datos de tarjetas en redes abiertas o publicas
Mantener un programa de gestion de vulnerabilidades	Usar y actualizar constantemente un software antivirus
	Desarrollar y mantener de forma seguridad sistemas y aplicaciones
Implementar medidas de control de acceso	Restringir el acceso a la informacion según need to know
	Asignar un unico ID a cada usuario de la red para trazabilidad de transacciones
Monitorizar y testear frecuentemente las redes	Restringir el acceso fisico a la informacion de las tarjetas
	Auditar y monitorear todos los accesos a los recursos de red y datos de la s tarjetas
Mantener una politica de seguridad de la informaciòn	Testear de forma regular la seguridad de los sistemas y procesos
	Mantener una politica que gestione la seguridad

Ilustración 2 (Elaboración propia)

En la ilustración 2 se especifican políticas y actividades de PCI para aplicar en las redes corporativas que buscan mitigar el riesgo, responsabilidades y costes potenciales en caso de fraudes o incidentes con la información financiera y critica de los clientes, genera confianza a los clientes ante el uso de buenas prácticas de seguridad, facilita el uso de estándares de privacidad y seguridad.

PCI-DSS 3.0 se ha desarrollado para facilitar la medición de seguridad de los datos de tarjeta de crédito a nivel mundial. Las normas no buscan ir en contradicción de las normas establecidas en los países, más bien busca complementar y apoyar las políticas ya establecidas, el firewall es un dispositivo que controla el trafico entre la red interna y externa, a nivel interno también se pueden proteger los servidores críticos que contiene información de los clientes.

(Shihab & Misdianti, 2014)

Para evitar intrusiones se recomienda no utilizar contraseñas por defecto o predeterminadas a demás le permite realizar la trazabilidad de las transacciones, es recomendable la utilización de métodos de cifrado que garanticen que el intruso requiera violar mecanismos adicionales como las claves de encriptación.

(Shihab & Misdianti, 2014)

Con el paso del tiempo han aumentado el número de aplicaciones y recursos que exponen la red a diferentes tipos de ataques, los seguimientos realizados a las organizaciones revelan que los ataques se están dando también desde el interior de las compañías las ACL (Listas de control de acceso) son sentencias que se configuran en los routers y switchs capa 3 los cuales permiten o deniegan el tráfico entre los host por lo tanto se hace importante el control de tráfico en la red interna para garantizar la seguridad y el uso óptimo del ancho de banda en la red. La complejidad de las sentencias depende del tamaño de la red, los parámetros que se controlan y la dependencia entre ellas, es muy importante que se configuren las sentencias de una manera adecuada se debe realizar monitoreo a los indicadores de los equipos en términos de CPU y procesamiento porque se pueden ver afectado el performance de los equipos y en consecuencia se terminan afectando servicios a nivel general en la red.

(Liu, Torng, & Meiners, 2011)

Los usuarios pueden tener configuraciones de permitir y denegar acceso a los servicios por lo general se configuran por zonas o unidades lógicas (vlans) de estaciones de red o servidores, los servicios están asociados a puertos los cuales son configurados en las sentencias, las reglas pueden ser permanentes o temporales su comportamiento esta dado en la medida que las estáticas no varían en el tiempo mientras que las temporales incluyen el factor tiempo y rangos de puertos.

(Maity, Bera, & Ghosh, 2012)

METODOLOGÍA

La metodología seleccionada para el diseño de red es PPDIOO, toda la infraestructura del cliente es CISCO adicionalmente el motor de enrutamiento para las sedes es EIGRP el cual es un estándar abierto por Cisco para que las empresas puedan operar sin restricciones por el uso de diferentes proveedores.

Metodología Cisco Diseño de red PPDIOO

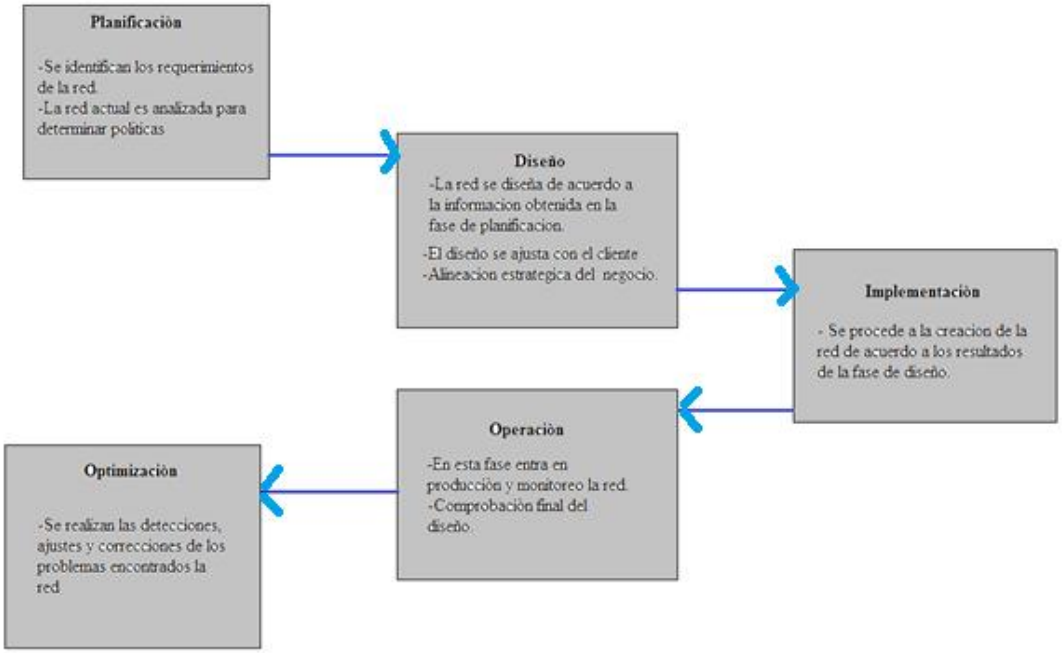


Figura3. Metodología Cisco Diseño de red PPDIOO. **Elaboración propia**

buscamos proveer el diseño más adecuado para la nueva sede PSeco de Allus, la estructura metodológica se tomó teniendo en cuenta los requerimientos de Allus, la estructura jerárquica de red, el modelo OSI y requerimientos de alta disponibilidad de servicios.

Planificación

En esta fase del modelo identificamos al cliente, sus expectativas las características de la red y el contexto general de la compañía, Multienlace es una empresa líder en el mercado de contact center y BPO especializada en la tercerización de servicio a clientes corporativos para la atención de usuarios finales tiene una red para 13000 usuarios en todo el país, los usuarios de la red son representantes de servicio al cliente corporativos con conocimientos básicos de sistemas, con capacitación para el uso de las aplicaciones de cada cliente, la información de los clientes es crítica por lo tanto se deben implementar políticas para garantizar los mejores niveles de control y disminuir las vulnerabilidades de seguridad que afecten la continuidad del negocio se tiene clasificados los incidentes según la afectación lo que genera un nivel de prioridad y SLA determinado, no hay restricción de protocolos en la red, se necesita tráfico priorizado para los servicios de voz, se tienen analistas de telecomunicaciones que velaran por la integridad de la red, su optimo performance, atención de incidentes y configuración de servicios, la sede PSeco tendrá los equipos de telecomunicaciones en cuartos técnicos por piso y los servicios de data center estarán en la sede Berrío a la cual se debe acceder a través de una solución anillada por 2 tecnologías de acceso diferentes con conmutación automática para garantizar la continuidad de servicios ante fallas en cualquiera de los 2 brazos, el hardware de las estaciones terminales es determinado por cada cliente, ante las grandes inversiones en infraestructura el presupuesto es limitado, los equipos se trasladaran en su mayoría de las sedes satélites por

lo tanto se hace necesario realizar los cálculos por aplicaciones que consume la operación para determinar los volúmenes de tráfico y determinar si los equipos y cableado que se tienen disponibles soportan los requerimientos de la red , el cableado estructurado será implementado por el proveedor que construye el edificio bajo la premisa de la alta disponibilidad de la red y las altas posibilidades de escalamiento de los servicio es necesario dimensionar el cableado estructurado para que soporte temas de crecimientos y volúmenes de tráfico, el direccionamiento de la red es 172.20.0.0 /16, es una red integrada de voz y datos, deberá tener acceso a los servidores en el data center Berrio, se debe brindar alta disponibilidad de acceso a los servicios la anterior información fue suministrada por los analistas de telecomunicaciones y el gerente.

Las pruebas ejecutadas por el área de seguridad a todas las áreas de la organización (servidores, red, infraestructura, telefonía, grabación y desarrollo) que están implicados de una u otra manera con las políticas de seguridad han sido evaluadas exitosamente y se considera que la seguridad de la red debe mejorar un 10% por medio de la implementación de PCI-DSS. Este 10% corresponde al valor de mejora partiendo de que ya esta implementadas, operativas y monitoreadas las políticas de seguridad a nivel de toda la organización.

Objetivos del negocio nueva sede	Prioridad en %
Mejorar los tiempos de implementación de los nuevos clientes	45
Mas estaciones de trabajo para crecimiento de los nuevos de clientes	45
Mejorar la seguridad de la red	10

***Tabla1*. Objetivos del negocio ajustando a los nuevos requerimientos**

La tabla 1. Detalla los objetivos de la nueva sede a partir de la nueva implementación.

Aspectos técnicos	Metas	Prioridad %
Disponibilidad	Mantener el mayor tiempo posible la red operativa y sin incidentes este valor es crítico porque permite realizar la facturación a los clientes por hora de conexión de los asesores	60
Escalabilidad	Permitir el crecimiento de los	35

	usuarios en la red sin afectar el performance	
Administración de la red	**Gestionar de manera remota y optima las actualización de IOS de los equipos de telecomunicaciones y captura remota de las estaciones de trabajo para el soporte remoto**	**5**

Tabla2. **Porcentaje de incidencia de los Aspectos técnicos**

Tabla 2 **. Menciona y detalla los aspectos técnicos y su porcentaje de participación en el proyecto de la nueva sede PSeco**

Diseño

En la fase de diseño de la red se tomó como estructura organizacional el modelo jerárquico de la red, modelo OSI los servicios críticos de voz los cuales requieren implementación de QoS y las políticas de seguridad de PCI-DSS

Tabla comparativa topologías de red

TOPOLOGÌA	CARACTERÌSTICA	VENTAJA	DESVENTAJA
ESTRELLA	NODO CENTRAL	Disminuye la probabilidad de fallas conectando los equipos a un nodo central el nodo reenvía las comunicaciones a todos los puntos de la red permitiendo la comunicación entre dispositivos periféricos, escalabilidad de la red, Facilidad en el diagnóstico de fallas, permite la desconexión de host en la red sin generar incidentes, facilidad en la instalación y administración.	la carga pasa por el nodo central lo que implica una alta responsabilidad en la comunicación, debe soportar un alto nivel de tráfico, con el crecimiento de la red aumenta el consumo de recursos en el dispositivo central, fallas en el nodo central inactivan la red.
ARBOL	COMBINA TOPOLOGIAS DE BUS Y ESTRELLA	Posee nodos periféricos que transmiten desde y hacia otros nodos no necesitan actuar como repetidores	Si falla un enlace que conecta al nodo el nodo queda por fuera
BUS	UNICO CANAL TRONCAL	Fácil integración de nuevos equipos. Menos conexiones cableadas	Difícil diagnostico cuando se presentan caídas en la red, alta dependencia del cableado central.
MIXTA	NO HAY UN PATRON DE ENLACES DEFINIDO	Combina las ventajas de otras redes	En redes complejas es difícil la administración y configuración
ANILLO	CONECTA LOS EQUIPOS EN	Pocos conflictos con los usuarios	las fallas de los elementos del anillo

	FORMA DE CIRCULO CON CABLE CENTRAL		pueden afectar la red
MALLA	RENDIMIENTO BALANCEADO PARA LA RED	Favorable para los esquemas de alta disponibilidad cuando se tienen varias conexiones no requiere nodo central y se reducen los riesgos de afectaciones y mantenimiento	Alto costo por el uso de recursos para garantizar la redundancia de la red.

(«Diseño y desarrollo de una aplicación para el estudio comparativo de topologías de red», s. f.)

Tabla3. **Comparación topologías de red**

La tabla 3 Describe las fortalezas y desventajas de cada una de las topologías de red.

Analizando la tabla de topologías de red y teniendo en cuenta la alta disponibilidad que se requiere para las operaciones se concluyó que la topología más adecuada es estrella en malla.

Diseño en la capa core

Conectividad L2L sedes PSeco – Datacenter Berrio

La solución de conectividad hacia el data center en la sede Berrío se diseño e implementó por parte del proveedor L2L con 2 enlaces por lo tanto se relacionan los parámetros que se solicitaron en el RFP, los cuales el proveedor debe cumplir en su totalidad y de parte de Allus se deben realizar las pruebas correspondientes para garantizar la correcta entrega del servicio.

El proveedor seleccionado brindó una solución L2L con tecnología de red independiente para los 2 enlaces, la transmisión de datos y voz entre las sedes PSeco y Berrio debe soportar servicios de comunicación bajo estándar IP de manera que permita la integración de servicios al data center, es una solución anillada con conmutación automática menor a 50 ms en capa 2 para el proveedor, no se comparten vlans con el proveedor del servicio, la disponibilidad contratada es de 99,8%, esta disponibilidad se calculará mensualmente bajo control a los informes de disponibilidad y SLA.

La solución implementada consta de 2 canales, un canal punto a punto con tecnología DWDM (Dense Wavelength Division Multiplexing) a 600Mbps. El segundo enlace de la solución es un canal en Metroethernet a 600Mbps. Los enlaces se entregan a 2 switchs Core multicapa en cada sede.

Los anchos de banda se determinaron siguiendo las recomendaciones de los clientes para acceso a las diferentes aplicaciones.

El cliente Banco solicita que el acceso a las aplicaciones se garantice un BW de 70K por asesor según la información suministrada por el área de telecomunicaciones se instalarán para este cliente 550 asesores.

Para el cliente televisión se instalarán 420 asesores, cada asesor de la operación consume 50K según la información brindada por el cliente en el análisis de aplicativos.

Para la vlan de Aseguramiento el cliente corporativo exige que cada asesor tenga garantizado un BW de 90K de un total de 600 las cuales son las 3 vlans que se iniciará operación la sede.

La siguiente es la tabla calculada para las operaciones que van a ser trasladadas inicialmente.

Cálculos anchos de banda por asesor y operación

CLIENTE	ASESORES	BW X ASESOR	TOTAL
Banco	550	230 Kbits	126,5M
Televisión	420	400K Kbits	168M
Aseguramiento	600	140K Kbits	84M
TOTALES	1570	770 Kbits	336M

Tabla4. **Cálculos anchos de banda por número de asesores y operación.**

La tabla 4 relaciona la información suministrada por los clientes corporativos sobre el consumo promedio estimado para cada usuario, el número de asesores contratados para la atención a los clientes finales y el BW total para la operación.

Por política del administrador de red los servicios se calculan en el peor de los escenarios a las máximas capacidades para garantizar que los servicios de voz y datos no se

afecten ante un incidente en cualquier de los brazos así se evitan incidentes de alta prioridad.

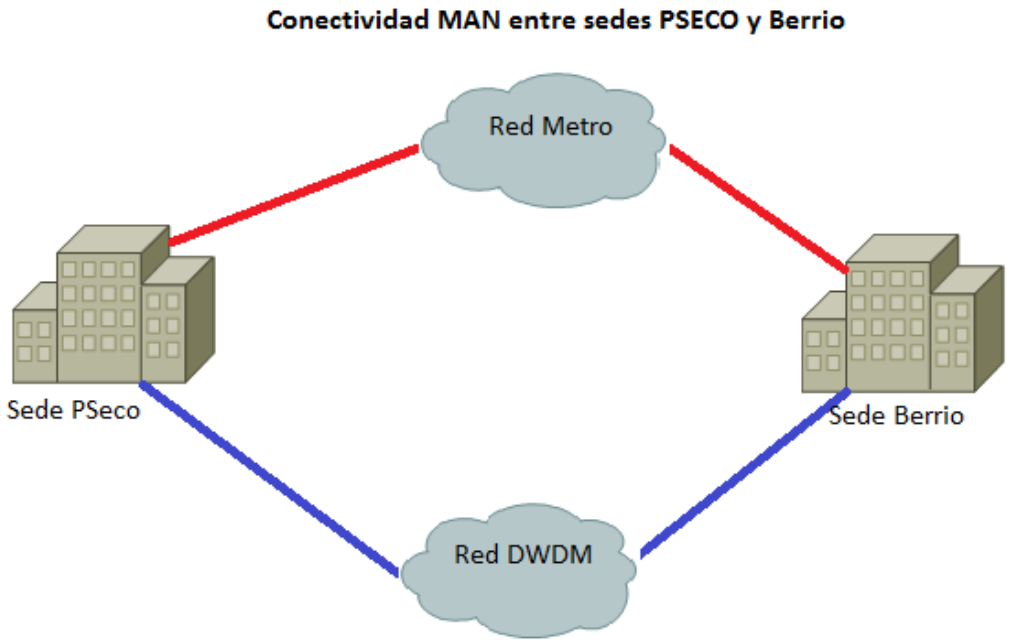


Figura4. Conectividad MAN sedes PSeco Berrio**. (Elaboración propia a partir de íconos Cisco)**

La solución DWDM es una tecnología sobre fibra óptica que permite transmitir información de muchas longitudes de onda los cuales son multiplexados por un transmisor DWDM los cuales utilizan amplificadores llamados EDFAs que compensan la pérdida del

sistema por efectos de la atenuación, al final de la red los demultiplexores individualiza los canales y son detectados por receptores que entregan la señal.

(Aloisio et al., 2012)

El servicio Metroethernet está basado en la conmutación de capa 2 del modelo OSI ofrece un puerto de alta capacidad de tráfico a través de una interfaz Ethernet las redes de transmisión proveen altas capacidades de ancho de banda troncal, deben ser servicios de alta confiabilidad, la red Metroethernet consta de un grupo de SW y nodos donde se realiza el transporte de manera transparente, al ingresar la trama a la red Metroethernet es encapsulada, los identificadores de la trama se insertan y por lo tanto está en el dominio de la red y no de las MACs de usuario, todas las vlans actúan como una gran red LAN en la red Metroethernet.

(Padmaraj et al., 2005)

Enlaces L2L PSeco-Berrio

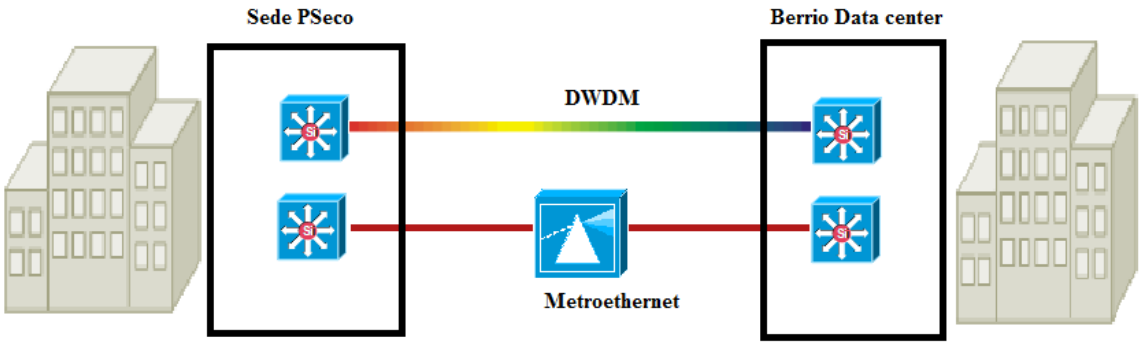


Figura4. **Enlaces L2L PSeco-Berrio. (Elaboración propia a partir de íconos Cisco)**

La figura 4 muestra los 2 enlaces con diferente tecnología que se tendrán entre el data center y la sede PSECO

La selección de los equipos de telecomunicaciones se tomó bajo las siguientes premisas. Se trata de una red corporativa para 1500 usuarios, con tráfico de voz priorizado en la red, con condiciones de escalabilidad para el optimo crecimiento de la red, con capacidad para la configuración de protocolos HSRP y STP porque se tiene enlace redundante, prestación para configuración de vlans las cuales se implementaron para cada operación, alto

forwardig de paquetes por minuto para los enlaces contratados de 600 M, alta disponibilidad en la red LAN entre los equipos Core y distribución, los SW de acceso no deben tener una cantidad alta de usuarios conectados para disminuir las probabilidades de afectación de la operación ante puntos de falla, capacidad para implementación de políticas de QoS, requerimientos para administración de los equipos bajo SNMP y gestión remota con SSH bajo los parámetros mencionados se seleccionaron los siguientes equipos para core, distribución y acceso

Allus posee 2 Switchs Cisco 3750 Catalyst los cuales en la medida de lo posible deben ser utilizados después de analizar el datasheet de los equipos y los requerimientos de red se encuentra que son equipos con todas las prestaciones técnicas requeridas para la implementación de la red LAN.

SW Core Principal

```
SW_L3_PPAL_PTO-SECO#sh vers
Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M), Version 12.2(55)SE5, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 09-Feb-12 18:14 by prod_rel_team
Image text-base: 0x00003000, data-base: 0x02800000

ROM: Bootstrap program is C3750E boot loader
BOOTLDR: C3750E Boot Loader (C3750X-HBOOT-M) Version 12.2(53r)SE2, RELEASE SOFTWARE (fc1)

SW_L3_PPAL_PTO-SECO uptime is 1  weeks, 6 days, 12 hours, 54 minutes
System returned to ROM by power-on
System restarted at 02:26:30 gmt Thu Sep  3 2015
System image file is "flash:/c3750e-universalk9-mz.122-55.SE5/c3750e-universalk9-mz.122-55.SE5.bin"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

License Level: ipservices
License Type: Permanent
Next reload license Level: ipservices

cisco WS-C3750X-24 (PowerPC405) processor (revision A0) with 262144K bytes of memory.
Processor board ID FDO1707P0WN
Last reset from power-on
```

Figura5. **(Aplicación comando show version en SW Cisco 3750X)**

La figura 5 muestra el equipo 3750X seleccionado para la capa Core y sus especificaciones técnicas básicas.

Para la capa de distribución se analizó la posibilidad de instalar recursos disponibles que se tenían en otras sedes, como se mencionó anteriormente la alta inversión en la sede limita

los recursos financieros y la compra de equipos por lo tanto se debe analizar si los recursos actuales disponibles tiene el performance requerido para un óptimo desempeño en la red.

