1 PROBLEMA

En una arquitectura de red compleja el mas minimo detalle produce grandes fallas por lo cual hay que ser minucioso con todos los aspectos de configuración, en el caso de Clover una combinacion de pequeños problemas lograron una inestabilidad en la red; los problemas se generaron progresivamente con el crecimiento de la emrpesa y con el requerimiento de nuevos servicios se hicieron mas evidentes los defectos en el diseño de la red. A continuación en el diagrama 1.1 se aprecia las diferentes variables que generaron los problemas internos de la compañía.

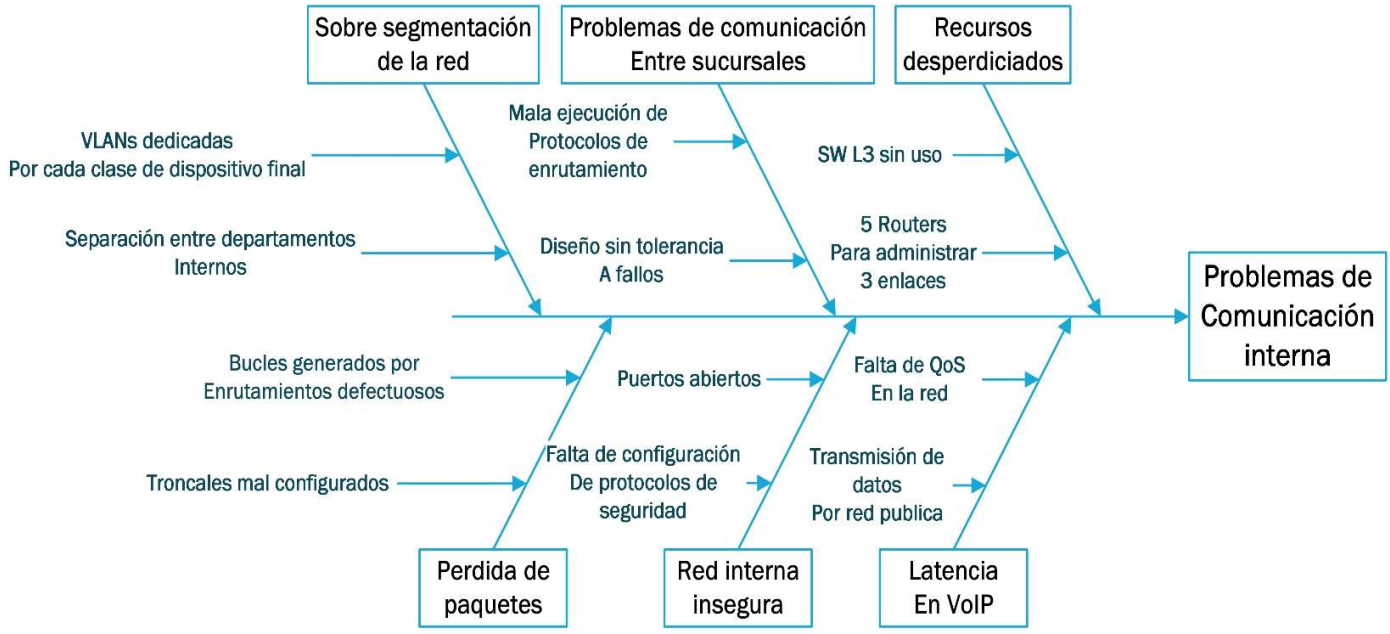


Diagrama 1.1 "*Causa efecto*"

La sobre segmentación de la red, los problemas de comunicación entre sucursales, el diseño sin tolerancia a fallos, falta de configuración de seguridad y QoS son algunos de los factores que van sumando en contra de la eficacia de la red interna de la compañía, dando como resultado perdidas de tiempo en la ejecución de las tareas diarias. En el mundo moderno la perdida de tiempo se traduce en perdida de dinero para las empresas de cualquier tamaño, la frutración de los usuarios tambien es un gran factor que se refleja en su productividad, cosa que pasa cuando los servicios tecnologicos no se ejecutan correctamente.

2 SOLUCIÓN

Por motivos de confidencialidad los equipos, direcciones IP, conexiones en puertos e ISP han sido cambiados al igual que algunas soluciones no se pueden ni detallar como la interconexión de sucursales, VPNS y encriptación de información.

