4 Informe de Actividades Profesionales

Desde Julio del 2009, me desempeño como Network Consulting Engineer (NCE) de la empresa Cisco Systems. En dicha posición, mis actividades son muy variadas, demandantes, y esenciales para la empresa y para los clientes. Las actividades que desarrollo de manera cotidiana forman todas parte del servicio conocido como Network Optimization Service.

A continuación se presentará un resumen del servicio de Network Optimization Service, así como los detalles de las dos actividades que elegí para profundizar sobre ellas: la Auditoría de Red (Network Audit) para una empresa petrolera española, y la elaboración de un Reporte de Mejores Prácticas para una red de Servicios Administrados en México.

4.1 Antecedentes - Network Optimization Service (NOS) de Cisco Systems

El Servicio de Optimización de Red de Cisco Systems toma un enfoque global para fortalecer la infraestructura de red de un cliente en aspectos como: Seguridad, Wireless, Routing & Switching, Data Center y Comunicaciones Unificadas.

El equipo de expertos de Cisco (Network Consulting Engineers, Systems Engineers, Systems Architects, entre otros) trabaja como complemento al personal del cliente para ayudar en:

- Fortalecimiento de la infraestructura de red
- Adopción de nuevas opciones de seguridad e integrarlas de forma natural en la red del cliente
- Mejorar la disponibilidad y el soporte para dispositivos de red inalámbricos, dado el gran crecimiento que estas tecnologías han tenido
- Preparar el ambiente de red para soportar nuevas tecnologías y aplicaciones y ayudar en asegurar la alineación de los requerimientos técnicos y de negocio de cada cliente.

Para ayudar a cumplir esas metas, el servicio NOS combina la evaluación de la red del cliente, soporte y conocimiento de la red en un solo paquete integrado, diseñado para transformar la red del cliente en el activo generador de ingresos que se espera. El servicio se enfoca en la optimización de la red, de las siguientes 3 formas:

- **Preparar la Red**: la red del cliente se evalúa para ayudar así a mejorar el desempeño y preparar la infraestructura para futuros cambios.

- **Mejorar la Red**: El soporte de la red del cliente hace la red más resistente, estable y predecible.

- **Hacer Más Inteligente a la Red**: el conocimiento de la red ayuda a que el propio equipo de expertos del cliente aumente su auto-suficiencia a través de la compartición del conocimiento y prácticas de vanguardia.

El Servicio NOS incluye una serie de entregables y actividades con beneficios muy importantes, entre las cuales se encuentran las siguientes

Actividades y Entregables	Beneficios para el cliente

• **Auditoría de Tecnología o Protocolo**: Se analizan los KPIs[9] dispositivos de red, relevantes al inventario de Hardware, estabilidad, desempeño, configuración y fallas. Al final se emite un reporte con las recomendaciones basadas en mejores prácticas. • **Reporte de Fin de Soporte y Fin de Vida de Hardware y Software**: muestra información personalizada acerca de las fechas en que los diferentes productos de HW y SW de Cisco alcanzarán su fin de soporte y fin de vida, para poder realizar una planeación adecuada de la renovación y minimizar cualquier posible riesgo a la inversión. Al final se entrega un reporte con los hallazgos y recomendaciones.	Los reportes, auditorías y recomendaciones de soporte de Hardware ayudan al cliente a: • Mejorar la visibilidad de los riesgos de posibles accesos no controlados a la red, mediante la identificación de equipos fuera de gestión. • Identificar proactivamente problemas que pudieran afectar el desempeño y la estabilidad a través de la recolección de datos y análisis de tendencias. • Mejorar el desempeño y la estabilidad de los equipos de red mediante la identificación de tendencias y proveyendo recomendaciones para modificar diferentes atributos en el equipo. • Identificar problemas con el potencial de afectar los dispositivos de la red. • Planear y administra más efectivamente la estandarización de equipos mediante la notificar acerca de fechas límite relativas al soporte de HW y SW de equipos en la red.
• **Reportes de Mejores Prácticas de Configuración:** Se analizan las configuraciones de todos los dispositivos de la red, comparándolas con una base de datos de las mejores prácticas de configuración para cada tecnología o protocolos, para así poder identificar configuraciones no recomendadas. Al final se entrega un reporte con las recomendaciones pertinentes. • **Reporte Personalizado de Configuración:** A diferencia del reporte anterior, el Reporte Personalizado se apoya en plantillas específicas para la implementación que de cada tecnología realiza el cliente. Así, este Reporte identifica desviaciones de los estándares que el cliente ha definido, para poder corregirlos. Al final, se entrega un Reporte con los hallazgos. • **Reporte de Recomendación Proactiva de Software**: consiste en una recomendación del SW que debe usar el cliente en sus equipos para cumplir con sus necesidades de negocio.	El soporte de SW y Reportes de Análisis de Configuración ayudan al cliente a: ● Mejorar la seguridad y la resistencia de la red al notificar sobre dispositivos y versiones de SW que están afectados por problemas conocidos y proveer recomendaciones para mitigar el riesgo. ● Mejorar el desempeño, confiabilidad y funcionalidad de la red al proveer la información necesaria para instalar el SW correcto para cumplir las necesidades de negocio. ● Mejorar la consistencia y estandarización de las configuraciones mediante recomendaciones para modificar atributos de los elementos de red.
• **Revisión de Diseño:** Cisco ayuda al cliente en la revisión de sus prioridades de diseño, metas y requerimientos para modificar la infraestructura y diseño de red existentes,	La Revisión de Diseño ayuda al cliente a: ● Mejorar la estabilidad y disponibilidad de la red apoyando al cliente en la evolución y

[9] **KPI: Key Perfomance Indicators**: Indicadores críticos del desempeño de un equipo de red en diferentes áreas clave

proveyendo recomendaciones sustentadas por un grupo de expertos en diseño de redes. Las Revisiones de Diseño pueden realizarse en dos modalidades: Diseño de Bajo Nivel (profundamente detallado) y Diseño de Alto Nivel (un enfoque mucho menos detallado).	validación de sus estándares de diseño. ● Impulsar la predictibilidad guiando al cliente para realizar ajustes finos en los parámetros de los equipos y protocolos, ajustándose con las metas de diseño establecidas. ● Responder de manera efectiva a problemas que puedan surgir cuando se realizan cambios a la red. ● Guiar al cliente en la implementación de los nodos que componen su red, ya sea en implementaciones nuevas o sustituciones de equipo, para así reducir el riesgo de contingencias durante la implementación.

Para este Informe de Actividades Profesionales, me enfocaré en los siguientes entregables:

- Auditoría de Tecnología realizada para una compañía petrolera basada en España
- Diseño para la Migración de Routers y Activación del Servicio de WCCP en el Centro de Datos de una Entidad de Recaudación de Impuestos

Las siguientes secciones presentarán el desarrollo de cada uno de esos proyectos, bajo la siguiente estructura:

- Antecedentes del Tema
- Definición del Problema
- Análisis y Metodología Empleada
- Participación Profesional
- Resultados y Aportaciones

4.2 Auditoría de Red para una Empresa Petrolera Española

4.2.1 Antecedentes del Tema

Las Auditorías de Red son un entregable crítico del Servicio de Optimización de Red. Las auditorías son diseñadas para Proveedores de Servicios y Empresas de tamaño variado, y proporcionan una valoración exhaustiva de la salud de la red del cliente al examinar temas como Fallas, Capacidad, Configuración Desempeño, Seguridad y Diseño. En resumen, permiten obtener una acertada imagen del estado del desempeño actual de una red, y sus resultados son el medio con el cual se inician los procesos de optimización de una red.

Las auditorías son críticas porque al realizarse de manera proactiva permiten identificar áreas de riesgo y proporcionan recomendaciones para realizar cambios en los dispositivos, servicios y protocolos; cambios que conducen a una mayor disponibilidad de red y una confiabilidad mejorada. Son el mecanismo fundamental para obtener una línea base sobre la cual se medirá el desempeño de una red. Mediante la implementación de las recomendaciones que arroja una Auditoría de Red, los clientes reducen parámetros como el Mean Time To Repair (MTRR) en caso de fallas de HW, así como la ocurrencia de fallas de configuración; logran además el estar listos para la implementación de nuevos servicios incluso cuando se cuenta con restricciones presupuestarias, tan comunes el día de hoy.

Pueden realizarse Auditorías de Red de varias tecnologías, algunas de ellas son:

- IP/MPLS
- Routing y LAN Switching
- Carrier Ethernet
- IP Video

También se cuenta con una combinación de las anteriores, para cubrir las necesidades específicas del cliente. Se le conoce como Auditoría Personalizada (Custom Audit) y es la que se explicará en este documento

4.2.2 Definición del problema

Una empresa petrolera española, con presencia en más de 30 países y con más de 37000 empleados a nivel mundial, contrató el servicio de NOS recientemente en España, para que Cisco colaborara en la Optimización de sus servicios de red.

Como primer paso, fue necesario el obtener la mayor cantidad de información de la red, en particular de uno de sus sitios: un Centro de Datos ubicado en Madrid. Esto debido a que el sitio es crítico para la operación de la empresa y tenía la más alta prioridad para el proceso de Optimización, debido a fallas que se habían reportado.

Para profundizar en el conocimiento de la red, en reuniones con el cliente se determinó que la primer actividad a realizar sería la entrega de todo el conjunto de reportes descritos en la sección 4.1. En particular, el entregable que otorgaría mayor valor en cuanto a la cantidad de información que arroja es la Auditoría de Red, así que éste sería el prioritario.

Todo el proceso anterior fue liderado por el equipo de Servicios Avanzados de Cisco en España. Sin embargo, poco después del inicio del proyecto, debido a circunstancias imprevistas, se llegó a la conclusión de que se requería de apoyo adicional de otras áreas para llevar a buen término dicho proyecto.

En este punto es cuando el área a la que pertenezco fue requerida para tomar el liderazgo del proyecto. Las razones para ello fueron:

- El reconocimiento a nivel Latinoamérica de la experiencia, nivel de conocimientos y calidad del trabajo del grupo
- La posibilidad de que los documentos se elaboraran totalmente en español: el grupo al que pertenezco es el único dentro de todo Cisco que cuenta con la capacidad de realizar este tipo de documentos 100% en español.