Se mencionan las características generales de la línea Catalyst 2960 X y XR pero el análisis está orientado al datasheet del Sw Cisco Catalyst 2960-X el cual es el equipo disponible.

● 24 o 48 puertos Gigabit Ethernet con un rendimiento de reenvío de velocidad de línea

● Gigabit factor de forma pequeño conectable (SFP) o 10G SFP + enlaces ascendentes

● FlexStack Plus para el apilamiento de hasta 8 switches con 80 Gbps de rendimiento de la pila (opcional)

● Power over Ethernet Plus (PoE +) el apoyo de hasta 740W de presupuesto PoE

● 24 puertos PoE conmutador sin ventilador para el despliegue fuera del armario de cableado

● Reducción del consumo de energía y las características avanzadas de administración de energía

● Interfaces de gestión de Ethernet y USB para operaciones simplificadas

● Visibilidad de aplicaciones y planificación de la capacidad con integrada NetFlow-Lite

Características de software ● Base LAN o LAN Lite Cisco IOS®

● Garantía limitada de por vida mejorada (E-LLW) que ofrece el próximo día hábil sustitución de hardware

(«Cisco Catalyst 2960-X Series Switches Data Sheet», s. f.)

Los switches Catalyst 2960-X incluyen una única fuente de alimentación fija y están disponibles con el IOS LAN Base Cisco o conjunto de funciones LAN Lite. Catalyst modelos de switch 2960-XR incluyen una fuente de alimentación modular reemplazable en campo y tienen capacidad para una segunda fuente de alimentación. Catalyst 2960-XR está disponible sólo con el conjunto de características Cisco IOS IP Lite.

(«Cisco Catalyst 2960-X Series Switches Data Sheet», s. f.)

Modelo	10/100/1000 Ethernet Ports	Uplink Interfaces	Cisco IOS Software Image	Available PoE Power	FlexStack-Plus Capabilit
Cisco Catalyst 2960X-24TD-L	24	2 SFP+	LAN Base	-	Y

Todos los switches Catalyst 2960-X Series utilizan una única imagen universal del software Cisco IOS para todos los SKU. En función del modelo del interruptor, la imagen de IOS de Cisco configura automáticamente la LAN Lite, LAN Base o conjunto de funciones IP Lite.

Modelos LAN Lite han reducido la funcionalidad y capacidad de ampliación para las pequeñas implementaciones con los requisitos básicos. Cisco Catalyst 2960-X Familia de

interruptores están disponibles con los conjuntos de funciones LAN Base y LAN Lite y Catalyst 2960-XR familia de switches son conjuntos de características IP Lite disponibles.

Cada modelo de conmutador está atado a un nivel de funciones específicas; LAN Lite no se puede actualizar a LAN y LAN Base Base no se puede actualizar a IP Lite.

● Protocolos de enrutamiento unicast IP (estática, Routing Information Protocol Version 1 [RIPv1], RIPv2, RIPng y EIGRP-Stub) son compatibles con las aplicaciones de enrutamiento de red.

Los switches Cisco Catalyst serie 2960-X proporcionan una gama de características de seguridad para limitar el acceso a la red y mitigar las amenazas, entre ellas:

Asignación de VLAN basada en MAC

● permite a diferentes usuarios para autenticarse en diferentes VLANs. Esta característica permite que cada usuario tenga una VLAN de datos diferente en la misma interfaz.

● Cisco TrustSec utiliza SXP para simplificar la seguridad y la aplicación de políticas de toda la red. Para obtener más información acerca de las soluciones de seguridad de Cisco TrustSec, visite cisco.com/go/TrustSec.

● Integral 802.1X Características de controlar el acceso a la red, incluyendo la autenticación flexible, modo monitor 802.1x, y RADIUS Cambio de Autorización.

● IPv6 Primera-Hop Seguridad mejora de capa 2 y capa 3 acceso a la red de proliferación de dispositivos IPv6 especialmente dispositivos BYOD. Protege contra la publicidad canallas del router, la falsificación de direcciones, respuestas DHCP falsos y otros riesgos introducidos por la tecnología IPv6.

● Sensor de dispositivos y Clasificador de dispositivos permiten perfiles de dispositivos versátiles sin costura incluyendo dispositivos BYOD. También permiten Cisco Identidad Services Engine (ISE) a las políticas de seguridad basadas en identidad disposición. Esta función está disponible tanto en el 2960-X y las familias de productos 2960-XR.

● Cisco Confianza Técnica Ancla permite una fácil distribución de una única imagen universal para todos los modelos de Catalyst 2960-X mediante la verificación de la autenticidad de las imágenes del IOS. Esta tecnología permite el cambio a realizar comprobaciones de integridad IOS en el arranque mediante la verificación de la firma, verificando el Patrimonio de confianza en Administración y autenticación de la licencia.

(«Cisco Catalyst 2960-X Series Switches Data Sheet», s. f.)

● Amenaza de Defensa de Cisco ofrece incluyendo Seguridad Portuaria, Dynamic ARP Inspection y IP Source Guard.

● VLAN privadas restringen el tráfico entre los hosts en una segmento común mediante la segregación del tráfico en la capa 2, convirtiendo un segmento de difusión en un acceso múltiple de no difusión como segmento. Esta característica está disponible en función de IP-Lite establecer solamente.

Privado ◦ VLAN Edge proporciona seguridad y aislamiento entre los puertos del switch, lo que ayuda a garantizar que los usuarios no pueden husmear en el tráfico de otros usuarios.

● Reverse Path Forwarding función Unicast (uRPF) ayuda a mitigar los problemas causados por la introducción de la (falsa) dirección de origen mal formado o forjado IP en una red descartando paquetes IP que carecen de una dirección IP de origen verificable. Esta característica está disponible en función de IP-Lite establecer solamente.

● multidominio autenticación permite a un teléfono IP y un PC para autenticarse en el mismo puerto de switch mientras que colocarlas en voz apropiada y VLAN de datos.

● listas de control de acceso (ACL) para IPv6 e IPv4 para la seguridad y calidad de servicio ACE.

ACL ◦ VLAN en todas las VLAN impiden que los datos no autorizada fluye de ser un puente dentro de VLAN.

◦ Router ACL definen las políticas de seguridad en interfaces enrutadas para el control de plano y tráfico de datos plano. IPv6 ACL se pueden aplicar para filtrar el tráfico IPv6.

ACL basadas en puertos ◦ para Capa 2 interfaces permiten las políticas de seguridad que deben aplicarse en los puertos de conmutación individuales.

● Secure Shell (SSH) Protocolo, Kerberos y Simple Network Management Protocol Version 3 (SNMPv3) proporcionan seguridad de la red mediante la encriptación del tráfico de administrador durante las sesiones de Telnet y SNMP. Protocolo SSH, Kerberos y la versión criptográfica de SNMPv3 requieren una imagen especial software criptográfico debido a las restricciones de exportación de Estados Unidos.

(«Cisco Catalyst 2960-X Series Switches Data Sheet», s. f.)

● Switched Puerto Analyzer (SPAN), con el apoyo de datos bidireccional, permite Cisco Intrusion Detection System (IDS) para tomar medidas cuando se detecta un intruso.

● TACACS + y RADIUS de autenticación facilita el control centralizado del conmutador y restringe a los usuarios no autorizados alteren la configuración.

● Dirección MAC de notificación permite a los administradores a ser notificados de los usuarios añaden o eliminan de la red.

● seguridad multinivel en el acceso a la consola impide que usuarios no autorizados puedan alterar la configuración del switch.

● Unidad de datos de protocolo de puente (BPDU) Guardia apaga Spanning Portuarias Árbol interfaces habilitadas rápido cuando se reciben las BPDU para evitar bucles de topología accidentales.

● Spanning Tree Root Guardia (STRG) evita que los dispositivos de borde no pierda el control del administrador de la red se conviertan en nodos raíz del protocolo Spanning Tree.

● filtrado IGMP proporciona autenticación de multidifusión al filtrar los no suscriptores y limita el número de secuencias de multidifusión simultáneas disponibles por puerto.

● Asignación Dinámica VLAN es compatible a través de la implementación de la capacidad del cliente VLAN Membership Policy Server para proporcionar flexibilidad en la asignación de puertos a las VLAN. VLAN dinámica facilita la asignación rápida de direcciones IP.

(«Cisco Catalyst 2960-X Series Switches Data Sheet», s. f.)

Redundancia y Flexibilidad

Cisco Catalyst 2960-X Interruptores Series ofrecen una serie de características de redundancia y capacidad de recuperación para evitar cortes y ayudar a asegurar que la red sigue estando disponible:

● EtherChannel Cruz-pila proporciona la capacidad de configurar la tecnología de Cisco EtherChannel través de los diferentes miembros de la pila para alta resiliencia.

● de Flexlink proporciona redundancia de enlaces con el tiempo de convergencia a menos de 100 milisegundos.

● IEEE 802.1s / w protocolo Rapid Spanning Tree (RSTP) y Multiple Spanning Tree Protocol (MSTP) proporcionan Rapid Spanning-tree convergencia independiente de temporizadores Spanning Tree y también ofrecen el beneficio de Capa 2 balanceo de carga y procesamiento distribuido. Unidades apiladas se comportan como un único nodo de spanning-tree.

● Per-VLAN Rapid Spanning Tree (PVRST +) permite una rápida reconvergencia spanning-tree en una base por-VLAN spanning-tree, sin necesidad de la implementación de instancias de spanning-tree.

● Protocolo Cisco Hot Standby Router (HSRP) es compatible para crear redundante, falla topologías de enrutamiento seguros en 2960 XR-IP-Lite SKU.

● Auto-recuperación Switch-puerto (Error Desactivar) intenta automáticamente para reactivar un enlace que está desactivada debido a un error de red.

● Redundancia de alimentación con una segunda fuente de alimentación opcional en los modelos 2960-XR, o con un RPS externa en los modelos 2960-X.

(«Cisco Catalyst 2960-X Series Switches Data Sheet», s. f.)

Calidad mejorada de Servicio

Los switches Cisco Catalyst serie 2960-X ofrece la gestión del tráfico inteligente que mantiene todo fluya sin problemas. Mecanismos flexibles para el marcado, la clasificación, y la programación ofrecen un rendimiento superior para datos, voz y tráfico de vídeo, todo a velocidad de cable. Características de QoS primaria incluyen:

● Hasta ocho colas de salida por puerto y cola de prioridad estricta para que los paquetes de mayor prioridad sean atendidos por delante del resto del tráfico.

● forma de Round Robin (SRR) la programación y la gota de cola ponderada (DMP) para evitar la congestión.

● tasa basada en flujo de limitar y hasta 256 agregados o individuales por puerto.

● clase 802.1p de servicio (CoS) y código de servicios diferenciados Point (DSCP) de clasificación, con el marcado y reclasificación en función de cada paquete por fuente y la dirección IP de destino, dirección MAC, o Capa número de puerto 4 TCP / UDP.

● QoS Cruz-pila para permitir QoS para ser configurados a través de una pila de switches de la serie 2960-X.

● El Cisco comprometido tasa de información de la función (CIR) proporciona ancho de banda en incrementos tan bajos como 8 Kbps.

● Limitación de velocidad se proporciona sobre la base de la fuente y la dirección IP de destino, origen y destino de dirección MAC, Capa / información UDP 4 TCP, o cualquier combinación de estos campos, el uso de QoS ACL (ACL IP o MAC ACL), mapas de clase, y mapas de política.

Cisco Catalyst 2960-X Series conmutación Database Manager

Gestor de bases (SDM) Plantillas de certificados de LAN Base e IP Lite conmutación permite al administrador para optimizar automáticamente el ternario memoria (TCAM) la asignación de contenido direccionable a las características deseadas en base a requisitos de despliegue específico. MAC, números de ruta, seguridad y calidad de servicio de escalabilidad depende del tipo de plantilla que se utiliza en el interruptor.

(«Cisco Catalyst 2960-X Series Switches Data Sheet», s. f.)

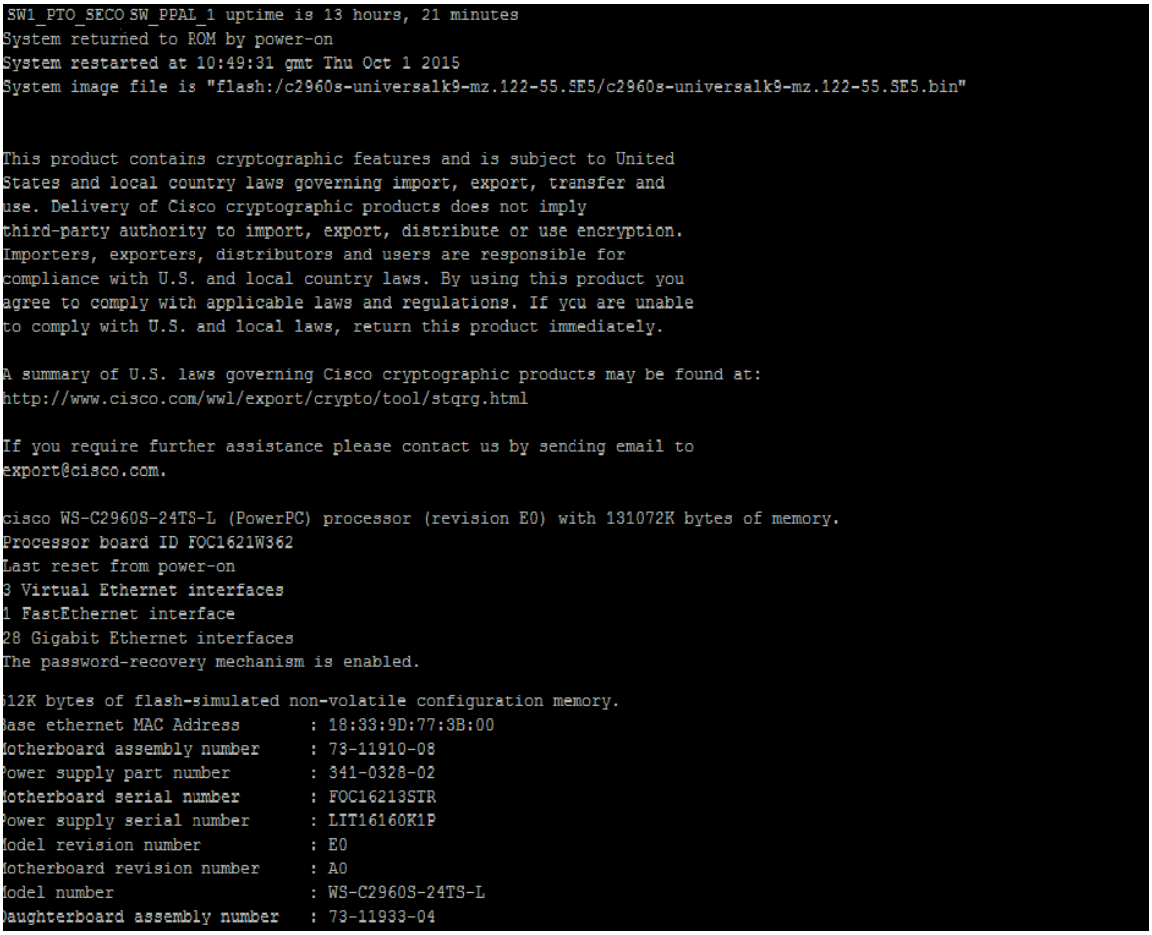


Figura 6. **(Aplicación comando show version en SW Cisco 2960S)**

La figura 6 muestra el equipo Core 2960S seleccionado para la capa de distribución y sus especificaciones técnicas básicas.

```
cisco WS-C2960-24TT-L (PowerPC405) processor (revision F0) with 61440K/4088K bytes of memory.
Processor board ID FOC1318V4DA
Last reset from power-on
2 Virtual Ethernet interfaces
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:25:83:D2:F1:80
Motherboard assembly number     : 73-11473-05
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC13191JW0
Power supply serial number      : AZS130904U4
Model revision number           : F0
Motherboard revision number     : A0
Model number                    : WS-C2960-24TT-L
System serial number            : FOC1318V4DA
Top Assembly Part Number        : 800-29859-02
Top Assembly Revision Number    : B0
Version ID                      : V05
CLEI Code Number                : COM3L00BRD
Hardware Board Revision Number  : 0x01


Switch Ports Model              SW Version            SW Image
------ ----- -----              ----------            ----------
*    1 26    WS-C2960-24TT-L    12.2(50)SE1           C2960-LANBASEK9-M


Configuration register is 0xF
```

Figura 7. **(Aplicación comando show version en SW Cisco 2960)**

La figura 6 muestra el equipo Core 2960 seleccionado para la capa de acceso y sus especificaciones técnicas básicas.

Implementación

En los switchs Core del Datacenter y la sede PSeco se asignaron y configuraron los puertos para la conexión de los enlaces L2L.

La configuración de las interfaces asociadas a la conexión de los enlaces L2L fue la siguiente:

Sh run de la configuración de la interfaz G1/0/24 en el SW Core PSeco principal

```
interface GigabitEthernet1/0/24
 description PTO SECO-BERRIO
 no switchport
 dampening
 ip address 172.20.217.69 255.255.255.252
 ip hello-interval eigrp 5 1
 ip hold-time eigrp 5 3
 carrier-delay msec 0
 delay 1
```

***Ilustracion3,* Configuración interfaz en el Sw Core PSeco**

Sh run de la configuración interfaz Gi1/0/2 en el SW Core Berrío para la comunicación con la sede PSeco por medio del enlace L2L.

```
interface int Gi1/0/2
 description L2L PTO-SECO
 no switchport
 dampening
 ip address 172.20.217.70 255.255.255.252
 ip hello-interval eigrp 5 1
 ip hold-time eigrp 5 3
```

***Ilustracion4,* Configuración interfaz Gi1/0/2 en el Sw Core Berrío para el enlace L2L**

Las ilustraciones 3 y 4 describen el proceso y resultado de la configuración de la interfaces involucradas en el switch core para la comunicación entre PSeco y el data center por medio del enlace L2L.

Con el comando description registramos un nombre o identificador para la interfaz que relaciona o asocia el servicio, el comando no switchport permite registrar el direccionamiento IP en la interfaz aplicada, la sentencia ip address permitió agregar la dirección IP en mascara 30 donde tenemos 2 direcciones IPs disponibles (172.20.217.69 y 172.20.217.70) asignados para el enlace DWDM en cada extremo del enlace, con el comando dampening generamos la configuración para que el puerto se ponga en shutdown en el caso de intermitencias sobre los enlaces, la interfaz se habilita con el comando no shutdown.

Configuración interfaces enlace Metroethernet

Configuración interfaz SW Core secundario PSECO en la interfaz Gi1/0/20 para la conexión al data center por medio del enlace Metroethernet

```
L3_CONTING_PTO-SECO#sh run int Gi1/0/20
Building configuration...

Current configuration : 133 bytes
!
interface GigabitEthernet1/0/20
 description BERRIO_METRO
 no switchport
 dampening
 ip address 172.20.217.97 255.255.255.252
end
```

Configuración interfaz Gi1/45 en el SW Core backup Berrio (Datacenter) conexión por medio del enlace Metroethernet

```
ONT L3 BERRIO #sh run int Gi1/45
 Building configuration...

 Current configuration : 105 bytes
 !
 interface GigabitEthernet1/45
  description PSECO-METRO
  no switchport
  dampening
  ip address 172.20.217.98 255.255.255.252
 end
```

Bajo el siguiente RFC se solicitó aprobación de la actividad al comité de riesgos e incidentes.

RFC	FECHA	HORA	DURACIÓN	EJECUTOR	OBJETIVO	DESCRIPCIÓN	JUSTIFICACIÓN	CLIENTE	RIESGO	CONTINGENCIA	PLAN DEVOLUCIÓN
RFC-M20154,017882	25/09/2015	11:00	45 min	Miguel Angel Rubiano	Realizar pruebas de conectividad y conmutación para los enlaces de la nueva sede PSeco	Pruebas de ping para validar comunicación a las redes del data center Generar tráfico por la interfaces de los 2 enlaces L2L. Ingresar al Sw Core ppal y aplicar sobre la interfaz Gi 1/0/24 el aumento el delay a 100 para forzar la conmutacion del tráfico al otro enlace. Ingresar al SW Core Backup y aplicar sobre la interfaz Gi 1/0/20 el aumento el delay a 100 para forzar la conmutacion del tráfico al otro enlace.	Garantizar la comunicación de la nueva sede PSeco con el data center Berrio	N/A, no hay riesgo para clientes	N/A los servicios no están en producción	N/A los servicios no están en producción	N/A los servicios no están en producción

Después de configurar las interfaces de los Switchs Core, se realizó la instalación de los equipos en el nodo en su respectivo rack por parte de Allus, el proveedor instaló las fibras y el Metronid para realizar la conversión del medio fibra-Ethernet y se realizaron las pruebas de conectividad hacia el Datacenter garantizando la conmutación del tráfico por las 2 soluciones Metroethernet y DWDM ante incidentes en cualquiera de los 2 enlaces L2L

Las pruebas ejecutadas por Allus fueron exitosas, garantizaron acceso a los servidores del Datacenter donde se alojan las aplicaciones y la conmutación del tráfico en la solución anillada como evidencia se adjunta las imágenes de las gráficas de tráfico de los enlaces que garantizan la conmutación y los comandos aplicados sobre la interfaz para simular incidente en el enlace L2L.

