ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“DISEÑO E IMPLEMENTACIÓN DE LA RED DE UN SISTEMA DE TRANSPORTE”

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

AUTOR:

RONALD EDUARDO ORELLANA VERDEZOTO

GUAYAQUIL, OCTUBRE 2021

AGRADECIMIENTO

Quiero expresar mi gratitud a Dios, quien con su bendición llena mi vida.

De igual manera agradezco a mi familia, pues es mi soporte en los buenos y malos momentos.

A mis compañeros de maestría, quienes son parte fundamental de este proceso y a ESPOL que a pesar de las adversidades de la pandemia brindó los mecanismos necesarios para finalizar el programa académico.

DEDICATORIA

Este trabajo está dedicado a mis padres Eduardo y Jakie, quienes con su amor, paciencia y esfuerzo me han permitido cumplir este sueño; gracias por inculcar en mí el ejemplo de esfuerzo y valentía, pero sobre todo, de no temer a las adversidades.

A mi hermana Arianna, quien ha sido mi orgullo y mi motivación para ser mejor y superarme cada día.

A mi novia Karem, quien estuvo junto a mí siempre, apoyándome a lo largo de este camino.

TRIBUNAL DE SUSTENTACIÓN

.....	.....
MISG. Lenin Freire Cobo	**MSIG. Juan Carlos García**
COORDINADOR MSIG	PROFESOR MSIG

RESUMEN

El presente documento tiene como objetivo informar el desarrollo del diseño e implementación de la red que tiene un sistema de transporte, así como los diferentes protocolos utilizados y sistemas empleados.

En cada sección se detallan las configuraciones que tiene la red considerando: segmentación de redes, topología redundante, seguridad, gestión, escalabilidad, confiabilidad y disponibilidad.

Palabras Clave: Anillo, localidad, switch, nodo de acceso, vlan, CdC.

ÍNDICE GENERAL

ABREVIATURAS

BOL	Sistema de Tickets
CdC	Cuarto de Control
CCTV	Circuito Cerrado de Televisión
CPE	Customer Premises Equipement
DNS	Domain Name System
EMP	Ethernet Management Port
FO	Fibra Óptica
GTC	Sistema de Gestión
IEEE	Institute of Electricals and Electronics Engineers
IP	Internet Protocol
LAN	Local Area Network
MEG	Sistema de Sonido
NMS	Network Management System
OLT	Optical Line Terminal
OSPF	Open Shortest Path First
PCR	Punto de Conexión de Red
SCA	Sistema de Control de Accesos
SFP	Small Form-factor Pluggable Transceiver
VC	Virtual Chasis

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Este proyecto corresponde a la infraestructura de red de un proyecto de transporte urbano masivo.

Existen 5 localidades distribuidas a lo largo de todo el recorrido: E1, E2, E3, E4, E5 y CdC (Cuarto de Control). El CDC no es una localidad de pasajeros como tal, pues se ubica en la misma edificación de la localidad 4.

El proyecto es el resultado de varios sistemas que conforman el sistema de transporte como tal: Tickets (BOL), Sonido (MEG), Monitoreo (GTC), CCTV, Telefonía (TEL/INT), Controles de Acceso (SCA), Red Corporativa (CORP), Internet y, por supuesto, la infraestructura de red que permite la integración de todo lo mencionado.

La red es la infraestructura de red que efectúa el papel de columna vertebral de todos los sistemas de transporte mencionados.

CAPÍTULO 1

GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA

El proyecto está comprendido por 5 localidades y una sala de supervisión (CDC), las cuales constan de varios sistemas como: CCTV, Telefonía, Tickets, Control de accesos, Gestión técnica centralizada, Wifi, entre otros, y deben comunicarse entre sí a través de la red.

Dada la necesidad planteada en los requerimientos funcionales del proyecto y del sistema, se debe diseñar y dimensionar la infraestructura requerida en equipamiento activo y pasivo.

A continuación, se realizará un análisis de los requerimientos que afectaron al diseño de la infraestructura de red desde los siguientes

puntos de vista:

- Topología física de red
- Roles especiales de ciertas localidades
- Características de alta disponibilidad
- Requerimientos lógicos de red

En los casos que sea necesario se abordarán detalles específicos del diseño.