A continuación se presentará la Metodología para una Auditoría de Red.

4.2.3 Análisis y Metodología para una Auditoría de Red

El primer paso para poder realizar casi todos los entregables de NOS (y por supuesto, la Auditoría de Red) consiste en la instalación de un dispositivo que recolecta toda la información necesaria de la red del cliente. Dicho dispositivo se conoce como Cisco Network Collector[10]

4.2.3.1 Recolección de la Información: Cisco Network Collector

CNC es una herramienta automatizada de descubrimiento de equipos de red e inventario de los mismos. CNC hace un seguimiento de todos los elementos de red del cliente. Para definir qué equipos constituyen la red del cliente, al CNC se le carga una lista de los mismos en un archivo semilla (*seed file*).

Los datos en forma cruda son analizados usando una base de datos de Capital Intelectual basado en Reglas[11]. Los datos analizados se emplean como base para la generación de casi todos los entregables del Servicio de NOS.

CNC no es una herramienta de monitoreo de red, su función es la recolección de datos, no el monitoreo en tiempo real. En lo que respecta a la seguridad de los datos del cliente, los datos son recolectados y transportados de forma segura a servidores dentro de la infraestructura de Cisco, usando como transporte HTTPS/SSL con el estándar de encripción AES-128. Información sensible como los passwords de los equipos son removidos previamente al envío de los datos.
La siguiente figura muestra cómo se realiza la recolección de datos de CNC y el análisis de los mismos de forma esquemática.

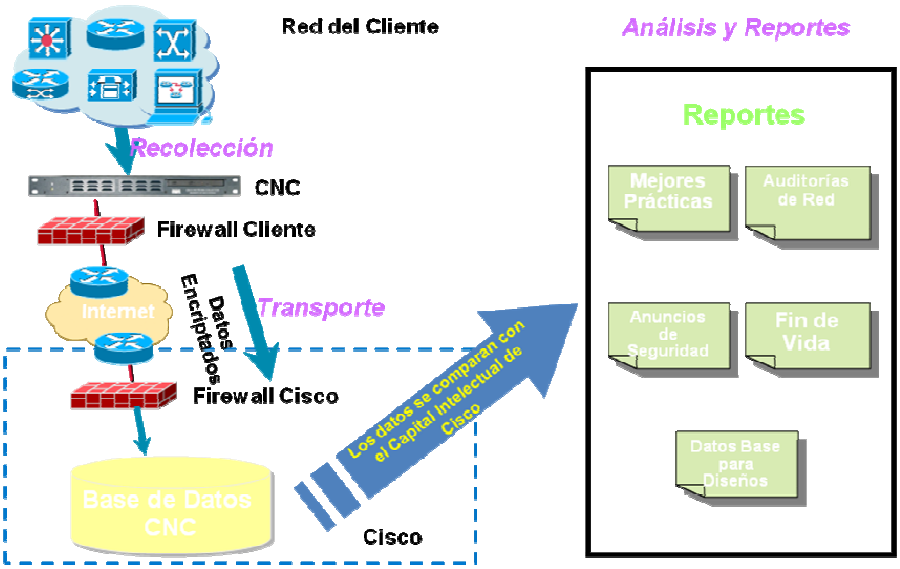

Figura 16. Arquitectura de operación de Cisco Network Collector

La instalación la realiza un NCE en estrecha colaboración con el cliente. Para el caso de la Auditoría para la Compañía Petrolera Española, esta actividad fue realizada por NCEs de España.

[11] Los detalles del Capital Intelectual Basado en Reglas son datos confidenciales de Cisco y por tanto se omiten.

En cuanto a los flujos de comunicación necesarios, CNC requiere comunicarse vía Telnet, Ping y SNMP con todos los equipos que tenga en su *seed file*. Además, requiere tener una salida a Internet para poder alcanzar al servidor de base de datos de CNC instalado en Cisco y realizar el envío de los datos para su posterior análisis.

4.2.3.2 Verificación de la Integridad de la Información para la Auditoría

Una vez que se ha logrado la comunicación entre el CNC y todos los dispositivos de la red del cliente, se realiza la recolección de la información y el envío de la misma a la base de datos de CNC en Cisco. El tiempo de recolección de datos es variable y puede ser de 1 a 7 días.

Cuando un cliente solicita una Auditoría de Red, el NCE verifica mediante una herramienta interna de Cisco (vía web) que:

- Se cuente con datos de todos los dispositivos: así se asegura que la Auditoría abarcará toda la red
- Los datos no tengan más de 36 horas de antigüedad: para que la información sea lo más actual posible

Estas dos condiciones, así como el análisis posterior de la información aseguran que la Auditoría será exitosa.

4.2.3.3 Generación de la Auditoría

Una vez constatado que la Auditoría Personalizada abarcará los elementos deseados, el NCE comienza la generación de la misma. Los pasos son:

1. El NCE emplea una herramienta web de Cisco (propietaria y confidencial) para generar solicitar la generación de la Auditoría
    a. Dado que se trata de una Auditoría Personalizada, el NCE selecciona las tablas y KPIs de interés (previamente definidos con el cliente) que serán incluidos en la auditoría
2. Se define el tiempo de recolección de datos para la Auditoría (desde 1 hasta 7 días).
3. El CNC comienza la recolección de datos de todos los dispositivos usando SNMP y conectándose a los equipos vía SSH para ejecutar comandos de visualización.
4. Los datos se envían a la base de datos de CNC como se explicó en la sección 4.2.3.1
5. Comienza el análisis de datos con base en el Capital Intelectual Basado en Reglas desarrollado por Cisco. Este análisis se realiza de forma automática
6. Una vez terminado el análisis automático, el NCE recibe los documentos de la Auditoría

Hasta este punto, la Auditoría Personalizada podría ser entregada al cliente. Sin embargo, para el caso de la Compañía Petrolera Española, se requería que la Auditoría Personalizada fuera entregada con un amplio análisis y ejemplos para cada excepción que se encuentre. De esta manera, la Auditoría se personaliza aún más.

4.2.3.4 Contenido de la Auditoría Personalizada

El contenido de una Auditoría Personalizada es variable, y su alcance se define en conjunto con el cliente y el NCE.

La Auditoría proporciona un análisis en profundidad de fallas, configuración, capacidad y desempeño y muestra el análisis en múltiples niveles de reportes. Comprende un número variable de tablas con más de 400 KPIs. Los datos se organizan en resultados resumidos por nivel los cuales tienen un código de color diferente para una fácil identificación de recomendaciones que requieren una respuesta o acción urgente. Los resultados se agrupan a nivel de familia de dispositivos, para facilitar la comparación de nodos uno contra otro. Para cada nodo se muestra también un reporte detallado. El análisis exhaustivo y en profundidad permite que el personal de las áreas de Tecnologías de la Información del cliente comprenda la salud general de su red.

Entre los KPIs más importantes se encuentran:

- Alarmas de HW
- % de uso de CPU
- % de uso de memoria
- % de memoria fragmentada
- % de utilización de enlaces
- Tipos de errores en enlaces
- % de fallas en enlaces (cualquier tipo de enlace L2)
- Errores de configuración en enrutamiento: OSPF, EIGRP, BGP
- Errores de configuración en LAN switching
- Errores de Alta Disponibilidad (tanto de equipo como de protocolo)

La Auditoría muestra además una breve explicación de cada uno de los conceptos. Sin embargo, es importante tener en mente que no todos los clientes cuentan con el nivel de conocimientos necesarios para comprenderlos, como es el caso de la Compañía Petrolera Española. Este factor fue definitivo para la metodología seguida para la elaboración de esta Auditoría

La Auditoría no es un solo archivo, está compuesta por varios archivos, a saber:

- **Un archivo resumen**: es el documento que se entrega al cliente. Como su nombre lo indica, resume los resultados individuales de cada nodo, en un documento más manejable
- **Reportes detallados para cada nodo:** cada archivo contiene un número variable de tablas cuyos contenidos se explican a continuación. Para una fácil navegación, los reportes detallados se consultan desde un archivo HTML con menús de navegación que lo hacen más manejable.

El archivo resumen contiene las siguientes secciones:

- Resumen Ejecutivo
- Resumen de equipos que integran la Auditoría
- Notas del Auditor: espacio reservado para que el NCE responsable de la Auditoría haga comentarios específicos para la misma.
- Tablas de Comparación para Switches y Routers: tablas en las cuales se organizan los equipos de la auditoría que presentaron excepciones, presentados del equipo con mayor número de excepciones al equipo con menor número de las mismas
- Tabla de Lista de Tareas de Auditoría: es la parte medular del resumen. Se muestra cada excepción, los equipos que la provocaron, y una breve explicación de la misma.

Por otra parte, existe también un reporte detallado para cada dispositivo; dicho reporte está estructurado en diferentes tablas que agrupan características de Hardware, Software, diferentes tecnologías, protocolos, etc.

Cada tabla contiene diferentes parámetros que fueron medidos durante el tiempo que duró la auditoría. Los parámetros que pertenecen a una misma área se encuentran en la misma tabla. Se tiene una tabla, por área, por equipo.