El proveedor a través de un generador inyecta tráfico sobre los 2 enlaces L2L Sobre las interfaces Gi1/0/24 del Sw Core Principal y en el SW Core Secundario en la interfaz Gi 1/20 y se aplica delay sobre dichas interfaces

SW Core Principal

```
SW_L3_PPAL_PTO-SECO#sh int status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/0/24  L2L PTO_SECO-BERRI connected    routed     a-full a-1000 10/100/1000BaseTX
```

Figura6. **Estado de la interfaz del enlace L2L aplicando el comando sh interface status**

Se aumenta el delay con los siguientes comandos ejecutados en la interfaz Gi 1/0/24 para forzar al tráfico por el otro enlace L2L

Se configura un delay alto en interfaz Gi1/0/20 del Switch secundario

```
SW_L3_PPAL_PTO-SECO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_L3_PPAL_PTO-SECO(config)#int Gi1/0/24
SW_L3_PPAL_PTO-SECO(config-if)#delay 100
SW_L3_PPAL_PTO-SECO(config-if)#^Z
```

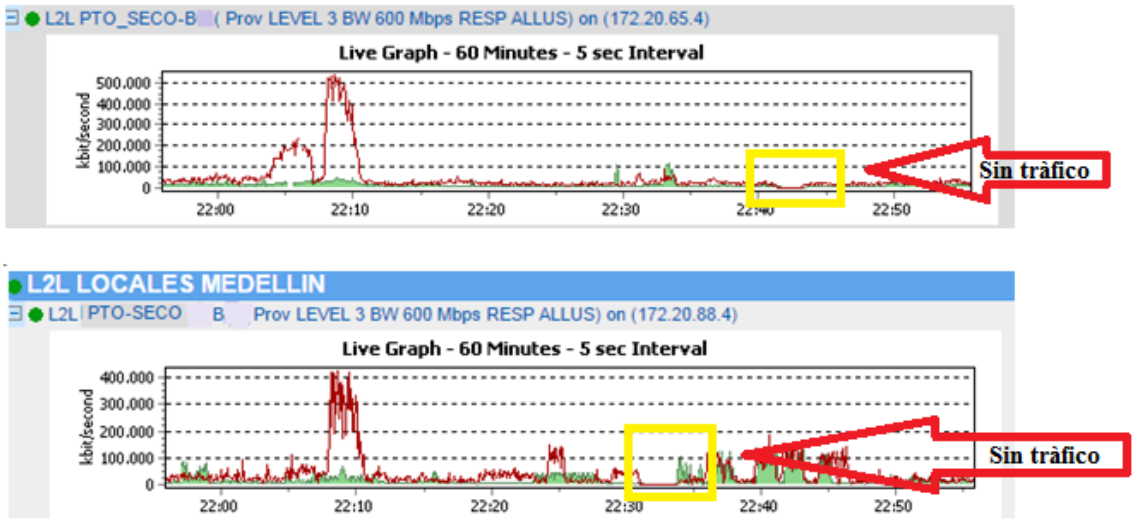
Figura7. **Modificación del delay para conmutar el tráfico al otro enlace L2L**

Se configura un delay bajo en interfaz Gi1/0/20 del Switch secundario

```
SW_L3_CONTING_PTO-SECO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_L3_CONTING_PTO-SE(config)#int Gi1/0/20
SW_L3_CONTING_PTO-SE(config-if)#delay 1
```

Figura8. **Modificación del delay para restablecer el tráfico por el canal L2L**

Gráficas de conmutación del tráfico



.

***Figura9*. Evidencia conmutacion de trafico por los enlaces L2L**

La figura muestra la conmutacion del tráfico entre los 2 enlaces L2L.

Configuración de VLANS

Se ejecutó la configuración de las vlans para los clientes de la sede PSeco bajo la política de vlan por puerto toda la organización tiene configurado el servicio en sus equipos es exigencia del administrador de red mantener el estándar de administración en todas las sedes, no se hace subnetting ni supernetting en las redes de Allus, dicha configuración implica seleccionar una red disponible del segmento 172.20.0.0/16 para la configuración se seleccionaron las vlan 160, 161 y 162 y como nemotecnia se relaciona el tercer octeto con la vlan para el ejemplo citado la vlan 160 está asociada al segmento 172.20.160.0 siempre con

mascara 24, el personal de servidores configura en el server DHCP y reserva de las 15 primeras direcciones IP las vlans mencionadas anteriormente con default Gateway siempre la primera IP, el Core principal debe tener la segunda IP disponible del segmento, el Core de contingencia la tercera IP del segmento, la cuarta IP está apuntando a un servidor DHCP, para las configuraciones de HSRP es importante seguir las siguientes políticas de configuración establecidas ; el grupo HSRP debe ser el mismo del tag o identificador de la vlan por ejemplo: la vlan 160 debe tener el grupo HSRP 160. Las prioridades deben ser 150 para el core principal y 50 para el core secundario.

Configuración vlan 160 y HSRP en SW Core Principal

```
SW_L3_PPAL_PTO-SECO#sh run int vl 160
Building configuration...

Current configuration : 201 bytes
!
interface Vlan160
 description Vlan Television
 ip address 172.20.160.2 255.255.255.0
 ip helper-address 172.20.161.4
 standby 160 ip 172.20.160.1
 standby 160 priority 150
 standby 160 preempt
end
```

Sh run de la Vlan 160 en el Core principal

```
vlan 160
 name TELEVISION
```

Configuración vlan 160 y HSRP en SW Core Backup PSeco

```
interface Vlan160
 description Vlan Television
 ip address 172.20.160.2 255.255.255.0
 ip helper-address 172.20.161.4
 standby 160 ip 172.20.160.1
 standby 160 priority 50
 standby 160 preempt
end
```

Sh run del Tag de la vlan 160 en Core Backup

```
vlan 160
 name TELEVISION
!
```

Sh run Tag vlan 161 en Core Principal

```
vlan 161
 name Bancos
!
```

Configuración vlan 161 y HSRP en Switch Core principal

```
SW_L3_PPAL_PTO-SECO#
SW_L3_PPAL_PTO-SECO#sh run int vl 161
Building configuration...

Current configuration : 196 bytes
!
interface Vlan161
 description Vlan BANCO
 ip address 172.20.161.2 255.255.255.0
 ip helper-address 172.20.161.4
 standby 161 ip 172.20.161.1
 standby 161 priority 150
 standby 161 preempt
end

SW_L3_PPAL_PTO-SECO#
```

Configuración vlan 161 y HSRP en Switch Core Backup

```
SW_L3_CONTING_PTO-SECO#sh run int vl 161
Building configuration...

Current configuration : 195 bytes
!
interface Vlan161
 description Vlan BANCO
 ip address 172.20.161.3 255.255.255.0
 ip helper-address 172.20.161.4
 standby 161 ip 172.20.161.1
 standby 161 priority 50
 standby 161 preempt
end
```

Sh run Tag vlan 161 en Switch Core Backup

```
vlan 161
 name BANCOS
```

Configuración vlan 162 y HSRP en Switch Core principal

```
SW_L3_PPAL_PTO-SECO#
SW_L3_PPAL_PTO-SECO#sh run int vl 162
Building configuration...

Current configuration : 202 bytes
!
interface Vlan162
 description Vlan ASEGURADORA
 ip address 172.20.162.2 255.255.255.0
 ip helper-address 172.20.162.4
 standby 162 ip 172.20.162.1
 standby 162 priority 150
 standby 162 preempt
end
```

Sh run Tag vlan 162 en el Switch Core principal

```
vlan 162
 name ASEGURADORA
```

Configuración vlan 162 y HSRP en Switch Core Backup

```
SW_L3_CONTING_PTO-SECO#sh run int vl 162
Building configuration...

Current configuration : 201 bytes
!
interface Vlan162
 description Vlan ASEGURADORA
 ip address 172.20.162.3 255.255.255.0
 ip helper-address 172.20.162.4
 standby 162 ip 172.20.162.1
 standby 162 priority 50
 standby 162 preempt
end

SW_L3_CONTING_PTO-SECO#
```

Sh run de la vlan 162 en el Switch Core Backup

```
vlan 162
 name ASEGURADORA
```

Cuando se configura la vlan en un puerto se crea la vlan por defecto en el Switch de acceso pero los nombres de la vlan que se asignan por defecto no sirven para identificar a que cliente se le asigno la vlan, Allus tiene más de 100 clientes corporativos constantemente se realizan movimientos de las vlans de una sede a otra, identificar la vlan por su nombre facilita la administración que realizan los analistas de redes.

Los pasos anteriormente descritos se realizaran para todas las operaciones que se instalen en la sede teniendo en cuenta la disponibilidad de la vlan

Se realiza troncalizaciòn de 2 interfaces para tener conexión entre los switches Core principal y backup y garantizar la continuidad de servicios ante fallas de uno de los equipos Core.

HSRP entre SW Core

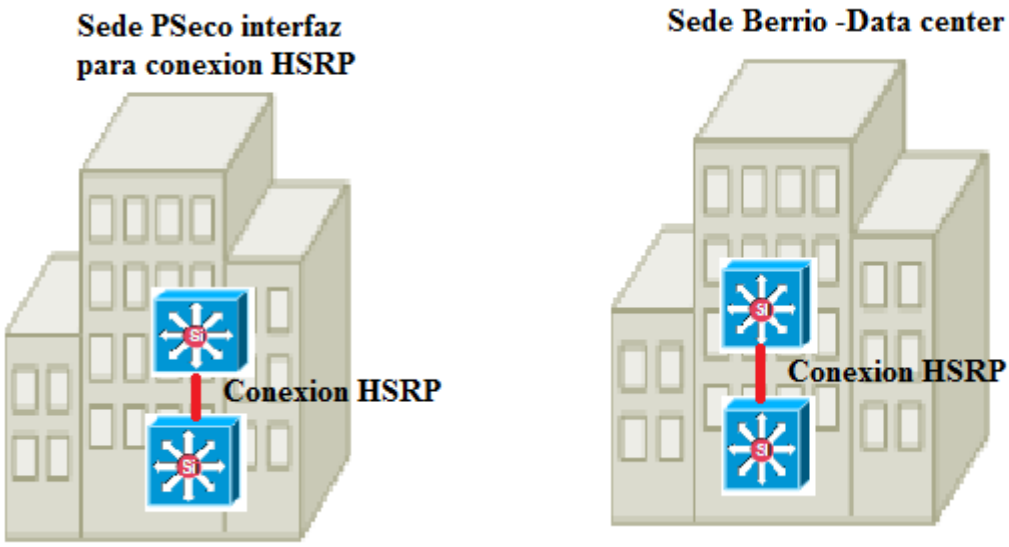


Figura9. HSRP entre SW Core. **(Elaboración propia a partir de iconos Cisco)**

Se realizó la configuración de las interfaces para la conexión entre los Switches Core.

Configuración interfaz Gi1/0/1 Switch Core Backup

```
SW_L3_CONTING_PTO-SECO#sh run int Gi1/0/1
Building configuration...

Current configuration : 248 bytes
!
interface GigabitEthernet1/0/1
 description HSRP
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

Configuración interfaz Gi1/0/2 Switch Core Principal

```
SW_L3_PPAL_PTO-SECO#sh run int Gi1/0/2
Building configuration...

Current configuration : 172 bytes
!
interface GigabitEthernet1/0/2
 description HSRP
 switchport trunk encapsulation dot1q
 switchport mode trunk
end
```

Sh run Usuario local

```
username mrubiano password 7
```

En algunas organizaciones los Sw de distribución se conocen como SW de Piso, la conexión de los Switch Core a distribución se configura bajo los siguientes comandos:

Configuración interfaz Gi1/0/3 con conexión al SW10 de PSeco

```
interface GigabitEthernet1/0/3
 description SW10_PTO_SECO
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

Sh run del EIGRP

```
router eigrp 5
 network 172.20.0.0
 no auto-summary
```

Allus para todas las sedes tiene configurado el segmento 172.20.0.0 /16 y su motor de enrutamiento es EIGRP por lo tanto se mantiene el mismo motor de enrutamiento y sistema autónomo 5 para continuar con las políticas implementadas en otras sedes con este protocolo se realiza el enrutamiento entre las sedes de Allus.

Este proceso se reproduce para todas las conexiones del SW Core hacia los Sw de distribución. Se relacionan por igual los mismos puertos para las conexiones a los SW de piso o distribución es decir el puerto Gi1/0/2 que tiene la conexión al Sw con hostname SW8_PTO_SECO por nemotecnia tendrá la misma conexión en el otro SW así garantizamos alta disponibilidad entre las capas de Core y distribución.

JERARQUIA DE RED

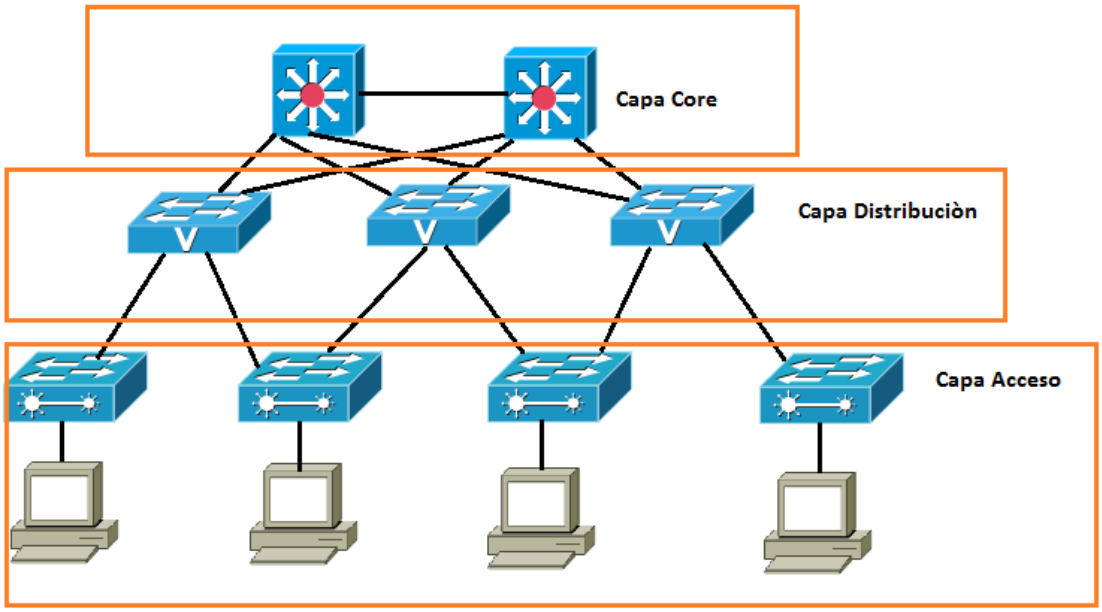


Figura8. JERARQUIA DE RED **(Elaboración propia a partir de íconos Cisco)**

En el SW Core principal de PSeco

```
SW_L3_PPAL_PTO-SECO#sh int status | i SW
Gi1/0/2   SW8_PTO_SECO       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/3   SW10_PTO_SECO      connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/4   SW4_PTO_SECO       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/5   SW9_PTO_SECO       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/6   SW7_PTO_SECO       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/7   SW3_PTO_SECO       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/8   SW_22_PTO_SECO     connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/9   SW1_PTO_SECO       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/10  SW2_PTO_SECO       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/11  SW5_PTO_SECO       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/12  SW12_PTO_SECO      connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/13  SW_15_PTO_SECO     connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/14  SW_15_PTO_SECO     connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/15  SW_16_PTO_SECO     connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/16  SW_18_PTO_SECO     connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/17  SW_17_PTO_SECO     connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/18  SW_21_PTO_SECO     connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/19  SW_19_PTO_SECO     connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/20  SW_20_PTO_SECO     connected    trunk      a-full a-1000 10/100/1000BaseTX
SW_L3_PPAL_PTO-SECO#
```

En el SW Core Backup de PSeco

```
SW_L3_CONTING_PTO-SECO#sh int status | i SW
Gi1/0/2   SW8_PTO_SECO       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/3   SW10_PTO_SECO      connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/4   SW4_PTO_SECO       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/5   SW9_PTO_SECO       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/6   SW7_PTO_SECO       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/7   SW3_PTO_SECO       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/8   SW_22_PTO_SECO     connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/9   SW1_PTO_SECO       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/10  SW2_PTO_SECO       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/11  SW5_PTO_SECO       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/12  SW12_PTO_SECO      connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/13  SW_15_PTO_SECO     connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/14  SW_15_PTO_SECO     connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/15  SW_16_PTO_SECO     connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/16  SW_18_PTO_SECO     connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/17  SW_17_PTO_SECO     connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/18  SW_21_PTO_SECO     connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/19  SW_19_PTO_SECO     connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/20  SW_20_PTO_SECO     connected    trunk      a-full a-1000 10/100/1000BaseTX
```

Sh run conexión consola

```
line con 0
 exec-timeout 10 10
 password 7 [redacted]
 logging synchronous
 length 0
 transport input ssh
```

Sh run de la configuración VTY

```
line vty 5 15
 exec-timeout 10 10
 password 7 [redacted]
 logging synchronous
 length 0
 transport input ssh
```

CAPA DE DISTRIBUCIÒN

En la capa de distribución a nivel lógico los switchs se configuraron con varias de las sentencias generales de configuración de switch anteriormente descritas en los Core como las conexiones VTY y consola por medio de SSH, los usuarios locales, los tag de las diferentes Vlans, la política de QoS para la voz, las configuraciones de SNMP, el banner motd que se describieron ampliamente en párrafos anteriores con su proceso de configuración y resultado, es importante mencionar que para temas de gestión se selecciona una vlan diferente a la vlan 1 por lo tanto queda en shutdown, para configurar la administración de la red en los SW capa 2 el proceso es el siguiente:

Cada equipo de telecomunicaciones tendrá asignada una IP diferente y válida para este caso dentro del segmento de red 172.20.200.0 /24 para el ejemplo de configuración citamos la Ip 172.20.200.100

```
SW1_PTO_SECO#sh run int vl 200
Building configuration...

Current configuration : 85 bytes
!
interface Vlan200
 ip address 172.20.200.100 255.255.255.0
 no ip route-cache
end
```

Los equipos seleccionados para esta capa son los Switch Cisco catalyst 2960 X de 24 puertos los cuales posee la organización de las sedes satélites y otros adquiridos para los temas de crecimiento de las operaciones y nuevos clientes , son switches con puertos Gigabit Ethernet (10/100/1000) los cuales se pueden configurar en stack o apilables hasta 8 equipos de la misma referencia para llegar hasta 80 Gbps, con funcionalidades de PoE, son equipos capa 2 con alimentación eléctrica redundante externa, con alta escalabilidad, permiten realizar control de tráfico ya que son compatibles con netflow que permite capturar, controlar y registrar el flujo de datos que cursa en los equipos como inversión

Para los contact center es crítico el tema de disponibilidad del servicio, la facturación a los clientes se hace por horas de conexión de los asesores y cada vez que se presente un incidente que afecte a un número importante de asesores se estará afectando negativamente los estados financieros por tal razón se busca desde todas las áreas de tecnología que los servidores, redes, bases de datos y demás áreas de producción tengan esquemas de contingencia que actúen rápidamente ante los diferentes incidentes, en la capa de distribución la mejor solución es una estrella en malla que garantice rutas diversas hacia los 2 Sw core para reducir los puntos de fallo de la red.

ALTA REDUNDANCIA CORE –DISTRIBUCIÒN

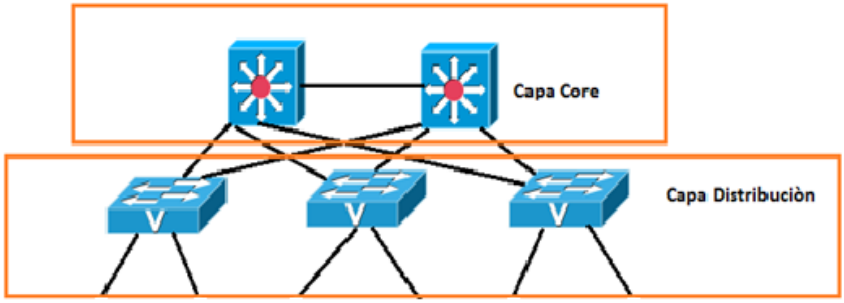


Figura9. **ALTA REDUNDANCIA CORE –DISTRIBUCIÒN (Elaboración propia a partir de íconos Cisco)**

La figura 9 Muestra las diferentes conexiones en caso de presentarse una falla entre las capas de core y distribución.

Capa de Acceso

En la capa de acceso a nivel lógico se continúa con el mismo esquema de la capa de distribución no se presentan cambios en la configuración básica de los switches se mantiene las configuraciones de las conexiones VTY y consola por medio de SSH, los usuarios locales, los tag de las diferentes Vlans, la política de QoS para la voz, las configuraciones de SNMP, configuración de una interface vlan para la administración de los equipos en el mismo segmento de red con su primer IP como default gateway, al banner motd solo se le

modifica el nombre del equipo cambian las políticas de configuración de los puertos de acceso los cuales tienen configuración forzada a 100 - full duplex.

A nivel físico los dispositivos seleccionados son los Switch Cisco 2960 son equipos con capacidad de integración de tráfico de voz, datos y video con administración escalable, con configuración de QoS, políticas de seguridad en puertos, configuración de vlans, función de supervisión de red por medio de netflow.

