DISEÑO E IMPLEMENTACIÓN DE UNA RED DE ALTA DISPONIBILIDAD PARA LA SEDE CRITICA EN ADECCO COLOMBIA

ANDRÉS MAURICIO LOZANO GONGORA

FUNDACION UNIVERSITARIA LOS LIBERTADORES
FACULTAD DE INGENIERIA Y CIENCIAS BÁSICAS
INGENIERIA DE SISTEMAS
BOGOTA, D.C.
2017

DISEÑO E IMPLEMENTACIÓN DE UNA RED DE ALTA DISPONIBILIDAD PARA LA SEDE CRITICA EN ADECCO COLOMBIA

ANDRÉS MAURICIO LOZANO GONGORA

Trabajo de Grado presentado como requisito para obtener el título de Ingeniero de Sistemas

Asesor
Augusto Jose Angel M
Docente Investigador

FUNDACION UNIVERSITARIA LOS LIBERTADORES
FACULTAD DE INGENIERIA Y CIENCIAS BÁSICAS
INGENIERIA DE SISTEMAS
BOGOTA, D.C.
2017

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____

FIRMA DEL PRESIDENTE DEL JURADO

_____

FIRMA DEL JURADO

_____

FIRMA DEL JURADO

Bogotá D.C., 15 de junio de 2017

RESUMEN

El presente proyecto tiene como objetivo realizar la optimización y brindar una alta disponibilidad en la red de la sede critica de ADECCO COLOMBIA que se ubica en la CL 73 con Cra 7 empleando switches de CAPA 3 en High Avability (HA) para la transmisión de datos

Desde la gerencia de tecnología se vio la necesidad de implementar una mejora en la red actual de transporte de datos para suplir los inconvenientes de una comunicación sin latencia, aprovechando al máximo las condiciones con las que cuenta la sede, para esto se desarrollar un modelo para esta sede, donde se permita el desarrollo de VLAN con alto nivel de estabilidad y disponibilidad para el uso de funcionarios de la compañía.

Palabras Claves: High Avability, VLAN, Switch, Estabilidad, Transmisión de datos

INTRODUCCIÓN

La informática en general y sobre todo a nivel de usuario, ha evolucionado en grandes y medianas empresas, colegios, universidades y lo que tenga una conexión a Internet hace parte de la cultura de los seres humanos, desde el último siglo XX, especialmente en los últimos 30 años con la explosión del acceso masivo a Internet, aparción de lineas de banda ancha, fibra óptica y muchas más tecnologías mejoran notablemente las comunicaciones en tiempo real.

Actualmente se puede observar que a medida que el tiempo pasa las comunicaciones se realizan de forma ágil, sin importar las distancias, esto se debe a las mejoras de los elementos que son utilizados para estos procesos, cada mejora se va proyectando de acuerdo con las necesidades del ser humano.

Hoy en día se observa que la mayoría de comunicaciones, por no decir todas se realizan mediante medio magnético, estos mensajes se transportan mediante un sistema físico llamado infraestructura de red, según el ministerio de telecomunicaciones (MINTIC) define infraestructura como los elementos físicos que proveen conectividad digital. Algunos ejemplos son las redes de fibra óptica nacional, las torres de telefonía celular con sus equipos y antenas, y las redes de pares de cobre, coaxiales o de fibra óptica tendidas a los hogares y negocios.

La mejor muestra de esto es que casi en todo el mundo tiene al menos un PC en casa y normalmente una conexión de banda ancha, por lo que se entiende el potencial de la tecnología de manera exponencial para integrarla en nuestras vidas de forma natural. Los niños no deben ver el ordenador como u aparato que solo sirve para jugar o que deban usar obligatoriamente cuando se les mande en el colegio o en el ámbito doméstico, sino mostrarles como una herramienta viva que les permitirá acceder a un mundo de información y calidad de vida, usarlo para su desarrollo vital cotidiano.

Un reto para los profesionales de IT en la nueva estructura globalizada, es brindar a las áreas críticas y no criticas una conectividad continua a los sistemas de información que debe estar estructurados en base de las nuevas alternativas de hosting (Datacenter) que ofrecen los proveedores ISP en Colombia.

Por lo anterior se estructura un proyecto de High Availability (HA) en la sede donde por decisiones administrativas va a fusionar todas las áreas críticas que generan el 97% del flujo de efectivo de la compañía. Para lograr esta implementación se propone centralizar en un modelo de capa 3 a nivel de Switching y bajar a estos la configuración de capa 2 que hasta este momento es responsabilidad del ISP.

CONTENIDO

Pág.

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

Pag.

JUSTIFICACIÓN

Es indispensable que la mejora continua en el desarrollo social que se lleva a cabo por parte del gobierno y de las entidades privadas interesadas que invierten en el país, se alinee con el desarrollo de TIC en Colombia. Debido a que las empresas de Telecomunicaciones requieren cada día la actualización de herramientas tecnológicas, que permitan una adecuada comunicación con el cliente.

En consecuencia, es necesario la implementación del presente proyecto de mejora el cual pretende ofrecer una mejor estructura de la red, renovación tecnológica de depósitos como switches, rectificación de puntos, amplitud en MB de los canales ya existentes, creación de Vlan dedicadas a áreas críticas del negocio.

El cambio se gestionará paulatinamente de la mano con el proveedor MCO Global quien estará como aliado estratégico en la ejecución del proyecto.

El proyecto beneficia la conexión interna de la empresa por que será de mayor robustez, calidad y capacidad de transferencias en todos sus procesos, ya que en esta sede se factura más del 80% de los ingresos de la compañía y esto a su vez afectaría el flujo de efectivo en caso falla del proceso.

1 OBJETIVOS

1.1 GENERAL

Diseñar e implementar una mejora en la infraestructura de la red de datos tanto física como lógica de Adecco para la sede de la calle 73, mediante la instalación de nuevos dispositivos de red para asegurar el performance y transferencia de datos

1.2 ESPECÍFICOS

- Identificar las falencias actuales de la red y relacionarlas a los protocolos de diseño y planeación existentes que encaminen a la mejora de la estructura de la empresa.

- Diseñar una mejora de la infraestructura de la red que sea flexible ante las ampliaciones y cambios que puedan surgir, preparada para las aplicaciones de comunicaciones presentes y futuras, instalada según estándares para asegurar la calidad y compatibilidad de las comunicaciones.

- Realizar la certificación de puntos para asegurar conexiones de calidad a nivel LAN.

2 DESCRIPCION DE LA EMPRESA

Adecco Group, consultora líder mundial en la gestión del talento humano con presencia en más de 60 países y más de 5000 oficinas, 32,000 colaboradores, conectamos 700,000 personas y 100,000 clientes a nivel mundial cada día.

Con el objetivo de brindar servicios estándar a nivel zonal, todos los países trabajan bajo normas de calidad ISO 9001. Adecco Group se especializa en asesorar empresas líderes ofreciendo soluciones integrales en Servicio Temporal, Selección de personal y consultoría de Talento Humano. En Colombia, Adecco cuenta con 36 sucursales ubicadas en 11 ciudades, 725 colaboradores que dan servicio a más de 1500 empresas nacionales y multinacionales.

Líder indiscutible del sector, es una de las 10 primeras empresas de Colombia en la creación de empleo directo e indirecto. Adecco tiene como filosofía un intenso compromiso y visión empresarial hacia el servicio, la flexibilidad para adaptarnos a las prácticas de cada empresa así como el deseo de invertir en relaciones de largo plazo, todo esto sustentado en nuestra trayectoria corporativa y empresarial.

3 MARCO TEÓRICO

3.1 VLAN

Una VLAN, acrónimo de virtual LAN (Red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.1 Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4).

Una VLAN consiste en dos o más redes de computadoras que se comportan como si estuviesen conectados al mismo conmutador, aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local (LAN). Los administradores de red configuran las VLAN mediante software en lugar de hardware, lo que las hace extremadamente fuertes.

3.2 PROTOCOLOS

Durante todo el proceso de configuración y funcionamiento de una VLAN es necesaria la participación de una serie de protocolos entre los que destacan el IEEE 802.1Q, STP y VTP (cuyo equivalente IEEE es GVRP). El protocolo IEEE 802.1Q se encarga del etiquetado de las tramas que es asociada inmediatamente con la información de la VLAN. El cometido principal de Spanning Tree Protocol (STP) es evitar la aparición de bucles lógicos para que haya un sólo camino entre dos nodos. VTP (VLAN Trunking Protocol) es un protocolo propietario de Cisco que permite una gestión centralizada de todas las VLAN.

El protocolo de etiquetado IEEE 802.1Q es el más común para el etiquetado de las VLAN. Antes de su introducción existían varios protocolos propietarios, como el ISL (Inter-Switch Link) de Cisco, una variante del IEEE 802.1Q, y el VLT (Virtual LAN Trunk) de 3Com. El IEEE 802.1Q se caracteriza por utilizar un formato de trama similar a 802.3 (Ethernet) donde solo cambia el valor del campo Ethertype, que en las tramas 802.1Q vale 0x8100, y se añaden dos bytes para codificar la prioridad, el CFI y el VLAN ID. Este protocolo es un estándar internacional y por lo dicho anteriormente es compatible con bridges y switches sin capacidad de VLAN.

Las VLAN y Protocolos de Árbol de Expansión. Para evitar la saturación de los switches debido a las tormentas broadcast, una red con topología redundante tiene que tener habilitado el protocolo STP. Los switches intercambian mensajes STP BPDU (Bridge Protocol Data Units) entre sí para lograr que la topología de la red sea un árbol (no tenga enlaces redundantes) y solo haya activo un camino para ir de un nodo a otro. El protocolo STP/RSTP es agnóstico a las VLAN, MSTP (IEEE 802.1Q) permite crear árboles de expansión diferentes y asignarlos a grupos de las VLAN mediante configuración. Esto permite utilizar enlaces en un árbol que están bloqueados en otro árbol.

En los dispositivos Cisco, VTP (VLAN trunking protocol) se encarga de mantener la coherencia de la configuración VLAN por toda la red. VTP utiliza tramas de nivel 2 para gestionar la creación, borrado y renombrado de las VLAN en una red sincronizando todos los dispositivos entre sí y evitar tener que configurarlos uno a uno. Para eso hay que establecer primero un dominio de administración VTP. Un dominio VTP para una red es un conjunto contiguo de switches unidos con enlaces trunk que tienen el mismo nombre de dominio VTP.

Los switches pueden estar en uno de los siguientes modos: servidor, cliente o transparente. «Servidor» es el modo por defecto, anuncia su configuración al resto de equipos y se sincroniza con otros servidores VTP. Un switch en modo cliente no puede modificar la configuración VLAN, simplemente sincroniza la configuración sobre la base de la información que le envían los servidores. Por último, un switch está en modo transparente cuando solo se puede configurar localmente pues ignora el contenido de los mensajes VTP.

VTP también permite «podar» (función VTP pruning), lo que significa dirigir tráfico VLAN específico solo a los conmutadores que tienen puertos en la VLAN destino. Con lo que se ahorra ancho de banda en los posiblemente saturados enlaces trunk.

Uno de los peores problemas que puede presentarse para un Switch es cuando escucha la misma dirección MAC (Medium Access Control) por dos interfaces físicas diferentes, este es un bucle que en principio, no sabría cómo resolver.2 Este problema si bien parece poco probable que pueda ocurrir, en realidad en redes grandes al tener cientos o miles de cables (muchos de ellos para redundancia), este hecho es tan sencillo como conectar el mismo cable en diferentes patch pannels que cierran un lazo sobre el mismo dispositivo, y en la realidad ocurre con cierta frecuencia, mayor, en la medida que más

grande sea la red LAN. También es un hecho concreto cuando el cableado se diseña para poseer caminos redundantes, justamente para incrementar la disponibilidad de la red.

Cuando físicamente se cierra un bucle, la topología pura de red “Jerárquica” deja de serlo y se convierte en una red “Malla”. Para tratar este problema el protocolo Spanning Tree crea una red “Jerárquica lógica (árbol Lógico)” sobre esta red “Malla Física”. Este protocolo crea “Puentes” (bridges) de unión sobre estos enlaces y define a través de diferentes algoritmos que se pueden configurar, cuál es el que tiene mayor prioridad, este puente de máxima prioridad lo denomina “Root Bridge” (o Puente Raíz) y será el que manda jerárquicamente las interfaces por las cuáles se separarán los diferentes dominios de colisión. Todo el control de STP se realiza mediante tramas llamadas BPDU (Bridge Protocol Data Unit) que son las que regulan los diferentes dominios de colisión. El parámetro que define esta jerarquía es el BID (Bridge Identifier) que está compuesto por el Bridge Priority + dirección MAC. El Bridge Priority es un valor configurable que por defecto está asignado en 32768.

En general este protocolo se configura de forma automática, y se basa en el orden de encendido de los diferentes Switchs de la red, siendo el primero que se pone en funcionamiento el que se auto designa “Root Bridge”, pero por supuesto se puede realizar de forma manual.

Cada switch reemplaza los BID de raíz más alta por BID de raíz más baja en las BPDU. Todos los switches que reciben las BPDU determinan en sus tablas que el switch que cuyo valor de BID es el más bajo será “su” puente raíz, y a su vez envían nuevas BPDU hacia sus otras interfaces con un ID más alto, incrementando el parámetro “Root Path Cost” (Que veremos en el ejemplo que sigue) informando con esta nueva BPDU a todo dispositivo que esté conectado físicamente a él cómo debe ir armándose este árbol. Si se desea configurar de forma manual, el administrador de red puede establecer jerarquía que desee configurando la prioridad de switch que sea “Root Bridge” en un valor más pequeño que el del valor por defecto (32768, todo valor debe ser múltiplo de 4096), lo que hace que este BID sea más pequeño y a partir de este “root” puede configurar la jerarquía o árbol si lo desea, o también al reconocer los demás switch a este “root”, de forma automática pueden generar el resto del árbol.

En las grandes redes actuales, se suelen establecer importantes relaciones entre las VLANs y el Core de las redes, donde el protocolo por excelencia suele ser MPLS (Multi Protocolo Label Switching)

3.3 DHCP

DHCP (siglas en inglés de Dynamic Host Configuration Protocol, en español «protocolo de configuración dinámica de host») es un servidor que usa protocolo de red de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. Así los clientes de una red IP pueden conseguir sus parámetros de configuración automáticamente.

3.3.1 Asignación de direcciones IP

Cada dirección IP debe configurarse manualmente en cada dispositivo y, si el dispositivo se mueve a otra subred, se debe configurar otra dirección IP diferente. El DHCP le permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva IP si fuera el caso en que el dispositivo es conectado en un lugar diferente de la red.

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

3.3.1.1 Asignación manual o estática

Asigna una dirección IP a una máquina determinada. Se suele utilizar cuando se quiere controlar la asignación de dirección IP a cada cliente, y evitar, también, que se conecten clientes no identificados.

3.3.1.2 Asignación automática

Asigna una dirección IP a una máquina cliente la primera vez que hace la solicitud al servidor DHCP y hasta que el cliente la libera. Se suele utilizar cuando el número de clientes no varía demasiado.

3.3.1.3 Asignación dinámica

El único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada dispositivo conectado a la red está configurado para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la

instalación de nuevas máquinas clientes.

Algunas implementaciones de DHCP pueden actualizar el DNS asociado con los servidores para reflejar las nuevas direcciones IP mediante el protocolo de actualización de DNS establecido en RFC 2136 (Inglés).

El DHCP es una alternativa a otros protocolos de gestión de direcciones IP de red, como el BOOTP. DHCP es un protocolo más avanzado, pero ambos son los usados normalmente.[1]

3.4 PROTOCOLO HSRP

El Hot Standby Router Protocol es un protocolo propiedad de CISCO que permite el despliegue de routers redundantes tolerantes a fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers. Es un protocolo muy similar a VRRP.

3.4.1 Características Protocolo HSRP

El funcionamiento del protocolo HSRP es el siguiente: Se crea un grupo (también conocido por el término inglés Clúster) de routers en el que uno de ellos actúa como maestro, enrutando el tráfico, y los demás actúan como respaldo a la espera de que se produzca un fallo en el maestro. HSRP es un protocolo que actúa en la capa 3 del modelo OSI administrando las direcciones virtuales que identifican al router que actúa como maestro en un momento dado.

3.4.2 Funcionamiento

Supongamos que disponemos de una red que cuenta con dos routers redundantes, RouterA y RouterB. Dichos routers pueden estar en dos posibles estados diferentes: maestro (Router A) y respaldo (Router B). Ambos routers intercambian mensajes, concretamente del tipo HSRP hello, que le permiten a cada uno conocer el estado del otro. Estos mensajes utilizan la dirección multicast 224.0.0.2 y el puerto UDP 1985.