Para mayor claridad, usaré como ejemplo el equipo Switch 1. Para este se tienen las siguientes tablas (entre otras):

- Switch Memory Table
- Flash Information
- System Power Table
- Line Card Power Exception Table
- Temperature Table
- Weekly CPU Utilization Graph
- System High Availability
- Protocol High Availability
- IP Multilayer Switching Configuration
- Cisco Express Forwarding Statistics Table
- Software and Hardware Statistics Table

Continuando con nuestro ejemplo, se explicarán los contenidos de la tabla “Switch Memory Table” para el equipo Switch 1. Esta tabla contiene una lista de todos los tipos y cantidades de memoria encontrada en los dispositivos auditados. La información contenida en ella permite realizar una comparación entre dispositivos similares, basándose en éstas características. Esto puede usarse para determinar posibles problemas de memoria y ayudar en upgrades, entre otras cosas. Dicha tabla contiene la siguiente información:

- Nombre del equipo
- Tipo de tarjeta procesadora (CPU)
- Memoria Total
- Memoria Utilizada
- Memoria Libre
- % de Memoria Libre
- % de Memoria Fragmentada

La tabla luce como la siguiente:

Switch Memory Table

Host Name	Processor Type	Total Memory (MB)	Used Memory (MB)	Free Memory (MB)	Free Mem %	Frag Mem %	NREPs
Switch1-RP-5	I/O	64	9.94	54.06	84.47	0.11	0
Switch1-RP-5	Processor	372.86	75.71	297.16	79.7	20.65	0
Switch1-standby-SP	I/O	64	9.94	54.06	84.47	0	0
Switch1-standby-SP	Processor	351.06	103.85	247.21	70.42	18.26	0
Switch1-standby-RP	I/O	64	9.94	54.06	84.47	0.11	0

Para cada parámetro, Cisco ha definido (con base en su experiencia con redes de clientes, complementadas con estudios, pruebas en laboratorio y grupos de expertos en diferentes tecnologías) cuáles son los valores óptimos, así como también los valores de umbral. Generalmente hay dos valores

de umbral: el umbral de riesgo medio y el umbral de riesgo alto. Al sobrepasar esos valores, se comienza a comprometer la integridad del equipo o tecnología en cuestión[12].

Si el valor de un parámetro rebasa cualquiera de los valores de umbral, se dice que se tiene una **excepción**. Dicha excepción también puede ser de riesgo medio (la excepción se marca en amarillo) y de riesgo alto (la excepción se marca en rojo).

4.2.4 Participación profesional

La parte más importante de la elaboración de la Auditoría Personalizada es el análisis y la complementación de la información que contiene automáticamente. Esto debido a que, como ya se indicó, no todos los clientes cuentan con el nivel de conocimientos necesario para poder comprender a cabalidad los conceptos expuestos. Como NCE, mi participación profesional más importante fue en este punto precisamente.

La sección más importante de la Auditoría Personalizada y la que toma más tiempo analizar es la Lista de Tareas de Auditoría. En ella radica prácticamente todo el valor del documento ya que explica detalladamente cada excepción, en qué equipos se presenta así como las acciones a tomar para corregirla.

Para mayor claridad usaré un ejemplo. La siguiente tabla es un extracto de la información que contiene la Lista de Tareas de Auditoría contenida en el archivo resumen, al ser generada de forma automática. En ella se observan las siguientes columnas:

- **Hostname**: nombre del equipo
- **Exception**: nombre de la excepción
- **Frequency Count:** número total de ocurrencias de la excepción
- **Auditor Comments**: comentarios con los que es recibido el Reporte de la Auditoría Personalizada después de ser generada. Estos comentarios son generados de forma automática

Host Name	Exception	Frequency		Auditor Comments
		Count	Severity	
Router 1 Router 2 Router 3 … Router N Switch 1 Switch 2 Switch 3 … Switch N	Multicast Fast Switching	136	■	Multicast Fast Switching should be enabled under PIM enabled interfaces using the interface configuration command "ip mroute-cache".
Router 1 Router 2 Router 3 … Router N Switch 1	CEF Switching	68	▯	To optimize router/interface performance CEF Switching should be enabled globally and on each interface using the interface command "ip route-cache cef" where available.

[12] La manera en que estos umbrales fueron definidos queda fuera del alcance de este documento

Switch 2 Switch 3 … Switch N				
Router 1 Router 2 Router 3 … Router N Switch 1 Switch 2 Switch 3 … Switch N	Fast Switching	65		To optimize router/interface performance Fast Switching should be enabled using the interface command "ip route-cache".

Es el Análisis de esta tabla la parte más importante de la Auditoría, debido a que, por regla general, se pueden tener más de 100 excepciones, entre riesgo alto, medio y bajo. Es la tarea que consume más tiempo ya que cada una de esas excepciones debía investigarse, comprenderse y reinterpretarse para hacerla más accesible para la audiencia a la cual iba dirigido el documento.

4.2.4.1 Análisis y Complemento de la Información en la Auditoría

Analizando la información de la sección anterior, se puede llegar a varias conclusiones:

- La longitud de la información contenida en la Auditoría guarda una relación directa con el número de equipos sobre los cuales se efectúe y las excepciones que se presenten
- Para cada equipo, además de la Lista de Tareas de Auditoría, se tienen además un reporte detallado
- La información que contiene por default la Lista de Tareas de Auditoría es escueta y breve

Por lo anterior, mi participación profesional como NCE fue complementar la Auditoría Automática con lo siguiente:

1. **Explicación detallada de cada excepción**: la explicación debe ser técnicamente rigurosa, pero breve y condensada, lo cual conlleva complejidad: investigar y condensar complejos conceptos tecnológicos en un breve espacio y con la mayor claridad posible.
2. **Análisis específico de la excepción en los nodos que la dispararon**: para entregar un Reporte de valor agregado al cliente, se verificó puntualmente en algunos nodos la excepción de que se trata, explicando las razones por las que se presenta, y el origen que puede tener la excepción.
3. **Elaboración de un Resumen Ejecutivo en español**: el personal de la Compañía Petrolera Española hizo una solicitud especial para que la Auditoría fuera presentada en inglés, pero con un Resumen Ejecutivo en español, que refleje los hallazgos más importantes.

La metodología empleada para cumplir los objetivos anteriores fue:

- Comprender el significado de cada excepción
- Investigación sobre el parámetro al que se refiere cada excepción, apoyándome en herramientas como:
    - Portal en Internet de Cisco.com
    - Libros publicados por Cisco Press
    - Experiencia propia y de otros NCEs

- Procesamiento de la información recopilada, enfocándose en la claridad y sin perder el rigor técnico
- Revisión personalizada en cada dispositivo de red del cliente para las excepciones más relevantes
- Resumir los hallazgos más importantes

A continuación se explicará cómo realicé una explicación más detallada de algunas de las excepciones de riesgo alto, para tener información más completa. Sólo se presentan algunas debido a que la metodología para todas las excepciones es la misma y sería redundante presentarlas todas. La información que se plasmó para complementar cada excepción fue escrita por mí, con base en información consultada en las fuentes ya mencionadas.

Excepciones de riesgo alto

Las excepciones de riesgo alto son las siguientes:

Multicast Fast Switching: la Auditoría, por default, sólo dice lo siguiente: ***"Multicast Fast Switching should be enabled under PIM enabled interfaces using the interface configuration command "ip mroute-cache".***

Si durante el proceso de la Auditoría se encuentra que el equipo en cuestión está realizando Multicast Routing (verificando la existencia de los siguientes comandos `ip multicast-routing` (a nivel global) y `ip pim` (a nivel de interface)), y además se detecta que en las interfaces con "ip pim" falta el comando "`ip mroute-cache`", entonces la excepción se dispara.

Complementé la explicación de la excepción con el siguiente comentario:

> *En plataformas con arquitectura distribuida, fast-switching permite que los routers proporcionen un mejor desempeño en el reenvío de paquetes, comparado con process-switching.*
>
> *En primer lugar, el primer paquete dirigido hacia un destino es reenviado a través de process-switching. Sin embargo, en fast-switching, el resultado de la consulta del destino en la tabla de enrutamiento se almacena en un cache de rutas. Todos los paquetes subsecuentes para ese destino se reenvían usando fast-switching, el cual no requiere que la tarjeta procesadora se involucre para realizar una consulta de la tabla de enrutamiento. Los frames de capa 2 son reescritos y enviados a las interfaces de salida. El procesador de interface calcula el CRC (Cyclic Redundancy Check), en lugar de la RP.*
>
> *En Multicast Fast-Switching, el cache de rutas debe almacenar información para la fuente, el grupo de multicast, y las múltiples interfaces de salida, a diferencia de unicast fast-switching, en donde se requiere un cache únicamente con información de la dirección destino y la interface de salida.*
>
> *El contar con Multicast Fast-Switching habilitado en todas las interfaces con multicast aumenta en gran medida el desempeño del equipo, ya que libera al procesador central de la tarea de realizar búsquedas de destinos en la tabla de enrutamiento (esto ocurrirá, como ya se estableció, sólo para el primer paquete dirigido a un destino cuya información no se encuentra en el cache de rutas).*
>
> *Se recomienda revisar la configuración en los dispositivos que dispararon esta excepción y que están realizando multicast- routing.*

Esta excepción es considerada de riesgo alto debido a que, si se permite que la tarjeta procesadora se encargue de la búsqueda de los destinos para cada paquete multicast, entonces su rendimiento se verá seriamente comprometido, además de que representa un desperdicio de recursos ya que las tarjetas de interface cuentan con un CPU y memorias capaces de realizar estas actividades.

CEF Switching: la auditoría, por default, sólo dice lo siguiente: "***To optimize router/interface performance CEF Switching should be enabled globally and on each interface using the interface command "ip route-cache cef" where available.***"

Si durante el proceso de Auditoría se encuentra que un equipo que realice unicast routing no tiene el comando "`ip cef`" o "`ip cef-distributed`" a nivel global, o "`ip route-cache cef`" a nivel de interface, entonces la excepción se dispara.

Complementé la explicación de la excepción con el siguiente comentario:

Para realizar el correcto reenvío de los paquetes, un router debe en primer lugar determinar si el destino el paquete se encuentra en su tabla de enrutamiento, así como la interface de salida y la información necesaria para reescribir el encabezado de capa 2.

A lo largo de la historia del Sistema Operativo Cisco IOS, han sido desarrollados múltiples métodos de switching. Cisco Express Forwarding es el método más rápido y eficiente de todos. Esto se debe a que, a diferencia de otros métodos de switching en los cuales la información de los encabezados de capa 2 se calcula bajo demanda, en CEF se calculan por adelantado todos los encabezados de capa 2 para todos los destinos que el router tiene en su tabla de enrutamiento. Gracias a esto, CEF constituye el método más rápido y eficiente de switching.