Mapa de Conexión Data Center - PSeco

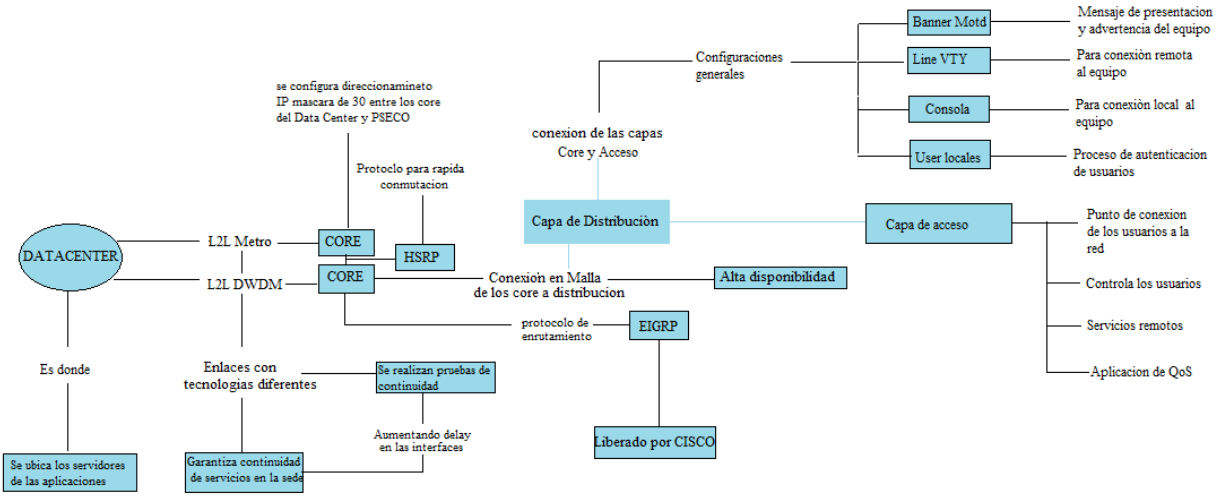


Figura10. **Mapa de conexión Data Center – red LAN PSECO**

La figura 10 muestra el mapa de conexión entre el data center y la topología de conexión de capas de Core, distribución y acceso de la sede PSeco.

```
SW_PS_ACCESO_4#sh int status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        notconnect   160          full    100 10/100BaseTX
Fa0/2                        notconnect   160          full    100 10/100BaseTX
Fa0/3                        notconnect   160          full    100 10/100BaseTX
Fa0/4                        notconnect   160          full    100 10/100BaseTX
Fa0/5                        connected    160          full    100 10/100BaseTX
Fa0/6                        connected    160          full    100 10/100BaseTX
Fa0/7                        connected    160          full    100 10/100BaseTX
Fa0/8                        connected    160          full    100 10/100BaseTX
Fa0/9                        connected    160          full    100 10/100BaseTX
Fa0/10                       connected    161          full    100 10/100BaseTX
Fa0/11                       notconnect   161          full    100 10/100BaseTX
Fa0/12                       connected    161          full    100 10/100BaseTX
Fa0/13                       connected    161          full    100 10/100BaseTX
Fa0/14                       connected    161          full    100 10/100BaseTX
Fa0/15                       connected    161          full    100 10/100BaseTX
Fa0/16                       connected    161          full    100 10/100BaseTX
Fa0/17                       connected    161          full    100 10/100BaseTX
Fa0/18                       connected    161          full    100 10/100BaseTX
Fa0/19                       connected    161          full    100 10/100BaseTX
Fa0/20                       connected    162          full    100 10/100BaseTX
Fa0/21                       connected    162          full    100 10/100BaseTX
Fa0/22                       connected    162          full    100 10/100BaseTX
Fa0/23                       connected    162          full    100 10/100BaseTX
Fa0/24                       notconnect   162          full    100 10/100BaseTX
Gi0/1                        notconnect   159          full    100 10/100/1000BaseTX
Gi0/2     SWITCH_PPAL        connected    trunk      a-full a-1000 10/100/1000BaseTX
```

Figura11. **(Aplicación comando show interface status en SW Cisco 2960)**

La figura 11 muestra el estado de cada una de las interfaces, la vlan configurada en cada puerto, su velocidad y modo de transmisión.

Se implementaron las siguientes listas de control de acceso para cada una de las operaciones donde se permiten la red de servidores, grabación, las ACL se implementaron en los switchs Core en las interface vlan con el comando : ip access-gr 201 in las otras políticas de PCI-DSS son implementadas por otras áreas de la organización y por lo tanto solo se mencionan en la tabla

.

(dhcp)

access-list 201 permit udp any any eq 67

access-list 201 permit udp any any eq 68

(hsrp)

access-list 201 permit udp 172.20.160.0 0.0.255.255 host 224.0.0.2 eq 1985

(Servidores)

access-list 201 permit ip 172.20.160.0 0.0.255.255 172.20.45.0 0.0.0.255

access-list 201 permit ip 172.20.160.0 0.0.255.255 172.20.46.0 0.0.0.255

access-list 201 permit ip 172.20.160.0 0.0.255.255 172.20.47.0 0.0.0.255

access-list 201 permit ip 172.20.160.0 0.0.255.255 172.20.48.0 0.0.0.255

access-list 201 permit ip 172.20.160.0 0.0.255.255 172.20.49.0 0.0.0.25

(Avaya Telefonia)

access-list 201 permit ip 172.20.160.0 0.0.255.255 172.20.50.0 0.0.0.255

access-list 201 permit ip 172.20.160.0 0.0.255.255 172.20.51.0 0.0.0.255

access-list 201 permit ip 172.20.160.0 0.0.255.255 172.20.52.0 0.0.0.255

access-list 201 permit ip 172.20.50.0 0.0.0.255 172.20.160.0 0.0.255.255

access-list 201 permit ip 172.20.51.0 0.0.0.255 172.20.160.0 0.0.255.255

access-list 201 permit ip 172.20.52.0 0.0.0.255 172.20.160.0 0.0.255.255

Para la Allus las polìticas de PCI_DSS son de obligatorio cumplimiento y a través del área de seguridad se ejecuta y realiza monitoreo al cumplimiento de estas políticas, todas las normas de PCI-DSS son importantes y de obligatorio cumplimiento, no se tiene prioridad en su implementación porque cada área (servidores, telecomunicaciones, telefonía, grabación, infraestructura) es responsable de su implementación para este caso se relacionan las correspondientes al área de telecomunicaciones.

POLITICAS DE PCI-DSS

Construir y Mantener una red segura	Instalar y Mantener un Firewall
	No emplear parametros de seguridad y usuarios del sistema por defecto
Proteger los datos de las tarjetas	Proteger los datos almacenados en las tarjetas
	Cifrar la transmision de datos de tarjetas en redes abiertas o publicas
Mantener un programa de gestion de vulnerabilidades	Usar y actualizar constantemente un software antivirus
	Desarrollar y mantener de forma seguridad sistemas y aplicaciones
Implementar medidas de control de acceso	Restringir el acceso a la informacion según need to know
	Asignar un unico ID a cada usuario de la red para trazabilidad de transacciones
Monitorizar y testear frecuentemente las redes	Restringir el acceso fisico a la informacion de las tarjetas
	Auditar y monitorear todos los accesos a los recursos de red y datos de la s tarjetas
Mantener una politica de seguridad de la informaciòn	Testear de forma regular la seguridad de los sistemas y procesos
	Mantener una politica que gestione la seguridad

Tabla 1. **POLITICAS DE PCI-DSS (Elaboración propia)**

QoS para los paquetes de voz

Se realizan las configuraciones para que desde las interfaces de acceso los equipos de telecomunicaciones garanticen la priorización del tráfico de voz sobre los paquetes TCP de las aplicaciones de la operación durante toda la red, la política está aplicada en cada interfaz hasta llegar al server de voz CLAN e ILAN, el core del negocio de Allus son las llamadas de los usuarios finales que realizan a los asesores de las operaciones la configuración de la interfaz es la siguiente:

Mapa QoS

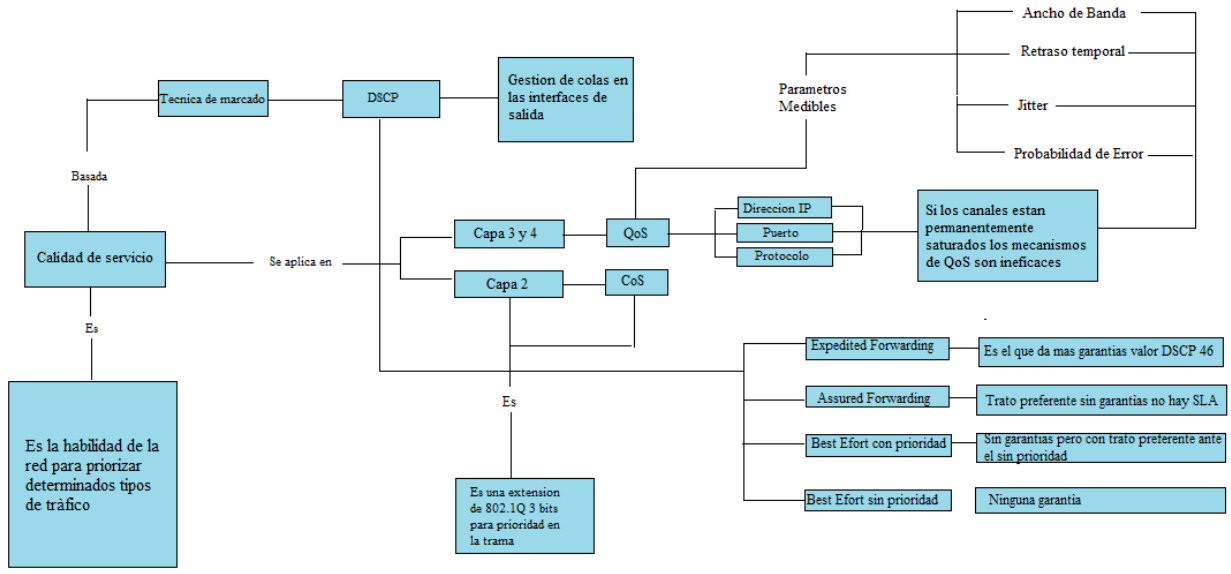


***Figura11*. Mapa QoS**

La figura 11 explica construcción del modelo de QoS

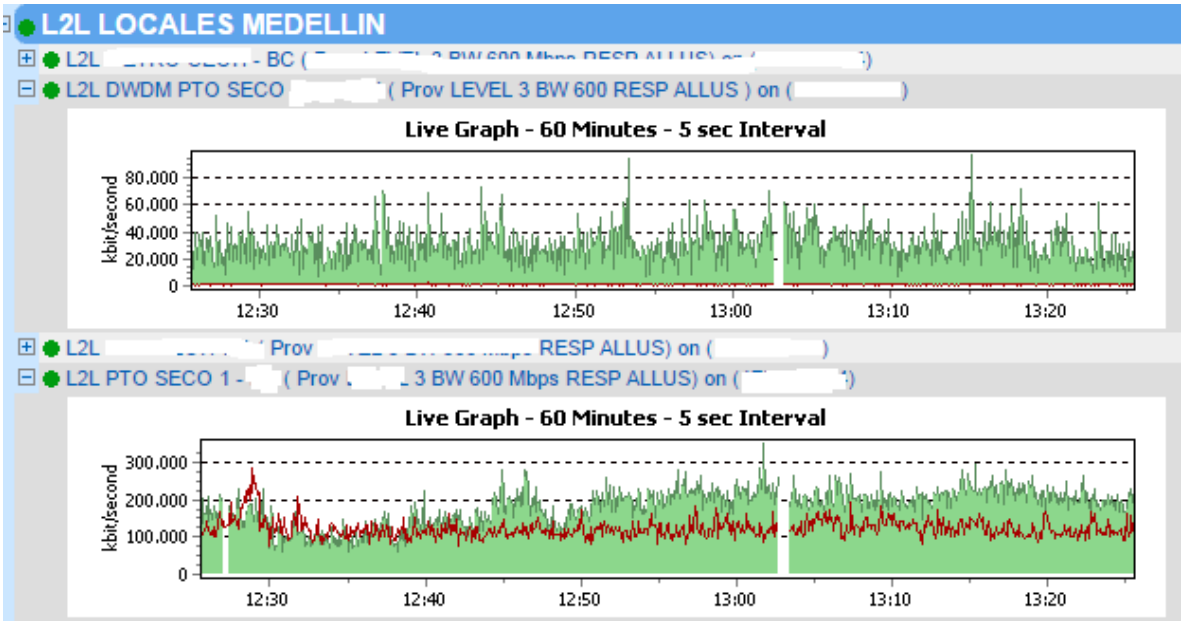
Configuración del Monitoreo en CACTI y PRTG

Estas herramientas de monitoreo y reporting tiene diferentes objetivos en el área de TI, se encuentran implementadas aunque ambas son generadoras de alertas de tráfico el pool de monitoreo de PRTG se realiza cada 10 segundos lo que permite hacer un seguimiento al comportamiento más exhaustivo en los enlaces L2L de las diferentes sedes y actuar proactivamente ante incidentes en los enlaces L2L allí se podrá observar más rápidamente las intermitencias, caídas y comportamientos inadecuados de los enlaces, CACTI actúa más como un generador de informes sobre comportamientos de CPU, memoria y tráfico. Cacti también genera alertas de conectividad por pérdidas de ping pero como su pool de monitoreo es de 5 minutos no es una herramienta ágil en la detección de incidentes.

A continuación se describe el proceso mediante el cual se configura el monitoreo para los equipos todos los switchs core y de distribución por su importancia en el esquema de alta disponibilidad que requiere Allus son monitoreados en el Datacenter bajo el esquema de 7 x 24 x 365 por los técnicos de computo con la herramienta PRTG, los equipos de core, distribución y acceso son monitoreados en Cacti.

El proceso de configuración de Cacti PRTG se describe con más detalle en las imágenes relacionadas en los anexos.

Vista monitoreo de tráfico en la herramienta PRTG



Operación

Los servicios entran en la fase de operación o producción se realizan validaciones sobre la conectividad y comportamiento de los servicios a la operación. Se ejecutan diversas pruebas a los servidores y equipos de la red por medio de ping, ping con peso y varias repeticiones, Tracert y telnet, se verifican los tiempos de ping y Tracert sin presentar afectaciones o pérdidas de paquetes.

PLAN DE TRABAJO PRUEBAS DE CONECTIVIDAD				
PRUEBA	RESULTADO 1	RESULTADO 2	RESULTADO 3	RESULTADO 4
PING A SERVER BERRIO DESDE PC OPERACIÒN	3ms	4ms	3ms	5ms
PING A SERVER BERRIO DESDE PC OPERACIÒN	4ms	3ms	4ms	4ms
PING A BERRÌO DESDE CORE	1/5/9 ms	1/4/9 ms	1/4/9 ms	1/4/9 ms
PING CON PESO A BERRÌO	Success rate is 99 percent (1999/2000), round-trip min/avg/max = 1/4/142 ms	Success rate is 100 percent (2000/2000), round-trip min/avg/max = 1/4/25 ms	Success rate is 99 percent (1998/2000), round-trip min/avg/max = 1/4/143 ms	Success rate is 100 percent (2000/2000), round-trip min/avg/max = 1/4/23 ms
TRACERT BERRÌO	1 172.20.X.X 0 msec 8 msec 9 msec	1 172.20.X.X msec 8 msec 0 msec	1 172.20.X.X 0 msec 6 msec 8 msec	1 172.20.X.X 0 msec 9 msec 10 msec
TELNET BERRÌO	Exitoso	Exitoso	Exitoso	Exitoso
BW ENLACES L2L	150M	230M	180M	140M

PAL				
BW ENLACES L2L BCKUP	**60M**	**78M**	**67M**	**58M**
GRÀFICAS	**sin cortes**	**sin cortes**	**sin cortes**	**sin cortes**
MEMORIA CORE PPAL	**397.98 M**	**397.98 M**	**372.87 M**	**398.41 M**
CPU CORE PPAL	**16.00%**	**16.00%**	**16.00%**	**16.00%**
MEMORIA CORE BKP	**135.05 M**	**134.74 M**	**135.73 M**	**135.78 M**
CPU CORE PPAL BKP	**11.00%**	**11.00%**	**11.00%**	**11.00%**

Tabla 2. **Pruebas de conectividad hacia el server Berrío donde se alojan las aplicaciones que utiliza la operación para la atención a clientes.**

Los resultados de la tabla indican que se tiene buenos tiempos de ping a las aplicaciones en los servidores de la sede Berrío desde los PCs de la operación y desde los switches de Core, las pruebas de ping con peso nos relacionan el comportamiento del enlace ante una saturación del 90% en las pruebas ejecutadas no se perciben perdidas de paquetes ni tiempos altos, los enlaces presentan valores de tráfico adecuados para su capacidad, los valores de CPU y memoria en los SW Core son adecuados y no llegan al 25% de consumo. Los resultados obtenidos son favorables para el desempeño del tráfico en la red y las posibilidades de crecimientos futuros para nuevas operaciones.

No se presenta saturaciones de los enlaces L2L, se realiza monitoreo a los enlaces en la herramienta PRTG y no se presentan pérdidas o saturación. En las interfaces de los equipos no hay errores, CRCs o dropeos de paquetes.

Se realizan pruebas de acceso a los aplicativos donde se obtiene que el 100% de los asesores cargan las aplicaciones exitosamente, se realizan pruebas de análisis de tráfico con un snifer y se exporta la información de conexión de los asesores, no se presentan logs de desconexión en los Switchs core ni distribución, las conexiones son estables y los asesores no reportan problemas en los accesos a las diferentes aplicaciones en los anexos se pueden observar las capturas realizadas.

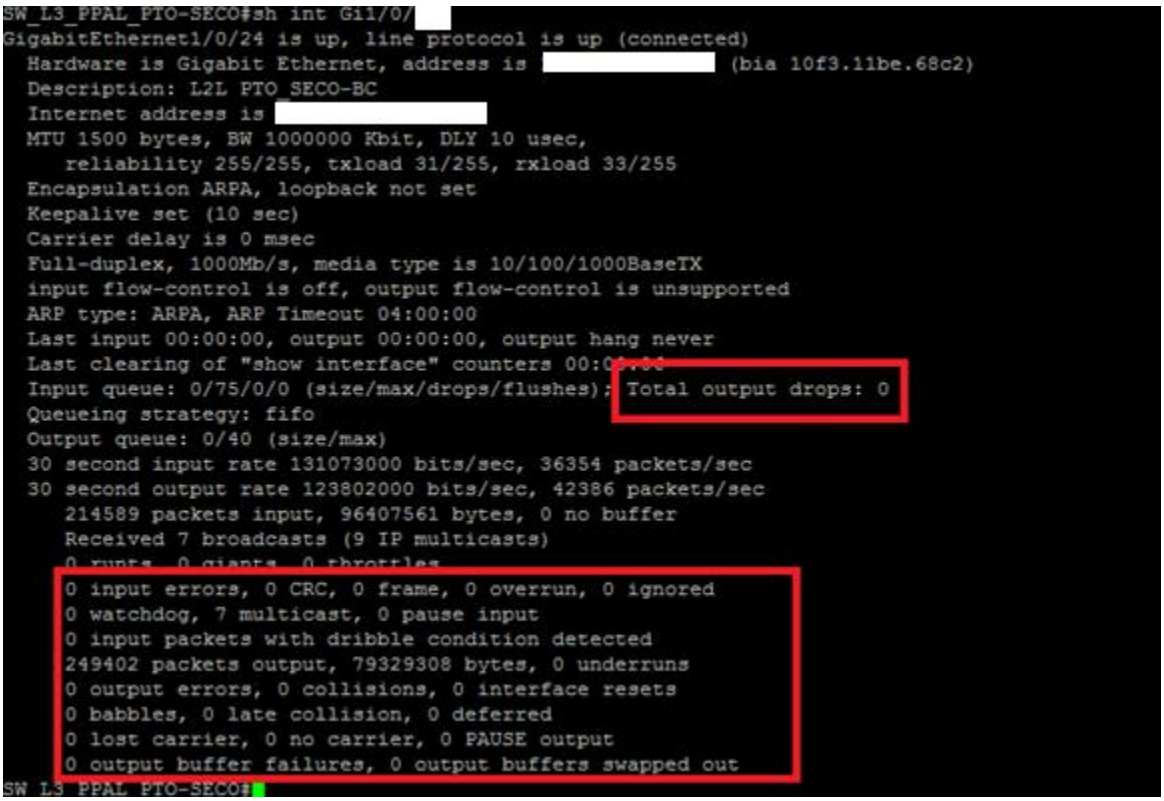


Figura12. **(Aplicación comando show interface Gi1/0/1 en SW Core Cisco3750X)**

La figura 12 muestra la configuración de la interface, se resalta que no se han presentado errores ni dropeos de paquetes desde la instalación del servicio.

La tabla de enrutamiento ha permanecido estable, no hay cambios en el protocolo de enrutamiento, no se presentan logs en los Switches ni en las interfaces y Sw multicapa, el servidor w-sus ha realizado las actualizaciones de los parches a las máquinas de la operación.

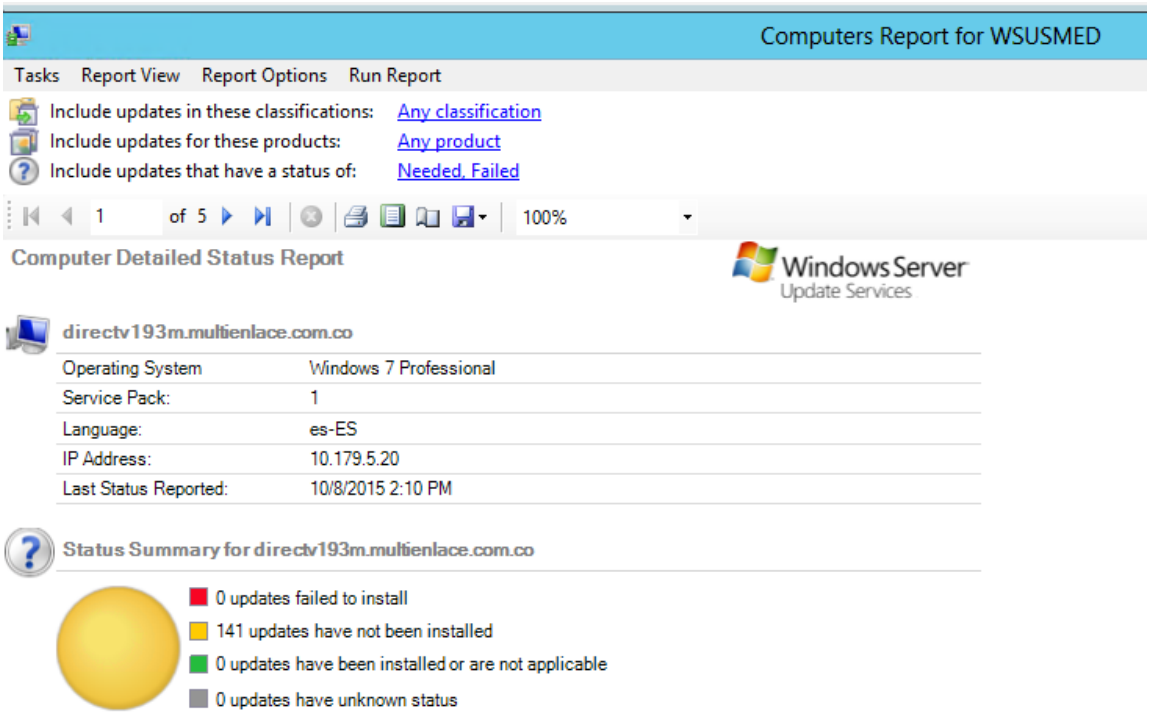


Figura13 **(Pantalla de actualizaciones realizadas por el servidor W-SUS).**

La figura indica el nivel de actualizaciones del sistema operativo generado hasta ese momento para las maquinas de la operación donde se evidencia conectividad al Datacenter.