1.1.1 DE LA TOPOLOGÍA FÍSICA DE LA RED

A continuación, se efectuará una descripción de cómo se realizó la distribución de las localidades, cómo se interconectan entre ellas y los sistemas hacia estas:

- Existen 5 localidades distribuidas durante todo el recorrido: E1, E2, E3, E4, E5 y CDC (Centro de Control). Esta última no es una localidad de pasajeros, pues se ubica en la misma edificación de la localidad 4.
- Si bien CDC no es una localidad de pasajeros adicional como tal, en la topología física y lógica (que se analizará más adelante) es considerada como si lo fuera, es independiente.
- Las seis localidades están enlazadas por fibra óptica de manera que se conforme un anillo, lo cual implica que habrá

redundancia en las rutas para alcanzar una determinada localidad en cada momento. Una ruta horaria y otra antihoraria.

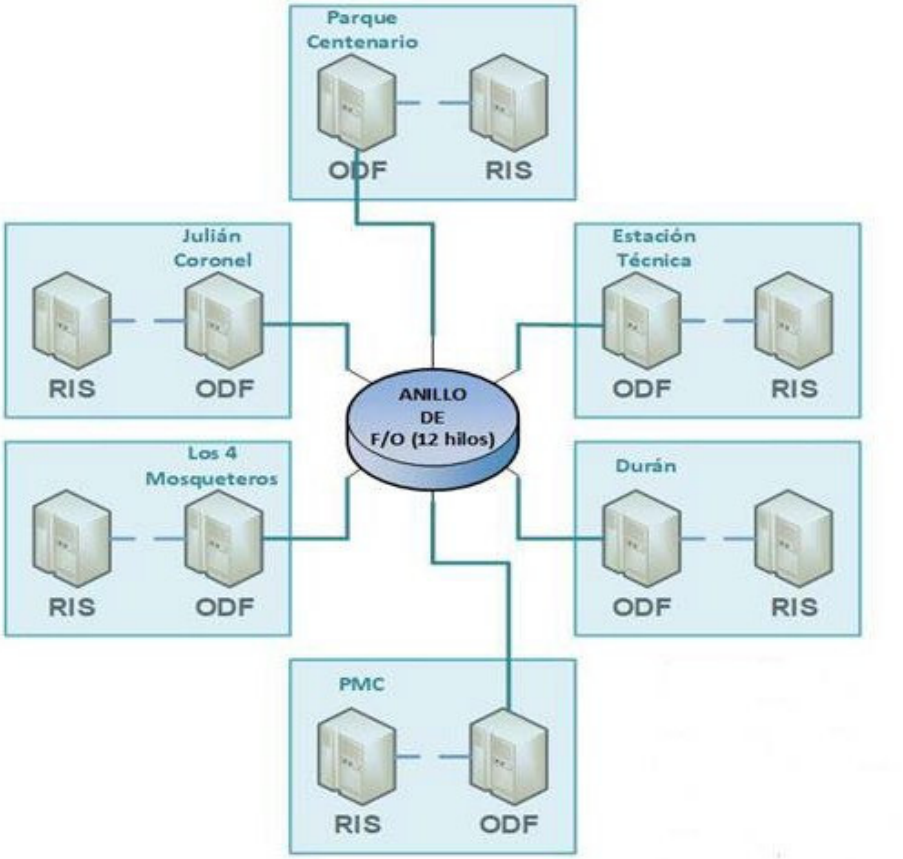

Figura 1.1. Topología física localidades.

Fuente: Autor

- El equipamiento que permitió la conformación del anillo fueron switches denominados de nodo acceso. Los equipos usados son de alta conmutación con capacidad de enlaces de fibra óptica a 10 Gbps y características de un Core de datos.

- Al interior de cada localidad, los diferentes sistemas de transporte se diseñaron para que se conecten a los switches de nodo de acceso.