Si el router maestro no envía mensajes de tipo hello al router de respaldo

[1] Comer, D. E. (1997). *Redes de computadoras, Internet e Interredes* (Vol. 2). G. Guerrero (Ed.). Prentice Hall.

dentro de un determinado período, el router respaldo asume que el maestro está fuera de servicio (ya sea por razones administrativas o imprevistas, tales como un fallo en dicho router) y se convierte en el router maestro. La conversión a router activo consiste en que uno de los router que actuaba como respaldo obtiene la dirección virtual que identifica al grupo de routers.

HSRP se encuentra disponible desde CISCO IOS 10.0, pero se han incorporado nuevas funcionalidades en las versiones 11 y 12.

3.4.3 Elección del Router "maestro"

Para determinar cual es el router maestro se establece una prioridad en cada router. La prioridad por defecto es 100. El router de mayor prioridad es el que se establecerá como activo. Hay que tener presente que HSRP no se limita a 2 routers, sino que soporta grupos de routers que trabajen en conjunto de modo que se dispondría de múltiples routers actuando como respaldo en situación de espera.

3.4.4 Paso de estado "respaldo" a estado "maestro"

El router en espera toma el lugar del router maestro, una vez que el temporizador holdtime expira (un equivalente a tres paquetes hello que no vienen desde el router activo, timer hello por defecto definido a 3 y holdtime por defecto definido a 10).

Los tiempos de convergencia dependerán de la configuración de los temporizadores para el grupo y del tiempo de convergencia del protocolo de enrutamiento empleado.

Por otra parte, si el estado del router maestro pasa a down, el router decrementa su prioridad. Así, el router respaldo lee ese decremento en forma de un valor presente en el campo de prioridad del paquete hello, y se convertirá en el router maestro si ese valor decrementado es inferior a su propia prioridad. Este proceso decremental puede ser configurado de antemano estableciendo un valor por defecto del decremento (normalmente, de 10 en 10).[2]

[2] AGUILAR CEVALLOS, Carlos David; CANCHIG, Veloso; PATRICIO, Edgar. Análisis de los protocolos de Alta disponibilidad de Gateways en la interconectividad LAN/WAN aplicadas al diseño de la red del MAGAP Cotopaxi. 2012.

3.5 PROTOCOLO VRRP

Virtual Router Redundancy Protocol (VRRP) es un protocolo de penetración no propietario definido en el RFC 3768 diseñado para aumentar la disponibilidad de la puerta de enlace por defecto dando servicio a máquinas en la misma subred. El aumento de fiabilidad se consigue mediante el anuncio de un router virtual como una puerta de enlace por defecto en lugar de un router físico. Dos o más routers físicos se configuran representando al router virtual, con sólo uno de ellos realizando realmente el enrutamiento. Si el router físico actual que está realizando el enrutamiento falla, el otro router físico negocia para sustituirlo. Se denomina router maestro al router físico que realiza realmente el enrutamiento y routers de respaldo a los que están en espera de que el maestro falle.

VRRP se puede usar sobre redes Ethernet, MPLS y Token Ring. El protocolo VRRP ha sido implementado más que sus competidores. Fabricantes como Alcatel-Lucent, Extreme Networks, Dell, Nokia, Siemens-Ruggedcom, Nortel, Cisco Systems, Inc, Allied Telesis, Juniper Networks, Huawei, Foundry Networks, Radware, Raisecom, Aethra y 3Com Corporation ofrecen routers y switches de nivel 3 que pueden utilizar el protocolo VRRP. También están disponibles implementaciones para Linux y BSD.

Hay que tener en cuenta que VRRP es un protocolo de router, no de routing. Cada instancia de VRRP se limita a una única subred. No anuncia rutas IP ni afecta a la tabla de encaminamiento.

3.5.1 Implementación

Un router virtual tiene que utilizar la siguiente dirección MAC: 00-00-5E-00-01-XX. El último byte de la dirección es el identificador de router virtual (Virtual Router IDentifier o VRID), que es diferente para cada router virtual en la red. Esta dirección sólo la utiliza un único router físico a la vez, y es la única forma de que otros routers físicos puedan identificar el router maestro en un router virtual. Los routers físicos que actúan como router virtuales deben comunicarse entre ellos utilizando paquetes con dirección IP multicast 224.0.0.18 y número de protocolo IP 112.

Los routers maestros tienen una prioridad de 255 y los de respaldo entre 1 y 254. Cuando se realiza un cambio planificado de router maestro se cambia su prioridad a 0 lo que fuerza a que alguno de los routers de respaldo se convierta en maestro más rápidamente. De esta forma se reduce el periodo de agujero negro.

3.5.2 La elección del router maestro

Un fallo en la recepción de un paquete de multicast del master durante un tiempo superior a tres veces el tiempo de anuncio hace que los routers de respaldo asuman que el router maestro está caído. El router virtual cambia su estado a "inestable" y se inicia un proceso de elección para seleccionar el siguiente router maestro de entre los routers de respaldo. Esto se realiza mediante la utilización de paquetes multicast.

Hay que hacer notar que los routers de respaldo únicamente envían paquetes multicast durante el proceso de elección. Una excepción a esta regla es cuando un router físico se configura para que derroque al master actual cuando se le introduzca en el router virtual. Esto permite al administrador de red forzar a que un router sea el maestro inmediatamente después de un arranque, por ejemplo cuando un router es más potente que otros o cuando un router utiliza el ancho de banda más barato. El router de respaldo con la prioridad más alta se convierte en el router maestro aumentando su prioridad a 255 y enviando paquetes ARP con la dirección MAC virtual y su dirección IP física. Esto redirige los paquetes del maestro caído al router maestro actual. En los casos en los que los routers de respaldo tengan todos la misma prioridad, el router de respaldo con la dirección IP más alta se convierte en el router maestro.

Todos los routers físicos que actúan como router virtual tienen que estar a un salto entre ellos. La comunicación dentro del router virtual se realiza periódicamente. Este periodo puede ajustarse cambiando el intervalo de anuncio. Cuanto más corto el intervalo de anuncio más pequeño será el tiempo de agujero negro a cambio de un aumento del tráfico de red. La seguridad se implementa respondiendo únicamente a los paquetes de primer salto, aunque se ofrecen otros mecanismos para su refuerzo, en particular para ataques locales.[3]

[3] LONDOÑO, Andrés Parra; GUERRERO, Fabio G. Esquema de redundancia y distribución de carga de alta disponibilidad para la prestación de telefonía IP usando SIP. 2009.

4 INGENIERÍA DEL PROYECTO

4.1 DESCRIPCIÓN DE LA SITUACIÓN ACTUAL

En la sucursal de Adecco Cl 73, la conexión a internet se muestra un poco lenta debido a pequeñas intermitencias, en algunos casos reportada por los usuarios, caídas temporales de servicios de internet, y en general síntomas referente a rendimiento en transferencias.

Se propone generar la revisión de todos los puntos de red disponibles en la sucursal mediante la certificación de cada punto para asegurar la calidad de conexiones, cambiara cables UTP en casos específicos para evitar cables vencidos, instalación y configuración Switch Core Juniper en instalación de canales de datos redundantes de modo activo/activo

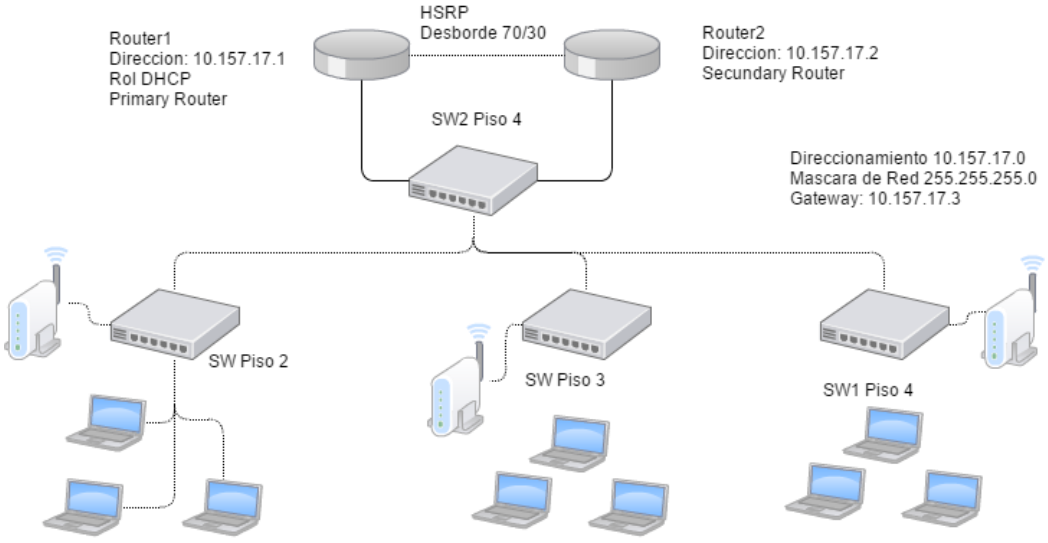

Ilustración 1 Distribución Inicial de Red para la Sede Calle 73

Según como se evidencia en la Ilustración 1 podemos apreciar una red plana con una configuración de capa 3 realizada por el ISP a la cual ADECCO no tiene acceso alguno siendo dependientes del proveedor para cualquier cambio en red, además esta red está diseñada con una tabla de asignación IP 10.157.17.0/24 la cual se queda corta para la cantidad de usuarios.

Estos se distribuyen de la siguiente manera

- En el Segundo Piso de la sucursal se alquila la oficina continua para

ampliación de la sede en este piso pasan de 22 usuario a casi 70 usuarios

- En el tercer piso se traslada un grupo de trabajo crítico de la compañía con unos 32 usuarios adicionales este piso se comparte con otra línea de negocio donde se pueden ubicar unos 20 usuarios
- En el cuarto piso hay 110 usuarios y es otra sede critica para la facturación del negocio
- Incluye instalar varios dispositivos de red como impresoras, CCTV, y según las políticas corporativas habilitar 3 redes Wifi Administrativos – Invitados y Dispositivos Móviles

No solo el problema está en la disponibilidad de la red, lo pequeña que puede ser el direccionamiento, sino que si vemos el monitoreo de la DB (Ver Ilustración 2) podemos apreciar un comportamiento basta ardido en las transacciones que entran y salen desde esta sede

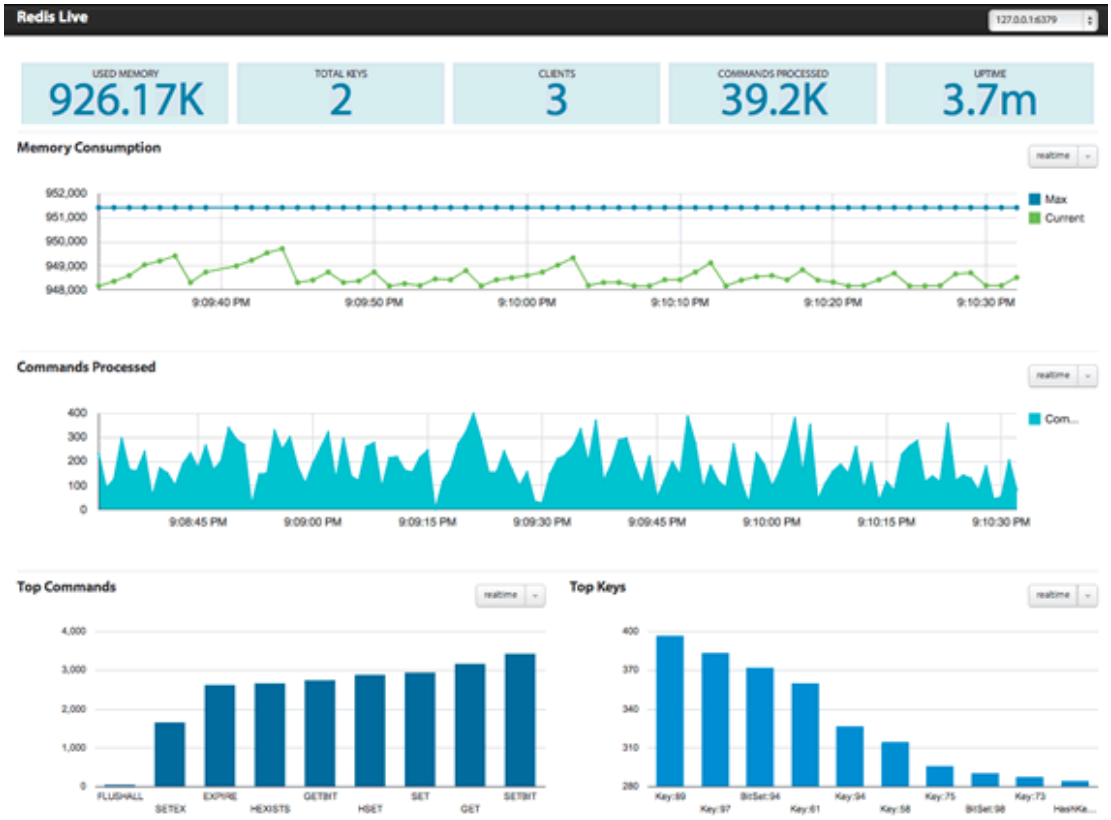

Ilustración 2 Comportamiento transaccional de la Base Datos

4.2 REQUERIMIENTOS DE INFORMACIÓN

La sede tiene una topología e infraestructura que no posee la capacidad para soportar el ingreso diario de miles de transacciones por día, acompañado de un número importantes de ingreso de nuevas personas diarias a nuestro sistema conectándose simultáneamente a la red de datos. Sin embargo, la constante falla en la red hace que en su mayoría los malestares por intermitencia Superen índices no deseados.

Debido a esto se requiere realizar una proyección que nos permita evidenciar los problemas que tiene infraestructura y la red de la empresa. se va a realizar una mejora en el diseño actual de la infraestructura y especialmente de esta sede, debido a sus constantes fallos de red, que dependen en gran medida a la topología que actualmente se encuentra implementada allí, presentando la desventaja, que se produzcan problemas de tráfico y colisiones de manera repetitiva. Por lo tanto se ve necesario realizar cambios oportunos porque en este momento no dispone de la velocidad necesaria para efectuar los procedimientos que se ejecuten y tampoco brinda la confiabilidad debido a las constantes caídas de la red.

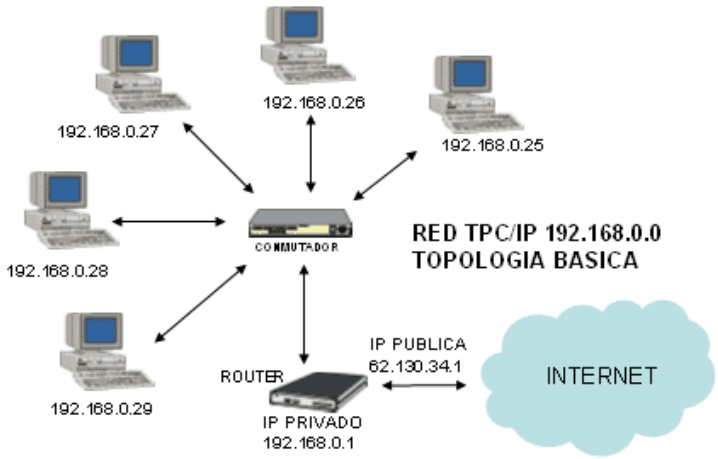

Ilustración 3Topología de Red de la Calle 73

4.3 MODELAMIENTO DEL SISTEMA

Adecco está interesado en recibir propuestas de aprovisionamiento, instalación, configuración y soporte de las plataformas de los equipos de Core para la red LAN para una de sus sedes, se espera que estos equipos cumplan las siguientes funciones:

- Segmentación de la red LAN mediante VLAN.
- Gateway por defecto independiente por cada VLAN, para realizar balaceo (VRRP).
- Redundancia y conmutación automática en caso de caída.
- Soportar DHCP para cada VLAN
- La instalación y configuración se necesita en dos etapas, para la primera se contemplan las siguientes actividades:
- Revisión física el cableado estructurado, verificar marquillado en faceplate, patch panel y patchcord.