Al habilitarse a nivel global, CEF se habilita también en todas las interfaces que lo soportan (el comando "`ip route-cache cef`" aparece en la configuración de cada interface). Este comando asegura que se empleará CEF para el switching de paquetes que entran por dichas interfaces. Ocasionalmente, si se requiere deshabilitar CEF en alguna interface individual, esto se puede hacer con el comando "no ip route-cache cef".

Esta excepción se dispara si se descubre que el comando "`no ip route-cache cef`" se encuentra en alguna interface o si no se encuentra el comando "`ip cef`" a nivel global.

Por lo anterior, se recomienda el empleo de CEF si la versión de sistema operativo y el modelo de plataforma en uso lo soportan. Si la excepción se presenta en equipos que no soportan CEF, esta excepción puede ser ignorada para dichas plataformas sin riesgo alguno.

Fragmented Memory: la auditoría, por default, sólo dice lo siguiente: "***If the Fragmented memory is highlighted yellow, the fragmented memory needs to be watched closely to determine if memory is being properly freed for future use. It may be necessary to reload the box if the fragmented percentage continues to increase. If the Fragmented memory is bold red the box should be scheduled for reload to free up non-continuous memory space.***" Nunca se explica qué es la memoria fragmentada.

La excepción se dispara si la memoria fragmentada calculada en el último día de la Auditoría es mayor en más del 10% al valor obtenido durante el primer día.

Complementé la explicación de la excepción con el siguiente comentario:

El tener memoria fragmentada significa que un proceso ha consumido una gran cantidad de memoria de procesador y después ha liberado la gran mayoría, dejando sin embargo fragmentos de memoria todavía asignados, ya sea por el proceso original o por otros procesos que también reservaron memoria al mismo tiempo. Si el mismo evento ocurre en muchas ocasiones, la memoria se puede fragmentar en bloques muy pequeños, al grado en que todos los procesos que requieren un fragmento de memoria más largo no pueden obtener la memoria que requieren. Esto puede afectar la operación del dispositivo al punto en que es imposible conectarse a él.

Este problema se caracteriza por un valor muy pequeño (menos de 20000 bytes) en la columna "Largest" del comando "`show memory`", pero a la vez un valor suficiente en la columna "Freed" (1 MB o más), o alguna otra disparidad muy grande en los valores de las dos columnas. Esto puede suceder cuando el dispositivo tiene muy poca memoria disponible, ya que no existe una rutina de desfragmentación en el sistema operativo Cisco IOS.

Si se sospecha de problemas de fragmentación de memoria, inhabilite algunas interfaces. Esto debe liberar los bloques fragmentados. Si esta solución funciona, la memoria se está comportando de forma normal y lo único que debe hacerse es agregar más memoria. Si por el contrario, el apagar las interfaces no ayuda, entonces es probable que se esté en presencia de un defecto de software (bug). En este caso, el mejor curso de acción es contactar al Technical Assistance Center (TAC) de Cisco para abrir un caso de soporte, con la información que se solicite para la resolución del caso.

Errores de Cyclic Redundancy Check: la auditoría, por default, sólo dice lo siguiente: ***"The output of "show interfaces" commands on Cisco devices includes numerous counters. One such counter is Cyclic Redundancy Check (CRC), which counts the number of times (that is, for how many packets) the checksum generated by the originating station, or far end device, does not match the checksum calculated from the data received."***

Complementé la explicación de la excepción con el siguiente comentario:

Cyclic Redundancy Check (CRC) es un esquema común de verificación de errores, el cual detecta y descarta datos corruptos. Un valor de CRC se genera por medio de un cálculo realizado en el dispositivo que origina los datos. El dispositivo destino compara este valor con el obtenido por su propio cálculo, para determinar si han ocurrido errores durante la transmisión. En primer lugar, el dispositivo origen realiza un conjunto predeterminado de cálculos sobre los contenidos del paquete a ser enviado, e incluye los resultados de dichos cálculos en el paquete mismo, antes de enviarlo. El dispositivo destino realiza los mismos cálculos sobre el paquete y entonces compara su propio valor con el contenido en el paquete. Si los valores son los mismos, el paquete se considera válido. Si los valores son diferentes, entonces el paquete contiene errores y es descartado.

Cuando se opera en modo full-duplex en interfaces Ethernet, los errores de CRC deben ser mínimo. Si el número de errores de CRC aumenta, verifique que no exista la condición de duplex mismatch. Esto se presenta cuando en un enlace Ethernet, una de las interfaces del enlace opera en full-duplex, mientras la otra opera en modo half-duplex. El resultado de este error es un desempeño extremadamente lento, conectividad intermitente y una pérdida de conexión. Otras causas posibles de errores de capa 2 son cables dañados, un puerto físico dañado, o problemas de Hardware.

Para determinar la razón para esta excepción, siga los siguientes pasos:

Verifique si el contador de errores de CRC se incrementa, usando continuamente el comando "show interfaces". Si el valor no se incrementa durante un periodo de tiempo que óptimamente debe ser de un día mínimo, entonces se trata de un valor acumulado de un problema pasado. Se sugiere en ese caso entonces ejecutar el comando "clear counters interface" para que la excepción no se vuelva a presentar erróneamente en futuras auditorías.

% de Tráfico Hardware Switched: la información contenida por default en la Auditoría es la siguiente: ***"Check the interface level and the traffic to determine which traffic is being software switched. A newer supervisor card may be required or some features may have to be disabled or changed if the percentage is high and performance has been affected."***

Complementé la explicación de la excepción con el siguiente comentario:

A lo largo del tiempo han existido diferentes formas en las que un router puede realizar el reenvío de la información. En las plataformas más recientes, prácticamente todo el tratamiento que se debe realizar a un paquete, así como las consultas a las diferentes tablas de un router, se realiza en Hardware, usando ASICs[13]. Esto incrementa en gran medida el desempeño y la velocidad con que una plataforma realiza el reenvío de información.

Sin embargo, la utilización de algunas características requieren que dichos tratamientos se realicen en software, con lo cual se ralentiza el reenvío de la información y se desperdician los recursos disponibles en el dispositivo.

Se debe trabajar en conjunto con el NCE local para constatar si se están empleando algunas características que impidan que el tráfico sea reenviado en software y de ser posible, hacer un uso reducido de dichas características.

Para evitar ser redundante y prolongar este Informe en exceso, las anteriores son todas las excepciones que se explicarán. La metodología para explicar el resto de ellas fue la misma, independientemente del riesgo.

4.2.5 Resultados y Aportaciones

Este proyecto arrojó resultados muy satisfactorios, los cuales pueden ser agrupados en resultados positivos para el cliente y resultados positivos para Cisco Systems.

Los resultados positivos para el cliente fueron:

1. La Auditoría permitió identificar varios puntos de atención que estaban causando un desempeño pobre en su Centro de Datos, de manera proactiva. Gracias a la Auditoría, el cliente tuvo la oportunidad de identificar las causas de posibles problemas incluso antes de que estos se presentaran, ahorrando con ello tiempo, dinero y sin comprometer la operación del negocio.
2. Al ser entregada en español, el cliente manifestó una profunda satisfacción con la Auditoría, y con los contenidos de la misma. En palabras de la responsable de Tecnología del cliente: ***"agradezco el trabajo realizado en LATAM y aprecio el valor y detalle de todos los***

[13] **ASICs: Application Specific Integrated Circuits.** Circuitos Integrados que son programados para realizar funciones específicas sobre los datos que son transportados en un dispositivo de red. Al realizarse en Hardware, se gana en velocidad y capacidad de procesamiento.

informes entregados. Los informes nos han ayudado muchísimo y estoy creando un informe ejecutivo para mi director".

3. Gracias a las explicaciones ampliadas contenidas en la Auditoría, el cliente amplió sus conocimientos sobre los parámetros que deben tomarse en cuenta para mantener los equipos de su Centro de Datos operando en un niveles óptimos.

Los resultados positivos para Cisco fueron:

1. La satisfacción del cliente con la Auditoría y las posteriores consultas sentó las bases para que se ampliara la gama de servicios que el cliente contrató a Cisco. Así, ahora ya se cuenta con contratos de NOS no sólo para su Centro de Datos, sino para toda su Red Corporativa. El impacto en el tema de negocio fue muy importante.
2. Dada la calidad del entregable y el nivel de satisfacción de parte de los NCEs en España, se abrió una posición nueva para el área en la que me desempeño, para tener una persona trabajando de forma dedicada al mercado de España desde México. Dicha plaza la ocupo desde marzo de 2011. Ello demuestra que el trabajo fue realizado óptimamente y sobrepasando incluso las expectativas, fomentando la creación de empleos. Actualmente, soy la persona asignada al mercado de la Unión Europea.
3. Al mostrar el equipo de Servicios Avanzados de Cisco que los entregables elaborados en español tenían el mismo nivel de calidad que los entregados en inglés, se sentaron las bases para que una amplia variedad de empresas basadas en países de habla hispana tengan acceso a estos entregables, abriendo así una nueva oportunidad de negocio para la empresa.

4.3 Diseño para la Migración de Routers y Activación del Servicio de WCCPv2 en el Centro de Datos de una Entidad de Recaudación de Impuestos

4.3.1 Antecedentes del Tema

Este proyecto nace a partir de que una Entidad de Recaudación de Impuestos en México enfrentara problemas de desempeño en sus routers de frontera hacia la red MPLS de su Proveedor de Servicios Administrados, debido a la activación de WCCPv2.

A continuación se explicarán algunos conceptos necesarios para comprender cabalmente las partes involucradas en el proyecto, el modelo de operación de las mismas así como un resumen de la topología de la Red concerniente.

Servicios Administrados de Red

Como una Red de Servicios Administrados se entiende al modelo de operación en el cual una entidad o empresa (en este caso, la Entidad de Recaudación de Impuestos) publica una licitación para solicitar que una empresa Proveedora de Servicios de Internet (ISP, Internet Service Provider) sea la encargada de administrar toda su infraestructura de red.