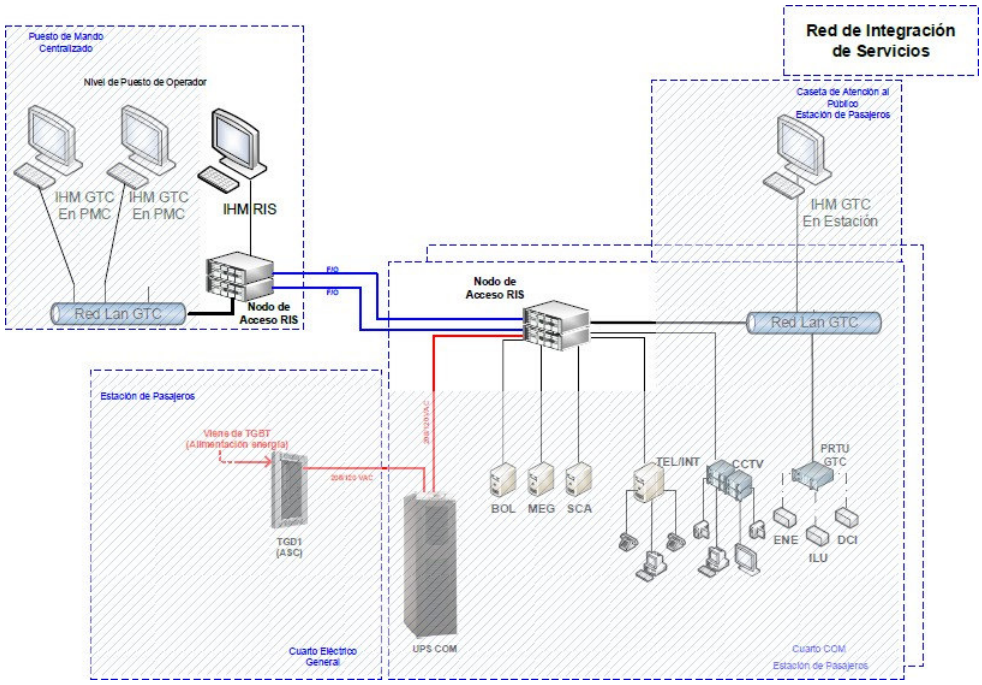

Figura 1.2. Topología física localidades (2).

Fuente: Autor

- Es importante mencionar que cada sistema tiene su propio switch, que a su vez se conecta al switch de nodo acceso como se mencionó anteriormente.
- En definitiva, la topología de conexión física de la red es un anillo y cada nodo miembro de este es el centro de una topología anidada en estrella, si se considera la conexión de los switches de sistemas de transporte.

- Es necesario recalcar que los switches usados por los sistemas de transporte de CCTV, Red Corporativa (CORP) y Telefonía (TEL/INIT) poseen la característica PoE+ (802.3at). Esto se debe a que se requiere que se alimenten cámaras propias del sistema de CCTV y también teléfonos IP respectivamente.

1.1.2 DE LOS ROLES ESPECIALES DE LAS LOCALIDADES

Más adelante, en la sección de diagramas de red, se evidenciará que, aunque todas las localidades son similares, existen ciertas diferencias en el rol asignado especialmente a algunas de ellas:

- En CDC, aunque esta ubicación no es una localidad, topológicamente se la trata como una más. CDC, desde el punto de vista de infraestructura de red, tiene asignado el rol de congregar todos los servidores de los diferentes sistemas de transporte.
- En este sentido, los switches de nodo de acceso proporcionan la conectividad necesaria para que los servidores pueden comunicarse al resto de la red. Es importante nuevamente enfatizar que los servidores de cada sistema se interconectarán a un switch de borde, el que finalmente se conecta hacia el switch de nodo de acceso.

- En esta localidad, por ejemplo, se conectan los Call Servers de la PABX OXE, los NVR (Network Video Recorder) de CCTV, PIS (Passenger Information System) de Sonido, etc.
- En esta localidad también se interconectan los switches de las Pilonas en cascada a través del switch de CCTV. Además, se ubica el servidor NTP.
- En la localidad 4 es donde llegan los proveedores de otros servicios externos. Aquí es donde se interconectan los CPE (Customer Premises Equipment) de dichos servicios. Aquí se conectan los firewalls y se administra la conectividad externa.
- Es un rol importante de esta localidad el redistribuir a las demás localidades el acceso a estos servicios externos. Un claro ejemplo de esto se encuentra en el acceso a Internet y a la troncal SIP – PSTN. Oportunamente se analizará cómo son las conexiones y los mecanismos de distribución.
- De manera adicional, aquí se interconectan ciertos equipos que también permiten la interconexión de servicios exterior como por ejemplo las cámaras moviles, y Access Points para la provisión de WiFi.