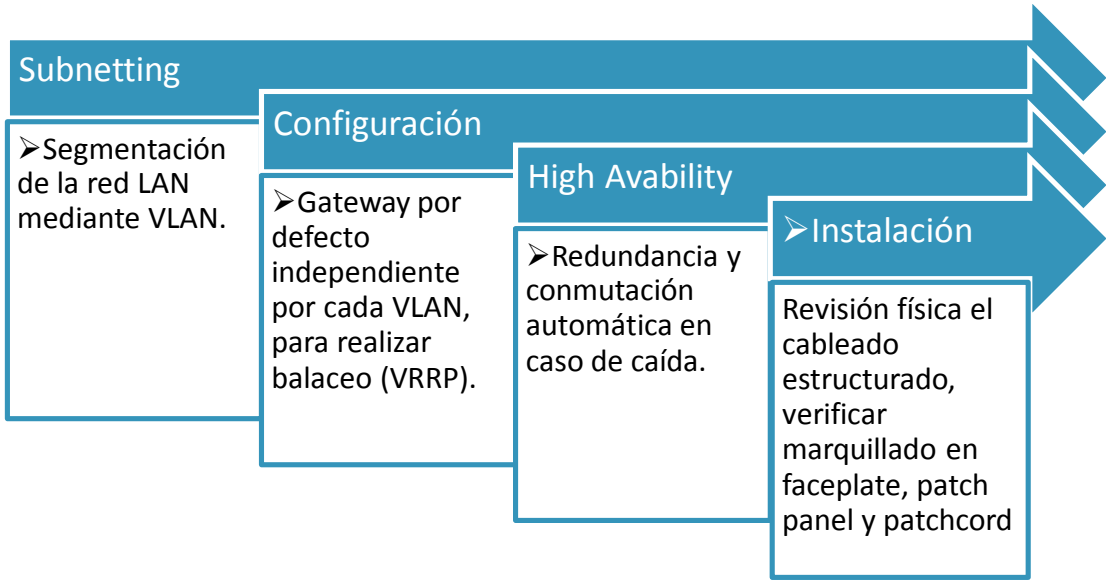

Ilustración 4 Modelamiento lineal para puesta en marcha del proyecto

4.3.1 Instalación de Equipos de core.

- Segmentación de la red LAN y configuración en el equipo de Core.
- Configuración de balanceo.
- Configuración de protocolos VRRP.
- Configuración de VLAN en los Switch de acceso.
- Para la segunda fase se necesitan las siguientes actividades:
- Movimiento de los Switch del cuarto piso al tercer piso.

4.4 DESCRIPCIÓN DEL SISTEMA

En la siguiente tabla se describe las características de la red Actual:

DESCRIPCION VLAN	VLAN ID	NETWORK	GATEWAY	RESERVAS IP	OBSERVACIONES
NETWORK	VLAN10	10.157. 17.0	10.157.99.1	DHCP	Desborde a backup al saturar Canal PAL

Tabla 1 Situación inicial de la CI 73

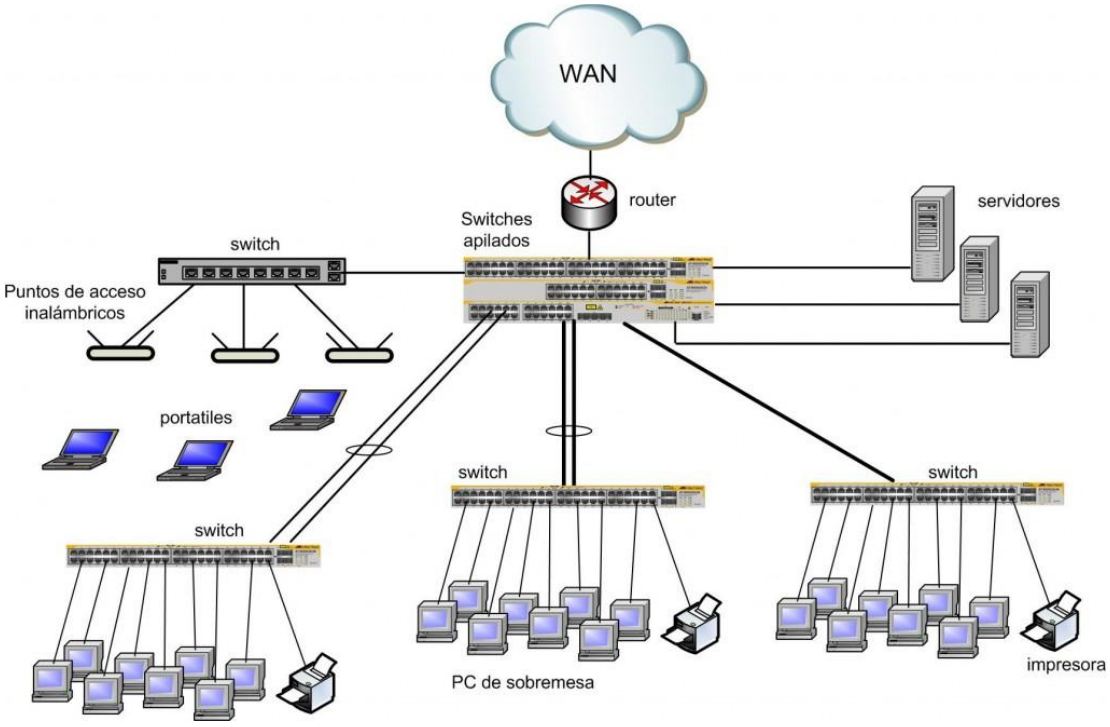

Ilustración 5 Distribución de red Para la sede por pisos

Este modelo muestra la conformación de la red LAN antes del proyecto donde se evidencia una distribución sin escala dependiente del ISP y de donde solo se conecta una serie de dispositivos con un ruteo LAN simple

La red que se tiene las siguientes características:

DESCRIPCION VLAN	VLAN ID	NETWORK	GATEWAY	RESERVAS IP	OBSERVACIONES
ADMON NETWORK	VLAN0	10.157.99.0	10.157.99.1	Sin DHCP	ALTA DISPONIBILIDAD
WIFI INVITADOS	VLAN1	10.157.100.0/25	10.157.100.1	Primeras 5 ip	Se debe contemplar que esta Vlan solo tiene acceso a internet no debe tener autenticación de firewall
WIFI MOBILE	VLAN2	10.157.100.128/25	10.157.100.129	Primeras 5 ip	PRIORIDAD ALTA
CSC	VLAN10	10.157.12.0/24	10.157.12.1	Primeras 50 IP	PRIORIDAD ALTA
PAYROLL	VLAN11	10.157.17.0/24	10.157.17.1	Primeras 50 IP	Tentativa dependiente de la configuración que se pueda hacer sobre los teléfonos
BPO - SALES MARKETING	VLAN12	10.157.15.0/24	10.157.15.1	Primeras 50 IP	
TELEFONIA	VLAN14	10.157.101.0/24	10.157.101.1	Primeras 50 IP	
PERMANENT - SELECCIÓN - CONTROLLER	VLAN15	10.157.13.0/24	10.157.13.1	Primeras 50 IP	

Tabla 2 Red LAN a Implementar

La implementación se va a realizar en dos etapas, en la primera se realizará toda la configuración de VLAN, default Gateway, DHCP y Calidad de Servicios en un Switch 3300-24T Juniper, para la segunda etapa se tiene contemplada la configuración de alta disponibilidad y balanceo de carga por medio del protocolo VRRP, de esta manera minimizar cualquier impacto o posible afectación a la red.

A continuación se describe a profundidad cada una de las etapas.

Descripcion	Verificación
Validación del cableado estructurado de la oficina	Ok
Envió de correo a Telefónica con requerimientos para la implementación fase I	Ok
Entrega de Switch Ex3300-24T Pre configurado	Ok
Programar ventana de mantenimiento para Fase I	Ok
Tener las herramientas para la actualización: portátil, cable consola, cable UTP y memoria USB.	Ok

Tabla 3 Fase 1: Instalación de SwCore y Segmentación de RED

Esta fase busca Instalar físicamente el SwCore para la Sede de la 73 de ADECCO.

El objetivo es tener la CAPA 3 de la sede configurada en este equipo

De esta fase se busca los siguientes resultados:

- Configurar la Segmentación de la red descrita en la tabla 2
- Configurar los servidores DHCP para cada uno de los segmentos de RED.
- Configuración de firewall filters para los segmentos de red correspondientes a la wifi.
- Identificar mejoras en el diseño para aplicar en la implementación de la HA.

4.5 TOPOLOGÍA FASE I

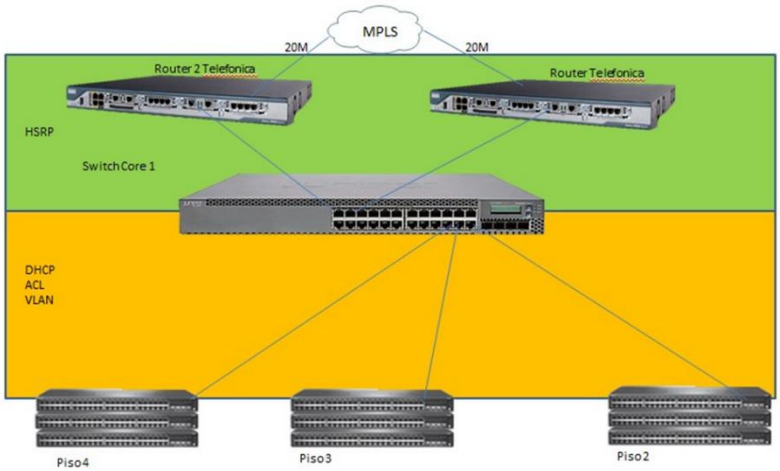

Ilustración 6 Topología fase I de conexión

Instalación SW Core 2 e implementación de Alta disponibilidad

- Esta fase busca Instalar un segundo Switch EX3300-24T para configurar redundancia y balance de cargas mediante el protocolo VRRP para las subredes que son críticas para ADECCO.
- De esta fase se busca los siguientes resultados:
- Implementar mejoras resultado del análisis de la fase I
- Realizar la petición de configuración del protocolo HSRP para las subredes criticas al Proveedor de servicios(Telefónica)
- Implementar el protocolo VRRP en los dos Switch de Core para la redundancia y balance de carga.

4.6 TOPOLOGÍA FASE II

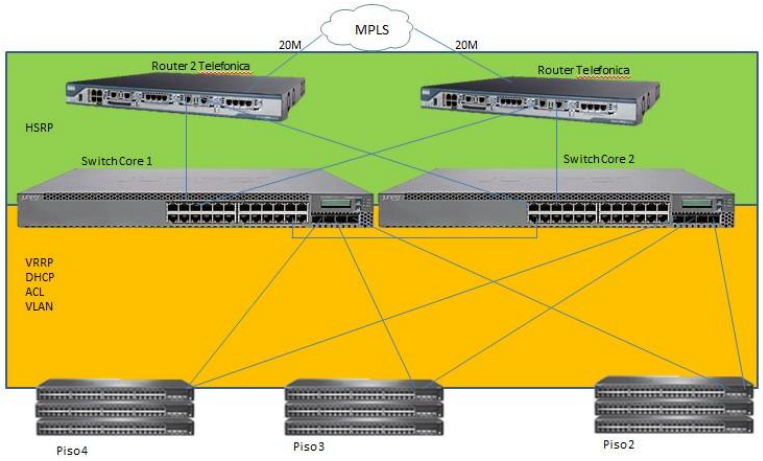

Ilustración 7 Topología fase II de conexión

5 EVALUACIÓN ECONÓMICA DEL PROYECTO

- Afectación de los servicios de red en las migraciones al nuevo esquema de plataforma de red
- Modificación a la topología planeada por falta de equipos de telecomunicaciones o servidores.
- Retraso en tiempos y fechas por eventualidades y procesos críticos de ADECCO que requieran asignación de fechas específicas
- Retraso en tiempos y fechas generados por la instalación de los servicios del proveedor de servicios (MCO).

Los equipos que formarán parte de la nueva red MPLS y considerados en el presente análisis serán proporcionados por la empresa Telefónica, la cual brindará a la operadora, soporte técnico especializado en los equipos suministrados, durante las fases de instalación, puesta en servicio y pruebas.

Los equipos serán administrados por un sistema de gestión local el cuál va a ser instalado en una computadora portátil que estará a cargo del personal técnico de ADECCO, el mismo que va a ser capacitado en el manejo y utilización del sistema de gestión.

Para que la nueva red MPLS propuesta quede operativa, no será necesario una infraestructura nueva, se reutilizará la existente tanto de fibra óptica como de espacios físicos en las estaciones.

5.1 SERVICIOS RED MPLS.

Entre los servicios que se espera brindar, con la nueva red MPLS que se es materia del presente proyecto están los siguientes:

- Servicios de Contenido.
- Enlaces Corporativos a bajo costo.
- Proveer anchos de banda bajo demanda, configurados por el responsable de IT.
- Servicios de Banda Ancha para Internet.

5.2 ANÁLISIS ECONÓMICO.

En el análisis económico describimos el presupuesto necesario para obtener la nueva red MPLS propuesta ADECCO., se ha realizado también el cálculo del retorno de la inversión (TIR), el cual indica que este proyecto es factible.

5.3 PRESUPUESTO PARA LA IMPLEMENTACIÓN DE LA RED MPLS.

Se han tomado en cuenta precios referenciales (no reales), de los equipos que van a ser utilizados. El total de la Inversión asciende a USD 13.200.

5.4 ANÁLISIS DE RETORNO DE INVERSIÓN.

Una vez que se ha estimado la inversión inicial, que es de USD 13.200, se ha estimado un tiempo aproximado de 10 meses para el cálculo del retorno de la inversión, y verificar que el proyecto es rentable.

5.5 PRESUPUESTO DETALLADO

EQUIPOS Y MATYERIALES	Unidades	CANTIDAD	COSTO UNITARIO	COSTO	COSTO +IVA
Switch 24 puertos	Un.	1	$ 527.050	$ 527.050	$ 611.378
Cable UTP	metro	1673	$ 801	$ 1.340.598	$ 1.555.094
Cable RG59	metro	603	$ 751	$ 452.939	$ 525.409
Conector RG59 de presión	Un.	19	$ 250	$ 4.750	$ 5.510
Modem Radio	Un.	3	$ 1.584.436	$ 4.753.308	$ 5.513.837
Antena enlace microondas	Un.	3	$ 1.824.522	$ 5.473.566	$ 6.349.337
Conector RJ45	Un.	800	$ 50	$ 40.007	$ 46.408
Canaleta	metro	418	$ 16.210	$ 6.775.576	$ 7.859.668
Amarre 10”	Un.	1000	$ 80	$ 80.027	$ 92.832
Ponchadora UTP	Un.	5	$ 55.058	$ 275.291	$ 319.337
Ponchadora RG59	Un.	4	$ 65.066	$ 260.262	$ 301.904
Terminal RJ11/RJ45	Un.	30	$ 9.510	$ 285.311	$ 330.960
Fibra óptica mono-modo	metro	1984	$ 1.168	$ 2.318.157	$ 2.689.062
Terminales fibra smut	Un.	8	$ 9.503	$ 76.025	$ 88.189
Caja de empalme	Un.	3	$ 270.420	$ 811.261	$ 941.063
Transceiver	Un.	4	$ 250.582	$ 1.002.329	$ 1.162.701
Cable eléctrico calibre 12	metro	1731	$ 702	$ 1.214.459	$ 1.408.773
Breaker con protección de	Un.	5	$ 7.001	$ 35.005	$ 40.606
Toma corriente regulado	Un.	30	$ 8.508	$ 255.253	$ 296.093
Caja breaker	Un.	5	$ 85.128	$ 425.639	$ 493.741
Sistema de tierras	Un.	28	$ 155.353	$ 4.349.890	$ 5.045.873
Cinta aislante	Un.	30	$ 6.004	$ 180.131	$ 208.952
Tubería galvanizada 1/2"	metro	400	$ 5.002	$ 2.000.699	$ 2.320.811
TOTAL EQUIPOS Y RECURSOS				$ 32.937.533	$ 38.207.538
				TRM DEL RECURSO $2900	$ 13.175

Tabla 4 Presupuesto detallado de la ejecución

NOMBRE DEL RECURSO -> ACTIVIDADES DESARROLLADAS	TIEMPO LABORADO	COSTO
Gerente de Proyecto	434 horas	$ 13.721.051
Diseño e implementación de la red WAN, LAN y voz para el ADECCO	434 horas	$ 13.721.051
Coordinador de Consultoría y diseño	72 horas	$ 1.991.765
Diseño topología de red	56 horas	$ 1.549.151
Contratación	16 horas	$ 442.614
Coordinador de adquisiciones	32 horas	$ 885.230
Procura	32 horas	$ 885.230
Coordinador de implementación y puesta en Marcha	212 horas	$ 5.236.289
Montaje SEDE central	86 horas	$ 2.124.155
Ingeniero Preventa	56 horas	$ 1.217.191
Diseño topología de red	56 horas	$ 1.217.191
Ingeniero Planeación red	16 horas	$ 347.769
Aprobación mapping	16 horas	$ 347.769
Analista de Compras	32 horas	$ 569.076
Procura	32 horas	$ 569.076
Ingeniero de gestión de instalaciones	197.5 horas	$ 3.122.016
Montaje SEDE central	86 horas	$ 1.359.460
Proyectista Bogotá	16 horas	$ 252.923
Visita de obra civil	16 horas	$ 252.923
Electricista Bogotá	4 horas	$ 37.091
Revisión puesta a tierra	4 horas	$ 37.091
Experto en cableado estructurado Bogotá	12 horas	$ 129.958
Verificación diseño cableado estructurado y eléctrico	8 horas	$ 86.638
Revisión instalación puntos de red LAN	4 horas	$ 43.319
Cuadrilla instalaciones fibra y cableado UTP Bogotá	56 horas	$ 1.960.858
Instalación y empalmes planta externa	40 horas	$ 1.400.613
Ejecución obra civil tendido de fibra interno (desde empalme externo hasta caja OB	16 horas	$ 560.245

Técnicos expertos en cableado estructurado Bogotá	16 horas	$ 140.061
Ejecución cableado estructurado	8 horas	$ 70.031
Instalación puntos de red	8 horas	$ 70.031
Ingeniero de aprovisionamiento de Proyectos	37 horas	$ 584.884
Instalación de equipos	2.4 horas	$ 37.938
Pruebas de Funcionamiento y puesta en marcha	4.2 horas	$ 66.392
Instalación de equipos	2.4 horas	$ 37.938
Pruebas de Funcionamiento y puesta en marcha	4 horas	$ 63.231
Instalación de equipos	6 horas	$ 94.846
Pruebas de Funcionamiento y puesta en marcha	2.4 horas	$ 37.938
Instalación de equipos	6 horas	$ 94.846
TOTAL		**$ 55.365.879**

Tabla 5 Costos invisibles del proyecto

Debido a que Adecco tiene personal en misión y especializado para cada actividad planteada, se hace un análisis de los costos invisibles del proyecto donde solo se tiene en cuenta el tiempo invertido y se proyecta con los valores que implícitamente dentro de la compañía están ya evaluados como costos de nomina

6 BENEFICIOS DE LA IMPLEMENTACIÓN

La compañía enfrenta continuamente diferentes presiones que la obliga a mejorar los niveles de servicios informaticos, reducir costos y mejorar sus controles. Para resolver esta situación, se ha recurrido a un modelo operativo en el cual la entidad se especializa en brindar un servicio altamente transaccional para distintas unidades de negocio a fin de reducir costos, consolidar funciones administrativas y evitar la duplicación de esfuerzos entre ellas.