Monitoreo de los equipos en Cacti

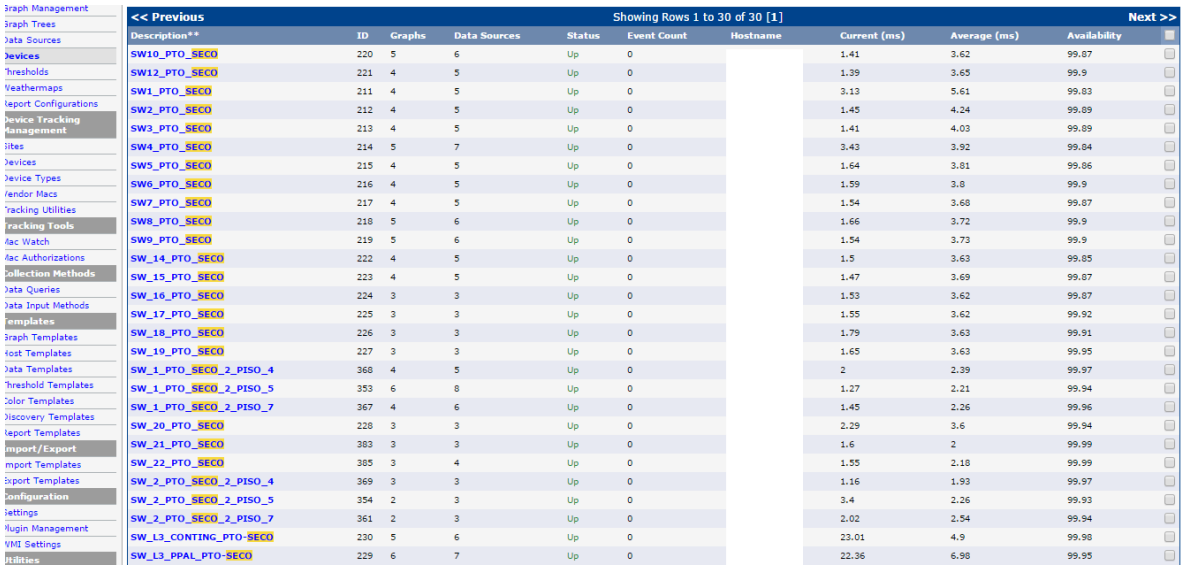


Figura14. **(Pantalla de monitoreo de los switchs de la sede PSeco).**

La figura muestra los switches monitoreados de la sede PSeco, su estado, consumo de CPU y tiempo de disponibilidad.

La herramienta CACTI reporta valores de CPU adecuados para los SW monitoreados

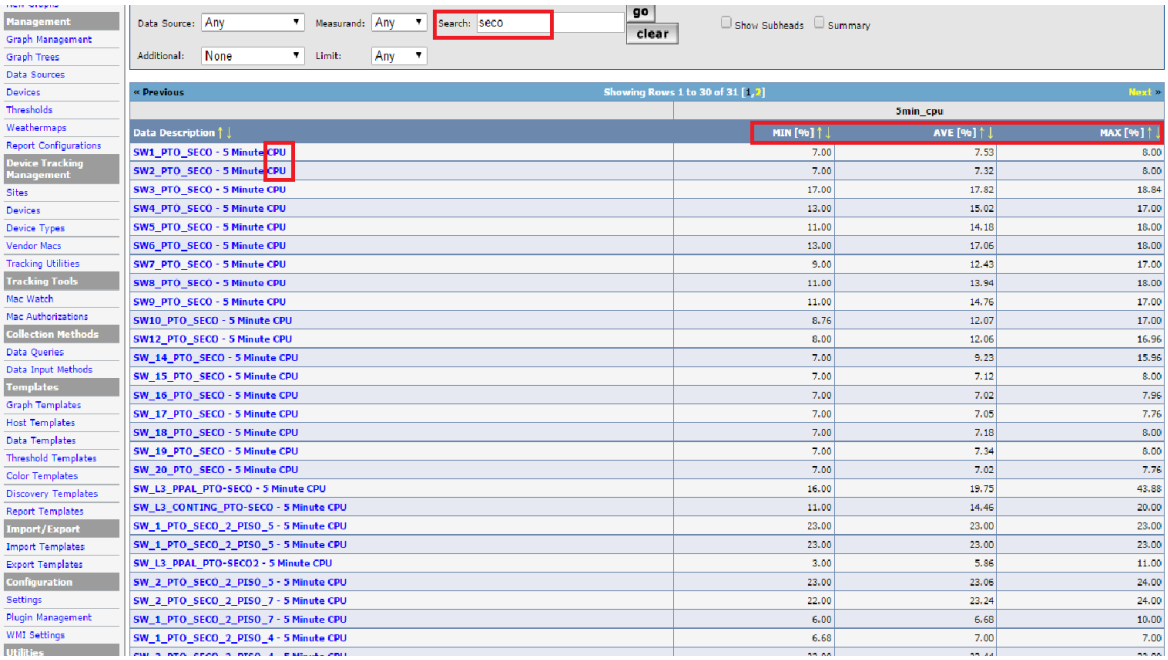


Figura15. **(Pantalla de monitoreo CPU de los switchs de la sede PSeco).**

La figura 12 muestra los switches monitoreados de la sede PSeco y los valores de consumo de CPU mínimo, promedio y máximo.

Monitoreo al tráfico en Cacti

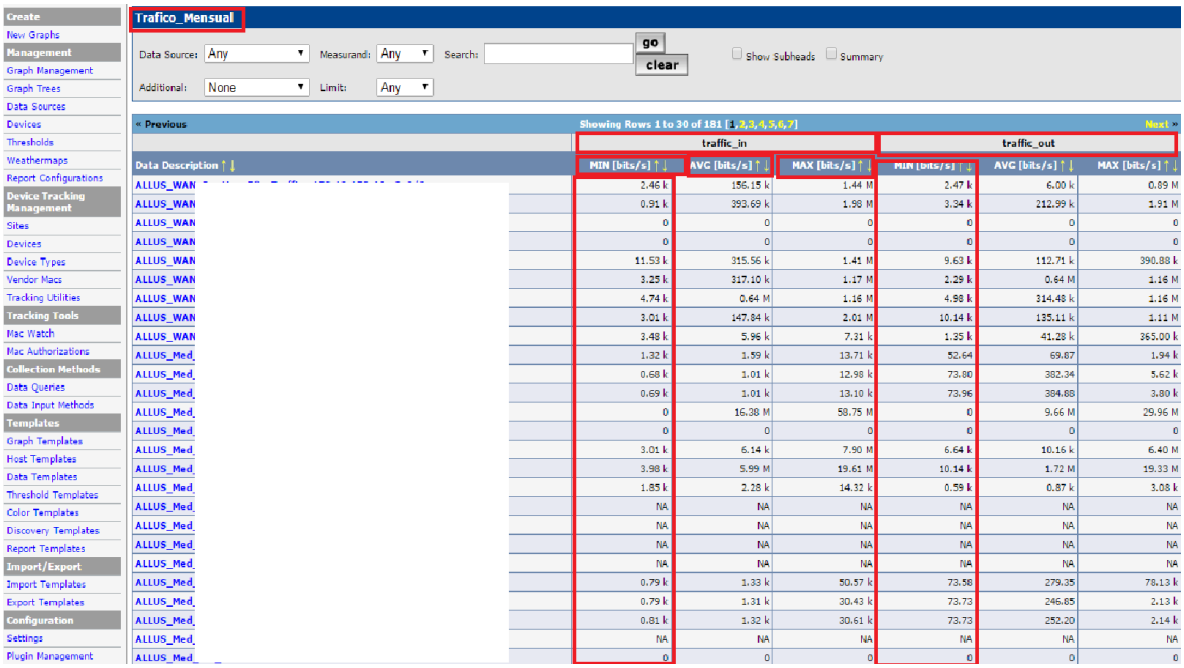


Figura16. **(Pantalla de monitoreo tráfico de los switchs de la sede PSeco).**

La figura 16 muestra los switches monitoreados de la sede PSeco y los valores de tráfico mensual entrante y saliente.

Monitoreo a la memoria de los equipos en Cacti

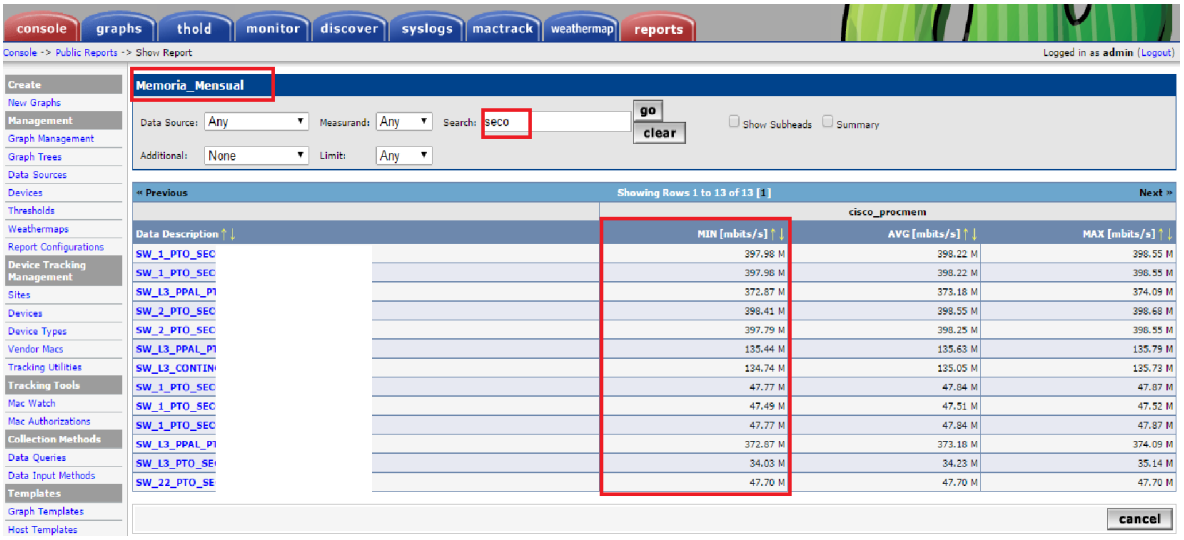


Figura17. (Pantalla de monitoreo memoria de los switchs de la sede PSeco).

La figura 17 muestra los switches monitoreados de la sede PSeco y los valores de memoria mensual mínimo, promedio y máximo.

Las figuras 15, 16 y 17 evidencian la instalación y configuración de los diferentes switches en la red de la sede PSeco y el monitoreo que se está efectuando a los equipos para analizar las estadísticas mensualmente y observar el performance de los equipos de telecomunicaciones en tráfico, memoria y CPU.

OPTIMIZACIÒN

Hasta el momento la red a tenido un buen comportamiento porque no se han reportado incidentes sobre los servicios de red, las pruebas de continuidad se efectuaron exitosamente, no se han presentado problemas con la calidad de la voz, no hay logs en el los switchs de los equipos que informen problemas del protocolo de enrutamiento, las tablas de enrutamiento han permanecido estables, no hay errores en las interfaces ni drops es importante aclarar que en el momento la red está a un 60% de su capacidad instalada.

El monitoreo debe continuar exhaustivamente para validar cambios en el comportamiento de la red y tráfico cuando se terminen de instalar el resto de operaciones.

RESULTADOS Y DISCUSIÓN

A continuación presentamos los resultados de la metodología implementada y los resultados de las configuraciones aplicadas en los Switchs es importante mencionar que mucha información fue cambiada o modificada para preservar la información de clientes, seguridad de la red y confidencialidad de la información.

Respecto al monitoreo se evidencia en la imagen el monitoreo de los equipos configurados en la herramienta Cacti

Figura18 **.Consola monitoreo de equipos**

La figura 13 relaciona los equipos monitoreados en Cacti por medio de la consola donde se pueden observar las alertas y se genera una alarma sonora para notificar el incidente.

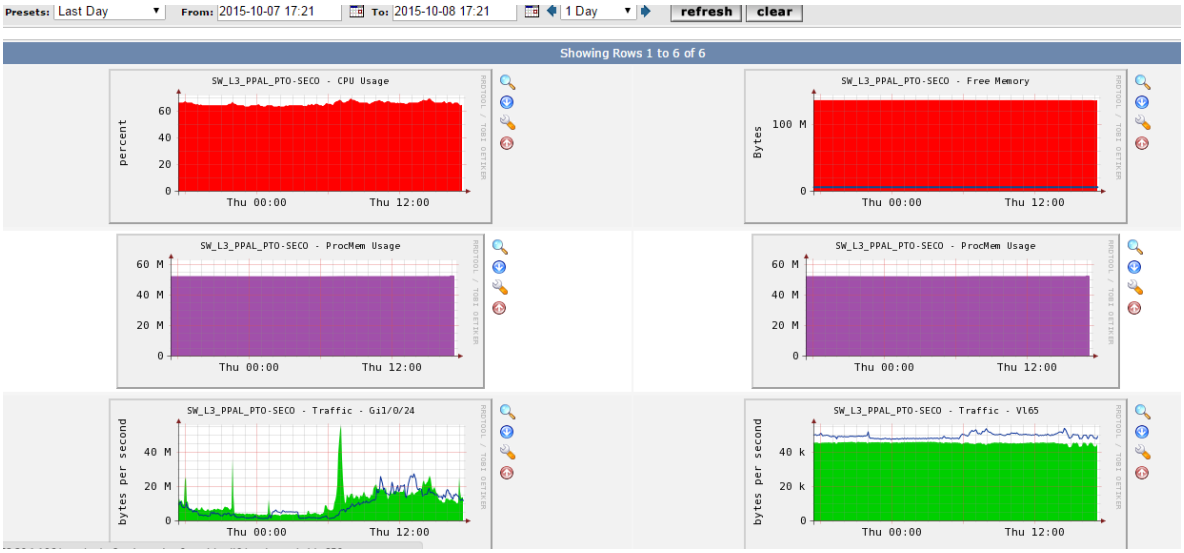


Figura19 **.Monitoreo de equipos en Cacti**

En la figura 19 se observa el comportamiento de memoria, CPU y trafico de un equipo seleccionado para analizar su comportamiento en un intervalo determinado.

Figura20 **.Monitoreo de tráfico en los enlaces por medio de la herramienta PRTG.**

La figura 20 muestra los niveles de tráfico en Kbits contra el tiempo que cursan por el enlace en un intervalo determinado.

La siguiente tabla relaciona el control de servicios y comportamiento del ancho de banda desde la instalación de los equipos.

PRUEBAS Y RESULTADOS DE CONECTIVIDAD ENTRE PSECO Y BERRÌO				
PRUEBA	**RESULTADO 1**	**RESULTADO 2**	**RESULTADO 3**	**RESULTADO 4**
PING A SERVER BERRIO	3ms	4ms	3ms	5ms
PING A SERVER BERRIO	4ms	3ms	4ms	4ms
PING A BERRIO DESDE CORE	1/5/9 ms	1/4/9 ms	1/4/9 ms	1/4/9 ms
PING CON PESO A BERRIO	Success rate is 99 percent (1999/2000), round-trip min/avg/max = 1/4/142 ms	Success rate is 100 percent (2000/2000), round-trip min/avg/max = 1/4/25 ms	Success rate is 99 percent (1998/2000), round-trip min/avg/max = 1/4/143 ms	Success rate is 100 percent (2000/2000), round-trip min/avg/max = 1/4/23 ms

TRACERT BERRIO	1 172.20.X.X 0 msec 8 msec 9 msec	1 172.20.X.X 0 msec 8 msec 0 msec	1 172.20.X.X 0 msec 6 msec 8 msec	1 172.20.X.X 0 msec 9 msec 10 msec
TELNET BERRIO	Exitoso	Exitoso	Exitoso	Exitoso
BW ENLACES L2L PAL	150M	230M	180M	140M
BW ENLACES L2L BCKUP	60M	78M	67M	58M
GRAFICAS	sin cortes	sin cortes	sin cortes	sin cortes
MEMORIA CORE PPAL	397.98 M	397.98 M	372.87 M	398.41 M
CPU CORE PPAL	16.00%	16.00%	16.00%	16.00%
MEMORIA CORE BKP	135.05 M	134.74 M	135.73 M	135.78 M
CPU CORE PPAL BKP	11.00%	11.00%	11.00%	11.00%

Tabla 8. Pruebas y resultados sobre conectividad entre PSeco y Data center Berrío

Los resultados obtenidos en las diferentes pruebas indican que los enlaces y equipos de la red LAN están comportándose de manera adecuada, los tiempos de ping tiene un promedio de 4 milisegundos tanto desde el core como desde los host, los Tracert están garantizando que los servicios se alcanzan a través de los enlaces y equipos implementados, el telnet garantiza la conexión exitosa a los servidores donde se alojan las aplicaciones, el

nivel tráfico en los enlaces L2L es soportado por los enlaces de 600 M, las graficas de monitoreo no han presentado cortes, los equipos de telecomunicaciones registran niveles de CPU, tráfico y memoria adecuados para una correcta operación.

Se implementó una estrella en malla entre los SW Core y de distribución para garantizar que ante incidentes en la red el tráfico pueda conmutar por las conexiones.

Después de analizar el modelo de conexión de las otras sedes al data center por medio de anillos independientes donde se presenta conexión bajo el modelo sede – data center con 2 enlaces con infraestructura diferente, se orientó la discusión en el modelo de integrar varias sedes bajo un mismo anillo con diferentes tecnologías de acceso entre cada una las sedes por medio de diferentes proveedores y rutas diversas para disminuir costos de operación, para Allus no es un modelo óptimo porque la importancia de la alta disponibilidad de enlaces para la continuidad del negocio no le permite asumir los riesgos de dejar una sede inactiva porque son los proveedores quienes tienen el control de los enlaces y no pueden validar que efectivamente no se tengan puntos de falla común.

CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

Se diseña e implementa la red LAN para la sede PSeco de Allus la principal fortaleza de la red es la alta disponibilidad basada en la redundancia que se obtiene en las diferentes capas del modelo jerárquico de red. Las pruebas de conectividad fueron exitosas con excelentes tiempos de respuesta y pruebas de saturación sobre el ancho de banda tanto para la red LAN como para el anillo L2L, se configuró el protocolo de enrutamiento EIGRP porque esta implementado en las otras sedes, la infraestructura de las red en su totalidad es Cisco.

Después de analizar la tabla de topologías de red y la importancia de la alta disponibilidad de servicios en la red se determina que la topología de estrella en malla es la más adecuada para garantizar acceso a las aplicaciones que permitan la atención de clientes finales la operación de los esquemas de continuidad del negocio y los niveles de servicio pactados con los clientes corporativos.

Se implementa la solución de conexión hacia el data center Berrio a través de 2 enlaces en tecnologías diferentes DWDM y Metroethernet, conectados a 2 Sw core que actúan como principal y backup en cada extremo de la solución, se realiza la prueba de

conectividad hacia las aplicaciones del data center y conmutación automática del tráfico en horas de la madrugada que garantiza que ante posibles fallas en uno de los brazos del anillo el otro esté en capacidad de transportar la voz y los datos con alto performance como debilidad de la solución hacia el data center está en que no se realiza la prueba desconectando la interfaz en horario hábil para validar los tiempos de conmutación del tráfico, para el negocio de contact center la facturación está basada en las horas ACD las cuales son las horas de conexión de los asesores en las que se encuentran disponibles para recibir y atender llamadas de los clientes al realizarse las pruebas en horarios de alto impacto se afectan los indicadores de servicio de la operación por llamadas colgadas y no contestadas, a los asesores se les afecta el tiempo de conexión estos factores implican un alto costo económico a la organización.

Para garantizar la alta disponibilidad de servicios se implementa conexión redundante entre los Switchs de la capa core y distribución, se tiene conexión entre los equipos Core principal y backup hacia cada uno de los SW de piso como fortaleza esta la conexión troncalizada entre los equipos y las políticas de QoS para dar prioridad a los paquetes de voz en todos los niveles de la topología, como se ha venido realizando paulatinamente la migración de las sedes satélites se evalúa la capacidad de los recursos instalados los cuales se encuentran todavía en garantía por el fabricante con IOS actualizado y cumplen los requerimientos tomados en cuenta en las fases de planeación, diseño e implementación en la metodología de diseño de redes PDDIOO de Cisco

La seguridad de la red se implementa aplicando las políticas de PCI-DSS solicitadas por los clientes corporativos las cuales son herramientas complementarias a las políticas de seguridad establecidas con frecuencia en las organizaciones algunas de las políticas más relevantes de PCI-DSS son: la no utilización de parámetros de seguridad y usuarios por defecto, usar y garantizar la actualización del antivirus, restricciones de acceso a la información que no es necesaria para el desempeño de la labor diaria, usuarios únicos para realizar trazabilidad de las transacciones y procesos, bloqueo de puertos USB en los equipos de la operación, está prohibido el acceso de celulares, equipos portátiles y unidades de almacenamiento como discos duros extraíbles, memorias USB.

Cada cliente tiene asignada una vlan la cual no se comparte para garantizar que no se tenga acceso recursos innecesarios o información crítica de los diferentes clientes, se tiene políticas de cerramiento en vidriera para individualizar las operaciones, bajo la premisa de que cada operación o cliente tiene su vlan se configuran ACLs por vlan que limita el acceso a los diferentes servicios y aplicaciones del data center.

Los equipos Core, distribución y acceso de la sede se configuran de manera que envíen alertas al correo corporativo de los analistas y personal del data center encargado de realizar el monitoreo de los equipos de telecomunicaciones por pérdidas de ping a los switchs, Cacti es una herramienta orientada a la captura de información, recopilación y análisis de estadísticas y tiene un pool de monitoreo de 5 minutos por lo tanto no es la herramienta más adecuada para actuar rápidamente ante incidentes de red, PRTG es una

herramienta orientada al reporte rápido de incidentes su pool está configurado para capturar estadísticas cada 10 segundos lo que la hace una herramienta muy versátil pero genera también genera un número importante de falsas alertas.

Se realizan pruebas de acceso a los aplicativos donde se obtiene que el 100% de los asesores cargan las aplicaciones exitosamente, en condiciones de producción todos los asesores deben alcanzar los aplicativos, no se tiene perfiles que excluyan acceso a determinadas aplicaciones se realizan pruebas de análisis de tráfico con un snifer, se adjunta reporte de conexión a las aplicaciones en Excel por parte de los usuarios, no se presentan logs de desconexión en los Switchs de core y distribución, las conexiones son estables los asesores no reportan problemas en los accesos a las diferentes aplicaciones y no hay reporte de incidentes a la mesa de ayuda.