1.1.3 DE LAS CARACTERÍSTICAS DE ALTA DISPONIBILIDAD

El diseño para la red que soportará las operaciones de todos los sistemas de transporte, debe cumplir con las siguientes características:

- Redundancia eléctrica: los componentes de la red deberán tener redundancia N+N a nivel de fuentes de poder. Es decir, si el equipo necesita 1 fuente de poder para operar a capacidad completa, deberá existir una fuente adicional de respaldo.
- Redundancia de Nodo: implica que no debe haber un único punto de falla en el acceso a la red. Es decir, se debe colocar redundancia N+N, lo que implica un razonamiento similar al del punto anterior. Dicho de otra manera, se debe colocar un equipo adicional al necesario.
- Redundancia de enlace: implica que los accesos vía Ethernet hacia los nodos de acceso también deben ser redundantes en el tipo N+N. Esto implica que para que haya redundancia de enlace, debe haber redundancia de nodo ya que un enlace será ocupado por cada nodo respectivamente. Una conexión hacia el nodo de acceso 1 y otra hacia el nodo de acceso 2.
- La redundancia de enlace no solamente implica el acceso hacia la red, sino que fundamentalmente entre los nodos también.

- Redundancia de rutas: esta característica es inherente y resultante de la descripción de funcionamiento, dado a la topología de conexión.
- Balance de carga: la redundancia de los tipos mencionados arriba no debe implicar que se tiene un dispositivo (o enlace) adicional en standby o espera. Se solicita que estos estén en modo activo – activo.

1.1.4 DE LOS REQUERIMIENTOS LÓGICOS DE RED

- En esencia, la topología lógica es la misma que la física, es decir un anillo en la conexión entre switches de nodo de acceso y una estrella anidada considerando las conexiones de los switches de cada sistema al nodo de acceso.
- Cada nodo de acceso es considerado una unidad enrutable independiente, es decir un Router, detrás del cual existe una colección de redes conectadas directamente con su propio direccionamiento de red (y por tanto VLAN independiente).
- Lo mencionado con anterioridad, permite enfatizar el hecho de que, considerando la topología en anillo, no existe un punto único de enrutamiento (o de Gateway por defecto) que permita las conexiones entre diferentes VLANs o hacia redes externas.

- En este sentido, cada switch de nodo de acceso es su propio Gateway por defecto de sus redes conectadas directamente y, a su vez, participa activamente como miembro de un protocolo de enrutamiento interno (IGP) por el cual este conoce cómo llegar hacia otras VLANs desde otros nodos de acceso o redes externas.
- El Protocolo de enrutamiento interno es aquel que posee las mejores características de convergencia, permite el cálculo de la mejor ruta en un instante dado y es flexible para la interacción con otros protocolos. Este es el caso de OSPF Unicast.
- Uno de los requerimientos fundamentales para el diseño de red es el tiempo de convergencia en caso de ruptura del anillo, el cual se ha puesto como límite máximo en 5 segundos. Esto se debe a que, como se ha mencionado, la topología de anillo permite dos rutas para alcanzar cualquier localidad en un momento dado. En este escenario, en caso de ruptura, el protocolo de enrutamiento debe converger rápidamente para continuar con las comunicaciones a través del segmento no afectado.
- Dado el requerimiento del punto anterior, resulta necesario modificar el comportamiento de OSPF para lograr una rápida

convergencia, esto se lo hará a través de la modificación de parámetros referentes a timers y a la inclusión de protocolos auxiliares como BFD (Bidirectional Forward Detection).

- El sistema de transporte de Sonido hará sus transmisiones desde CDC a través de un grupo de difusión. Esto hace necesaria la inclusión de un protocolo de enrutamiento multicast, por lo que por facilidad se ha escogido a PIM-SM.