Para la cantidad de fallas que presentaba la red lo más adecuado era cambiar el diseño actual en ese momento por un diseño que cumpla con los cuatro pilares de la arquitectura de red que son:

- Escalabilidad
- Tolerancia a fallos
- QoS
- Seguridad

Escalabilidad

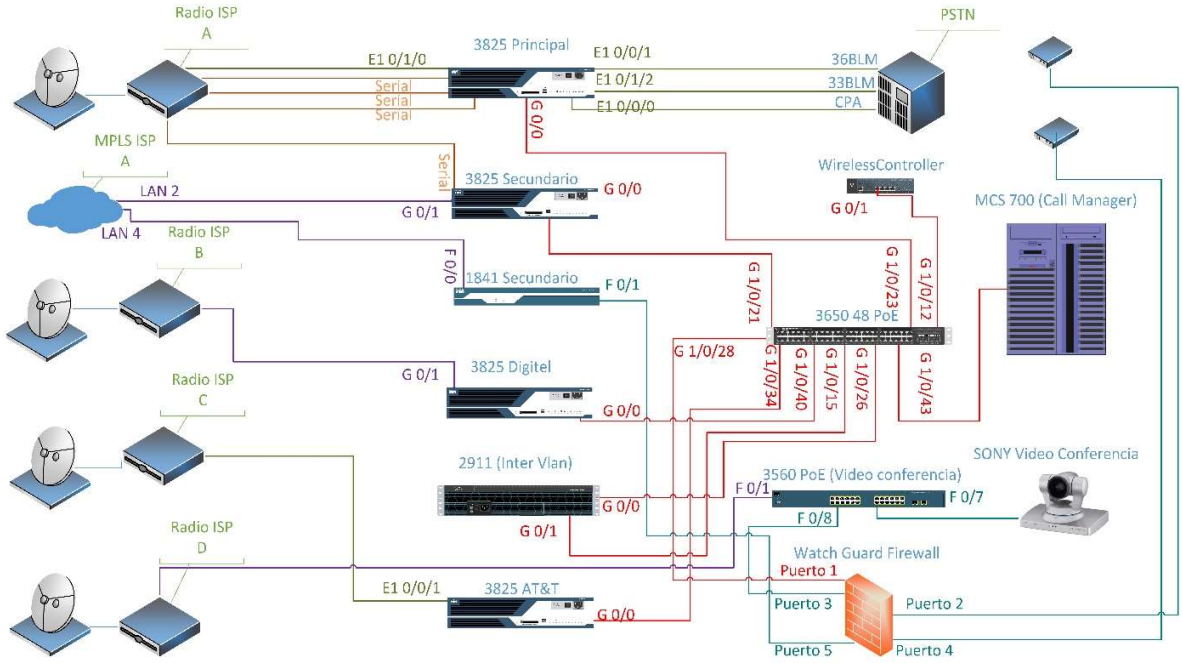
La característica de anticipar el crecimiento de la red y poder soportarlo, es necesario hacer una proyección en el crecimiento de la empresa para determinar de forma correcta no solo el pool de direcciones IP sino también los equipos necesarios para implementar la red, los servicios que se pueden entregar a los usuarios y soportar un posible cambio de tecnología. Con respecto a la escalabilidad se hizo un cambio importante en la segmentación de red, reduciendo el número de VLANS como se aprecia en el cuadro 1.1:

Vlan	RED	Rango Sub RED	Mascara	Host	ID Vlan
Admin	10.20.0.0	10.20.0.1 - 10.20.0.63	255.255.255.192	62	1
Datos	10.20.2.0	10.20.2.1 - 10.20.3.254	255.255.128.0	510	2
Voz	10.20.4.0	10.20.4.1 - 10.20.5.254	255.255.128.0	510	3
Servidores	**10.17.0.65**	**10.17.0.66 – 10.17.0.128**	**255.255.255.192**	**62**	17
	10.17.0.129	**10.17.0.130 - 10.17.0.192**	**255.255.255.192**	**62**	21
	10.17.1.65	**10.17.1.66 - 10.17.1.128**	**255.255.255.192**	**62**	18
	10.17.10.0	**10.17.10.1 - 10.17.10.63**	**255.255.255.192**	**62**	11
Acceso	10.17.30.0	10.17.30.1 - 10.17.30.63	255.255.255.192	62	30
Videoconferencia	10.17.20.0	10.17.20.1 - 10.17.20.12	255.255.255.240	14	20