Se recomienda a la organización analizar el cambio de política de vlan por puerto a vlan por MAC, Allus constantemente realiza actividades de migración de clientes a otras sedes esto incide negativamente generando sobrecostos operativos porque se debe contratar personal técnico e ingenieros que ejecuten las actividades de expansión y cambios de sedes de los clientes en horario fuera de operación normalmente en las noches y fines de semana, adicionalmente los servicios de plataformas de telefonía y grabación las licencias deben estar asociadas a las MACs de los equipos lo que facilitaría el trabajo de esas áreas.

En la visita realizada para conocer el funcionamiento y estado general de la red se encontraron falencias en la administración del cableado en otras sedes, peinar los racks adecuadamente para mantener el orden y la facilidad en la atención de incidentes en los cuartos técnicos.

Como trabajo futuro se encontraron varios equipos con IOS desactualizado y otros que están próximos a quedar por fuera de soporte y garantía, es necesario diseñar el plan de trabajo para actualizar los equipos, Peinar los cuartos técnicos que se encuentran desorganizados y realizar la compra, instalación y configuración de los nuevos switchs teniendo prelación por los Core que están próximos a salir de soporte por parte del fabricante.

Anexos

Característica	Beneficio
facilidades	• Configuración automática de nuevas unidades de pila o stacks que elimina reconfiguración.
Uso y Despliegue	• Protocolo de configuración dinámica de host (DHCP) de configuración automática de varios switches mediante un servidor de arranque facilita la instalación del interruptor.
	• La versión de Cisco IOS Software automático de comprobación y actualización ayudan a asegurar que todos los miembros de la pila tienen la misma versión de software.
	• QoS automático (AutoQoS) simplifica la configuración QoS en la voz sobre IP (VoIP) redes mediante la emisión de la interfaz y los comandos de Global Switch para detectar teléfonos IP de Cisco, clasificar el tráfico y ayudar a permitir la configuración de la cola de salida.
	• Gestión de la configuración Maestro ayuda a garantizar que todos los interruptores se actualizan automáticamente cuando el interruptor maestro recibe una nueva versión del software.
	• Gestión de la configuración maestra ayuda a garantizar que todos los interruptores se actualizan automáticamente cuando el interruptor maestro recibe una nueva versión del software.

	• Negociación automática en todos los puertos selecciona automáticamente el modo de transmisión de medio o dúplex completo para optimizar el ancho de banda.
	• Protocolo de troncal dinámico (DTP) facilita la configuración troncal dinámico en todos los puertos del switch.
	• Protocolo de Port Aggregation (PAgP) automatiza la creación de grupos de Cisco Fast EtherChannel ® o grupos Gigabit EtherChannel para enlazar a otro switch, router, o un servidor.
	• (LACP) Link Aggregation Control Protocol permite la creación de Ethernet canalizar con equipos que se ajusten a IEEE 802.3ad. Esta función es similar a la tecnología de Cisco EtherChannel y PAgP.
	• DHCP Relay permite que un agente de retransmisión DHCP para transmitir las peticiones DHCP en el servidor DHCP de la red.
	• IEEE 802.3z compatible con 1000BASE-SX, 1000BASE-LX / LH, 1000BASE-ZX, 1000BASE-T, y CWDM apoyo físico-interfaz a través de un módulo SFP-reemplazable proporciona una flexibilidad sin precedentes en el despliegue interruptor.
	• Existe una configuración predeterminada para ayudar a asegurar que el interruptor se puede conectar rápidamente a la red y puede pasar el tráfico con mínima intervención del usuario. Esta configuración predeterminada existe incluso si no hay ninguna configuración almacenada en la memoria Flash.

	• Interfaz de cruce automática dependiente del medio (MDIX) ajusta automáticamente la transmisión y recepción de pares si se instala un tipo de cable incorrecto (cruzado o recto).
Cisco EnergyWise	• Cisco EnergyWise para las emisiones de gases de efecto invernadero y la optimización operacional de costos mediante la medición, reporte y la reducción del consumo de energía en toda la infraestructura de la empresa, mucho más allá del ámbito de las TI.
Disponibilidad y escalabilidad	
Redundancia Superior de fallos de copia de seguridad	1: N maestro redundancia permite que cada miembro de la pila para servir como un maestro, proporcionando la más alta fiabilidad para el reenvío.
	La tecnología Cisco CrossStack UplinkFast (CSUF) proporciona una mayor redundancia y capacidad de recuperación de la red a través de la convergencia rápida spanning-tree (menos de 2 segundos) a través de una pila de switches con la tecnología Cisco StackWise.
	● Cruz-Pila EtherChannel ofrece la posibilidad de configurar la tecnología de Cisco EtherChannel través de los diferentes miembros de la pila para alta resiliencia.
	● Protocolo Rapid Spanning Tree IEEE 802.1w (RSTP) ofrece Rapid Spanning-tree convergencia independiente de temporizadores Spanning Tree y también ofrece el beneficio de procesamiento distribuido.

	● Unidades apiladas se comportan como un único nodo de spanning-tree.
	● Per-VLAN Rapid Spanning Tree (PVRST +) permite una rápida reconvergencia spanning-tree en una base por-VLAN spanning-tree, sin necesidad de la implementación de instancias de spanning-tree.
	● Protocolo Cisco Hot Standby Router (HSRP) es compatible para crear redundantes, topologías de enrutamiento a prueba de fallos.
	● Protocolo unidireccional Enlace Detección (UDLD) y UDLD agresivo permiten enlaces unidireccionales causados por cableado o fallas de puerto de fibra óptica incorrectas que se detecten y discapacitados en las interfaces de fibra óptica.
	● recuperación automática del interruptor puertos (errdisable) intenta automáticamente para reactivar un enlace que está desactivada debido a un error de red.
	● Sistemas de alimentación redundantes de soporte de Cisco RPS 2300 y RPS 675 proporciona superiores redundancia de alimentación de fuente para hasta 6 dispositivos de red Cisco, lo que mejora la tolerancia a fallos y el tiempo de actividad de red.
	● Enrutamiento Igualdad de costo para el balanceo de carga y redundancia.

	● Ancho de banda de la agregación de hasta 16 Gbps a través de la tecnología 10 Gigabit EtherChannel, 8 Gbps a través de la tecnología Gigabit EtherChannel, y hasta 800 Mbps a través de la tecnología Fast EtherChannel mejora la tolerancia a fallos y ofrece mayor velocidad de ancho de banda agregado entre los switches y routers y servidores individuales.
	● Ancho de banda de enlace ascendente se puede actualizar fácilmente mediante la adición de una versión de 10 Gigabit Ethernet a una pila de cableado-armario y la sustitución de la Ethernet Gigabit con enlaces ascendentes 10 Gigabit Ethernet sin tener que cambiar de pares de fibra.
Alto rendimiento de enrutamiento IP	● Cisco Express Forwardig arquitectura de enrutamiento de hardware proporciona extremadamente enrutamiento IP de alto rendimiento.
	● Protocolos de enrutamiento unicast IP Básico (estática, Routing Information Protocol Version 1 [RIPv1], RIPv2 y RIPng) son compatibles con las aplicaciones de enrutamiento de pequeña red.
	● Enrutamiento IPv6 (OSPFv6 y EIGRPv6) apoyo en el hardware para un máximo rendimiento. Se requiere la licencia servicios IP.
	● Protocolos de enrutamiento unicast IP Avanzado (Open Shortest Path First [OSPF], gateway interior Routing Protocolo [IGRP], IGRP mejorado [EIGRP], Border Gateway Protocol Version 4 [BGPv4, IS-ISv4]) son compatibles con el equilibrio de carga y la construcción escalable LANs. Se requiere que la imagen de los servicios IP.

	● basada en políticas de encaminamiento (PBR) permite un control superior al facilitar la redirección de flujo independientemente del protocolo de enrutamiento configurado. Se requiere que la imagen de los servicios IP.
	● HSRP proporciona balanceo de carga dinámico y conmutación por error para los enlaces enrutados; hasta 32 enlaces HSRP apoyados por unidad o pila.
	● Enrutamiento entre VLAN IP para la plena enrutamiento de nivel 3 entre 2 o más VLAN.
	● Protocol Independent Multicast (PIM) para el enrutamiento de multidifusión IP es compatible, incluyendo el modo PIM escasa (PIM-SM), el modo denso PIM (PIM-DM), y el modo de escasa densa PIM. Se requiere que la imagen de los servicios IP.
	• Enrutamiento es posible a través de la pila.
	Se recomiendan interfaces virtuales 128 de conmutación (SVIS). Máximo de 1000 son compatibles (en función del número de rutas y entradas de multidifusión). 468 puertos enrutados son apoyados por pila.
Integración Características de Cisco IOS Software	● por puerto de difusión, multidifusión, y el control de tormentas de unidifusión impide estaciones finales defectuosas degraden el rendimiento general del sistema.

Optimización del ancho de banda	● Apoyo Tree Protocol IEEE 802.1d Spanning para conexiones troncales redundantes y redes libres de bucles simplifica la configuración de la red y mejora la tolerancia a fallos.
	● TSVP + permite la Capa 2 de reparto de carga en los enlaces redundantes para utilizar eficientemente la capacidad adicional inherente a un diseño redundante
	● IEEE 802.1s Multiple Spanning Tree Protocol permite una instancia de spanning-tree por VLAN, para la Capa 2 de reparto de carga en los enlaces redundantes.
	● Enrutamiento Igualdad costo facilita el equilibrio de carga de capa 3 y la redundancia a través de la pila.
	● Dirección de proxy local Resolution Protocol (ARP) trabaja en conjunto con Private VLAN Edge para minimizar las emisiones y maximizar el ancho de banda disponible.
	● La VLAN1 puede ser desactivada en cualquier enlace individuo troncal VLAN.
	● VLAN Trunking Protocol (VTP) Consumo de poda límites de ancho de banda en los troncos de IVE por tráfico de difusión inundaciones sólo en enlaces troncales necesarias para llegar a los dispositivos de destino.
	● Internet Group Management Protocol (IGMP) espionaje ofrece cliente rápido une y las hojas de secuencias de multidifusión y los límites de tráfico de vídeo de ancho de banda intensivo sólo a los solicitantes.

	● Registro Multicast VLAN (MVR) envía continuamente secuencias de multidifusión en una VLAN de multidifusión, mientras que el aislamiento de las corrientes de suscriptor VLANs por razones de ancho de banda y de seguridad.
	● Hasta 48 grupos EtherChannel son apoyados por pila.
Stacking Escalable	● Apilamiento Cisco StackWise crea un interruptor de interconexión de 32 Gbps. El apilamiento no requiere puertos de usuario. Hasta 9 unidades pueden apilarse juntos durante un máximo de 468 puertos 10/100, 468, 108 puertos 10/100/1000 puertos ópticos de agregación, nueve 10 puertos Gigabit Ethernet, o cualquier mezcla de los mismos. Combinaciones de puertos adicionales pueden ser creados por el apilamiento juntos los switches de la serie Cisco Catalyst 3750 y los switches Cisco Catalyst 3750-E Series.
QoS y Control	
QoS avanzada	pila QoS permite QoS para ser configurados a través de toda la pila.
	Clase ● 802.1p de servicio (CoS) y servicios diferenciados punto de código se proporciona (DSCP) la clasificación de campo, utilizando el marcado y reclasificación en función de cada paquete por fuente y la dirección IP de destino, origen y destino de dirección MAC, o Capa de Control 4 Transmisión Protocolo / User Datagram Protocol (TCP / UDP) número de puerto.
	● Control del plano de Cisco y los datos del plano QoS ACL en todos

	los puertos ayudan a garantizar la correcta marca en función de cada paquete.
	4 colas de salida por puerto ayudan a activar la gestión diferenciada de hasta 4 tipos de tráfico a través de la pila.
	● forma de Round Robin (SRR) programación ayuda a garantizar la priorización diferencial de los flujos de paquetes de forma inteligente el mantenimiento de las colas de ingreso y colas de salida.
	(DMP) proporciona evitar la congestión en las colas de entrada y salida antes de que ocurra una interrupción.
	● cola de prioridad estricta ayuda a asegurar que los paquetes de mayor prioridad son atendidas por delante del resto del tráfico.
	● No hay penalización de rendimiento para la capacidad QoS altamente granulares.
Limitación Granular de velocidad	● Cisco comprometido tasa de información de la función (CIR) proporciona ancho de banda en incrementos tan bajos como 8 Kbps.
	Limitación de velocidad se proporciona sobre la base de la fuente y la dirección IP de destino, origen y destino de dirección MAC, Capa / información UDP 4 TCP, o cualquier combinación de estos campos, el uso de QoS ACL (ACL IP o MAC ACL), mapas de clase, y mapas de política.
	● Datos asincrónica fluye hacia arriba y abajo de la estación final o en el enlace ascendente se administran fácilmente usando la directiva de

	entrada y la configuración de salida.
	● Hasta 64 agregados o individuales policers están disponibles por Fast Ethernet o puerto Ethernet Gigabit.
Seguridad de la red	
Características de la seguridad para toda la red	● IEEE 802.1x permite la seguridad dinámica, basada en el puerto, proporcionando la autenticación de usuarios.
	● IEEE 802.1x con asignación de VLAN permite una asignación de VLAN dinámica para un usuario específico, independientemente de donde se conecta el usuario.● IEEE 802.1x with VLAN assignment allows a dynamic VLAN assignment for a specific user regardless of where the user is connected.
	● IEEE 802.1x con VLAN de voz permite a un teléfono IP para acceder a la VLAN de voz, independientemente del estado del puerto autorizado o no autorizado.
	● IEEE 802.1x y la seguridad del puerto se proporcionan para autenticar el puerto y administrar el acceso a la red para todas las direcciones MAC, incluida la del cliente.
	● IEEE 802.1x con una asignación ACL permite políticas específicas de seguridad basadas en la identidad, independientemente de donde se conecta el usuario.
	● IEEE 802.1x con VLAN invitada permite a los huéspedes sin clientes

802.1x para tener acceso a la red limitado en la VLAN de invitados.
● ACL VLAN de seguridad de Cisco en todas las VLAN evitan que los datos no autorizadas flujos de ser un puente dentro de las VLAN.
● estándar de Cisco y ACL del router de seguridad extendidos IP definen las políticas de seguridad en interfaces enrutadas para el control de plano y tráfico de datos plano.
● ACL basadas en puertos de Capa 2 interfaces permiten las políticas de seguridad que deben aplicarse en los puertos de conmutación individuales.
● Secure Shell (SSH) Protocolo, Kerberos y Simple Network Management Protocol Version 3 (SNMPv3) proporcionan seguridad de la red mediante la encriptación del tráfico de administrador durante las sesiones de Telnet y SNMP. Protocolo SSH, Kerberos y la versión criptográfica de SNMPv3 requieren una imagen especial software criptográfico debido a las restricciones de exportación de Estados Unidos.
● Private VLAN Edge proporciona seguridad y aislamiento entre los puertos de conmutación, lo que ayuda a garantizar que los usuarios no pueden husmear en el tráfico de otros usuarios.
● Dinámico ARP Inspection ayuda a garantizar la integridad del usuario al evitar que usuarios malintencionados explotando la naturaleza insegura del protocolo ARP.

	● DHCP Snooping evita que usuarios malintencionados spoofing un servidor DHCP y el envío de direcciones falsas. Esta característica es utilizada por otras características de seguridad primaria para prevenir una serie de otros ataques como el envenenamiento ARP.
	● IP Source Guard evita que un usuario malintencionado spoofing o hacerse cargo de la dirección IP de otro usuario mediante la creación de una mesa de unión entre la dirección del cliente IP y MAC, el puerto y VLAN.
	● Bidirectional data support on the Switched Port Analyzer (SPAN) port allows a Cisco Intrusion Detection System (IDS) to take action when an intruder is detected.
	● TACACS + y autenticación RADIUS facilitan el control centralizado del conmutador y restringir a los usuarios no autorizados alteren la configuración.
	● notificación de direcciones MAC permite a los administradores ser notificados de los usuarios añaden o eliminan de la red.

	● DHCP Snooping ayuda a los administradores con mapeo constante de IP a direcciones MAC. Esto se puede usar para prevenir los ataques que intentan envenenar la base de datos DHCP de unión y en evaluar límite de la cantidad de tráfico DHCP que entra en un puerto del conmutador.
	● La seguridad portuaria asegura el acceso a un puerto de acceso o troncal basada en la dirección MAC.
	● Después de un plazo específico, la característica de envejecimiento elimina la dirección MAC del conmutador para permitir que otro dispositivo se conecte al mismo puerto.
	● límite de confianza proporciona la capacidad de confiar en los ajustes de prioridad QoS si un teléfono IP está presente y para desactivar el ajuste de la confianza en el caso de que se retira el teléfono IP, lo que impide que un usuario malintencionado anulando las políticas de priorización en la red.
	● seguridad multinivel en el acceso a la consola impide que usuarios no autorizados puedan alterar la configuración del switch.
	● El modo de dirección-learning seleccionable por el usuario simplifica la configuración y mejora la seguridad.
	● unidad de datos de protocolo de puente (BPDU) guardia cierra Spanning interfaces habilitadas para PortFast árbol cuando se reciben las BPDU para evitar bucles de topología accidentales.

	● Spanning Tree Root Guardia (STRG) evita que los dispositivos de borde no en el control del administrador de la red se conviertan en nodos raíz del protocolo Spanning Tree.
	• Filtrado IGMP proporciona autenticación de multidifusión al filtrar los no suscriptores y limita el número de secuencias de multidifusión simultáneas disponibles por puerto.
	• Asignación Dinámica VLAN es compatible a través de la implementación de la capacidad del cliente VLAN Membership Policy Server para proporcionar flexibilidad en la asignación de puertos a las VLAN. VLAN dinámica facilita la asignación rápida de direcciones IP.
	• Cisco CMS Software security wizards ease the deployment of security features for restricting user access to a server as well as to a portion or all of the network.
	● 1000 entradas de control de acceso (ACE) son compatibles.
manejabilidad	
Manejabilidad	• Soporte del software Cisco IOS CLI proporciona una interfaz de

Superior	usuario común y conjunto de comandos con todos los routers y switches Cisco Catalyst de escritorio de Cisco.
	Cambio de plantillas de gestor de bases para el acceso, enrutamiento, y el despliegue de VLAN permite al administrador para maximizar fácilmente la asignación de memoria para las características deseadas en base a requisitos de despliegue específico.
	• Troncos de VLAN pueden crearse desde cualquier puerto, utilizando ya sea basada en estándares 802.1Q tagging o Cisco Inter-Switch Link (ISL), la arquitectura VLAN.
	• Se admiten Hasta 1005 VLAN por switch o apilar y hasta 128 instancias de spanning-tree por switch.
	• 4000 VLAN IDs are supported.
	• VLAN de voz simplifica las instalaciones de telefonía, manteniendo el tráfico de voz en una VLAN separada para facilitar la administración y resolución de problemas.
	• Cisco VLAN Trunking Protocol (VTP) soporta VLANs dinámicas y configuración tronco dinámico en todos los interruptores.
	Enrutador Protocolo de administración de Cisco Grupo de interruptores cliente.

	• Snooping IGMP proporciona cliente rápido une y las hojas de secuencias de multidifusión y los límites de tráfico de vídeo de ancho de banda intensivo sólo a los solicitantes.
	Interruptor remoto Puerto Analyzer (RSPAN) permite a los administradores supervisar de forma remota puertos en una red de conmutación de Capa 2 de cualquier otro cambio en la misma red.
	• Para mejorar la gestión del tráfico, monitoreo y análisis, el monitoreo remoto incorporado (RMON) agente de software es compatible con 4 grupos RMON (historial, estadísticas, alarmas y eventos).
	• Capa 2 traceroute facilita la resolución de problemas mediante la identificación de la ruta física que un paquete desde el origen al destino.
	• Todos los 9 grupos RMON están soportados a través de un puerto SPAN, que permite la supervisión del tráfico de un puerto único, un grupo de puertos, o toda la pila de un solo analizador de red o sonda RMON.
	• Sistema de nombres de dominio (DNS) proporciona una resolución de dirección IP con la definida por el usuario-
	• Trivial File Transfer Protocol (TFTP) reduce el costo de administración de actualizaciones de software mediante la descarga desde una ubicación centralizada.
	• Protocolo de sincronización de red (NTP) proporciona una indicación de la hora exacta y consistente para todos los interruptores de la intranet.