6.1 BENEFICIOS DE LOS DE UNA RED HA

- Procesos estandarizados
- Mejor control
- menor costo hora hombre (HH)
- Economías de escala
- Mayor rendimiento de la inversión en TI
- 26% Restructuración de negocio y redución de costos
- 23% Contar con una plataforma común que soporte un crecimiento de escala
- 11% concentraciones económicas
- 10% Cambios de sistemas, ERP y tecnologías
- 9% Mayor control interno

6.2 DEMOSTRACIONES Y PRUEBAS DE MONITOREO

Dentro de las demostraciones de rendimiento vemos la grafica de monitoreo de trafico entrante y saliente de la red implementada, esa grafica es tomada en un intervalo de una hora critica

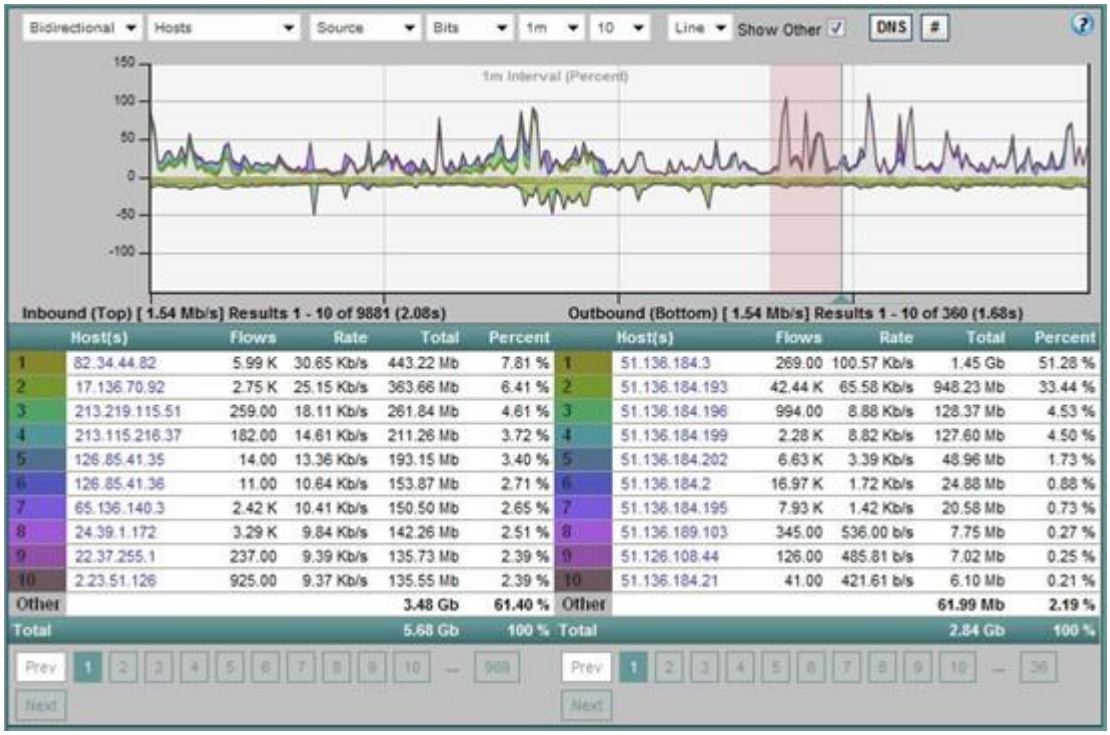

Ilustración 8 Trafico Inbound / Oudnound

Ahora bien, en una evaluación estadística este comportamiento se evidencia a partir de ítems exclusivos que muestran las transacciones críticas de la red para la unidad de negocio, especialmente las transaccionales de SQL, monitoreo de protocolos HTTP y HTTPS

Ilustración 9 Monitoreo de transacciones para servicios críticos por Filter ACL

En cuanto a la estabilidad de la red se muestra la Ilustración de estabilidad de red sin pérdida de paquetes

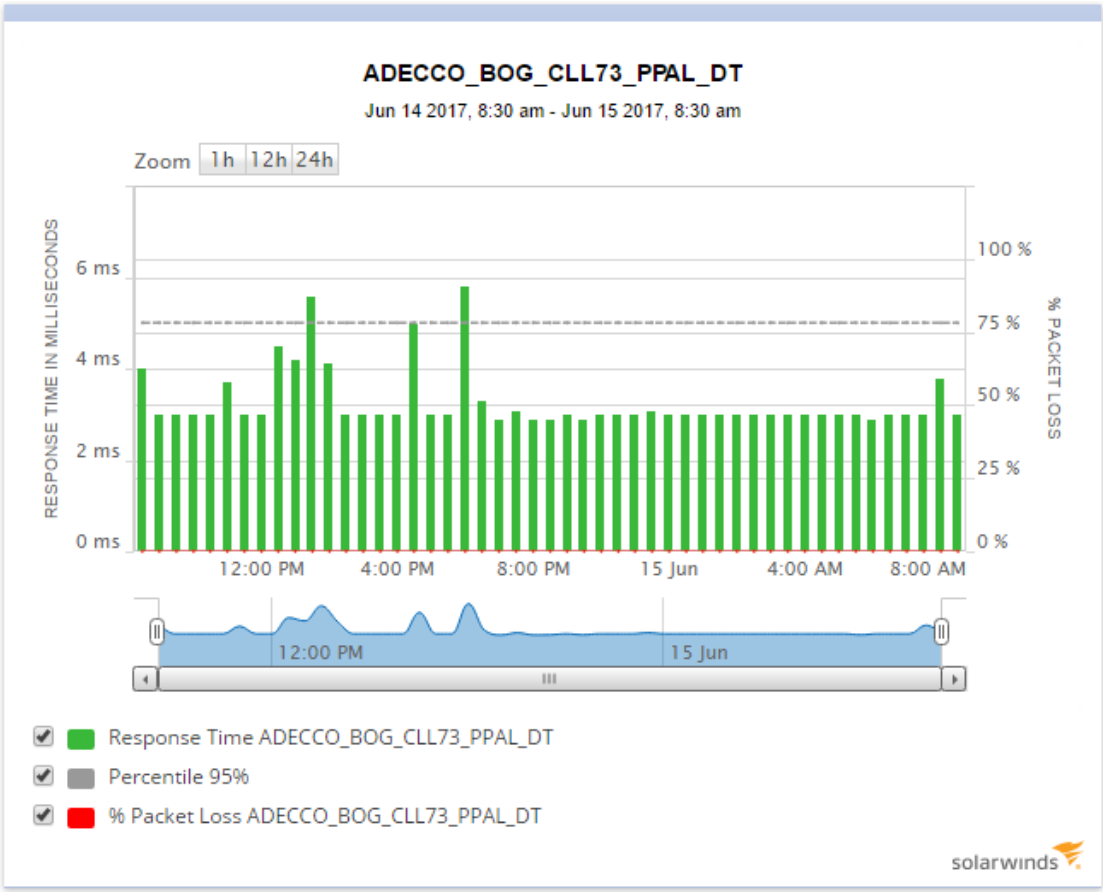

Ilustración 10 Monitoreo de Trafico y perdida de paquetes para el canal principal

Availability Statistics HELP

PERIOD	AVAILABILITY
Today	100,000 %
Yesterday	100,000 %
Last 7 Days	98,986 %
Last 30 Days	99,738 %
This Month	99,459 %
Last Month	100,000 %
This Year	97,691 %

Ilustración 11 Estadísticas de disponibilidad de la red

7 ALCANCES DEL PROYECTO

7.1 EQUIPOS INSTALADOS SEDE CALLE 73

En la sede Cll.73 se instalaron los siguientes elementos de hardware.

Switches CORE			
Cantidad	**Nombre**	**Descripción**	**Seriales**
2	EX3300-24T	24 Base T y 4 uplink	SGD0214380317 SGD0216150770
6	EX-SFP-10GE-USR	SFP+ 10 Gigabit Ethernet Ultra Short Reach	SAA15463VNXU SAA15463VNZB SAA15483VUN6 SAA15463VNYV SAA15493VY7D SAA15463VNZ0
Licenciamiento			
2	EX-24-EFL	Licencia para funcionalidades	RTU00019230831 RTU00019230832
Soporte de Fabricante			
2	SVC-SD-	Soporte SameDay	

Tabla 6 Hardware a instalado o entregado

Nota: los EX-SFP-10GE-USR fueron entregado a Adecco, los cuales van a ser usados cuando se cambie el medió de los troncales entre pisos.

7.2 DISEÑO LÓGICO DE LA SOLUCIÓN

7.2.1 *Topología Lógica De La Sede Calle 73*

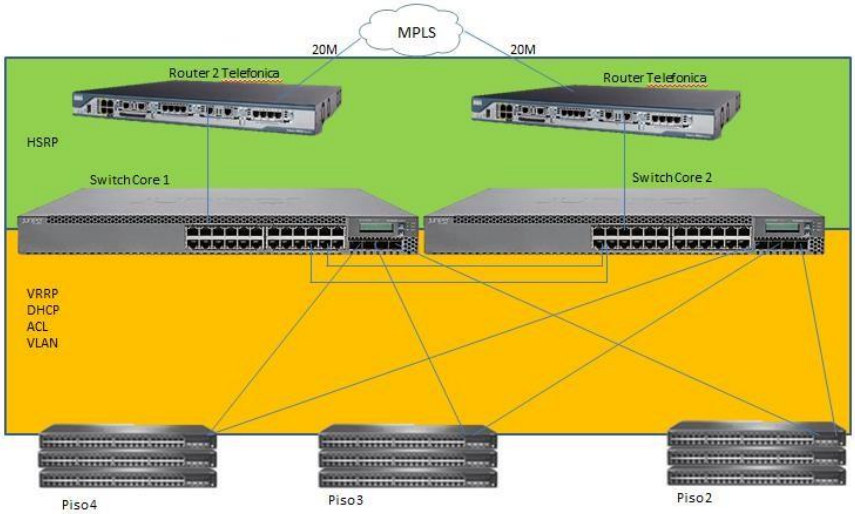

Ilustración 12 Topología lógica sede Calle 73

7.2.2 Direccionamiento ip de los switch sede calle 73

Los Switch Core de la calle 73 se pueden administrar a través de los siguientes servicios:

- Consola
- Ssh
- Telnet
- JWEB

El acceso a cada servicio se realiza por medio de la dirección IP de la interfaz, más no por la IP virtual. En la siguiente tabla se muestra la dirección IP para gestión de los Switch Juniper, 3COMM y HP

Ubicación/piso	Switch	Hostname	Dirección IP definitiva	Usuario	Password
4	Rack1	SW1_CORE_73	10.157.99.2	root	Xxxxxxxx
4	Rack1	SW2_CORE_73	10.157.99.3	root	Xxxxxxxx
4	Rack2		10.157.99.10	admin	Xxxxxxxx
4	Rack1		10.157.99.11	admin	Xxxxxxxx
3	Rack1-1		10.157.99.12	admin	Xxxxxxxx
3	Rack1-2		10.157.99.13	admin	Xxxxxxxx
3	Rack2-3		10.157.99.14	admin	Xxxxxxxx
2	Rack1-1		10.157.99.15	admin	Xxxxxxxx
2	Rack2-2		10.157.99.16	admin	Xxxxxxxx

Tabla 7 Tabla de ubicación locgica usuarios y claves

7.3 CONFIGURACIÓN

7.3.1 Lineamientos De Configuración

La configuración Lógica de los Switch de Core se realizó bajo los siguientes lineamientos:

- Creación de Nuevas VLAN para asignar nuevos segmentos de Red y eliminar el problema de direccionamiento insuficiente.
- Configuración de Redundancia para las VLAN asignadas a unidades de negocio críticas para Adecco.
- Distribución de trafico entrante y saliente por los dos enlaces que tiene actualmente Adecco con TELEFONICA.
- Administrar Capa 3 y servidores DHCP desde los Switch Core.
- Políticas de seguridad para las VLAN de WIFI.

Bajo estos lineamientos se configuró en el Switch lo siguiente:

7.3.2 Nuevas VLAN

En la siguiente tabla se muestran las nuevas VLAN y su respectivo direccionamiento IP:

DESCRIPCION VLAN	VLAN ID	NETWORK	GATEWAY	RESERVAS IP	OBSERVACIONES
ADMON NETWORK	4	10.157.99.0	10.157.99.1	Sin DHCP	ALTA DISPONIBILIDAD
WIFI INVITADOS	2	10.157.100.0/25	10.157.100.1	Primeras 5 ip	
WIFI MOBILE	3	10.157.100.128/25	10.157.100.129	Primeras 5 ip	
CSC	10	10.157.12.0/24	10.157.12.1	Primeras 50 IP	PRIORIDAD ALTA
PAYROLL	11	10.157.17.0/24	10.157.17.1	Primeras 50 IP	PRIORIDAD ALTA
BPO -SALES	12	10.157.15.0/24	10.157.15.1	Primeras 50 IP	
TELEFONIA	14	10.157.101.0/24	10.157.101.1	Primeras 50 IP	VLAN LOCAL
PERMANENT - SELECCIÓN – CONTROLLER	15	10.157.13.0/24	10.157.13.1	Primeras 50 IP	
Red GW-Core	100	10.157.102.0/28	10.157.102.1 10.157.102.2	N/A	VLAN Router Telefonica –Switch core

Tabla 8 Direccionamiento a implementar en la red LAN de ADECCO

7.3.3 Configuración de DHCP

Para las VLAN dedicadas a la conexión de usuarios locales se creó un servidor DHCP en el Switch el cual entrega direccionamiento de acuerdo a la VLAN en la cual esté conectado el usuario final. En la Tabla 2 se muestran los parámetros de dirección IP de RED, Mascara, Gateway por defecto y reservas de direcciones IP para cada una de las subredes de calle 73.

7.3.4 Configuración de VRRP

Para configurar redundancia para cada uno de los segmentos de red de la sede de Adecco Calle 73, se utilizó el protocolo VRRP (Virtual Router Redundancy Protocol), donde los Switches de Core actúan como una plataforma de enrutamiento virtual. Permitiendo a los hosts de las subredes a hacer uso de plataformas de enrutamiento redundantes configurando únicamente una sola dirección como Gateway por defecto.

Los Switches con VRRP comparten la dirección IP correspondiente a la ruta predeterminada configurada en los hosts.

En VRRP uno de los Switch cumple el rol de maestro (activo) y el otro es backup, esta configuración se realiza por cada uno de los segmento de la red de la sede de calle 73, lo que permite granularidad en la configuración. Si el Switch Maestro falla, el que tiene el roll de backup se convierte en el nuevo maestro, proporcionando una plataforma virtual de direccionamiento por omisión y permitir el tráfico en la LAN y WAN.

Con la granularidad de la configuración de VRRP por segmento de Red se logra que uno de los Switch sea el maestro de unas VLAN y el otro Switch sea el maestro para otras VLAN, en la siguiente tabla se describen la direcciones ip de cada interfaz VLAN, cuál es su dirección virtual y cuál es su Switch Maestro.