Originalmente, la Entidad de Recaudación de Impuestos administraba su propia red, pero al paso del tiempo fue evidente que esto implicaba gran esfuerzo y gastos innecesarios en capacitación, ya que asuntos propios de la administración de una red de datos estaban fuera del alcance de los conocimientos de su personal. Por ello, se decidió publicar una licitación para que la empresa que ganara la misma tuviera la responsabilidad de operar la red, con los beneficios de contar con una empresa experta en redes de datos (un ISP) para la operación cotidiana de la red.

Como parte de la licitación, un requerimiento específico es que sea cual fuere el ISP que ganase la licitación, éste debía contratar el servicio de NOS de Cisco Systems. Esta solicitud fue el resultado de una experiencia previa de Cisco Systems México con el sector gubernamental, proyecto en el cual las partes involucradas quedaron muy satisfechas con el servicio de NOS.

Producto de esta licitación, la red fue “partida” en dos secciones: una de ellas fue entregada para su operación a un ISP (ISP 1) que cubriría los sitios más importantes, mientras la otra sección fue entregada a otro ISP (ISP 2) que administraría todos los sitios en los cuales el ISP 1 no tuviera cobertura geográfica.

Además, dada la importancia y el volumen de información que maneja la entidad gubernamental, todos sus servidores de almacenamiento de información y donde yacen sus aplicaciones se encuentran en dos Centros de Datos. Estos Centros de Datos son administrados a su vez por otras 2 compañías especializadas.

Como se puede imaginar, el contar con 4 compañías administrando una red de datos gubernamental complica mucho la implementación y validación de nuevos servicios, aumentando en mucho la complejidad del proyecto para todas las partes involucradas, pero en especial para Cisco Systems al fungir como consejero técnico para todas las partes involucradas.

Conceptualmente tenemos entonces, las siguientes entidades involucradas:

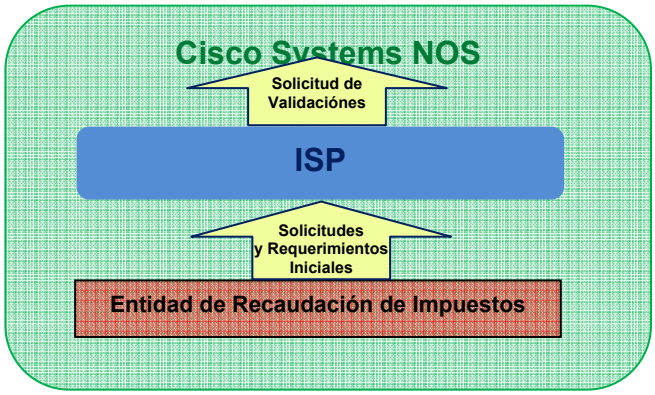

Figura 17. Modelo de Operación de una red de Servicios Administrados

La figura anterior busca explicar la metodología de operación de la red: de la Entidad de Recaudación de Impuestos surgen los requerimientos de nuevos servicios, implementación de funcionalidades y nuevos diseños. Estos requerimientos son canalizados al ISP, quien se encarga de dar cumplimiento a dichas solicitudes, no sin antes solicitar la validación de las soluciones propuestas al equipo de Servicios Avanzados de Cisco Systems. El papel de Cisco Systems es funcionar como una entidad que protege y da confianza a las partes involucradas, en especial al cliente final (Entidad de Recaudación de Impuestos) respecto a que los nuevos diseños, implementaciones de nuevas tecnologías, etc., cumplen con las mejores prácticas de la industria.

Topología Física del Centro de Datos

De forma general, se conoce como un Centro de Datos a un sitio de la infraestructura de red de una empresa, en el cual se ubican los servidores que almacenan la información más crítica de la empresa.

El Centro de Datos también alberga otros elementos de HW para proveer funciones más específicas. Una arquitectura de datos bien diseñada se compone de varios módulos con funciones específicas. Entre dichos módulos se encuentran, entre otros:

- Módulo de conexión a Internet
- Módulo de Seguridad (incluye firewalls, equipo de control de Acceso, IPS)
- Módulo de conexión a la red WAN
- Módulo de Optimización de Aplicaciones
- Módulo de Interconexión a entidades externas

Por lo general, un Centro de Datos es propiedad de una empresa dedicada a ofrecer servicios de *hosting* y almacenamiento. Esta empresa renta espacios en rack para que otras empresas instalen ahí sus equipos de red y servidores. Este modelo de operación es práctico porque empresas que por su tamaño o porque la naturaleza de su negocio principal es diferente a las Tecnologías de la Información, tienen acceso a servicios que de otra forma les serían negados tanto por costos como por conocimientos.

Como ya se mencionó, el Centro de Datos no es propiedad ni del cliente ni del ISP, sino de una empresa independiente. Cada cliente o ISP se conecta a la infraestructura del Centro de Datos a través de un

Módulo de Interconexión WAN. El equipamiento de este módulo sí pertenece a cliente y es operado por el ISP.

Desde el punto de vista de equipamiento y funcionalidades, el Módulo de Interconexión WAN Centro de Datos de la Entidad de Recaudación de Impuestos tiene como características:

- Un máximo de 50 usuarios de red
- Equipamiento mínimo: router CPE multiservicios con interfaz óptica POS STM1 o Gigabit Ethernet
- Equipo de control de acceso a la red
- Firewall externo, un dispositivo de IPS
- Sistema de aceleración y optimización de aplicaciones para terminar las sesiones de los sitios remotos

La siguiente figura muestra la topología del Centro de Datos. Dentro de los recuadros rojos se encuentran los equipos involucrados en el Diseño que nos atañe. Sólo se muestran los módulos principales; los detalles del resto de los módulos quedan fuera del alcance del proyecto.

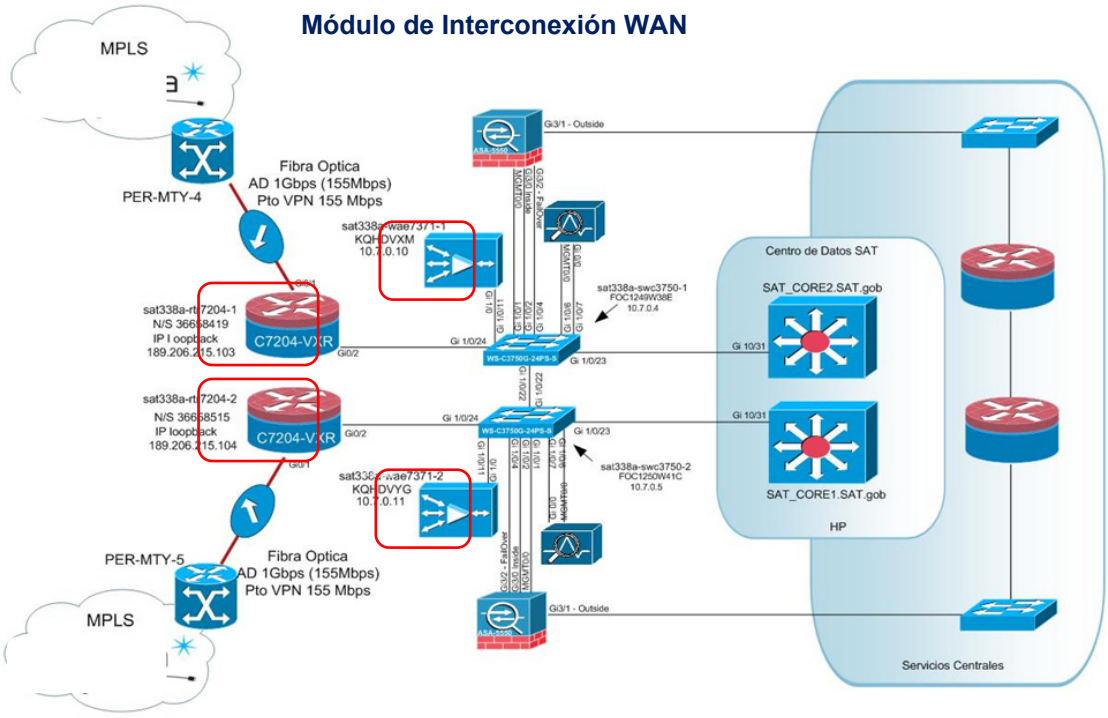

Figura 18. Módulo de Interconexión WAN

4.3.2 Definición del Problema

Se identificaron las siguientes causas para dichos problemas:

1. La Entidad de Recaudación de Impuestos solicitó a su Proveedor de Servicios Administrados la activación del servicio de WCCP (Web Cache Control Protocol) en sus routers de frontera hacia la red MPLS. WCCP optimiza la operación de las solicitudes de usuarios hacia páginas web.
2. Los Routers iniciales (Cisco 7204VXR) son plataformas que realizan muchas de sus tareas en Software, incluído WCCP. Esto provocó que la activación de esta funcionalidad tuviera un impacto negativo y directo en el desempeño del equipo.
3. El volumen de tráfico que empleaban los routers del Centro de Datos era tan alto, que al momento de activar WCCP el nivel de procesamiento alcanzado en los equipos provocó que los mismos dejaran de operar

Los problemas anteriores tuvieron como consecuencia que la Entidad de Recaudación de Impuestos solicitara el apoyo de Cisco Systems para obtener una solución satisfactoria a la problemática encontrada.

4.3.3 Análisis y Metodología Empleada

La metodología seguida para la conclusión de este proyecto se puede resumir en los siguientes pasos:

1. Definición del nuevo modelo de router que sustituiría a los actuales
2. Determinación de las funcionalidades actuales y futuras
3. Definición de la versión de SW a emplear en los nuevos routers
4. Elaboración de configuración *draft* para nuevos routers 7604
5. Determinación de una línea base de desempeño de los equipos actuales
6. Sustitución de los routers actuales por los nuevos 7604 sin activar WCCP y monitoreo de los nuevos equipos
7. Activación de WCCP y monitoreo de servicios
8. Optimización gradual de diferentes aplicaciones
9. Retiro de routers 7204 VXR y Conclusión del Proyecto

Los detalles de cada paso forman parte de mi Participación Profesional en el proyecto, y se explican a continuación.