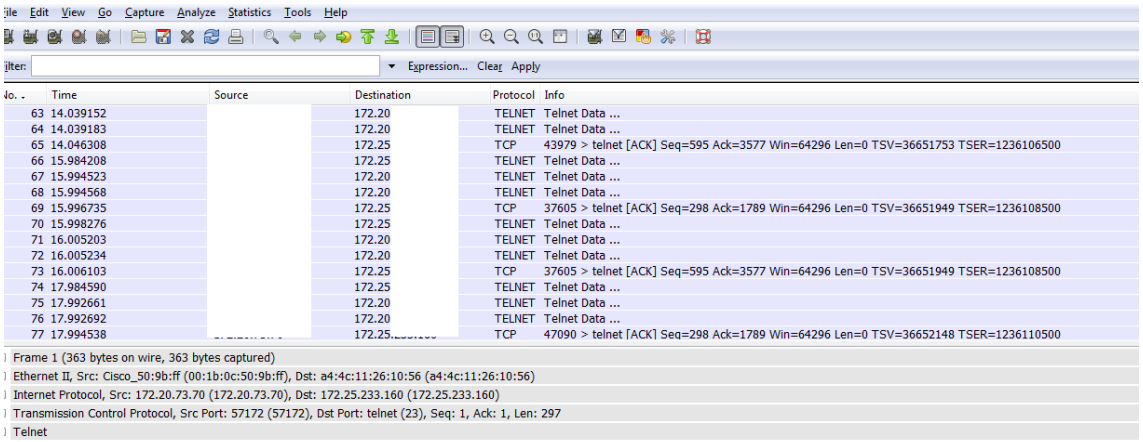
	• Multifunción LED por puerto para el estado del puerto; modo half-duplex y full-duplex; y 10BASE-T, 100BASE-TX y 1000BASE-T indicación, así como indicadores LED de estado de nivel interruptor para el sistema, redundante-fuente de alimentación, y la utilización del ancho de banda proporcionan un sistema integral y conveniente gestión visual.
	• SPAN funciona a través de todos los puertos en una pila.
Cisco Network Assistant Software	● Software Asistente de red de Cisco proporciona una interfaz de administración basada en web fácil de usar, a través de un navegador Web estándar.
	● Configuración del puerto simplificado a través de Cisco Smartports.
	● Cisco AVVID (Arquitectura para voz, video y datos integrados) necesitan sólo unas entradas del usuario para configurar automáticamente el interruptor para gestionar de manera óptima los diferentes tipos de tráfico: voz, video, multidifusión y datos de alta prioridad.
	● Un asistente de seguridad se proporciona para restringir el acceso no autorizado a las aplicaciones, servidores y redes.
	● Software Asistente de red de Cisco permite la gestión de una pequeña red de Cisco Catalyst 3750-E, 3750, 3560-E, 3560, 3550, 2960 y 2950 Series Switches a través de una única dirección IP, sin la limitación de estar ubicado físicamente en el mismo armario de cableado. Compatibilidad completa ayuda a asegurar cualquier combinación de

	estos interruptores se puede manejar con una serie de conmutadores Cisco Catalyst 3750.
	● actualización de arrastrar y soltar Cisco IOS Software simplifica el proceso de actualización del software IOS de Cisco por que no impliquen un servidor Trivial File Transfer Protocol (TFTP).
	• La función de actualización de software permite a un solo clic de actualización de software de múltiples switches en una comunidad de Cisco Catalyst 3750-E, 3750, 3560-E, 3560, 3550, 2960, y 2950 Series Switches. Clonación de configuración facilita el despliegue rápido de redes. El interruptor maestro actualiza automáticamente cada pila.
	● Software Asistente de Cisco Network se ha ampliado para incluir configuraciones de funciones de varias capas, como los protocolos de enrutamiento, ACLs, y los parámetros de calidad de servicio.
	● agrupación Cisco es ahora compatible con el descubrimiento y miembro de la creación del clúster a través de un único Cisco Catalyst 3750 Switch Series enrutan hop, permitiendo que toda la LAN que se gestiona a través de una única interfaz web (y con una única dirección IP, si se desea).
	● Cisco Network Assistant Software Modo Guía asiste en la configuración de las poderosas funciones avanzadas a través de

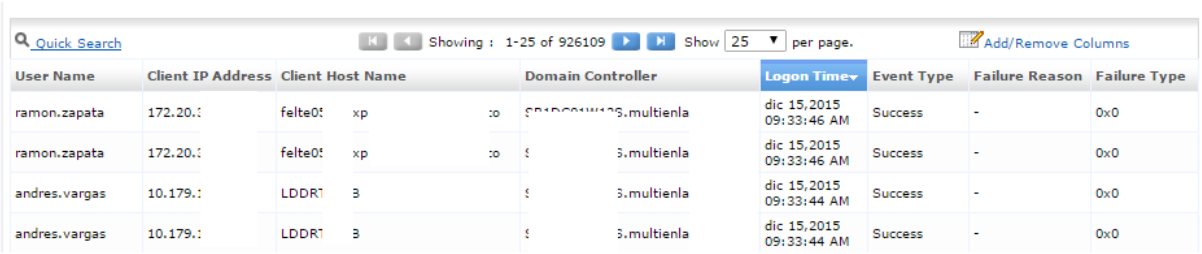
	instrucciones paso a paso.
	● Cisco Network Assistant Software proporciona ayuda en línea mejorado para la asistencia sensible al contexto.
	● La interfaz gráfica fácil de usar proporciona una vista de mapa de topología y el panel frontal de la agrupación y pilas.
	● Capacidades de configuración multidispositivo y multipuerto permiten a los administradores ahorrar tiempo mediante la configuración de funciones a través de múltiples conmutadores y puertos simultáneamente.
	● Gestión basada en Web para un punto de acceso inalámbrico Cisco Aironet se inicia haciendo clic en el icono correspondiente en el mapa de topología.
	● La interfaz de usuario personalizada permite la modificación de los intervalos de sondeo, vistas de tabla y otros ajustes dentro de Cisco Software CMS y conserva estos ajustes.
	● Notificación de alarma proporciona notificación por correo electrónico automatizado de errores de la red y los umbrales de alarma.
puertos inteligentes	● macros simples ayudan a habilitar las características avanzadas de QoS con un comando en lugar de múltiples comandos en el archivo de configuración.
Web Setup Fácil	● utilidad de configuración del navegador Web permite a un solo clic de

	inicialización para las direcciones IP y las contraseñas.
Soporte Cisco Works	● El software de gestión de red Cisco Works proporciona capacidades de gestión en función de cada puerto y por switch, que proporciona una interfaz de gestión común para los routers de Cisco, switches y hubs. Stacking es compatible.
	● SNMPv1, v2c y v3 apoyo y la interfaz Telnet ofrece una gestión integral en banda, y una consola de administración basada en CLI proporciona detallada gestión fuera de banda.
	● Versiones Cisco Discovery Protocol 1 y 2 ayuda permiten a una estación de gestión de red CiscoWorks para el descubrimiento del interruptor automático.
	● La solución de gestión de LAN CiscoWorks 2000 proporciona soporte.

(«Cisco Catalyst 3750 Series Switches Data Sheet», s. f.)



User Name	Client IP Address	Logon Time	Event Type	Failure Reason	Failure Type
briayan.henao		dic 14,2015 05:26:41 PM	Success	-	0x0
cindy.rodriguez.z		dic 14,2015 05:28:04 PM	Success	-	0x0
andres.vargas		dic 15,2015 06:34:24 AM	Success	-	0x0
yesica.cespedes		dic 14,2015 09:26:48 AM	Success	-	0x0
laura.aguirre.p		dic 15,2015 08:00:04 AM	Success	-	0x0
franci.villa		dic 15,2015 08:03:51 AM	Success	-	0x0
prtg.scan		dic 14,2015 09:52:46 AM	Success	-	0x0
Omar.betancurt.d		dic 14,2015 05:33:59 PM	Success	-	0x0
sindy.pinilla		dic 15,2015 07:11:31 AM	Success	-	0x0
yuliet.ocampo		dic 14,2015 09:17:01 AM	Success	-	0x0
Diana.Giraldo.H		dic 14,2015 05:10:50 PM	Success	-	0x0



Quick Search Showing : 1-25 of 926109 Show 25 per page. Add/Remove Columns

User Name	Client IP Address	Client Host Name	Domain Controller	Logon Time	Event Type	Failure Reason	Failure Type
ramon.zapata	172.20.[illegible]	felte0[illegible] xp :o	[illegible].multienla	dic 15,2015 09:33:46 AM	Success	-	0x0
ramon.zapata	172.20.[illegible]	felte0[illegible] xp :o	[illegible].multienla	dic 15,2015 09:33:46 AM	Success	-	0x0
andres.vargas	10.179.[illegible]	LDDR[illegible] B	[illegible].multienla	dic 15,2015 09:33:44 AM	Success	-	0x0
andres.vargas	10.179.[illegible]	LDDR[illegible] B	[illegible].multienla	dic 15,2015 09:33:44 AM	Success	-	0x0

Evidencia conexión de usuarios a los servidores para alcance de las aplicaciones se modifica o elimina información del direccionamiento y servidores para garantizar confidencialidad de la información.

Los comandos ejecutados para configuración de la interfaz G1/0/24 en el SW Core PSeco principal

```
#conf t
 commands, one per line.  End with CNTL/Z.
(config)#int Gi1/0/24
(config-if)#description PTO SECO-BERRIO
(config-if)#no switc
(config-if)#no switchport
(config-if)#
(config-if)#dampening
(config-if)#ip address 172.20.217.69 255.255.255.252
(config-if)#no sh
(config-if)#no shutdown
(config-if)#
(config-if)#^Z
#
#
```

Comandos ejecutados para configuración de la interfaz Gi1/0/2 en el SW Core Berrío para la comunicación al data center con el enlace L2L.

```
#conf t
 commands, one per line.  End with CNTL/Z.
(config)#int Gi1/0/2
(config-if)#description PTO SECO
(config-if)#no switc
(config-if)#no switchport
(config-if)#
(config-if)#dampening
(config-if)#ip address 172.20.217.70 255.255.255.252
(config-if)#no sh
(config-if)#no shutdown
(config-if)#
(config-if)#^Z
#
#
```

Configuración interfaz Gi1/0/20 del SW Core Secundario PSeco

```
#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#int Gi1/0/20
(config-if)#description BERRIO METRO
(config-if)#no switchport
(config-if)#ip address 172.20.217.97 255.255.255.252
(config-if)#dampening
(config-if)#no shutdown
```

Pasos para configuración interfaz en el SW Core backup Berrio (Datacenter)

Por medio del enlace Metroethernet.

```
#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#int Gi1/45
(config-if)#no switchport
(config-if)#ip address 172.20.217.98 255.255.255.252
(config-if)#dampening
(config-if)#no shutdown
(config-if)#description PSECO-METRO
```

Con el comando description registramos un nombre o identificador para la interfaz que relaciona o asocia el servicio, el comando no switchport permite registrar el direccionamiento IP en la interfaz aplicada, la sentencia ip address permitió agregar la dirección IP en mascara 30 donde tenemos 2 direcciones IPs disponibles (172.20.217.69 y 172.20.217.70) asignados para el enlace DWDM en cada extremo del enlace, con el comando dampening generamos la configuración para que el puerto se ponga en shutdown en el caso de intermitencias sobre los enlaces, la interfaz se habilita con el comando no shutdown.

Pasos configuración vlan 160 y HSRP en Switch Core principal

```
SW_L3_PPAL_PTO-SECO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_L3_PPAL_PTO-SECO(config)#int vl 160
SW_L3_PPAL_PTO-SECO(config-if)#ip address 172.20.160.2 255.255.255.0
SW_L3_PPAL_PTO-SECO(config-if)#description Vlan Television
SW_L3_PPAL_PTO-SECO(config-if)#ip helper-address 172.20.161.4
SW_L3_PPAL_PTO-SECO(config-if)#standby 160 ip 172.20.160.1
SW_L3_PPAL_PTO-SECO(config-if)#standby 160 priority 150
SW_L3_PPAL_PTO-SECO(config-if)#standby 160 pree
SW_L3_PPAL_PTO-SECO(config-if)#standby 160 preempt
```

Pasos Tag de la vlan 160 en el Core principal

```
SW_L3_PPAL_PTO-SECO#
SW_L3_PPAL_PTO-SECO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_L3_PPAL_PTO-SECO(config)#vlan 160
SW_L3_PPAL_PTO-SECO(config-vlan)#name TELEVISION
SW_L3_PPAL_PTO-SECO(config-vlan)#^Z
SW_L3_PPAL_PTO-SECO#
```

Pasos configuración Vlan 160 y HSRP en Core Backup de PSeco

```
SW_L3_CONTING_PTO-SECO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_L3_CONTING_PTO-SE(config)#interface Vlan160
SW_L3_CONTING_PTO-SE(config-if)# description Vlan Television
SW_L3_CONTING_PTO-SE(config-if)# ip address 172.20.160.2 255.255.255.0
SW_L3_CONTING_PTO-SE(config-if)# ip helper-address 172.20.161.4
SW_L3_CONTING_PTO-SE(config-if)# standby 160 ip 172.20.160.1
SW_L3_CONTING_PTO-SE(config-if)#standby 160 priority 50
SW_L3_CONTING_PTO-SE(config-if)#standby 160 preempt
```

Tag vlan 160 en SW Core Backup

```
SW_L3_CONTING_PTO-SE(config)#vlan 160
SW_L3_CONTING_PTO-SE(config-vlan)#name TELEVISION
SW_L3_CONTING_PTO-SE(config-vlan)#^Z
SW_L3_CONTING_PTO-SECO#
```

Pasos configuración vlan 161 y HSRP en Switch Core principal

```
SW_L3_PPAL_PTO-SECO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_L3_PPAL_PTO-SECO(config)#interface Vlan161
SW_L3_PPAL_PTO-SECO(config-if)# description Vlan BANCO
SW_L3_PPAL_PTO-SECO(config-if)# ip address 172.20.161.2 255.255.255.0
SW_L3_PPAL_PTO-SECO(config-if)# ip helper-address 172.20.161.4
SW_L3_PPAL_PTO-SECO(config-if)# standby 161 ip 172.20.161.1
SW_L3_PPAL_PTO-SECO(config-if)# standby 161 priority 150
SW_L3_PPAL_PTO-SECO(config-if)# standby 161 preempt
SW_L3_PPAL_PTO-SECO(config-if)#end
SW_L3_PPAL_PTO-SECO#
SW_L3_PPAL_PTO-SECO#
```

Pasos configuración Tag vlan 161 en switch Core principal PSeco

```
SW_L3_PPAL_PTO-SECO#
SW_L3_PPAL_PTO-SECO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_L3_PPAL_PTO-SECO(config)#vlan 161
SW_L3_PPAL_PTO-SECO(config-vlan)#name Bancos
SW_L3_PPAL_PTO-SECO(config-vlan)#^Z
SW_L3_PPAL_PTO-SECO#
```

Pasos configuración vlan 161 y HSRP en Switch Core Backup

```
SW_L3_CONTING_PTO-SECO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_L3_CONTING_PTO-SE(config)#interface Vlan161
SW_L3_CONTING_PTO-SE(config-if)# description Vlan BANCO
SW_L3_CONTING_PTO-SE(config-if)# ip address 172.20.161.3 255.255.255.0
SW_L3_CONTING_PTO-SE(config-if)# ip helper-address 172.20.161.4
SW_L3_CONTING_PTO-SE(config-if)# standby 161 ip 172.20.161.1
SW_L3_CONTING_PTO-SE(config-if)# standby 161 priority 50
SW_L3_CONTING_PTO-SE(config-if)# standby 161 preempt
SW_L3_CONTING_PTO-SE(config-if)#end
SW_L3_CONTING_PTO-SECO#
```

Pasos configuración Tag vlan 161 en Switch Core Backup

```
SW_L3_CONTING_PTO-SE(config)#vlan 161
SW_L3_CONTING_PTO-SE(config-vlan)#name BANCOS
SW_L3_CONTING_PTO-SE(config-vlan)#^Z
SW_L3_CONTING_PTO-SECO#
```

Pasos configuración vlan 162 y HSRP en Switch Core principal

```
SW_L3_PPAL_PTO-SECO#
SW_L3_PPAL_PTO-SECO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_L3_PPAL_PTO-SECO(config)#interface Vlan162
SW_L3_PPAL_PTO-SECO(config-if)# description Vlan ASEGURADORA
SW_L3_PPAL_PTO-SECO(config-if)# ip address 172.20.162.2 255.255.255.0
SW_L3_PPAL_PTO-SECO(config-if)# ip helper-address 172.20.162.4
SW_L3_PPAL_PTO-SECO(config-if)# standby 162 ip 172.20.162.1
SW_L3_PPAL_PTO-SECO(config-if)# standby 162 priority 150
SW_L3_PPAL_PTO-SECO(config-if)# standby 162 preempt
SW_L3_PPAL_PTO-SECO(config-if)#end
SW_L3_PPAL_PTO-SECO#
```

Pasos configuración Tag vlan 162 en el Switch Core principal

```
SW_L3_PPAL_PTO-SECO#
SW_L3_PPAL_PTO-SECO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_L3_PPAL_PTO-SECO(config)#
SW_L3_PPAL_PTO-SECO(config)#vl 162
SW_L3_PPAL_PTO-SECO(config-vlan)#name ASEGURADORA
SW_L3_PPAL_PTO-SECO(config-vlan)#^Z
SW_L3_PPAL_PTO-SECO#
```

Pasos configuración vlan 162 y HSRP en Switch Core Backup

```
SW_L3_CONTING_PTO-SECO#
SW_L3_CONTING_PTO-SECO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_L3_CONTING_PTO-SE(config)#interface Vlan162
SW_L3_CONTING_PTO-SE(config-if)# description Vlan ASEGURADORA
SW_L3_CONTING_PTO-SE(config-if)# ip address 172.20.162.3 255.255.255.0
SW_L3_CONTING_PTO-SE(config-if)# ip helper-address 172.20.162.4
SW_L3_CONTING_PTO-SE(config-if)# standby 162 ip 172.20.162.1
SW_L3_CONTING_PTO-SE(config-if)# standby 162 priority 50
SW_L3_CONTING_PTO-SE(config-if)# standby 162 preempt
SW_L3_CONTING_PTO-SE(config-if)#end
SW_L3_CONTING_PTO-SECO#
```

Pasos configuración vl 162 en Core Backup

```
SW_L3_CONTING_PTO-SECO#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
SW_L3_CONTING_PTO-SE(config)#vlan 162
SW_L3_CONTING_PTO-SE(config-vlan)#name ASEGURADORA
SW_L3_CONTING_PTO-SE(config-vlan)#^Z
SW_L3_CONTING_PTO-SECO#
SW_L3_CONTING_PTO-SECO#
```

Se realizó la configuración de las interfaces para la conexión entre los Switches Core.

Pasos configuración interfaz Gi1/0/1 Switch Core Backup

```
SW_L3_CONTING_PTO-SE(config)#int GigabitEthernet1/0/1
SW_L3_CONTING_PTO-SE(config-if)#^Z
SW_L3_CONTING_PTO-SECO#
SW_L3_CONTING_PTO-SECO#
SW_L3_CONTING_PTO-SECO#
SW_L3_CONTING_PTO-SECO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_L3_CONTING_PTO-SE(config)#int GigabitEthernet1/0/1
SW_L3_CONTING_PTO-SE(config-if)#desc
SW_L3_CONTING_PTO-SE(config-if)#description HSRP
SW_L3_CONTING_PTO-SE(config-if)#switchport trunk encapsulation dot1q
SW_L3_CONTING_PTO-SE(config-if)#switchport mode trunk
SW_L3_CONTING_PTO-SE(config-if)#^Z
SW_L3_CONTING_PTO-SECO#
```

Pasos Configuración interfaz Gi1/0/2 Switch Core Principal

```
SW_L3_PPAL_PTO-SECO#
SW_L3_PPAL_PTO-SECO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_L3_PPAL_PTO-SECO(config)#int Gi1/0/2
SW_L3_PPAL_PTO-SECO(config-if)#description HSRP
SW_L3_PPAL_PTO-SECO(config-if)#switchport mode trunk
SW_L3_PPAL_PTO-SECO(config-if)#switchport trunk encapsulation dot1q
```

Se configuran los usuarios locales para la conexión a los equipos con el siguiente procedimiento.

```
#conf t
Enter configuration commands, one per line.  End with CNTL/Z.

(config)#username mrubiano privile
(config)#username mrubiano pass
(config)#username mrubiano password [redacted]
(config)#^Z
```

Pasos para la configuración de la interfaz Gi1/0/8 del SW Core

```
#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
config)#int GigabitEthernet1/0/8
config-if)#description SW1_PISO_4_PS
config-if)#switchport trunk encapsulation dot1q
config-if)#switchport mode trunk
config-if)#
config-if)#^Z
```

El motor de enrutamiento es EIGRP el cual se configuro con las siguientes sentencias

```
(config)#router eigrp 5
(config-router)#network 172.20.0.0
(config-router)#no auto-summary
(config-router)#^Z
```

En el SW Core Principal y Backup se configura el Banner motd

En el Core Principal

```
banner motd ^C
              ************************************
              ************************************
              ****                            ****
              ****          MEDELLIN          ****
              ****       CORE PPAL PTO SECO    ****
              ****                            ****
              ************************************
              ************************************
+---------------------------------------------------------------------------+
| Este sistema de computo (incluyendo todo su hardware y sus perifericos)|
| es de uso restringido. Cualquier utilizacion, modificacion o acceso no |
| autorizado a este sistema puede resultar en una accion disciplinaria o |
| acusacion legal.                                                        |
|                                                                         |
|#########################################################################|
+---------------------------------------------------------------------------+
^C
```

En el Core Secundario

```
banner motd ^C
              ************************************
              ************************************
              ****                            ****
              ****          MEDELLIN          ****
              ****    CORE CONTING PTO SECO    ****
              ****                            ****
              ************************************
              ************************************
+---------------------------------------------------------------------------+
| Este sistema de computo (incluyendo todo su hardware y sus perifericos)|
| es de uso restringido. Cualquier utilizacion, modificacion o acceso no |
| autorizado a este sistema puede resultar en una accion disciplinaria o |
| acusacion legal.                                                        |
|                                                                         |
|#########################################################################|
+---------------------------------------------------------------------------+
^C
```

Para realizar la conexión remota o VTY se configuró de la siguiente manera en los equipos.

```
SW_L3_PPAL_PTO-SECO(config)#line vty 5 15
SW_L3_PPAL_PTO-SECO(config-line)#exec-timeout 10 10
SW_L3_PPAL_PTO-SECO(config-line)#password 7 [illegible]
SW_L3_PPAL_PTO-SECO(config-line)#logging synchronous
SW_L3_PPAL_PTO-SECO(config-line)#length 0
SW_L3_PPAL_PTO-SECO(config-line)#transport input ssh
SW_L3_PPAL_PTO-SECO(config-line)#^Z
SW_L3_PPAL_PTO-SECO#
```

Configuración conexión por consola

```
SW_L3_PPAL_PTO-SECO#
SW_L3_PPAL_PTO-SECO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_L3_PPAL_PTO-SECO(config)#line con 0
SW_L3_PPAL_PTO-SECO(config-line)#exec-timeout 10 10
SW_L3_PPAL_PTO-SECO(config-line)#password 7 04091F562A7140190A36
SW_L3_PPAL_PTO-SECO(config-line)#logging synchronous
SW_L3_PPAL_PTO-SECO(config-line)#length 0
SW_L3_PPAL_PTO-SECO(config-line)#transport input ssh
```

Pasos configuración vlan administrativa

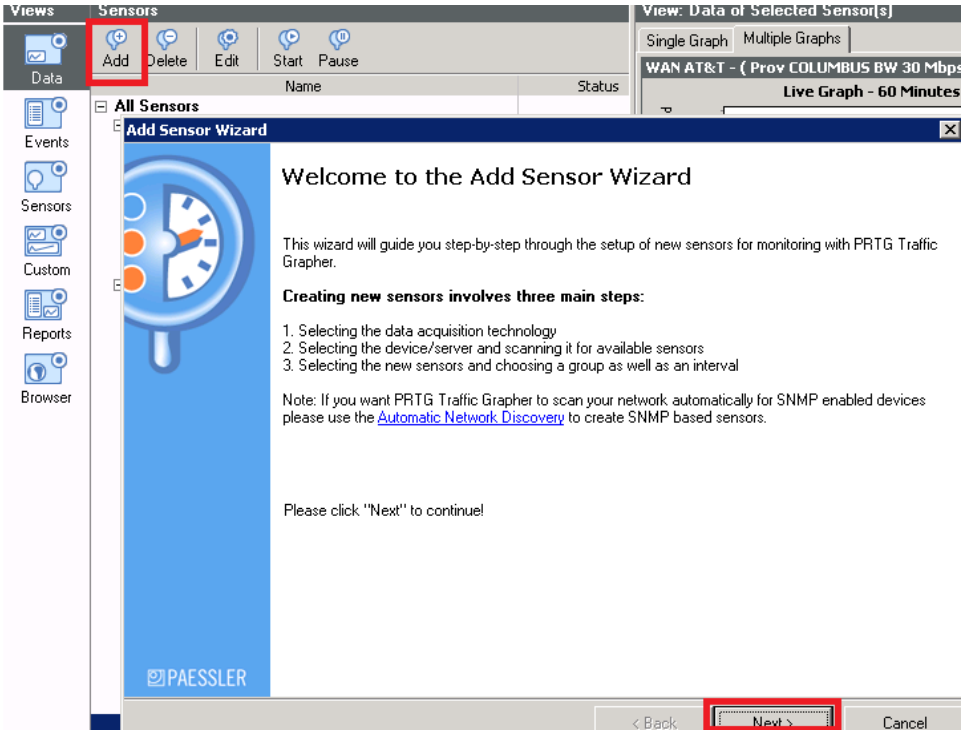
```
(config)#int vl 200
(config-if)#ip address 172.20.200.100 255.255.255.0
(config-if)#no ip route-cache
(config-if)#end
```

Se configura como default-gateway la primera IP del segmento.