DESCRIPCION VLAN	VLAN ID	IP virtual	SW_1	Sw_2	Switch Core Maestro
ADMON NETWORK	VLAN4	10.157.99.1	10.157.99.2	10.157.99.3	Switch_Core_1
WIFI INVITADOS	VALN2	10.157.100.1	10.157.100.2	10.157.100.3	Switch_Core_1
WIFI MOBILE	VALN3	10.157.100.129	10.157.100.130	10.157.100.131	Switch_Core_2
CSC	VLAN10	10.157.12.1	10.157.12.2	10.157.12.3	Switch_Core_1
PAYROLL	VLAN11	10.157.17.1	10.157.17.2	10.157.17.3	Switch_Core_2
BPO -SALES MARKETING	VLAN12	10.157.30.1	10.157.30.2	10.157.30.3	Switch_Core_2
TELEFONIA	VLAN14	10.157.101.1	10.157.101.2	10.157.101.3	Switch_Core_2
PERMANENT - SELECCIÓN - CONTROLLER	VLAN15	10.157.13.1	10.157.13.2	10.157.13.3	Switch_Core_1

Tabla 9 Direccionamiento VRRP

7.3.5 Configuración De Enrutamiento

En cada uno de los Switch se configuró una ruta por defecto hacia el Router al cual está conectado, en la siguiente tabla se muestra el puerto y Router de cada Switch de Core:

Switch	Puerto	Router	Puerto
Switch_Core_1	ge-0/0/22	ADECCO_CL73_PPAL	GigabitEthernet0/1
Switch_Core_2	ge-0/0/23	ADECCO_CL73_BCKUP	GigabitEthernet1/0/1

Tabla 10 Conexión Switch Core Router

Las Rutas estáticas configuradas en los Switch apuntan a una dirección virtual que comparten los Routers por medio del protocolo HRSP, estas direcciones ip tienen un Router con roll activo o master y otro que es back up, la asignación de estos roles se configuró de acuerdo a la conexión física del Router, por lo tanto el Switch_Core_1 tiene como Router master a ADECCO_CL73_PPAL y el Switch _Core_2 tiene como master a ADECCO_CL73_BCKUP.

Esta configuración quiere decir que los datos generados por las VLAN que tienen como Master en VRRP el Switch_Core_1 saldrán y entraran por el Router ADECCO_CL73_PPAL y los Datos de las VLAN que tiene como Master en VRRP el Switch_Core_2 saldrán y entraran por el Router ADECCO_CL73_BCKUP. En caso de caída de uno de los Router, las Vlan tendrán comunicación hacia la WAN por el Router que este activo.

7.3.6 Configuración De Firewalll Filter (ACL)

Se configuraron dos firewall filter, el primero se encarga de las políticas de seguridad aplicadas a red WIFI y el segundo de las políticas de HA para las redes no críticas para el Adecco. A continuación se profundiza en cada una:

El firewall filter DENY_NETWORK se encarga de bloquear el acceso de las redes asignadas a WIFI (Vlan 2 y 3) a la red interna y datacenter de Adecco(10.157.0.0/16 y 172.18.16.0/24).

El firewall filter NO_HA evita que las VLAN asignadas áreas que no son críticas para Adecco, en caso de la caída de uno de los canales, utilicen el canal activo, dando así prioridad únicamente a los segmentos de red más críticos para Adecco(PAYROLL y BPO)

7.3.7 Configuración De Protocolos Adicionales

Se configuró RSTP por la compatibilidad que tiene con los Switch 3COMM y HP que tiene la sede en la capa de Acceso.

LLDP es un protocolo de Capa 2 el cual permite conocer otros dispositivos conectados al Switch que soporten este protocolo, la configuración de este se realizó con el fin de aclarar la topología antes de la instalación y para que se pueda mantener control sobre la nueva topología.

Nota: los EX-SFP-10GE-USR fueron entregado a Adecco, los cuales van a ser usados cuando se cambie el medió de los troncales entre pisos.

El firewall filter NO_HA evita que las VLAN asignadas áreas que no son críticas para Adecco, en caso de la caída de uno de los canales, utilicen el canal activo, dando así prioridad únicamente a los segmentos de red más críticos para Adecco(PAYROLL y BPO)

7.3.8 Configuración De Protocolos Adicionales

Los protocolos adicionales que se configuraron fueron RSTP y LLDP.
Se configuró RSTP por la compatibilidad que tiene con los Switch 3COMM y HP que tiene la sede en la capa de Acceso.
LLDP es un protocolo de Capa 2 el cual permite conocer otros dispositivos conectados al Switch que soporten este protocolo, la configuración de este se realizó con el fin de aclarar la topología antes de la instalación y para que se pueda mantener control sobre la nueva topología.

7.3.9 Topología Final de Red

Al finalizar el proyecto la topologia final se entrega como se muestra a continuacion

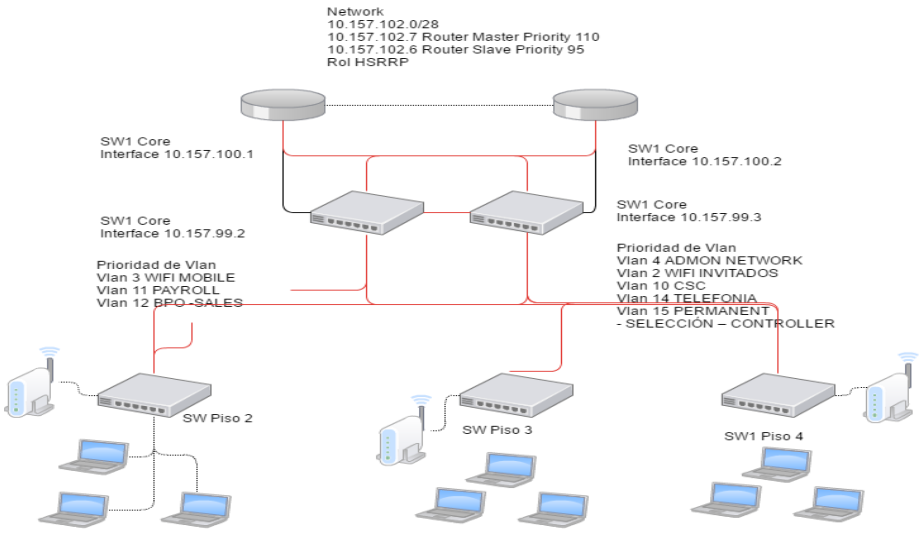

Ilustración 13 Topología Final para la Sede Critica

8 LIMITACIONES DEL PROYECTO

No se considera dentro del alcance:

- Configuración de equipos diferentes a los incluidos en esta propuesta.
- No incluye materiales de cableado energización y racks.
- No se incluye suministro de materiales o trabajos para adecuaciones de obra civil.
- La instalación de todos los dispositivos se contempla a cero metros.
- Configuraciones y actualizaciones que se requieran durante la implementación, sea servidores rackeables, blades, routers internos, routers externos, Switches de CORE, Switches de distribución, aplicaciones, software que hoy se encuentran en la red. Los cambios que se necesiten serán realizados por el cliente.
- No se incluye la configuración de Access Point.
- No se incluyen tiempos muertos que sean ajenos a MCO GLOBAL.

9 CRONOGRAMA

9.1 ETAPA 1

Paso	Ejecución	Tiempo Máximo Calculado (mins)	Caídas del servicio (segs)	Descripción	Responsable
1	Toma Back Up, Gateway Telefonica	10	0	Realizar Back Up de la configuración de los Router de Telefónica.	TELEFONICA
2	Toma de Back Up Sw de acceso	40	0	Realizar Back Up de los Switch de Acceso.	MCO GLOBAL/ADECCO
3	Desembalaje e instalación física Sw Core	30	0	Desembalaje e instalación en Rack del Switch de Core	MCO GLOBAL
4	Cambio de configuración en Routers	30	30	Cambio de configuración para la publicación de nuevas	TELEFONICA
5	Conexión de Patch Cord al Sw Core	30	10	Conexión de patch cord del Router y a los Switch de acceso	MCO GLOBAL/ADECCO
6	Pruebas de conectividad con cada una de las VLAN	30	30	Realizar pruebas con PC conectado directamente al SwCore de cada una	MCO GLOBAL/ADECCO
7	Afinamiento configuración al Switch de Core	30	30	Realizar configuraciones adicionales al Sw CORE a las precargadas para el	MCO GLOBAL
8	Configuración VLAN en SW de acceso.	60	60	Realizar la configuración de VLAN y Puertos en los	MCO GLOBAL/ADECCO
9	Pruebas de conectividad y aplicaciones en PC	60	0	Realiza pruebas de conectividad y aplicaciones para un grupo de PC en cada VLAN	MCO GLOBAL/ADECCO
Total (mins)		320	160		
Total (hrs)		5.3	2.6		

Tabla 11 Cronograma de ejecución Etapa I

9.2 ETAPA 2

Paso	Ejecución	Tiempo Máximo Calculado (mins)	Caídas del servicio (segs)	Descripción	Responsible
1	Toma Back Up, Gateway Telefonica	10	0	Realizar Back Up de la configuración de los Router de Telefónica.	TELEFONICA
2	Toma de Back Up Sw de Core	40	0	Realizar Back Up al Switch Core instalado en la Fase I.	MCO GLOBAL/ADECCO
3	Desembalaje e instalación física Sw Core	30	0	Desembalaje e instalación en Rack del Switch de Core	MCO GLOBAL
4	Cambio de configuración en Routers Telefónica	30	30	Cambio de configuración para la publicación de nuevas subredes	TELEFONICA
5	Conexión de Patch Cord al Sw Core	30	10	Conexión de patch cord del Router y a los Switch de acceso	MCO GLOBAL/ADECCO
6	Afinamiento configuración al Switch de Core	30	30	Realizar configuraciones adicionales al Sw CORE a las precargadas para el correcto funcionamiento	MCO GLOBAL
7	Pruebas de conectividad y aplicaciones en PC	60	0	Realiza pruebas de conectividad y aplicaciones para un grupo de PC en cada VLAN	MCO GLOBAL/ADECCO
Total (mins)		320	160		
Total (hrs)		5.3	2.6		

Tabla 12 Cronograma de ejecución Etapa I

9.3 PROCEDIMIENTO ROLL BACK FASE I

Paso	Ejecución	Tiempo Máximo Calculado (mins)	Caídas del servicio (segs)	Descripción	Responsable
1	Carga de back up a los Switch de accesos	60	60	Carga de la configuración de Backup a los Switch de acceso	MCO GLOBAL/ADECCO
2	Carga de BackUp a los Router	10	10	Carga de configuración de Backup a los Router telefónica	TELEFONICA
3	Desconexión de Sw Core	10	10	Desconexión de los patch cord de Sw Core y restauración de la	MCO GLOBAL/ADECCO
4	Protocolo de	40	0	Ejecutar el protocolo de pruebas	MCO GLOBAL y
Total (mins)		120			
Total (hrs)		2			

Tabla 13 Procedimiento Roll Back Fase I

9.4 PROCEDIMIENTO ROLL BACK FASE II

Paso	Ejecución	Tiempo Máximo Calculado (mins)	Caídas del servicio (segs)	Descripción	Responsable
1	Carga de back up al Switch Core	60	60	Carga de la configuración de Backup al Switch Core	MCO GLOBAL/ADECCO
2	Carga de Back UP a los Router Telefónica	10	10	Carga de configuración de Backup a los Router telefónica	TELEFONICA
3	Desconexión de Sw Core	10	10	Desconexión de los patch cord de Sw Core y restauración de la misma	MCO GLOBAL/ADECCO
4	Protocolo de Pruebas	40	0	Ejecutar el protocolo de pruebas	MCO GLOBAL y ADECCO
Total (mins)		120			
Total (hrs)		2			

Tabla 14 Procedimiento Roll Back Fase II

9.5 PROTOCOLO DE PRUEBAS

Para verificar el correcto funcionamiento se deben realizar las siguientes tareas:

Estas son las pruebas que se realizan sobre los equipos, los cuales serán tomados como verificación de funcionamiento correcto.

Prueba	Descripción de la Prueba	Resultad
1	Desde el Switch, Verificar el estado de los puertos.	Ok
2	Desde el Switch, Verificar acceso remoto.	Ok
3	Desde el Switch, Verificar versión del Firmware	Ok
4	Desde el Switch, Verificar configuración de VLAN	Ok
5	Desde el PC, Verificar conectividad a aplicaciones críticas.	Ok
6	Desde el PC, Verificar conexión a Internet	Ok
7	Desde teléfono IP, verificar encendido y conectividad	Ok

Tabla 15 Tabla de Verificación de Pruebas

10 RECOMENDACIONES

- El proyecto está diseñado para ser ejecutado por el área de tecnología de ADECCO, así como por parte de la empresa MCO, por lo tanto, es indispensable la documentación de cualquier cambio realizado en el diseño del mismo, dicha documentación servirá entonces para llevar un mejor control.
- Es indispensable también llevar a cabo buenas prácticas como mantener los sitios de trabajo limpios y ordenados, con el cableado identificado por color si es posible, con nodos etiquetados, Switches nombrados con una etiqueta y su correspondiente IP de administración; finalmente es importante tener instalado y funcionando un aire acondicionado.
- El diseño del proyecto está pensado para funcionar al 100% con equipo de la marca JUNIPER, por lo que se deberán de adquirir nuevos equipos conforme se requieran de dicha marca.
- El cambio de contraseñas deberá ser periódico para así mantener los equipos seguros.
- La asignación de los bloques de IP se llevará a cabo por el área de Telecomunicaciones del Área Central, por lo que cualquier requerimiento de implementación en la sede deberá ser autorizado por el área de tecnología.

11 CONCLUSIONES

Las investigaciones e implementaciones desarrolladas por los autores consultados para efecto del desarrollo del tema elegido para la realización del presente documento, resultaron de vital importancia para el estudio del mismo, donde se analizaron con detenimiento, con el propósito de obtener bases sólidas que permitan en la ejecución, la máxima optimización de la red de un edificio de operación critica

Para poder desarrollar los objetivos propuestos al inicio del documento, fue necesario tener un capitulo para el estudio de la red con la que cuenta la compañía, logrando observar los elementos indispensables para poder otorgar servicios de banda ancha móvil a los usuarios con los que cuenta la organización, para lo cual se contó con la decidida colaboración por parte de los funcionarios de la mencionada empresa, proporcionando la información necesaria, al igual que los tiempos y los elementos de red imprescindibles en la optimización de canal brindada por multicast.

Las pruebas desempeñadas en el último capítulo sirvieron para observar de una forma más descriptiva como la configuración de mejora considerablemente los recursos de canal, dejando una base para una futura implementación de aplicaciones digitales basadas en IP como por ejemplo IPTV, de esta forma él envió de varios canales en la topología de una red metro se verá por los elementos de networking como si solo se estuviera emitiendo un único canal, lo que conlleva a obtener mayores velocidades y una mejor calidad de servicio.

Y como ultimó podemos conlcuir que a partir de la implementacion de este proyecto ADECCO cuenta con una red en alta disponibiidad, redundancia electrica, de datos y conectividad con un mejor performance y estabilidad

12 Glosario

CRC: (CYCLICAL REDUNDANCY CHECKING) Verificación de Redundancia Cíclica. Método moderno de calcular un BCS que asegura que muy pocos errores se escaparán sin ser detectados. Tiene la enorme ventaja de que detecta errores cuando viene estos seguidos ("burst").(Ing. Oscar Molina Loría.)

VTP: son las siglas de VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco.

Ethertype: es una de dos octeto de campo de una trama Ethernet. Se utiliza para indicar qué protocolo se encapsula en la carga útil de la trama. El mismo campo también se utiliza para indicar el tamaño de algunas tramas Ethernet. EtherType se definió primero por el encuadre Ethernet II estándar, y posteriormente adaptado para la IEEE 802.3 estándar.

BPDU: Bridge Protocol Data Units (BPDUs) son tramas que contienen información del protocolo Spanning tree (STP). Los switches mandan BPDUs usando una única dirección MAC de su puerto como mac de origen y una dirección de multicast como MAC de destino (01:80:C2:00:00:00) .

Hay tres tipos de BPDUs:

- BPDU de configuración, usada por el protocolo Spanning tree para
- proveer información a todos los switches.
- TCN (Topology change), avisa sobre cambios en la topología.
- TCA (Topology change Acknowledgment), confirman la recepción del TCN.