Cuadro 1.1 *"Tabla de VLANs"*

Las VLANs de servidores no se modificaron por cuestiones de configuración de sistemas internos, lo que se muestra es la restructuración, anteriormente la tabla de VLANs contaba con 20 VLANs diferentes entre ellas una dedicada para impresoras, teléfonos inteligentes de empleados y una aparte para ejecutivos creando de esta manera una red con sobre segmentación por otro lado en el área de diseño

los equipos estaban muy mal administrados teniendo una cantidad absurda de equipos para las necesidades de la empresa, aumentando sus costos de mantenimiento y administración de los equipos, a continuación en el esquema 1.1:



Esquema 1.1 *"Núcleo y distribución"*

De esta manera se obtiene un diseño escalable con redundancia de interconexiones y fácil administración de la red, usando los routers principales para manejar los enlaces en la capa de núcleo, con su respectiva redundancia e implementando router on a stick, donde el router InterVlan se encarga del enrutamiento interno de la red se consigue una red más limpia donde se puede administrar de manera más eficaz y aun con este esquema tratando de aprovechar todos los equipos existentes quedaron dos Routers fuera del diseño debido a que no eran necesarios, cabe destacar que el Firewall se maneja por separado mediante una tercera empresa.

Tolerancia a fallas

En otras palabras la red debe poder soportar que el fallo de alguna ruta o interconexión no afecte el desempeño de la misma, en el caso estudio a pesar de contar con múltiples proveedores ISP no había un sistema Failover que pudiera dar sustento a la red debido a una falla, el Failover se realizó con éxito entre 3 proveedores de internet, 22 sucursales y 3 países, por motivos de confidencialidad no se puede detallar la solución no obstante el ambiente de trabajo constaba de equipos netamente Cisco y con una peculiar dificulta por proveedores que mantienen DNS dinámicos e incluso combina varios tipos de tecnología de última milla.

QoS (Calidad de servicio)

Posiblemente el requisito más importante a la hora de tener una red de nueva generación donde los equipos demandan un ancho de banda significativo y que hay que respetar el paso del tráfico para

garantizar un servicio óptimo, en el caso estudio el principal problema era alta latencia en las llamadas VoIP y perdida de paquetes en video llamadas, la solución para este problema en particular es la aplicación de políticas de control de calidad como garantizar el ancho de banda en la red, priorización de los paquetes conjunto de enlaces MPLS para lograr un canal limpio para el tráfico y por último en el apartado físico un cambio de estructura del cableado debido a que los equipos estaban muy alejados del nodo de acceso.

Seguridad

"Algunos detalles han sido obviados debido a términos de seguridad"

El factor más demandado de la industria sin duda alguna, en este caso solo se reforzó la seguridad interna debido a que una tercera empresa manejaba los firewall a nivel externo. La seguridad implementada se focalizo en los Switchs y en los Routers debido a que el 80% de los ataques informáticos provienen de una fuente interna, en el caso de los Switchs se aplicó políticas de seguridad donde se une la dirección MAC de los dispositivos finales con los puertos asignados en el Switchs con la acción de desconectar y apagar los puertos, de esta forma se asegura que el equipo asignado a ese punto sea el único que puede acceder a la red de manera cableada adicionalmente los protocolos de conexión externa han sido cambiados a SSH con un alto cifrado, en el lado de los Routers la seguridad se maneja con un servidor AAA para garantizar la entrada a los equipos conjunto de un servidor Sylog para poder corroborar las entradas al sistema.

3 RESULTADOS

Luego de dos arduos días de trabajo de implementación se logro los objetivos establecidos obteniendo como resultado una red de:

- Fácil administración y monitoreo
- Seguridad estable en la red interna
- Visión más amplia de las conexiones entre sucursales
- Estabilidad en comunicaciones VoIP y video llamadas
- Tolerancia a fallos
- Uso correcto de los equipos
- Documentación e identificación de toda la red
- Políticas de acceso y controles de mantenimiento

Una vez culminado el proyecto al cliente se entrega un documento con todo lo realizo durante el tiempo de trabajo, las configuraciones, planos detallados de conexiones, enlaces realizados y sugerencias para mantener una red en optimo uso al igual que el servicio de monitoreo 24/7.

¿Qué se necesitó para la implementación de proyecto?

Un equipo, que contaba de:

- 1 ingenieros de redes
- 4 técnicos de cableado estructurado

El diseño del proyecto tomo alrededor de 3 semanas de planeación y prueba todas las acciones fueron previamente probadas en un laboratorio contando con fases de simulación virtuales y físicas antes de poder implementar la solución.