4.3.4 Participación Profesional

Como NCE me vi involucrado en prácticamente todos los pasos definidos en la metodología para concluir satisfactoriamente el proyecto. Fungí como consultor técnico y punto de contacto entre el cliente y entidades internas de Cisco Systems.

4.3.4.1 Definición del nuevo modelo de router que sustituiría a los actuales

Una vez que se hubo determinado que los routers 7204 VXR no tenían la capacidad suficiente para manejar los volúmenes de tráfico actuales optimizando aplicaciones usando WCCP, el primer paso fue determinar qué modelo de router sería recomendado para sustituir a los 7204 VXR. Esta tarea fue realizada por el equipo de preventa de Cisco, quienes recomendaron la plataforma 7600.

La razón determinante para seleccionar los routers 7600 como sustitutos de los 7206 VXR es que toda la funcionalidad de WCCP se realiza en HW, empleando los ASICs específicos con los que cuenta el

router. De esta forma, WCCP se convierte en una funcionalidad que opera de forma independiente al volumen de tráfico que maneja el router

4.3.4.2 Determinación de las funcionalidades actuales y futuras

El siguiente paso fue obtener las configuraciones de los routers 7204 VXR, por una parte, y por otra empleando la herramienta CNC de la que ya se habló anteriormente, determinar las funcionalidades actuales. Este paso es importante debido a que la configuración y funcionalidades actuales constituyen la información que se requiere para determinar la versión de SW que se emplearía en los nuevos routers 7600, que es el siguiente paso a considerar.

Obviamente debía considerarse como funcionalidad fundamental WCCP.

4.3.4.3 Definición de la versión de SW a emplear en los nuevos routers

Además de contar con un HW confiable como el router 7600, el siguiente elemento para otorgar tranquilidad al cliente es contar con un software igualmente confiable.

Cisco cuenta con una enorme variedad de versiones de SW, ya que cada equipo de red puede emplear diferentes versiones de SW según los diferentes roles en que sea empleado. El SW más común de Cisco, IOS, está estructurado de tal forma que existen varios diferentes releases de SW cuya nomenclatura va cambiando a medida que se van publicando releases más actuales.

Una de mis actividades cotidianas como NCE es la Recomendación Proactiva de Software. El objetivo de esta actividad es determinar cuál es la versión de SW más apropiada en términos de funcionalidades, confiabilidad, estabilidad, seguridad, y tiempo de vida. Para determinar la versión de SW, se toman en cuenta factores como:

- Recomendación de las Unidades de Negocio de Cisco: las unidades de Negocio son grupos de trabajo internos que tienen como tareas:
  - Desarrollo de nuevos productos
  - Impulsar la penetración en el mercado de familias de productos Cisco ya existentes
  - Colaborar estrechamente con los equipos de desarrollo de SW para efectuar pruebas exhaustivas de HW y SW de manera conjunta. De estas pruebas, se obtienen las versiones recomendadas por cada plataforma
- Funcionalidades que el cliente usará
- Uso en redes reales: todo el SW es propenso a tener defectos, y en muchos de los casos, dichos defectos se encuentran sólo cuando el SW opera en ambientes reales. Cuando se realiza una recomendación de SW, un NCE debe analizar cuál de entre las versiones que eligió como candidatas es la que está instalada en un mayor número de equipos y a su vez es reciente, utilizando para ello los datos globales de CNC. Generalmente, se realiza un compromiso entre la versión más reciente y aquella que está instalada en el mayor número de equipos.

Cuando se tiene una versión candidata, se procede con el procedimiento de elaboración de un Reporte Proactivo de Software. En este Reporte analicé detalladamente los defectos que el SW tenga, revisando su impacto y emitiendo conclusiones y recomendaciones al respecto. Al final, aunque sea imposible tener un SW libre de defectos, lo que sí es posible es garantizar al cliente que el SW que utilizará en sus equipos esté libre de defectos que tengan un impacto directo en su operación.

Todas las tareas mencionadas fueron mi responsabilidad.

4.3.4.4 Elaboración de configuración draft para nuevos routers 7604

Una vez que fue definido el nuevo SW a emplear, el siguiente paso es verificar que las configuraciones originales sean soportadas sin problemas con el nuevo SW en los nuevos routers 7604.

Esta verificación la realicé en un laboratorio, y tuvo como objetivos

- Verificar que el HW propuesto sea reconocido sin problemas con el SW a utilizar
- Verificar que todos los features que se empleaban originalmente sean soportados sin problemas en la nueva plataforma.
- Prevenir situaciones inesperadas: en algunas ocasiones, al cambiar de SW, algunos comandos no son soportados o su nomenclatura cambia. El identificar estos cambios con anticipación da tranquilidad al cliente y permite a su vez eliminar posibles problemas que pudieran presentarse durante el proceso de migración.

Esta actividad involucró la elaboración de una topología de pruebas así como la solicitud de que dicha topología sea construida con equipo real. Esta actividad también fue realizada por mí.

La siguiente tabla muestra la configuración definitiva del router 7604. Las direcciones IP y password no son los reales, esto para proteger la confidencialidad del cliente. En azul se muestran los comandos nuevos que aparecen por default al usar la nueva combinación de SW y HW nuevo, mientras que en verde los comandos relacionados a WCCP.
Al final de la tabla se muestra también el comando “show module”, fundamental para verificar que todo el HW nuevo sea reconocido y opere sin problemas.