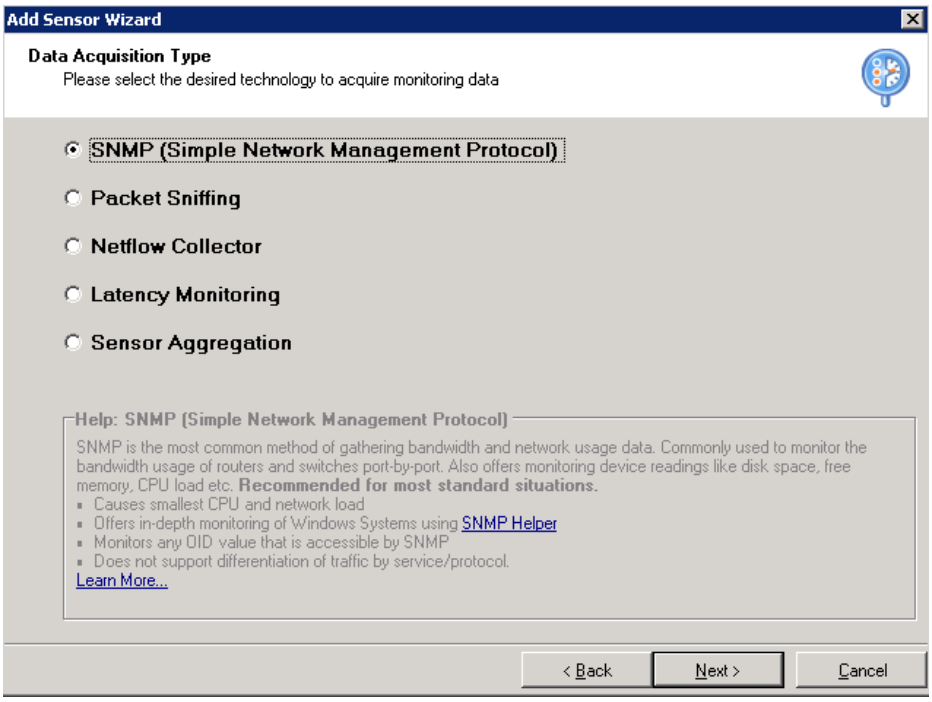
```
SW1_PTO_SECO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1_PTO_SECO(config)#ip default-gateway 172.20.200.1
SW1_PTO_SECO(config)#
```

CONFIGURACION PRTG

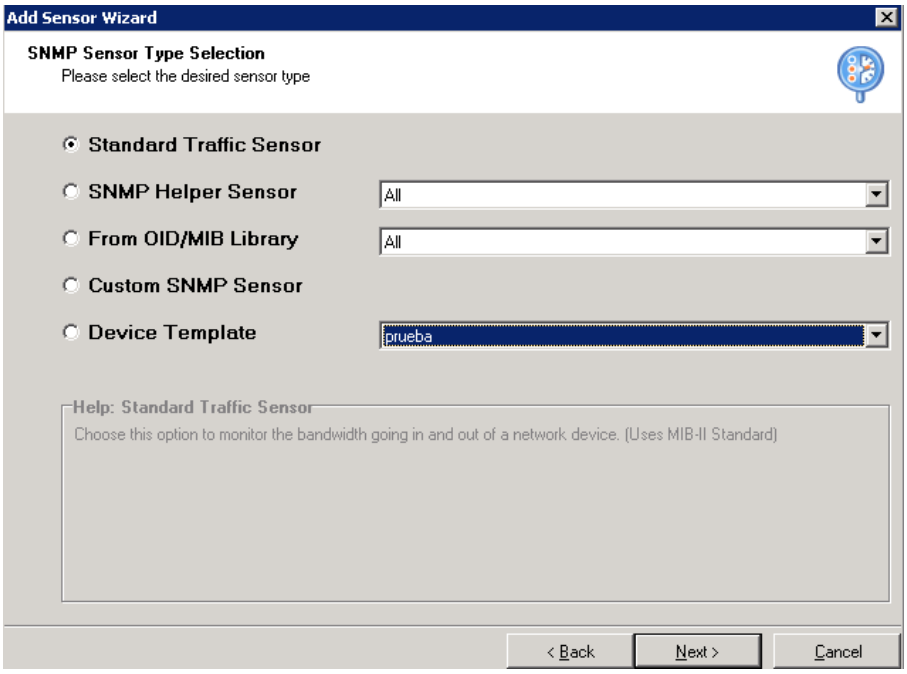
Se ingresa a la herramienta y se configuran los sensores dando click en el botón add y click en siguiente



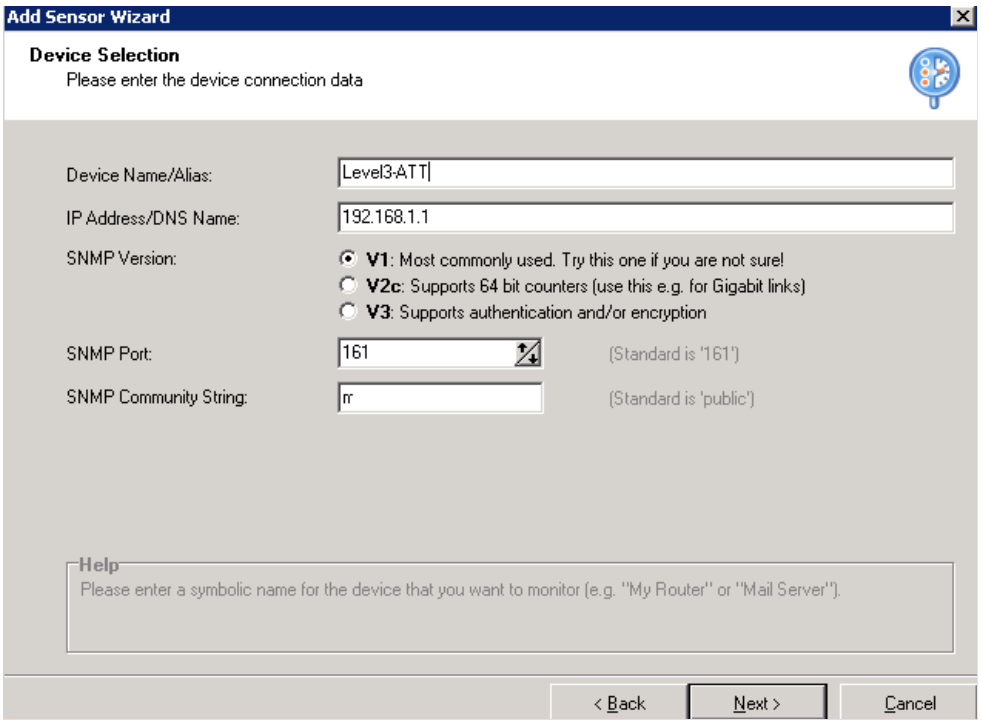
Se selección la opción de SNMP



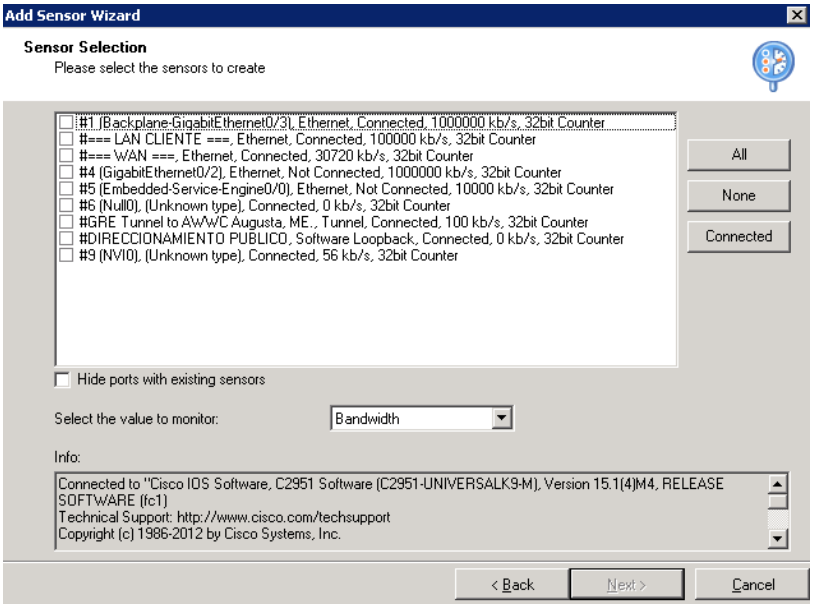
Se selecciona el sensor que se desee para este caso tráfico.



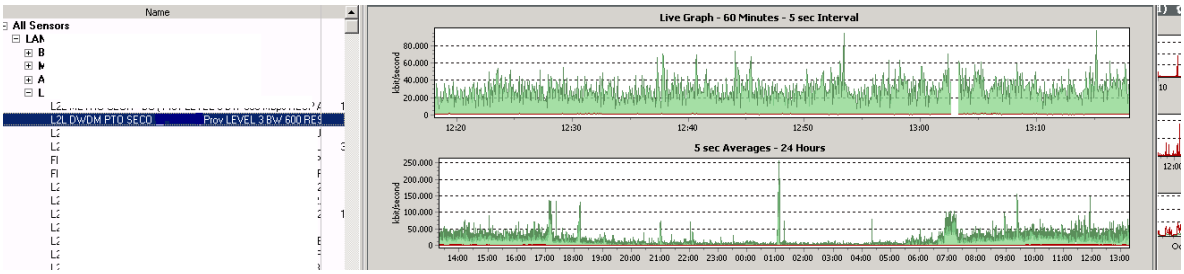
Se registra el nombre del sensor, la dirección IP, la versión de SNMP, el puerto del protocolo que es el 161 y la comunidad registrada en el switch para el caso multmed.



Se selecciona la interfaz a monitorear



En la siguiente imagen se observa la grafica de tráfico y el sensor configurado



Anexo sobre configuración del SW Core

```
**********************************************

**********************************************

****                                      ****

****              MEDELLIN                ****

****           CORE PPAL PSECO            ****

****                                      ****

**********************************************

**********************************************
```

+--+

| Este sistema de cómputo (incluyendo todo su hardware y sus periféricos)|

| es de uso restringido. Cualquier utilización, modificación o acceso no |

| autorizado a este sistema puede resultar en una acción disciplinaria o |

| **acusación legal.** |

| |

|###|

+---+

SW_L3_PPAL_PTO-SECO#sh run

Building configuration...

Current configuration : 28871 bytes

!

! Last configuration change at 02:56:42 gmt Mon XXXX by XXXXXXXXXX

!

version 12.2

no service pad

service tcp-keepalives-in

service timestamps debug datetime msec localtime show-timezone

service timestamps log datetime msec localtime show-timezone

service password-encryption

!

hostname SW_L3_PPAL_PSECO

!

boot-start-marker

boot-end-marker

!

logging buffered 65535

enable secret XXXXXXXXXXXXXXXXXXX

!

username msoporte password XXXXXXXXXXXXXXXXXXXX

clock timezone gmt -5

switch 1 provision ws-c3750x-24

system mtu routing 1500

ip routing

!

!

vtp mode transparent

!

!

spanning-tree mode rapid-pvst

no spanning-tree optimize bpdu transmission

spanning-tree extend system-id

spanning-tree vlan 1-200,1054-1056 priority 8192

!

!

!

!

vlan internal allocation policy ascending

!

vlan 160

 name

!

 vlan 161

 name

!

vlan 162

 name

!

!

!

interface GigabitEthernet1/0/1

description Vlan PTO SECO-BERRIO

 no switchport

 dampening

```
 ip address 172.XX.XX.XX 255.255.255.252
 delay 1
!
interface GigabitEthernet1/0/2
 description SW8_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk
 !
interface GigabitEthernet1/0/3
 description SW10_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/4
 description SW4_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk
 !
interface GigabitEthernet1/0/5
 description SW9_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
 !
interface GigabitEthernet1/0/6
 description SW7_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/7
 description SW3_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/8
 description SW_22_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk
 !
interface GigabitEthernet1/0/9
 description SW1_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface GigabitEthernet1/0/10
```

```
 description SW2_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk
 !
interface GigabitEthernet1/0/11
 description SW5_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk
 !
interface GigabitEthernet1/0/12
 description SW12_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/13
description SW_15_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk
 !
interface GigabitEthernet1/0/14
 description SW_15_PSECO
 switchport trunk encapsulation dot1q
```

```
 switchport mode trunk


interface GigabitEthernet1/0/15
 description SW_16_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/16
 description SW_18_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/17
 description SW_17_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk


interface GigabitEthernet1/0/18
 description SW_21_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk
 !
```

```
interface GigabitEthernet1/0/19
 description SW_19_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk
 !
interface GigabitEthernet1/0/20
 description SW_20_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/21
 description SW_23_PSECO
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/22
 description HSRP CONTING
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/24
 description L2L PSECO-BC
```

```
 no switchport
 dampening
 ip address 172.XX.XX.XX 255.255.255.252
 delay 1

interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface TenGigabitEthernet1/1/1
!
interface TenGigabitEthernet1/1/2
!
interface Vlan1
 no ip address
!
interface Vlan160
 description  Vlan Television
```

```
 ip address 172.XX.XX.XX 255.255.255.0
 ip helper-address 172.20.160,4
!
!
interface Vlan161
 description Vlan BANCO
 ip address 172.XX.XX.XX 255.255.255.0
 ip helper-address 172.20.161.4
!
!
interface Vlan162
 description Vlan  ASEGURADORA
 ip address 172.XX.XX.XX 255.255.255.0
 ip helper-address 172.20.162.4
!
!
router eigrp 10
 network 172.20.0.0
!
!
!
!
```

!

snmp-server community XXXXX RO

snmp-server community XXXXX RO

snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart

snmp-server enable traps transceiver all

snmp-server enable traps tty

snmp-server enable traps eigrp

snmp-server enable traps ospf state-change

snmp-server enable traps ospf errors

snmp-server enable traps ospf retransmit

snmp-server enable traps ospf lsa

snmp-server enable traps ospf cisco-specific state-change nssa-trans-change

snmp-server enable traps ospf cisco-specific state-change shamlink interface-old

snmp-server enable traps ospf cisco-specific state-change shamlink neighbor

snmp-server enable traps ospf cisco-specific errors

snmp-server enable traps ospf cisco-specific retransmit

snmp-server enable traps ospf cisco-specific lsa

snmp-server enable traps license

snmp-server enable traps auth-framework sec-violation

snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change inconsistency

snmp-server enable traps cluster

snmp-server enable traps config-copy

snmp-server enable traps config

snmp-server enable traps config-ctid

snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan

snmp-server enable traps energywise

snmp-server enable traps fru-ctrl

snmp-server enable traps entity

snmp-server enable traps event-manager

snmp-server enable traps hsrp

snmp-server enable traps ipmulticast

snmp-server enable traps power-ethernet group 1-9

snmp-server enable traps power-ethernet police

snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message

snmp-server enable traps cpu threshold

snmp-server enable traps rtr

snmp-server enable traps vstack

snmp-server enable traps bridge newroot topologychange

snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency

snmp-server enable traps syslog

snmp-server enable traps vtp

snmp-server enable traps vlancreate

snmp-server enable traps vlandelete

snmp-server enable traps flash insertion removal

snmp-server enable traps port-security

snmp-server enable traps envmon fan shutdown supply temperature status

snmp-server enable traps stackwise

snmp-server enable traps errdisable

snmp-server enable traps mac-notification change move threshold

snmp-server enable traps vlan-membership

tacacs-server host 172.XX.XX.XX timeout 5

tacacs-server directed-request

tacacs-server key XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

!

banner motd ^C

****

****

**** ****

**** MEDELLIN ****

**** CORE PPAL PSECO ****

**** ****

****

****

+--+

| Este sistema de computo (incluyendo todo su hardware y sus periféricos)|

| es de uso restringido. Cualquier utilización, modificación o acceso no |

| autorizado a este sistema puede resultar en una acción disciplinaria o |

| acusación legal. |

| |

|###|

+---+

^C

!

line con 0

exec-timeout 10 10

password XXXXXXXXXXX

logging synchronous

length 0

line vty 0 4

exec-timeout 10 10

password XXXXXXXXXXXXXX

logging synchronous

transport input ssh

line vty 5 15

exec-timeout 10 10

password 7 XXXXXXXXXXXXX

logging synchronous

transport input ssh

!

REFERENCIAS

Aloisio, A., Ameli, F., D'Amico, A., Giordano, R., Giovanetti, G., & Izzo, V. (2012). Performance Analysis of a DWDM Optical Transmission System. ***IEEE Transactions on Nuclear Science*****,** ***59*****(2), 251-255. http://doi.org/10.1109/TNS.2012.2183888**

Cisco Catalyst 2960-X Series Switches Data Sheet. (s. f.). Recuperado 8 de octubre de 2015, a partir de http://cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/data_sheet_c78-728232.html

Cisco Catalyst 3750 Series Switches Data Sheet. (s. f.). Recuperado 8 de octubre de 2015, a partir de http://cisco.com/c/en/us/products/collateral/switches/catalyst-3750-series-switches/product_data_sheet0900aecd80371991.html

Diseño y desarrollo de una aplicación para el estudio comparativo de topologías de red. (s. f.). Recuperado 15 de diciembre de 2015, a partir de http://orff.uc3m.es/handle/10016/12615#preview

Educarchile. (s. f.). Recuperado 10 de agosto de 2015, a partir de about:newtab

Liu, A. X., Torng, E., & Meiners, C. R. (2011). Compressing Network Access Control Lists. ***IEEE Transactions on Parallel and Distributed Systems*****,** ***22*****(12), 1969-1977. http://doi.org/10.1109/TPDS.2011.114**

Maity, S., Bera, P., & Ghosh, S. K. (2012). Policy Based ACL Configuration Synthesis in Enterprise Networks: A Formal Approach. En *2012 International Symposium on Electronic System Design (ISED)* (pp. 314-318). http://doi.org/10.1109/ISED.2012.72

Padmaraj, M., Nair, S., Marchetti, M., Chiruvolu, G., Ali, M., & Ge, A. (2005). Metro Ethernet traffic engineering based on optimal multiple spanning trees. *Wireless and Optical Communications Networks, 2005. WOCN 2005. Second IFIP International Conference on*, 568-572. http://doi.org/10.1109/WOCN.2005.1436090

Rajaravivarma, V. (1997). Virtual local area network technology and applications. *System Theory, 1997., Proceedings of the Twenty-Ninth Southeastern Symposium on*, 49-52. http://doi.org/10.1109/SSST.1997.581577

Shihab, M. R., & Misdianti, F. (2014). Moving towards PCI DSS 3.0 compliance: A case study of credit card data security audit in an online payment company. En *2014 International Conference on Advanced Computer Science and Information Systems (ICACSIS)* (pp. 151-156). http://doi.org/10.1109/ICACSIS.2014.7065872

Talib, M. A., Khelifi, A., & Ugurlu, T. (2012). Using ISO 27001 in teaching information security. *IECON 2012 - 38th Annual Conference on IEEE Industrial Electronics Society*, 3149-3153. http://doi.org/10.1109/IECON.2012.6389395

Yadong Li, Wenqiang Cui, Danlan Li, & Rui Zhang. (2011a). Research based on OSI model. *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*, 554-557. http://doi.org/10.1109/ICCSN.2011.6014631

Yadong Li, Wenqiang Cui, Danlan Li, & Rui Zhang. (2011b). Research based on OSI model. ***Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*****, 554-557. http://doi.org/10.1109/ICCSN.2011.6014631**

Yadong Li, Wenqiang Cui, Danlan Li, & Rui Zhang. (2011c). Research based on OSI model. ***Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*****, 554-557. http://doi.org/10.1109/ICCSN.2011.6014631**

APÉNDICE

Apéndice A

Dentro de las políticas de seguridad de la red y muy importante para las redes corporativas la implementación de un firewall, algunas aplicaciones que son utilizadas por los asesores de las diferentes líneas pueden acceder a servidores propios del cliente las políticas de PCI-DSS recomiendan siempre implementar un recurso de este tipo para evitar ataques externos que afecten el performance de la red, está encargado de permitir y denegar el tráfico entrante o saliente de la red, estos dispositivos están encargados de realizar el enrutamiento hacia los servidores externos bien sea por canales hacia los clientes o interfaz de salida para el acceso a internet a servicios publicados, pueden ser implementados en software o hardware, también tiene una interfaz DMZ donde se encuentran alojados los servidores que deben estar expuestos a los clientes. Hay varias generaciones de firewalls como lo son el filtrado de paquetes, de estado y aplicación.

FIRMA ESTUDIANTES _____

_____

_____

FIRMA ASESOR _____

FECHA ENTREGA: _____

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD _____

_____

RECHAZADO____ ACEPTADO____ ACEPTADO CON MODIFICACIONES_____

ACTA NO._____

FECHA ENTREGA: _____

FIRMA CONSEJO DE FACULTAD_____

ACTA NO._____

FECHA ENTREGA: _____