Enlace Truck: Para realizar esto existe un protocolo llamado 802.1q, que expecifica como deben ser tratados los Frames para que puedan ser entendidos por los equipos de comunicaciones, basicamente lo que hace es modificar el Frame Ethernet agregarle un TAG de 4 bytes (donde viaja la información de la vlan a la que pertenece el frame entre otros) y además de eso tiene que regenerar el FCS (Frame Check Sequence), que es el indicador si el paquete llego a destino sin problemas. entonces para hacerla entendible es algo como esto SW1-V1<-------Trunk802.1q-------->SW2-V1

Dominios de Colisión. Es un segmento de red que comparte el ancho de banda disponible entre múltiples dispositivos terminales; como consecuencia cuando dos o más dispositivos conectados al mismo segmento intentan comunicarse entre sí es posible que se produzca una colisión. En este sentido es deseable reducir el tamaño de los dominios de colisión, para lo cual se deben utilizar dispositivos que operan en la capa 2 o superiores del modelo OSI. Los hubs extienden los dominios de colisión, mientras que switches y routers los limitan. Los switches reducen las colisiones y permiten una mejor utilización del ancho de banda en los segmentos de red, ya que ofrecen un ancho de banda dedicado para cada segmento de red.Dominio de Colisiones

Dividir Dominios de Broadcast. Se trata de una porción de red en la que, a pesar de que pudo haber sido segmentada en capa 2 es aún una unidad a nivel de capa 3 por lo que un paquete de broadcast es transmitido a todos los puertos conectados. Si bien los switches filtran la mayoría de las tramas según las direcciones MAC de destino, no hacen lo mismo con las tramas de broadcast. Un conjunto de switches interconectados forma un dominio de broadcast simple. Para dividir dominios de broadcast es necesario implementar VLANs o dispositivos que operan en la capa 3 del modelo OSI, tales como switches multilayer o routers.

Broadcast: Se refiere al mensaje que se envia a todas las estaciones en una conexión lógica ("data link") multipunto.

Baudio: El número de señales transmitidos sobre un conexión lógica ("data link") cada segundo. El término baudio expresa la cantidad de señales viajando sobre un "data link" por unidad de tiempo (un segundo). Esto es una tasa ("rate"). Por lo tanto es incorrecto utilizar el término "baud rate" pues esto implica la aceleración de las señales. En una onda analógica una señal puede ser un cambio en su frecuencia, su amplitud o su fase o incluso la forma. Dos cambios posibles en la señal pueden direccionar (significar) cuatro bits (digitales). Por lo anterior, una manera incorrecta de usar el término baudio o "baud" es usarlo como sinónimo de "bits por segundo". Si usamos un elemento señalador para mover un bit, entonces "baudio" es igual a "bits por segundo" en números, pero no significa lo mismo exactamente. Si el elemento señalador transporta más de un bit (como los modems síncronos) el "bit rate " es un múltiplo de los baudios.

Binario: Es el nombre del sistema numérico de base 2.
Bit: Acrónimo de "BInary digiT" (dígito binario) lo que es la unidad básica y elemental de información en el mundo de las computadoras. Un bit es también un dígito en un número binario. Consiste de dos valores: cero (0) y uno (1).

También se entiende por bit a la información que se puede almacenar en una celda sencilla de memoria (flip-flop).

BPS. Bits Por Segundo; se refiere a la velocidad a la que la información es enviada sobre una conexión lógica ("data link")

Byte: Se le llama así a un grupo de bits que tiene un significado singular. Por ejemplo, un byte puede representar un caracter. Generalmente, un byte representa ocho bits.

Cable coaxial: Es un tipo de cable donde el conductor (alambre) que lleva la señal está completamente rodeado por el conductor "ground" (llamado escudo o trenza). El cable coaxial provee un ambiente de alta velocidad y mínima distorción para las señales.

Cluster: Configuración donde dos o más dispositivos comparten un modem.

Dedicada: Se refiere a un "data link" que está permanentemente conectada; no requiere establecer un procedimiento de llamadas para poder comunicarse entre estaciones. Usualmente se considera como lo opuesto de conmutar.

Direccion (ADDRESS): Un nombre, etiqueta, número o secuencia de bits que se usa para identificar: al receptor de un mensaje, a un dispositivo en particular en una línea multipunto, la trayectoria de una ruta, etc. Es un lugar único en la memoria, este también sirve para identificar un nodo en una red.

Distorsion: Cualquier cambio indeseado a una señal que pueda alterar su forma original.

FCS: (FRAME CHECK SEQUENCE) Es el nombre de la información de verificación de errores que está adherida cerca del final de un "frame" o marco en protocolos de bits. Esto es equivalente al BCS en protocolos de caracter.

Ghz: Giga Hertz; se refiere a billones de hertz.

IEEE802: Redes de Computadoras Ing. Oscar Molina Loría. Estos son los estandares para la coneccion física y electrica de LAN's desarrollado por IEEE (Institute of Electronic and Electrical Engineers).

Internet: Colección de redes de telecomunicación que incluye ARPAnet, MILnet, y NSFnet: (National Science Foundation net). Internet usa protocolos TCP/IP.

KBPS: Kilo Bits Por Segundo; se refiere a miles de bits por segundo.

Lan: (LOCAL AREA NETWORK) Red de Area Local, o más brevemente Red Local de Computadoras. Se refiere a una red de computadoras conectadas bajo un mismo protocolo y tipo de conexión física, sin modulación de la señal y en distancias cortas (menores generalmente a los 10 KM, por ejemplo el diámetro de un campus universitario).

LOOP: Arreglo de comunicaciones miltipunto donde las estaciones se conectan en forma de anillo o "loop". Todas las estaciones llevan a cabo la función de almacenaje y envío de datos. La estación anfitriona o "host" envía datos en una dirección "downlink direction" y recibe datos en otra dirección "uplink direction".

MODEM MOdulador/DEModulador; es un convertidor de señales. Un dispositivo que convierte señales de datos digitales y binarias a una señal compatible con el medio que se está utilizando.Access Point: significa punto de acceso. Se trata de un dispPAtivo utilizado en redes inalámbricas de área local (WLAN - Wireless Local Area Network), una red local inalámbrica es aquella que cuenta con una interconexión de computadoras relativamente cercanas, sin necesidad de cables, estas redes funcionan a base de ondas de radio específicas. El Access Point entonces se encarga de ser una puerta de entrada a la red inalámbrica en un lugar específico y para una cobertura de radio determinada, para cualquier dispositivo que solicite acceder, siempre y cuando esté configurado y tenga los permisos necesarios.

Protocolo: Este es el procedimiento (conjunto de pasos, mensajes, forma de los mensajes y secuenbcias) que se utiliza para mover la información de una localización a otra sin errores.

Ancho de banda: en conexiones a Internet el ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmlente en bit’s por segundo (bps), kilobits por segundo (kbps), o megabits por segundo (Mbps).

Área de trabajo: es el lugar del centro de trabajo, donde normalmente un trabajador desarrolla sus actividades.
Atenuación: disminución de la intensidad o fuerza de la señal.

Cable de par trenzado: dos conductores eléctricos aislados son entrelazados

para anular las interferencias de fuentes externas y diafonía de los cables adyacentes.

Cable UTP: (Unshielded Twisted Pair), par trenzado sin blindaje. Cable de telecomunicaciones universalmente utilizado para conectar equipos de escritorio a una red. Contiene cuatro pares de cables y se clasifica en categorías dependiendo de la velocidad de conducción: categorías 3, 4, 5, 5e, 6 y 7.

Circuito: lazo cerrado formado por un conjunto de elementos, dispositivos y equipos eléctricos, alimentados por la misma fuente de energía y con las mismas protecciones contra sobretensiones y sobretensión. No se toman los cableados internos de equipos como circuitos.

Conductores: es un hilo (alambre) o una combinación de hilos (cable) no aislados entre sí, adecuados para que por ellos circule una sola corriente eléctrica. También existen en forma de barras rectangulares y de diseños especiales. La mayoría es de aluminio, aluminio recubierto con cobre, cobre, debido a su bajo costo. Su capacidad de transportar corriente está relacionada con su número atómico.

Confiabilidad: capacidad de un dispositivo, equipo o sistema para cumplir una función requerida, en unas condiciones y tiempo dados. Equivale a fiabilidad.

Decodificador: los decodificadores son circuitos combinacionales basados en puertas lógicas que trasforman un código de tipo binario en código decimal. Su función consiste en activar una sola de sus salidas dependiendo del estado lógico en que se encuentren sus entradas.

Fibra óptica: empleado habitualmente en redes de datos como medio de transmisión; en el cual un hilo muy fino de material transparente, vidrio o materiales plásticos, nos permite enviar pulsos de luz que representan los datos a transmitir.

Hardware conexión: se refiere a los objetos físicos para que la conexión a la red funcione. Estos son por ejemplo router, el modem, el teléfono, el ordenador, etc.

Router: también conocido como encaminador, enrutador, direccionador o ruteador es un dispositivo de hardware usado para la interconexión de redes informáticas que permite asegurar el direccionamiento de paquetes de datos entre ellas o determinar la mejor ruta que deben tomar

Sistema de puesta atierra (SPT): grupo de elementos conductores equipotenciales, en contacto eléctrico con el suelo o una masa metálica de referencia común, que distribuye las corrientes eléctricas de falla en el suelo o en la masa. Comprende electrodos, conexiones y cables enterrados.

Switch: es un dispositivo de conmutación que permite el control de distintos equipos con tan sólo un monitor, un teclado y un ratón. Tienen "n" entradas y 2n salidas.

TIC: las tecnologías de la información y la comunicación (TIC) son todas aquellas herramientas y programas que tratan, administran, transmiten y comparten la información mediante soportes tecnológicos. La informática, Internet y las telecomunicaciones son las TIC más extendidas, aunque su crecimiento y evolución están haciendo que cada vez surjan cada vez más modelos. [4]

[4] STALLINGS, William, et al. *Comunicaciones y Redes de Computadores, 6aedición*. Prentice-Hall, 2000.
CALVO, Rafael Fernández. *Glosario básico inglés-español para usuarios de Internet*. Asociación de Técnicos de Informática (ATI), 2001.
TEJEDOR, Ramón Jesús Millán. *Redes de datos y convergencia IP*. Creaciones copyright, 2007.
SALAZA, Odalys Arencibia. GLOSARIO DE TÉRMINOS PARA EL TRABAJO EN RED.
PINEDA ESPINOS, JUAN ANTONIO, et al. *MONITOREO DE FALLOS EN CONMUTADORES DE DATOS DE REDES LAN*. 2010. Tesis Doctoral.

13 BIBLIOGRAFÍA

Project Management Institute, Guía del PMBOK (5 ed.) 'reilly, Head First PMP (3 ed.)

RMC Publication, INC, 2009. Rapid Learning to pass PMI's PMP Exam.

Unidad de planeación Minero Energética, 2013, Reglamento Técnico de Instalaciones Eléctricas – RETIE.

Giraldo Giraldo Alexandra (2006). Estudio de factibilidad de un sistema vsat de comunicaciones para televisión y multimedia, Universidad Del Quindío, Facultad de ingeniería, Ingeniería electrónica.

BADDI, Youssef; ECH-CHRIF El KETTANI, Mohamed Dafir. VNS-RP algorithm for RP selection in multicast routing protocol PIM-SM En: Multimedia Computing and Systems (ICMCS), 2012 International Conference on. Abril-Mayo, 2012. p. 595

CACHINERO, Juan Ángel. Análisis y modelado de multicast interdominio para el soporte de servicios de video. La Empresa [citado 7 agosto, 2014]. Disponible en internet: URL:http://oa.upm.es/1840/1/PFC_JUAN_ANGEL_CACHINERO_POZUELO.pdf

CISCO SYSTEMS. Cisco 7200 Series Routers [En linea]. La Empresa [citado 15 Septiembre, 2014]. Disponible en internet: < URL: http://www.cisco.com/c/en/us/products/routers/7200-series-routers/index.html>

CISCO SYSTEMS. Cisco ASR 1000 Series Aggregation Services Routers [En linea]. La Empresa [citado 20 Septiembre, 2014]. Disponible en internet: URL:http://www.cisco.com/c/en/us/products/routers/asr-1000-series-aggregationservices-routers/index.html

CISCO SYSTEMS. CLI Comands. En: Cisco Wireless LAN Controller Command Reference.,June, 2010, p. 2-1

CISCO SYSTEMS. Unicast, Anycast, Broadcast and Multicast [En linea]. La Empresa [citado 10 agosto, 2014]. Disponible en internet:

URL:http://www.cisco.com/c/en/us/products/collateral/physical-security/videosurveillance-manager/prod_white_paper0900aecd8073c232.html

CISCO, systems. Unicast, Anycast, Broadcast and Multicast [En linea]. La Empresa [citado 10 agosto, 2014]. Disponible en internet: URL:http://www.cisco.com/c/en/us/products/collateral/physical-security/videosurveillance-manager/prod_white_paper0900aecd8073c232.html

FORTINET. FortiOS Handbook for FortiOS 5.2 [En línea]. La Empresa [citado Octubre, 2014]. Disponible en internet: URL:http://docs.fortinet.com/fortigate/admin-guides

FORTINET. FortiOS Handbook for FortiOS 5.2 [En línea]. La Empresa [citado Octubre, 2014]. Disponible en internet: <URL: http://docs.fortinet.com/fortigate/admin-guides>