Verificación de la configuración y *features*

```
Building configuration...

Current configuration : 12663 bytes
!
upgrade fpd auto
version 12.2
!
!
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
localtime show-timezone
service password-encryption
service internal
service counters max age 10
!
hostname 7604-4-263
!
boot-start-marker
boot system disk0:c7600rsp72043-advipservicesk9-mz.122-33.SRD4.bin
boot-end-marker
!
logging message-counter syslog
logging buffered 16384 informational
no logging console
no logging monitor
enable secret 5 <removed>

!aaa new-model
!
!
ip subnet-zero
```

```
ip source-route
ip wccp 61
ip wccp 62
!
!
no ip domain lookup
!
!
!
!
vtp domain GRA
vtp mode transparent
mls ip multicast flow-stat-timer 9
mls flow ip interface-full
no mls flow ipv6
mls qos
mls cef error action reset
multilink bundle-name authenticated
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
redundancy
 main-cpu
  auto-sync running-config
 mode sso
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
vlan 7
 name *SS7*
!
vlan 10
 name *SERVER*
!
vlan 11
 name *USERS*
!
vlan 20,77
!
vlan 80
 name CP RNC
!
vlan 90
 name O&M
!
vlan 98
 name O&M_MSS
!
vlan 99
 name O&M_MGW
!
vlan 100
!
vlan 101
 name CP MGW
!
vlan 102
 name CP_MSS
!
vlan 151-152,154
!
vlan 201
 name UP MGW
!
vlan 302
 name *GB-IP-BGR2*
!
vlan 777
 name FOVER
!
```

```
vlan 810-811,983
!
vlan 1000
 name din-Victoria508-Cauquenes_TCTC
!
!
!
class-map match-any DataNormal
  match ip dscp af11
  match protocol napster
class-map match-any DataPlus
  match ip dscp af22
class-map match-any DataNormal-Conversacionales
  match ip dscp af22
  match access-group name DataNormalList
class-map match-any dscp-ef
  match ip dscp cs3  cs4
  match ip dscp af41  af42  af43
  match ip dscp ef
  match ip precedence 3
  match ip precedence 5
  match access-group name RealTimeVoiceList-IN
class-map match-any dscp-af22
  match ip precedence 2
  match ip dscp af31  af32  af33
  match ip dscp cs2  af31  af32
class-map match-any dscp-af11
  match ip precedence 1
  match ip dscp cs1
  match ip dscp cs1  af21  af22  af23
  match ip dscp af11
class-map match-any DataPlus-ConversacionalesPlus
  match access-group name DataPlusList
  match ip dscp af32
class-map match-any RealTimeVoice-Interactivos
  match ip dscp ef
  match access-group name RealTimeVoiceList
class-map match-any VideoConf-InteractivosPlus
  match ip dscp af42
class-map match-any RealTimeVoice
  match ip dscp ef
class-map match-any DataEspecial-FTP
  match access-group name DataEspecialList
!
policy-map SAT-5-1-64-15
  class RealTimeVoice-Interactivos
   set ip dscp ef
    priority
    police cir percent 5
  class VideoConf-InteractivosPlus
   set dscp af42
    bandwidth percent 1
  class DataPlus-ConversacionalesPlus
   set dscp af32
    bandwidth percent 64
  class DataNormal-Conversacionales
   set dscp af22
    bandwidth percent 15
  class DataEspecial-FTP
    bandwidth percent 1
  class class-default
policy-map SetDSCP
  class dscp-ef
   set ip dscp ef
  class dscp-af22
   set ip dscp af22
  class dscp-af11
   set ip dscp af11
policy-map ShapeSAT-5-1-64-15-SAT500
  class class-default
    shape average 500000000
   service-policy SAT-5-1-64-15
!
!
interface GigabitEthernet1/1
 no ip address
```

```
 shutdown
!
interface GigabitEthernet1/2
 ip address 2.2.2.2 255.248.0.0
 no ip proxy-arp
 media-type rj45
!
interface GigabitEthernet3/0/0
 ip address 1.1.1.1 255.255.255.0
 ip wccp 62 redirect in
 no negotiation auto
 cdp enable
 service-policy input SetDSCP
!
interface GigabitEthernet3/0/1
 ip address 1.1.2.1 255.255.255.0
 ip wccp 61 redirect in
 no negotiation auto
 cdp enable
!
interface GigabitEthernet3/0/2
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet3/0/3
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet3/0/4
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet4/1
 ip address 2.2.1.1 255.255.255.0
 speed 1000
 service-policy input SetDSCP
!
interface GigabitEthernet4/2
 ip address 2.2.2.1 255.255.255.0
 ip nbar protocol-discovery
 speed 1000
 service-policy output ShapeSAT-5-1-64-15-SAT500
!
interface GigabitEthernet4/3
 no ip address
 shutdown
!
interface GigabitEthernet4/4
 no ip address
 shutdown
!
!
!
(comandos omitidos por brevedad)
!
!
!
interface GigabitEthernet4/40
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan101
 description << ENLACE LAN CLIENTE >>
 ip address 192.168.201.5 255.255.255.248
 ip wccp 61 redirect in
 ip ospf priority 0
 standby 5 ip 192.168.201.4
 standby 5 priority 105
 standby 5 preempt
```

```
 standby 5 track 123 decrement 10
 service-policy input SetDSCP
!
ip default-gateway 172.16.0.1
ip classless
ip route 10.0.0.0 255.0.0.0 172.16.255.254
ip route 10.21.0.0 255.255.0.0 172.16.255.254
ip route 223.255.254.254 255.255.255.255 172.16.0.1
!
no ip http server
no ip http secure-server
!
ip access-list standard Filter-Prefix
 permit 172.21.1.0
ip access-list standard NextHopACL
 permit 192.168.201.3
 permit 192.168.201.2
ip access-list standard Redes-a-CLIENTE
 permit 192.168.63.16 0.0.0.15
 permit 10.181.0.0 0.0.255.255
 permit 99.90.16.0 0.0.0.255
 permit 192.168.219.0 0.0.0.255
 permit 223.223.223.0 0.0.0.255
 permit 192.168.220.0 0.0.0.255
 permit 10.6.13.0 0.0.0.255
 permit 10.6.14.0 0.0.0.255
 permit 10.6.15.0 0.0.0.255
 permit 10.6.16.0 0.0.0.255
 permit 10.6.17.0 0.0.0.255
 permit 10.6.18.0 0.0.0.255
 permit 10.6.19.0 0.0.0.255
 permit 10.6.20.0 0.0.0.255
 permit 10.6.21.0 0.0.0.255
!
ip access-list extended DataEspecialList
 permit ip host 10.51.67.144 host 10.55.231.26
 permit ip host 192.168.201.5 host 10.57.0.4
 permit ip host 10.51.67.201 host 10.7.0.13
 permit ip host 10.51.67.201 host 10.7.0.29
 permit ip host 10.51.67.201 host 10.55.231.27
ip access-list extended DataNormalList
 permit ip host 10.51.4.57 host 10.55.231.26
ip access-list extended DataPlusList
 permit ip host 192.168.214.213 host 10.55.228.182
 permit ip host 192.168.214.213 host 10.55.228.183
 permit ip host 192.168.214.213 host 10.55.228.184
 permit ip host 10.52.24.18 host 10.55.231.51
 permit ip host 10.52.24.19 host 10.55.231.51
 permit ip host 10.52.24.18 host 10.55.231.52
 permit ip host 10.52.24.19 host 10.55.231.52
 permit ip host 10.51.4.88 any
ip access-list extended RATE_LIMIT
 permit ip any host 99.95.140.224
 permit tcp any host 192.168.235.80 eq 41
 permit ip any host 192.168.235.80
ip access-list extended RealTimeVoiceList
 permit ip host 10.255.251.3 any
 permit ip host 10.255.251.35 any
 permit udp any range 16384 32767 any
 permit ip host 10.255.251.11 any
 permit ip host 10.255.251.27 any
 permit ip host 10.255.251.19 any
 permit udp any any range 16384 32767
 permit ip host 10.255.251.56 any
 permit ip host 10.255.251.67 any
ip access-list extended RealTimeVoiceList-IN
 permit udp any any range 16384 32767
 permit udp any range 16384 32767 any
 permit tcp any any eq 1720
 permit tcp any eq 1720 any
!
!
ip prefix-list Proveedor seq 5 permit 10.6.20.16/29
ip prefix-list Proveedor seq 10 permit 10.6.2.0/24
ip prefix-list Proveedor seq 15 permit 10.6.3.0/24
ip prefix-list Proveedor seq 20 permit 10.6.4.0/24
```

```
ip prefix-list Proveedor seq 25 permit 10.6.5.0/24
ip prefix-list Proveedor seq 30 permit 10.6.6.0/24
ip prefix-list Proveedor seq 35 permit 10.6.7.0/24
ip prefix-list Proveedor seq 90 permit 10.6.18.0/24
ip prefix-list Proveedor seq 95 permit 10.6.19.0/24
ip prefix-list Proveedor seq 100 permit 10.6.20.0/24
ip prefix-list Proveedor seq 105 permit 10.6.21.0/24
ip sla responder
ip sla 100
 icmp-echo 189.206.209.153 source-ip 189.206.209.154
 timeout 2000
 threshold 1000
 frequency 3
ip sla schedule 100 life forever start-time now
access-list 1 permit 10.7.0.11
access-list 1 permit 10.7.0.10
access-list 50 deny   101.30.224.224
access-list 50 permit any
access-list 91 permit 189.206.211.19
access-list 91 remark CA eHealth
access-list 91 permit 189.206.214.17
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 privilege level 15
 no login
!
exception crashinfo buffersize 80
!
end!
```

Verificación del estado del HW

```
7604-4-263#show module 1
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  1    2  Route Switch Processor 720 (Active)    RSP720-3C-GE       JAE1332FYZL

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  1  001c.584e.853c to 001c.584e.853f   5.9   12.2(33r)SRD 12.2(33)SRD4 Ok

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ------------ ------- -------
  1  Policy Feature Card 3       7600-PFC3C         JAE1332G8M5  1.2    Ok
  1  C7600 MSFC4 Daughterboard   7600-MSFC4         JAE1332G8WZ  1.4    Ok

Mod  Online Diag Status
---- -------------------
  1  Pass

7604-4-263#sh module 4
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  4   40  7600 ES+                               7600-ES+40G3CXL    JAE13136E56

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  4  0024.f94c.a970 to 0024.f94c.a9cf   1.0   12.2(33r)SRD 12.2(33)SRD4 Ok

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ------------ ------- -------
  4  7600 ES+ DFC XL             7600-ES+3CXL       JAE131261G5  1.0    Ok
  4  7600 ES+ 40xGE SFP          7600-ES+40G        JAE131051ZK  1.0    Ok

Mod  Online Diag Status
---- -------------------
```

```
4  Pass
```

Estos resultados fueron compartidos con el cliente, dándole así la garantía de que su configuración inicial con los features críticos como WCCP sería soportado en la nueva plataforma, y además de que la nueva plataforma operase correctamente con todo su nuevo HW.

4.3.4.5 Determinación de una línea base de desempeño de los equipos actuales

Como se explicó en la sección 3.5.1, una línea base es el nivel de desempeño que es aceptable cuando el sistema está manejando una carga de tráfico típica. Para este proyecto, el sistema son los routers 7204 VXR a ser sustituidos.

Los parámetros que se seleccionaron para determinar la línea base en los routers 7204 VXR fueron:

- Uso de memoria
- Uso de CPU
- Porcentaje de utilización de BW en sus diferentes enlaces

Para tener una muestra representativa de los valores anteriores se eligió un periodo de tiempo de 90 días. La responsabilidad de la obtención de estos valores recayó en el ISP encargado de administrar la red del cliente.

La siguiente figura muestra las gráficas proporcionadas por el cliente respecto al % de uso de CPU y BW:

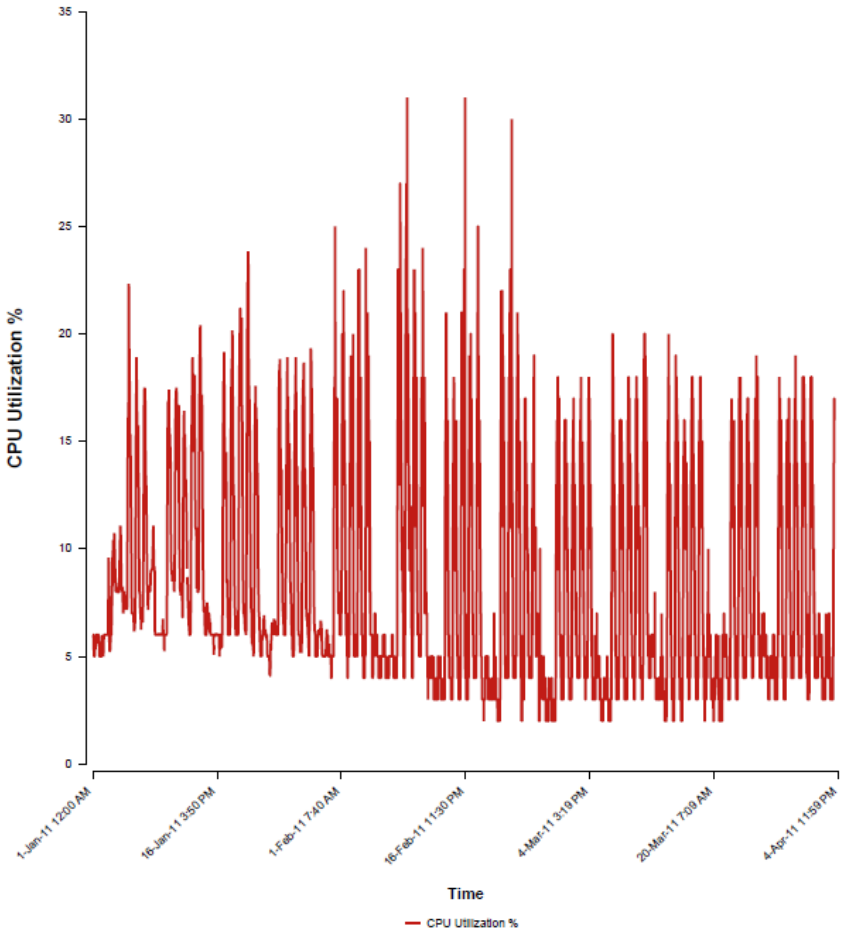

Figura 19. Utilización de CPU en 90 días, router 7204 VXR

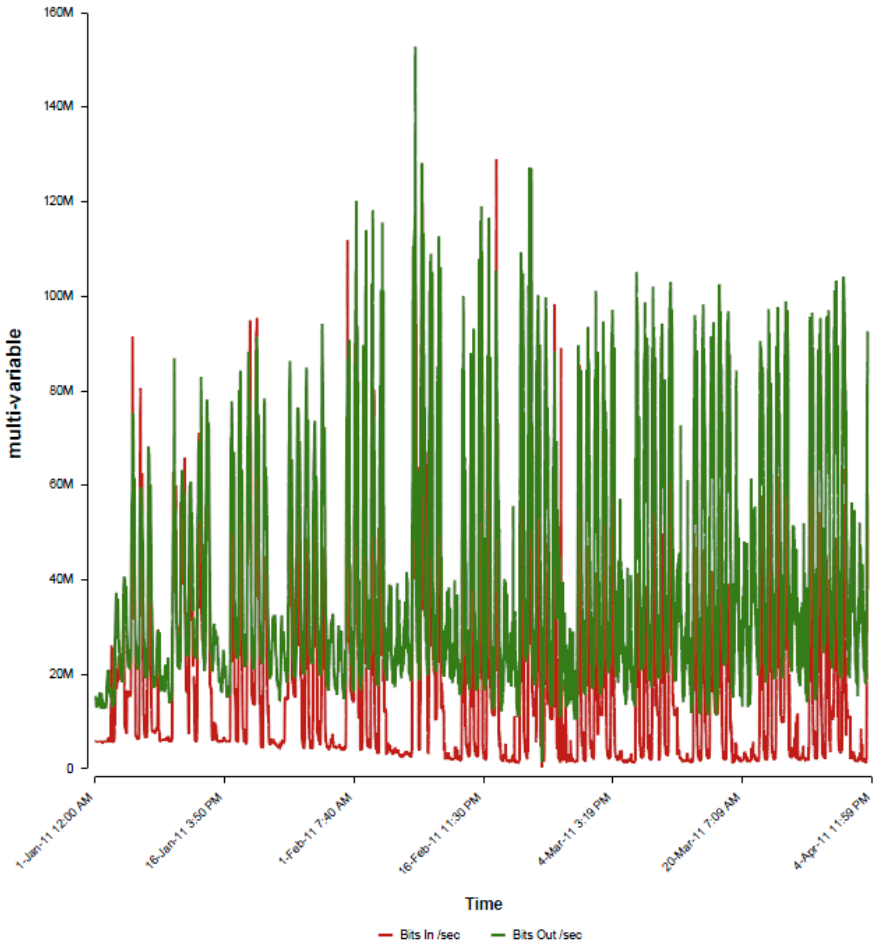

Figura 20. Utilización de BW Enlace WAN en 90 días, router 7204 VXR

Las tablas anteriores constituyen la línea base sobre la cual se compararía el desempeño una vez realizada la sustitución de los equipos.

4.3.4.6 Sustitución de los routers actuales por los nuevos 7604 sin activar WCCP

Una vez probado el HW y SW en laboratorio, así como habiendo sido determinada una línea base, procedí a apoyar al ISP en la sustitución de los routers actuales 7204 VXR por los nuevos 7604. Esta actividad implicaba afectación a todos los servicios, de modo que tuvo que realizarse por la noche.

Mi papel en este punto fue el realizar la coordinación de las actividades durante una ventana de mantenimiento nocturna, con duración aproximada de 6 horas. La coordinación fue realizada remotamente, mientras que las actividades en sitio fueron realizadas por personal del ISP. El cliente participó verificando que los servicios afectados fueran restaurados sin problema alguno.

Durante la ventana se verificó que las siguientes funcionalidades críticas funcionaran perfectamente:

- Conexiones Físicas

- Protocolos de Enrutamiento OSPF y BGP
- Autenticación, Autorización y Accounting (AAA)
- Monitoreo vía SNMP
- Switching en Capa 2
- Mecanismos de Alta Disponibilidad (tanto en HW como de next-hop)

Una vez instalados los nuevos equipos, se definió un periodo de 2 semanas para monitorear su comportamiento exhaustivamente, principalmente los parámetros de la línea base previamente definida.

No se consideró la activación de WCCP en esta actividad debido a que, como en los routers 7204 VXR anteriores la activación de WCCP fue la que provocó problemas de performance, opté por recomendar analizar el comportamiento de los 7604 con todas sus funcionalidades excepto WCCP, para poder tener certeza de que su operación fuera normal y poder discernir si WCCP volvía a presentar inconvenientes.

Cabe destacar que los routers 7204 VXR anteriores no fueron retirados del Centro de Datos, sino que la instalación de los nuevos se realizó instalándolos en racks nuevos y empleando nuevas fibras, para que en caso de falla, se pudieran conectar los routers anteriores simplemente intercambiando enlaces de fibra.

4.3.4.7 Activación de WCCP y monitoreo de servicios

Después de la instalación de los nuevos routers 7604, se procedió con la habilitación de WCCP. Como se explicó en secciones anteriores, WCCP trabaja en conjunto con WAEs. El router en donde se habilita WCCP realiza la redirección de las solicitudes de los hosts, mientras que los WAEs se encargan de optimizar el flujo de cada aplicación a optimizar a través de la red WAN.

En esta etapa recomendé habilitar WCCP únicamente sin optimizar las aplicaciones. El objetivo fue que como NCE tuviera oportunidad de analizar de forma separada la operación de WCCP (redirección de solicitudes de contenido), sin introducir en la ecuación los WAEs.

Se verificó que WCCP operara correctamente en los siguientes rubros:

- A nivel de interface
- Que los WAEs configurados dentro del grupo de servicio fueran visibles y alcanzables desde el router
- Que la redirección de paquetes hacia los WAE funcionara correctamente

Para la verificación a nivel de interface se ejecutó el comando **`show ip wccp interfaces`**. El output de dicho comando fue el siguiente:

```
7604-4-263# show ip wccp interfaces

WCCP interface configuration:
```

```
GigabitEthernet0/0/0

    Output services: 1
    Input services: 1
    Mcast services: 0
    Exclude In:      FALSE


GigabitEthernet0/0/1

    Output services: 1
    Input services: 1
    Mcast services: 0
    Exclude In:      FALSE

Vlan101

    Output services: 1
    Input services: 1
    Mcast services: 0
    Exclude In:      FALSE
```

Con el comando anterior verifiqué que WCCP operaba correctamente en las interfaces que fue habilitado.

Para verificar si los WAEs definidos eran vistos por el router 7604 se configuraron 2 WAEs dentro del grupo de servicio. Dicha verificación se realizó con el siguiente comando:

```
7604-4-263# show ip wccp 1 view

WCCP Cache Engines Visible

 10.168.88.11

 10.168.88.12

WCCP Cache Engines Not Visible:

 -none-
```

Ambos WAEs eran visibles y se podían alcanzar desde el router, con lo cual esta parte de la verificación funcionó correctamente

Respecto a la redirección, los comandos que se emplearon para la verificación de su funcionamiento fueron los siguientes:

```
7604-4-263# show ip wccp 61 detail

 WCCP Client information:
 WCCP Client ID: 10.1.1.14
 Protocol Version: 2.0
 State: Usable
 Redirection: GRE
 Packet Return: GRE
 Assignment: HASH
 Initial Hash Info: 00000000000000000000000000000000000000000000000000000000000000000000
 Assigned Hash Info: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
 Hash Allotment: 256 (100.00%)
 Packets Redirected: 678182
 Connect Time: 00:01:56
 Bypassed Packets
 Process: 0
 CEF: 0
```

Como se puede observar, el router estaba realizando exitosamente la redirección de paquetes hacia el WAE

4.3.4.8 Optimización gradual de diferentes aplicaciones

La fase de optimización gradual de aplicaciones se trabajó de cerca con el cliente, solicitándoles la lista de aplicaciones que deberían ser optimizadas. En este punto, el WAE comenzó a realizar su labor al optimizar los flujos de las aplicaciones definidas a través de la red WAN. El monitoreo del WAE y la comparación del desempeño de las aplicaciones antes y después de la aplicación fue realizado mediante aplicaciones propias del ISP.

Mi labor en esta parte fue validar la estrategia para analizar el desempeño y proveer algunos consejos para un monitoreo más efectivo, en conjunto con otros miembros del equipo de Cisco especializados en tecnologías de Data Center.

4.3.4.9 Retiro de routers 7204 VXR y Conclusión del Proyecto

Una vez transcurrido el periodo de dos semanas definido para monitorear el funcionamiento de los nuevos equipos 7604, se pudieron retirar sin problemas los equipos anteriores 7204 VXR, habiendo sido verificada en vivo la estabilidad y correcta operación de los nuevos equipos.

Al retirar los equipos anteriores del Centro de Datos y validar que el desempeño de los equipos nuevos en general, poniendo especial énfasis en la operación de la redirección de WCCPv2 y la optimización de aplicaciones en la red WAN, el proyecto pudo darse por concluido exitosamente.

4.3.5 Resultados y Aportaciones

Como resultado de este proyecto, destaca lo siguiente:

- Mi reputación y la de Cisco Systems como Consultor Técnico confiable se incrementó, al liderar exitosamente este complejo proyecto. Además, al estar estas actividades fuera del alcance de un contrato de NOS regular, se le ofreció un servicio de valor agregado al cliente.
- El cliente quedó muy satisfecho al constatar una mejora significativa en los tiempos de respuesta de sus aplicaciones optimizadas
- El desempeño de los nuevos equipos 7604 no se vio comprometido de forma alguna al activar WCCPv2, aumentando la estabilidad, seguridad, confiabilidad y capacidad de manejo de datos en el Centro de Datos.
- La realización de pruebas en laboratorio en un equipo real permitió identificar problemas potenciales antes de la implementación, con lo que se pudo notificar con la antelación necesaria al personal involucrado, reduciendo así la posibilidad de enfrentar situaciones no previstas.
- La conclusión exitosa de este proyecto benefició no solo al cliente o a Cisco Systems, sino principalmente a las personas que realizan sus declaraciones de impuestos vía Internet, ya que ahora los tiempos de respuesta y la capacidad de manejo de tráfico se incrementaron.