14 ANEXO

14.1 CONFIGURACION FINAL DE LOS SWITCH

CONFIGURACIÓN DE CLI PARA SWITCHES

A continuación, se detalla cada una de las configuraciones explicadas en el numeral anterior en el Switch 1, como las configuraciones son similares en ambos Switches, no se muestra las del Switch 2, sin embargo, con este informe se ajunta un back up de la configuración de los dos equipos.

```
root@SW1_CORE_73# show
## Last changed: 2016-02-15 11:46:26 UTC
version 12.3R6.6;
system {
    host-name SW1_CORE_73;
    root-authentication {
        encrypted-password "$1$s.Kjf2Wt$xvof9bbxLT78hxqc/mito.";
## SECRET-DATA
    }
    services {
        ssh;
        telnet;
        web-management {
            http;
        }
        dhcp {
            name-server {
                172.18.16.140;
                10.157.0.116;
            }
            pool 10.157.100.0/25 {
                address-range low 10.157.100.6 high
10.157.100.126;
                name-server {
                    8.8.8.8;
                }
                router {
                    10.157.100.1;
                }
            }
            pool 10.157.100.128/25 {
                address-range low 10.157.100.134 high
10.157.100.254;
                name-server {
                    8.8.8.8;
```

```
                }
                router {
                    10.157.100.129;
                }
            }
            pool 10.157.12.0/24 {
                address-range low 10.157.12.51 high
10.157.12.254;
                name-server {
                    172.18.16.140;
                    10.157.0.116;
                }
                router {
                    10.157.12.1;
                }
            }
            pool 10.157.17.0/24 {
                address-range low 10.157.17.51 high
10.157.17.254;
                router {
                    10.157.17.1;
                }
            }
            pool 10.157.101.0/24 {
                address-range low 10.157.101.51 high
10.157.101.254;
                router {
                    10.157.101.1;
                }
            }
            pool 10.157.13.0/24 {
                address-range low 10.157.13.51 high
10.157.13.254;
                router {
                    10.157.13.1;
                }
            }
            pool 10.157.30.0/24 {
                address-range low 10.157.30.51 high
10.157.30.254;
                router {
                    10.157.30.1;
                }
            }
        }
    }
    syslog {
        user * {
            any emergency;
```

```
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
}
chassis {
    aggregated-devices {
        ethernet {
            device-count 4;
        }
    }
    alarm {
        management-ethernet {
            link-down ignore;
        }
    }
}
interfaces {
    ge-0/0/0 {
        ether-options {
            802.3ad ae2;
        }
    }
    ge-0/0/1 {
        ether-options {
            802.3ad ae2;
        }
    }
    ge-0/0/2 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members all;
                }
            }
        }
    }
    ge-0/0/3 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members all;
```

```
            }
        }
    }
}
ge-0/0/4 {
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members all;
            }
        }
    }
}
ge-0/0/5 {
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members all;
            }
        }
    }
}
ge-0/0/6 {
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members 2-4;
            }
        }
    }
}
ge-0/0/7 {
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members all;
            }
        }
    }
}
ge-0/0/8 {
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
```

```
                members all;
            }
        }
    }
}
ge-0/0/9 {
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members all;
            }
        }
    }
}
ge-0/0/10 {
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members all;
            }
        }
    }
}
ge-0/0/11 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members 2;
            }
        }
    }
}
ge-0/0/12 {
    unit 0 {
        family ethernet-switching {
            port-mode access;
            vlan {
                members CSC;
            }
        }
    }
}
ge-0/0/13 {
    unit 0 {
        family ethernet-switching {
            port-mode access;
            vlan {
```

```
                members PAYROLL;
            }
        }
    }
}
ge-0/0/14 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/15 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members [ 10 CSC ];
            }
        }
    }
}
ge-0/0/16 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/17 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/18 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/19 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/20 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/0/21 {
    unit 0 {
        family ethernet-switching;
    }
}
```

```
ge-0/0/22 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members REDCORE;
            }
        }
    }
}
ge-0/0/23 {
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members REDCORE;
            }
        }
    }
}
ge-0/1/0 {
    unit 0 {
        family ethernet-switching;
    }
}
xe-0/1/0 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/1/1 {
    unit 0 {
        family ethernet-switching;
    }
}
xe-0/1/1 {
    unit 0 {
        family ethernet-switching;
    }
}
ge-0/1/2 {
    unit 0 {
        family ethernet-switching;
    }
}
xe-0/1/2 {
    unit 0 {
        family ethernet-switching;
    }
}
```

```
ge-0/1/3 {
    unit 0 {
        family ethernet-switching;
    }
}
xe-0/1/3 {
    unit 0 {
        family ethernet-switching;
    }
}
ae2 {
    aggregated-ether-options {
        lacp {
            active;
        }
    }
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members all;
            }
        }
    }
}
vlan {
    unit 1;
    unit 2 {
        family inet {
            filter {
                input DENY_NETWORK;
            }
            address 10.157.100.2/25 {
                vrrp-group 2 {
                    virtual-address 10.157.100.1;
                    priority 200;
                    preempt;
                    accept-data;
                }
            }
        }
    }
    unit 3 {
        family inet {
            filter {
                input DENY_NETWORK;
            }
            address 10.157.100.130/25 {
                vrrp-group 3 {
```

```
                virtual-address 10.157.100.129;
                priority 100;
                preempt;
                accept-data;
            }
        }
    }
}
unit 4 {
    family inet {
        address 10.157.99.2/24 {
            vrrp-group 1 {
                virtual-address 10.157.99.1;
                priority 200;
                preempt;
                accept-data;
            }
        }
    }
}
unit 10 {
    family inet {
        address 10.157.12.2/24 {
            vrrp-group 10 {
                virtual-address 10.157.12.1;
                priority 200;
                preempt;
                accept-data;
            }
        }
    }
}
unit 11 {
    family inet {
        address 10.157.17.2/24 {
            vrrp-group 11 {
                virtual-address 10.157.17.1;
                priority 100;
                preempt;
                accept-data;
            }
        }
    }
}
unit 12 {
    family inet {
        address 10.157.30.2/24 {
            vrrp-group 12 {
                virtual-address 10.157.30.1;
```

```
                        priority 100;
                        preempt;
                        accept-data;
                    }
                }
            }
        }
        unit 14 {
            family inet {
                address 10.157.101.2/24 {
                    vrrp-group 14 {
                        virtual-address 10.157.101.1;
                        priority 200;
                        preempt;
                        accept-data;
                    }
                }
            }
        }
        unit 15 {
            family inet {
                address 10.157.13.2/24 {
                    vrrp-group 15 {
                        virtual-address 10.157.13.1;
                        priority 200;
                        preempt;
                        accept-data;
                    }
                }
            }
        }
        unit 100 {
            family inet {
                address 10.157.102.4/28;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 10.157.102.1;
    }
}
protocols {
    igmp-snooping {
        vlan all;
    }
    rstp;
    lldp {
```

```
        interface all;
    }
    lldp-med {
        interface all;
    }
}
firewall {
    family inet {
        filter DENY_NETWORK {
            term ACCESS_10.157.100.0/25 {
                from {
                    destination-address {
                        10.157.100.0/24;
                    }
                }
                then accept;
            }
            term NO_ACCESS_10.157.0.0/16 {
                from {
                    destination-address {
                        10.157.0.0/16;
                    }
                }
                then {
                    reject;
                }
            }
            term NO_ACCESS_172.18.16/24 {
                from {
                    destination-address {
                        172.18.16.0/24;
                    }
                }
                then {
                    reject;
                }
            }
            term ACCEPT_ALL {
                then accept;
            }
        }
        filter NO_HA {
            term WIFI_MOB {
                from {
                    source-address {
                        10.157.100.128/25;
                    }
                }
                then {
```

```
                    reject;
                }
            }
            term PERMANENT {
                from {
                    source-address {
                        10.157.15.0/24;
                    }
                }
                then {
                    reject;
                }
            }
            term ACCEPT_ALL {
                then accept;
            }
        }
    }
}
ethernet-switching-options {
    secure-access-port {
        vlan BPO-SALE-MARKETING {
            examine-dhcp;
        }
        vlan CSC {
            examine-dhcp;
        }
        vlan PAYROLL {
            examine-dhcp;
        }
        vlan PERMANENT-SELECCION-CONTROLLER {
            examine-dhcp;
        }
        vlan TELEFONIA {
            examine-dhcp;
        }
        vlan WIFI_INVITADOS {
            examine-dhcp;
        }
        vlan WIFI_MOBILE {
            examine-dhcp;
        }
    }
    storm-control {
        interface all;
    }
}
vlans {
    ADMON_NETWORK {
```

```
        description Vlan_Administrativa;
        vlan-id 4;
        l3-interface vlan.4;
    }
    BPO-SALE-MARKETING {
        vlan-id 12;
        l3-interface vlan.12;
    }
    CSC {
        vlan-id 10;
        l3-interface vlan.10;
    }
    PAYROLL {
        vlan-id 11;
        l3-interface vlan.11;
    }
    PERMANENT-SELECCION-CONTROLLER {
        vlan-id 15;
        l3-interface vlan.15;
    }
    REDCORE {
        description RED_ROUTER_SWCORE;
        vlan-id 100;
        l3-interface vlan.100;
    }
    TELEFONIA {
        vlan-id 14;
        l3-interface vlan.14;
    }
    WIFI_INVITADOS {
        description WIFI_DE_INVITADOS;
        vlan-id 2;
        l3-interface vlan.2;
    }
    WIFI_MOBILE {
        description WIFI_PARA_MOVILES;
        vlan-id 3;
        l3-interface vlan.3;
    }
}

{master:0}[edit]
root@SW1_CORE_73# show | display set
set version 12.3R6.6
set system host-name SW1_CORE_73
set system root-authentication encrypted-password
"$1$s.Kjf2Wt$xvof9bbxLT78hxqc/mito."
set system services ssh
set system services telnet
```

```
set system services web-management http
set system services dhcp name-server 172.18.16.140
set system services dhcp name-server 10.157.0.116
set system services dhcp pool 10.157.100.0/25 address-range low
10.157.100.6
set system services dhcp pool 10.157.100.0/25 address-range high
10.157.100.126
set system services dhcp pool 10.157.100.0/25 name-server 8.8.8.8
set system services dhcp pool 10.157.100.0/25 router 10.157.100.1
set system services dhcp pool 10.157.100.128/25 address-range low
10.157.100.134
set system services dhcp pool 10.157.100.128/25 address-range
high 10.157.100.254
set system services dhcp pool 10.157.100.128/25 name-server
8.8.8.8
set system services dhcp pool 10.157.100.128/25 router
10.157.100.129
set system services dhcp pool 10.157.12.0/24 address-range low
10.157.12.51
set system services dhcp pool 10.157.12.0/24 address-range high
10.157.12.254
set system services dhcp pool 10.157.12.0/24 name-server
172.18.16.140
set system services dhcp pool 10.157.12.0/24 name-server
10.157.0.116
set system services dhcp pool 10.157.12.0/24 router 10.157.12.1
set system services dhcp pool 10.157.17.0/24 address-range low
10.157.17.51
set system services dhcp pool 10.157.17.0/24 address-range high
10.157.17.254
set system services dhcp pool 10.157.17.0/24 router 10.157.17.1
set system services dhcp pool 10.157.101.0/24 address-range low
10.157.101.51
set system services dhcp pool 10.157.101.0/24 address-range high
10.157.101.254
set system services dhcp pool 10.157.101.0/24 router 10.157.101.1
set system services dhcp pool 10.157.13.0/24 address-range low
10.157.13.51
set system services dhcp pool 10.157.13.0/24 address-range high
10.157.13.254
set system services dhcp pool 10.157.13.0/24 router 10.157.13.1
set system services dhcp pool 10.157.30.0/24 address-range low
10.157.30.51
set system services dhcp pool 10.157.30.0/24 address-range high
10.157.30.254
set system services dhcp pool 10.157.30.0/24 router 10.157.30.1
set system syslog user * any emergency
set system syslog file messages any notice
set system syslog file messages authorization info
```

```
set system syslog file interactive-commands interactive-commands
any
set chassis aggregated-devices ethernet device-count 4
set chassis alarm management-ethernet link-down ignore
set interfaces ge-0/0/0 ether-options 802.3ad ae2
set interfaces ge-0/0/1 ether-options 802.3ad ae2
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-
mode trunk
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan
members all
set interfaces ge-0/0/3 unit 0 family ethernet-switching port-
mode trunk
set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan
members all
set interfaces ge-0/0/4 unit 0 family ethernet-switching port-
mode trunk
set interfaces ge-0/0/4 unit 0 family ethernet-switching vlan
members all
set interfaces ge-0/0/5 unit 0 family ethernet-switching port-
mode trunk
set interfaces ge-0/0/5 unit 0 family ethernet-switching vlan
members all
set interfaces ge-0/0/6 unit 0 family ethernet-switching port-
mode trunk
set interfaces ge-0/0/6 unit 0 family ethernet-switching vlan
members 2-4
set interfaces ge-0/0/7 unit 0 family ethernet-switching port-
mode trunk
set interfaces ge-0/0/7 unit 0 family ethernet-switching vlan
members all
set interfaces ge-0/0/8 unit 0 family ethernet-switching port-
mode trunk
set interfaces ge-0/0/8 unit 0 family ethernet-switching vlan
members all
set interfaces ge-0/0/9 unit 0 family ethernet-switching port-
mode trunk
set interfaces ge-0/0/9 unit 0 family ethernet-switching vlan
members all
set interfaces ge-0/0/10 unit 0 family ethernet-switching port-
mode trunk
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan
members all
set interfaces ge-0/0/11 unit 0 family ethernet-switching vlan
members 2
set interfaces ge-0/0/12 unit 0 family ethernet-switching port-
mode access
set interfaces ge-0/0/12 unit 0 family ethernet-switching vlan
members CSC
```

```
set interfaces ge-0/0/13 unit 0 family ethernet-switching port-
mode access
set interfaces ge-0/0/13 unit 0 family ethernet-switching vlan
members PAYROLL
set interfaces ge-0/0/14 unit 0 family ethernet-switching
set interfaces ge-0/0/15 unit 0 family ethernet-switching vlan
members 10
set interfaces ge-0/0/15 unit 0 family ethernet-switching vlan
members CSC
set interfaces ge-0/0/16 unit 0 family ethernet-switching
set interfaces ge-0/0/17 unit 0 family ethernet-switching
set interfaces ge-0/0/18 unit 0 family ethernet-switching
set interfaces ge-0/0/19 unit 0 family ethernet-switching
set interfaces ge-0/0/20 unit 0 family ethernet-switching
set interfaces ge-0/0/21 unit 0 family ethernet-switching
set interfaces ge-0/0/22 unit 0 family ethernet-switching vlan
members REDCORE
set interfaces ge-0/0/23 unit 0 family ethernet-switching port-
mode trunk
set interfaces ge-0/0/23 unit 0 family ethernet-switching vlan
members REDCORE
set interfaces ge-0/1/0 unit 0 family ethernet-switching
set interfaces xe-0/1/0 unit 0 family ethernet-switching
set interfaces ge-0/1/1 unit 0 family ethernet-switching
set interfaces xe-0/1/1 unit 0 family ethernet-switching
set interfaces ge-0/1/2 unit 0 family ethernet-switching
set interfaces xe-0/1/2 unit 0 family ethernet-switching
set interfaces ge-0/1/3 unit 0 family ethernet-switching
set interfaces xe-0/1/3 unit 0 family ethernet-switching
set interfaces ae2 aggregated-ether-options lacp active
set interfaces ae2 unit 0 family ethernet-switching port-mode
trunk
set interfaces ae2 unit 0 family ethernet-switching vlan members
all
set interfaces vlan unit 1
set interfaces vlan unit 2 family inet filter input DENY_NETWORK
set interfaces vlan unit 2 family inet address 10.157.100.2/25
vrrp-group 2 virtual-address 10.157.100.1
set interfaces vlan unit 2 family inet address 10.157.100.2/25
vrrp-group 2 priority 200
set interfaces vlan unit 2 family inet address 10.157.100.2/25
vrrp-group 2 preempt
set interfaces vlan unit 2 family inet address 10.157.100.2/25
vrrp-group 2 accept-data
set interfaces vlan unit 3 family inet filter input DENY_NETWORK
set interfaces vlan unit 3 family inet address 10.157.100.130/25
vrrp-group 3 virtual-address 10.157.100.129
set interfaces vlan unit 3 family inet address 10.157.100.130/25
vrrp-group 3 priority 100
```

```
set interfaces vlan unit 3 family inet address 10.157.100.130/25
vrrp-group 3 preempt
set interfaces vlan unit 3 family inet address 10.157.100.130/25
vrrp-group 3 accept-data
set interfaces vlan unit 4 family inet address 10.157.99.2/24
vrrp-group 1 virtual-address 10.157.99.1
set interfaces vlan unit 4 family inet address 10.157.99.2/24
vrrp-group 1 priority 200
set interfaces vlan unit 4 family inet address 10.157.99.2/24
vrrp-group 1 preempt
set interfaces vlan unit 4 family inet address 10.157.99.2/24
vrrp-group 1 accept-data
set interfaces vlan unit 10 family inet address 10.157.12.2/24
vrrp-group 10 virtual-address 10.157.12.1
set interfaces vlan unit 10 family inet address 10.157.12.2/24
vrrp-group 10 priority 200
set interfaces vlan unit 10 family inet address 10.157.12.2/24
vrrp-group 10 preempt
set interfaces vlan unit 10 family inet address 10.157.12.2/24
vrrp-group 10 accept-data
set interfaces vlan unit 11 family inet address 10.157.17.2/24
vrrp-group 11 virtual-address 10.157.17.1
set interfaces vlan unit 11 family inet address 10.157.17.2/24
vrrp-group 11 priority 100
set interfaces vlan unit 11 family inet address 10.157.17.2/24
vrrp-group 11 preempt
set interfaces vlan unit 11 family inet address 10.157.17.2/24
vrrp-group 11 accept-data
set interfaces vlan unit 12 family inet address 10.157.30.2/24
vrrp-group 12 virtual-address 10.157.30.1
set interfaces vlan unit 12 family inet address 10.157.30.2/24
vrrp-group 12 priority 100
set interfaces vlan unit 12 family inet address 10.157.30.2/24
vrrp-group 12 preempt
set interfaces vlan unit 12 family inet address 10.157.30.2/24
vrrp-group 12 accept-data
set interfaces vlan unit 14 family inet address 10.157.101.2/24
vrrp-group 14 virtual-address 10.157.101.1
set interfaces vlan unit 14 family inet address 10.157.101.2/24
vrrp-group 14 priority 200
set interfaces vlan unit 14 family inet address 10.157.101.2/24
vrrp-group 14 preempt
set interfaces vlan unit 14 family inet address 10.157.101.2/24
vrrp-group 14 accept-data
set interfaces vlan unit 15 family inet address 10.157.13.2/24
vrrp-group 15 virtual-address 10.157.13.1
set interfaces vlan unit 15 family inet address 10.157.13.2/24
vrrp-group 15 priority 200
```

```
set interfaces vlan unit 15 family inet address 10.157.13.2/24
vrrp-group 15 preempt
set interfaces vlan unit 15 family inet address 10.157.13.2/24
vrrp-group 15 accept-data
set interfaces vlan unit 100 family inet address 10.157.102.4/28
set routing-options static route 0.0.0.0/0 next-hop 10.157.102.1
set protocols igmp-snooping vlan all
set protocols rstp
set protocols lldp interface all
set protocols lldp-med interface all
set firewall family inet filter DENY_NETWORK term
ACCESS_10.157.100.0/25 from destination-address 10.157.100.0/24
set firewall family inet filter DENY_NETWORK term
ACCESS_10.157.100.0/25 then accept
set firewall family inet filter DENY_NETWORK term
NO_ACCESS_10.157.0.0/16 from destination-address 10.157.0.0/16
set firewall family inet filter DENY_NETWORK term
NO_ACCESS_10.157.0.0/16 then reject
set firewall family inet filter DENY_NETWORK term
NO_ACCESS_172.18.16/24 from destination-address 172.18.16.0/24
set firewall family inet filter DENY_NETWORK term
NO_ACCESS_172.18.16/24 then reject
set firewall family inet filter DENY_NETWORK term ACCEPT_ALL then
accept
set firewall family inet filter NO_HA term WIFI_MOB from source-
address 10.157.100.128/25
set firewall family inet filter NO_HA term WIFI_MOB then reject
set firewall family inet filter NO_HA term PERMANENT from source-
address 10.157.15.0/24
set firewall family inet filter NO_HA term PERMANENT then reject
set firewall family inet filter NO_HA term ACCEPT_ALL then accept
set ethernet-switching-options secure-access-port vlan BPO-SALE-
MARKETING examine-dhcp
set ethernet-switching-options secure-access-port vlan CSC
examine-dhcp
set ethernet-switching-options secure-access-port vlan PAYROLL
examine-dhcp
set ethernet-switching-options secure-access-port vlan PERMANENT-
SELECCION-CONTROLLER examine-dhcp
set ethernet-switching-options secure-access-port vlan TELEFONIA
examine-dhcp
set ethernet-switching-options secure-access-port vlan
WIFI_INVITADOS examine-dhcp
set ethernet-switching-options secure-access-port vlan
WIFI_MOBILE examine-dhcp
set ethernet-switching-options storm-control interface all
set vlans ADMON_NETWORK description Vlan_Administrativa
set vlans ADMON_NETWORK vlan-id 4
set vlans ADMON_NETWORK l3-interface vlan.4
```

```
set vlans BPO-SALE-MARKETING vlan-id 12
set vlans BPO-SALE-MARKETING l3-interface vlan.12
set vlans CSC vlan-id 10
set vlans CSC l3-interface vlan.10
set vlans PAYROLL vlan-id 11
set vlans PAYROLL l3-interface vlan.11
set vlans PERMANENT-SELECCION-CONTROLLER vlan-id 15
set vlans PERMANENT-SELECCION-CONTROLLER l3-interface vlan.15
set vlans REDCORE description RED_ROUTER_SWCORE
set vlans REDCORE vlan-id 100
set vlans REDCORE l3-interface vlan.100
set vlans TELEFONIA vlan-id 14
set vlans TELEFONIA l3-interface vlan.14
set vlans WIFI_INVITADOS description WIFI_DE_INVITADOS
set vlans WIFI_INVITADOS vlan-id 2
set vlans WIFI_INVITADOS l3-interface vlan.2
set vlans WIFI_MOBILE description WIFI_PARA_MOVILES
set vlans WIFI_MOBILE vlan-id 3
set vlans WIFI_MOBILE l3-interface vlan.3

{master:0}[edit]
root@SW1_CORE_73# show | compare

{master:0}[edit]
root@SW1_CORE_73# commit
configuration check succeeds
commit complete

{master:0}[edit]
```

14.2 SHOW RUN ROUTER PRINCIPAL

```
ADECCO_CL73_PPAL#sh run
Building configuration...


Current configuration : 12038 bytes
!
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ADECCO_CL73_PPAL
!
boot-start-marker
boot-end-marker
!
```

```
logging buffered 6000
enable password 7 1403170709072526
!
aaa new-model
!
!
aaa authentication login default group radius local
aaa authorization console
aaa authorization exec default group radius if-authenticated
aaa accounting exec default
 action-type start-stop
 group radius
!
!
!
!
!
!
aaa session-id common
clock timezone COL -5
!
no ipv6 cef
ip source-route
ip cef
!
!
!
!
ip domain name telecom.esp
multilink bundle-name authenticated
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-3602065217
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3602065217
 revocation-check none
 rsakeypair TP-self-signed-3602065217
!
!
crypto pki certificate chain TP-self-signed-3602065217
 certificate self-signed 01
  3082024F 308201B8 A0030201 02020101 300D0609 2A864886 F70D0101
04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
```

```
  69666963 6174652D 33363032 30363532 3137301E 170D3131 30323232
31373031
  34355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33
36303230
  36353231 3730819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281
  8100B66D 8B85F70F 7A992BD6 45492740 D7FEED68 EFB61373 0A6F3342
DA108EA3
  1DDF45F5 16B0C224 32E0F4FB 402A25D2 60E1C021 48F9D1B5 1D3875D4
DA58A1F5
  E0F6A6BE 209C7117 DDE46D69 2512A4A5 DCE688DA BB588E12 12E214B7
50ED22A6
  8BCA93B5 8B16E55B BF474449 C3F86E1F 62ADD159 EFBC6413 6708DF47
2F1CE52E
  77B90203 010001A3 77307530 0F060355 1D130101 FF040530 030101FF
30220603
  551D1104 1B301982 17796F75 726E616D 652E796F 7572646F 6D61696E
2E636F6D
  301F0603 551D2304 18301680 14F29D78 9F561757 269AC67B 0D83B6BF
1633FD7B
  19301D06 03551D0E 04160414 F29D789F 56175726 9AC67B0D 83B6BF16
33FD7B19
  300D0609 2A864886 F70D0101 04050003 81810022 DA536436 3EE687C4
D025CDDA
  CD9CB235 28735BB0 1AD147E9 D1A1FE76 6D2702C0 A1757742 EC8ADC96
9371C1A7
  C2418ED5 AA75C463 E46D8F97 D953B043 F6C3480D D4CDB3EF D07EC698
380D8B1A
  4EFB0CB8 3F1DD118 E2168769 FB066E25 7A20F13D F10AABE1 5F340AC0
AC962947
  32C601CD 7EB9545C 7AF56774 C0250590 A88035
        quit
voice-card 0
!
!
!
!
!
!
license udi pid CISCO2901/K9 sn FTX150901KR
hw-module pvdm 0/0
!
!
!
archive
 log config
  hidekeys
```

```
username telecom privilege 15 password 7
0010400A575D5B085E22184D5914
username adecco privilege 7 view adecco secret 5
$1$raCL$8zA6F6FvAQPJf8IY5Ki7J0
!
redundancy
!
!
ip ssh version 2
!
track 1 ip sla 1 reachability
!
track 200 ip sla 200 reachability
!
class-map match-all Marc-Voz
 match access-group name VOZ
class-map match-all voice
 match  dscp ef
!
!
policy-map ip-wan-qos
 class voice
    priority 2048
   police cir 2048000
 class class-default
    bandwidth 18432
policy-map marcacion-dscp-voz
 class class-default
  set dscp default
policy-map shape-20480K
 class class-default
    shape peak 20480000
  service-policy ip-wan-qos
policy-map marcacion-dscp
 class class-default
  set dscp default
!
!
!
!
!
interface Loopback0
 ip address 10.10.2.19 255.255.255.255
 h323-gateway voip bind srcaddr 10.10.2.19
 service-policy input marcacion-dscp-voz
!
interface Loopback500
 description GESTION_RADIUS_SIGRES_CORPORATIVO
 ip address 172.19.100.182 255.255.255.255
```

```
!
interface GigabitEthernet0/0
 description WAN_31000 PTO 4/1/23
 no ip address
 load-interval 30
 duplex auto
 speed auto
 service-policy output ip-wan-qos
!
interface GigabitEthernet0/0.1100
 bandwidth 20480
 encapsulation dot1Q 1100
 ip address 10.10.1.78 255.255.255.252
 ip flow ingress
 ip flow egress
!
interface GigabitEthernet0/1
 description LAN
 no ip address
 load-interval 30
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.100
 description LANtoSW1
 encapsulation dot1Q 100
 ip address 10.157.102.7 255.255.255.240
 ip flow ingress
 ip flow egress
 standby 1 ip 10.157.102.1
 standby 1 priority 110
 standby 1 preempt delay minimum 40
 standby 1 track 1 decrement 30
 standby 2 ip 10.157.102.2
 standby 2 priority 95
 standby 2 preempt
!
router bgp 65300
 no synchronization
 bgp log-neighbor-changes
 network 10.10.2.19 mask 255.255.255.255
 network 10.157.102.0 mask 255.255.255.240
 network 172.19.100.182 mask 255.255.255.255
 redistribute static
 neighbor 10.10.1.77 remote-as 3816
 neighbor 10.10.1.77 version 4
 neighbor 10.10.1.77 route-map balance_outgoing out
 no auto-summary
!
```

```
ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip flow-cache timeout active 1
ip flow-export source Loopback500
ip flow-export version 5
ip flow-export destination 172.22.65.34 2055
ip flow-top-talkers
 top 40
 sort-by bytes
!
ip route 0.0.0.0 0.0.0.0 172.18.17.3 200
ip route 10.157.12.0 255.255.255.0 10.157.102.4
ip route 10.157.13.0 255.255.255.0 10.157.102.4
ip route 10.157.17.0 255.255.255.0 10.157.102.4
ip route 10.157.30.0 255.255.255.0 10.157.102.4
ip route 10.157.99.0 255.255.255.0 10.157.102.4
ip route 10.157.100.0 255.255.255.128 10.157.102.4
ip route 10.157.100.128 255.255.255.128 10.157.102.4
!
!
ip prefix-list redes_backup seq 5 permit 10.157.30.0/24
ip prefix-list redes_backup seq 10 permit 10.157.17.0/24
ip prefix-list redes_backup seq 15 permit 10.157.100.128/25
ip radius source-interface Loopback500
ip sla 1
 icmp-echo 10.10.1.77 source-ip 10.10.1.78
 frequency 20
ip sla schedule 1 life forever start-time now
ip sla 200
 icmp-echo 10.10.1.77 source-ip 10.10.1.78
 frequency 20
ip sla schedule 200 life forever start-time now
access-list 10 permit 172.19.100.179
access-list 20 remark -- GESTION_SIGRES --
access-list 20 permit 172.28.1.115
access-list 20 permit 172.28.1.127
access-list 20 permit 172.28.1.128 0.0.0.31
access-list 20 remark --------------------
access-list 20 permit 172.22.65.32 0.0.0.7
access-list 23 permit 10.10.10.0 0.0.0.7
access-list 30 remark SOLAR_WINDS
access-list 30 permit 172.22.65.34
access-list 30 permit 172.22.65.36
access-list 30 permit 172.22.65.32 0.0.0.31
```

```
access-list 100 permit ip 10.157.17.0 0.0.0.127 any
access-list 100 permit ip host 10.10.2.19 any
access-list 100 permit ip host 172.19.100.182 any
access-list 110 permit ip 10.157.17.128 0.0.0.127 any
!
route-map balance_outgoing permit 10
 match ip address prefix-list redes_backup
 set as-path prepend 65300 65300 65300
!
route-map balance_outgoing permit 20
!
route-map OUT permit 10
 match ip address 110
 set as-path prepend 65300
!
route-map OUT permit 20
 match ip address 100
 set as-path prepend 65300 65300 65300
!
route-map REDES_LAN permit 0
 match tag 10
!
!
snmp-server community totem_ro RW 20
snmp-server community movistar_Mas RO 30
radius-server host 172.29.23.2 auth-port 1812 acct-port 1813 key
7 113D4A2944345B2255097F6079
radius-server host 172.29.23.1 auth-port 1812 acct-port 1813 key
7 113D4A2944345B2255097F6079
!
control-plane
!
!
voice-port 0/0/0
 cptone CO
!
voice-port 0/0/1
 cptone CO
!
voice-port 0/1/0
 cptone CO
!
voice-port 0/1/1
 cptone CO
!
voice-port 0/2/0
 cptone CO
!
voice-port 0/2/1
```

```
 cptone CO
!
voice-port 0/3/0
 cptone CO
!
voice-port 0/3/1
 cptone CO
!
!
mgcp fax t38 ecm
!
!
dial-peer voice 3 voip
 description DIAL-PEER-HACIA-CARTAGENA
 destination-pattern 51
 session target ipv4:10.10.2.4
 codec g729r8 bytes 30
 ip qos dscp ef signaling
 no vad
!
dial-peer voice 4 voip
 description DIAL-PEER-HACIA-MEDELLIN
 destination-pattern 40
 session target ipv4:10.10.2.5
 codec g729r8 bytes 30
 ip qos dscp ef signaling
 no vad
!
dial-peer voice 5 voip
 description DIAL-PEER-HACIA-MANIZALES
 destination-pattern 61
 session target ipv4:10.10.2.6
 codec g729r8 bytes 30
 ip qos dscp ef signaling
 no vad
!
dial-peer voice 6 voip
 description DIAL-PEER-HACIA-PALMIRA
 destination-pattern 21
 session target ipv4:10.10.2.7
 codec g729r8 bytes 30
 ip qos dscp ef signaling
 no vad
!
dial-peer voice 7 voip
 description DIAL-PEER-HACIA-PEREIRA
 destination-pattern 62
 session target ipv4:10.10.2.8
 codec g729r8 bytes 30
```

```
 ip qos dscp ef signaling
 no vad
!
dial-peer voice 8 voip
 description DIAL-PEER-HACIA-RIONEGRO
 destination-pattern 41
 session target ipv4:10.10.2.9
 codec g729r8 bytes 30
 ip qos dscp ef signaling
!
dial-peer voice 9 voip
 description DIAL-PEER-HACIA-CALI-INDUSTRIAL
 destination-pattern 20
 session target ipv4:10.10.2.10
 codec g729r8 bytes 30
 ip qos dscp ef signaling
 no vad
!
dial-peer voice 11 voip
 description DIAL-PEER-HACIA-BARRANQUILLA
 destination-pattern 52
 session target ipv4:10.10.2.12
 codec g729r8 bytes 30
 ip qos dscp ef signaling
 no vad
!
dial-peer voice 13 voip
 description DIAL-PEER-HACIA-BOGOTA-CALLE70
 destination-pattern 13
 session target ipv4:10.10.2.15
 codec g729r8 bytes 30
 ip qos dscp ef signaling
 no vad
!
dial-peer voice 70 voip
 description DIAL-PEER-HACIA-BUCARAMANGA
 destination-pattern 70
 session target ipv4:10.10.2.2
 codec g729r8 bytes 30
 ip qos dscp ef signaling
!
dial-peer voice 1 voip
 description DIAL-PEER-HACIA-BOGOTA
 destination-pattern 10
 session target ipv4:10.10.2.1
 ip qos dscp ef signaling
 no vad
!
dial-peer voice 16 voip
```

```
 description DIAL-PEER-HACIA-BOGOTA-Cll98
 destination-pattern 11
 session target ipv4:10.10.2.3
 codec g729r8 bytes 30
 ip qos dscp ef signaling
!
dial-peer voice 40 pots
 preference 1
 destination-pattern 81
 port 0/0/0
!
dial-peer voice 42 pots
 preference 3
 destination-pattern 81
 port 0/1/0
!
dial-peer voice 43 pots
 preference 4
 destination-pattern 81
 port 0/1/1
!
dial-peer voice 45 pots
 preference 2
 destination-pattern 84
 port 0/2/1
!
dial-peer voice 46 pots
 preference 3
 destination-pattern 84
 port 0/3/0
!
dial-peer voice 2 voip
 description DIAL-PEER-HACIA-BOGOTA-UNICENTRO
 destination-pattern 11
 session target ipv4:10.10.2.3
 codec g729r8 bytes 30
 ip qos dscp ef signaling
 no vad
!
dial-peer voice 14 voip
 description DIAL-PEER-HACIA-CRA-7-CON-55
 destination-pattern 80
 session target ipv4:10.10.2.17
 codec g729r8 bytes 30
 ip qos dscp ef signaling
!
dial-peer voice 15 voip
 description g729r8 bytes 30
 ip qos dscp ef signaling
```

```
!
dial-peer voice 18 voip
 destination-pattern 82
 session target ipv4:10.10.2.20
 codec g729r8 bytes 30
 ip qos dscp ef signaling
!
dial-peer voice 41 pots
 preference 2
 destination-pattern 81
 port 0/0/1
!
dial-peer voice 44 pots
 preference 1
 destination-pattern 84
 port 0/2/0
!
dial-peer voice 47 pots
 preference 4
 destination-pattern 84
 port 0/3/1
!
dial-peer voice 10 voip
 description DIAL-PEER-HACIA-CALI-NORTE
 destination-pattern 22
 session target ipv4:10.10.2.11
 codec g729r8 bytes 30
 ip qos dscp ef signaling
 no vad
!
dial-peer voice 91 voip
 description ADECCO_IBAGUE_KR5
 destination-pattern 91
 session target ipv4:10.10.2.100
 codec g729r8 bytes 30
 ip qos dscp ef signaling
!
dial-peer voice 93 voip
 description ADECCO_EL_LAGO
 destination-pattern 92
 session target ipv4:10.10.2.25
 codec g729r8 bytes 30
 ip qos dscp ef signaling
!
dial-peer voice 94 voip
 description DIAL-PEER-HACIA-BARRANCABERMEJA
 destination-pattern 94
 session target ipv4:10.10.2.150
 codec g729r8 bytes 30
```

```
 ip qos dscp ef signaling
 no vad
!
!
!
!
gatekeeper
 shutdown
!
privilege exec level 7 show startup-config
privilege exec level 7 show
banner motd ^CCC

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXX

                          !!! ATENCION !!!

USTED ESTA CONECTADO A UN EQUIPO PROPIEDAD DE TELEFONICA-TELECOM,
LOS

CAMBIOS Y ACCESO AL MISMO ESTA RESTRINGIDO SOLO PERSONAL
AUTORIZADO.
                          !!! GRACIAS !!!

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXX
^C
!
line con 0
line aux 0
 transport preferred none
 transport output telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 privilege level 15
 password 7 120D001B17080309
 transport input telnet ssh
!
scheduler allocate 20000 1000
ntp access-group peer 10
ntp server 172.19.100.179
end

ADECCO_CL73_PPAL#
```