1.1.5 DE LOS REQUERIMIENTOS DE MONITOREO NMS

- Se implementó un NMS (Network Management System) de la misma marca de los switches de nodo acceso y de los switches de borde donde se interconectaron los diferentes sistemas de transporte.
- El NMS permitió realizar tareas administrativas (monitoreo y configuración) a nivel de toda la infraestructura de red.
- Desde este software se monitorea gráficamente el estado de la topología global en infraestructura de red.
- El software posee un módulo de alarmas y notificaciones obtenidas vía SNMP con diferentes niveles de criticidad.
- Se obtiene reportes diarios sobre el desempeño de la red.

- Las configuraciones que pueden realizarse desde el NMS son a nivel de capa 2, típicamente a nivel de configuración de puertos y VLANS.
- El NMS permite tener varios perfiles de usuarios para el monitoreo y gestión de la plataforma.
- El software tiene las licencias pertinentes para permitir la conexión tanto de equipamiento de la misma marca como de terceros.
- En el CDC, ubicado en la Localidad 4, existe una computadora designada para el monitoreo de la solución. Su principal objetivo es la utilización del NMS.

1.2 SOLUCIÓN PROPUESTA

La red tiene como función principal permitir la comunicación entre los equipos de cada sistema, ubicados a lo largo de las diferentes localidades de la línea y conformando el Sistema Integral, permitiendo el transporte de datos, haciendo uso del medio Fibra Óptica, interconectando los diferentes sistemas que componen la red de telecomunicaciones y de supervisión/monitoreo de todas las localidades con el Centro de Control (“CDC”), obteniéndose en tiempo prácticamente real la información requerida por el personal que realiza las labores de supervisión de manera centralizada en toda la línea.

Dicho sistema está compuesto por equipos de red que concentran la información de los sistemas o servicios y la transmiten a través de la fibra óptica que interconecta cada localidad de la línea.

Los sistemas que hacen uso de la red son los siguientes:

- Sistema de Gestión Centralizada (GTC)
- Sistema de Control de Acceso (SCA)
- Sistema de Tickets (BOL)
- Sistema de Sonido (MEG)
- Sistema de Operación de los Equipos Teleférico (TLF)
- Sistema de Telefonía (TEL)
- Red Corporativa
- WIFI

Para esto, se implementó un anillo de fibra entre las 5 localidades y el CDC, segmentado en diferentes VLANs y de forma redundante, aplicando el modelo jerárquico de núcleo colapsado e implementando un esquema de seguridad perimetral de red.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1 DISEÑO

En esta sección se abordarán los diferentes aspectos del diseño de la red, entre ellos: temas de hardware, topologías implementadas, direccionamiento y configuraciones realizadas.

2.1.1 EQUIPAMIENTO Y SOFTWARE

Los switches empleados para el diseño fueron los siguientes:

- Nodos de acceso:
  - Switch capa 3 con 24 puertos 10/100/1000 y 4 uplinks a 10 Gbps en fibra.
  - Fuente de poder redundante para switches.

  - Transceiver para conexión de fibra óptica con capacidad a 10 Gbps.
  - Cable de stacking de 40 cm.
- Equipos de borde para sistemas de transporte:
  - Switch capa 2+ con 24 puertos 10/100/1000 y uplinks 1 Gbps en fibra. Este modelo es PoE+ (802.3at), lo que implica que los puertos pueden energizar un equipo hasta 30W. Será usado principalmente para energizar cámaras de CCTV y teléfonos IP. Estos switches son también ocupados para el sistema red corporativa (CORP)
  - Switch capa 2+ con 24 puertos 10/100/1000 y uplinks 1 Gbps en fibra. Este modelo no es PoE y será usado para los sistemas de Control de Acceso (SCA), Tickets (BOL)
  - Switch capa 2+ con 24 puertos 10/100/1000 y uplinks 1 Gbps en fibra. Este modelo no es PoE y será usado para el sistema GTC.
  - Tranceivers para conexión de fibra óptica con capacidad a 1 Gbps.
- Software NMS:
  - Omnivista 2500 NMS

2.1.2 DIRECCIONAMIENTO IP

Respecto del direccionamiento, se ha mencionado en secciones anteriores que cada nodo de acceso es un router independiente, sus redes conectadas directamente pertenecen a diferentes sistemas de transporte. Para el direccionamiento se escogió un patrón determinado que permite identificar rápidamente la pertenencia de una red y/o VLAN en particular:

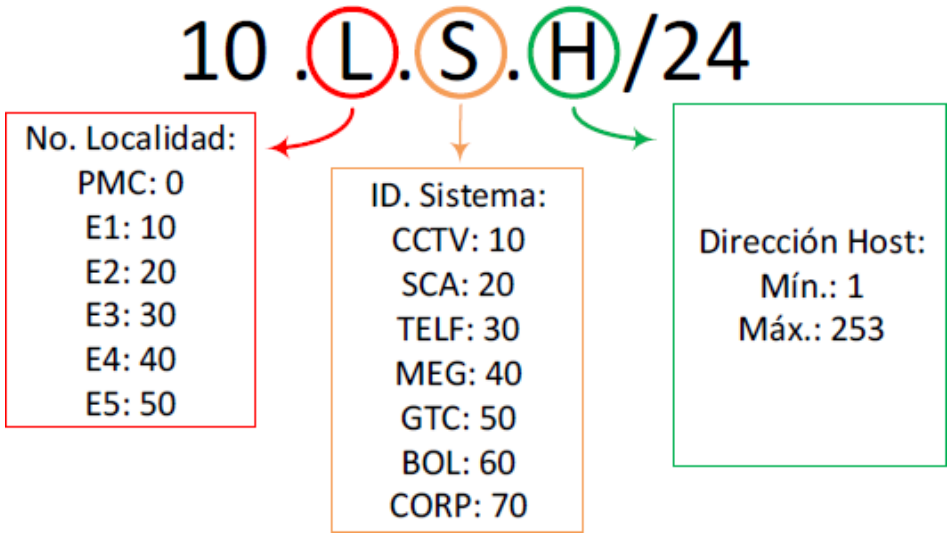

Figura 2.1. Patrón de direccionamiento IP

Fuente: Autor

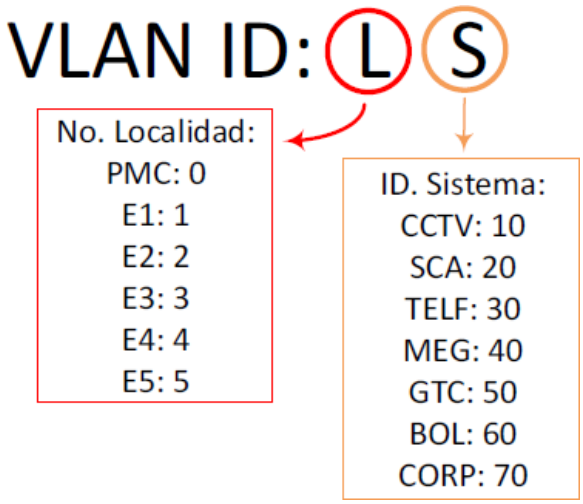

Figura 2.2. Patrón de ID de Vlans

Fuente: Autor

En la siguiente tabla se puede verificar la correspondencia entre redes de los sistemas de la red:

Localidad	Dirección de red	Gateway	Vlan ID	Sistema
CDC	10.0.10.0/24	10.0.10.254	10	CCTV
	10.0.20.0/24	10.0.20.254	20	SCA
	10.0.30.0/24	10.0.30.254	30	TELEFONÍA
	10.0.40.0/24	10.0.40.254	40	SONIDO
	10.0.50.0/24	10.0.50.254	50	GTC
	10.0.60.0/24	10.0.60.254	60	TICKETS
E1	10.10.10.0/24	10.10.10.254	110	CCTV
	10.10.20.0/24	10.10.20.254	120	SCA
	10.10.30.0/24	10.10.30.254	130	TELEFONÍA
	10.10.40.0/24	10.10.40.254	140	SONIDO

	10.10.50.0/24	10.10.50.254	150	GTC
	10.10.60.0/24	10.10.60.254	160	TICKETS
	10.10.70.0/24	10.10.70.254	170	CORPORATIVO
E2	10.20.10.0/24	10.20.10.254	210	CCTV
	10.20.20.0/24	10.20.20.254	220	SCA
	10.20.30.0/24	10.20.30.254	230	TELEFONÍA
	10.20.40.0/24	10.20.40.254	240	SONIDO
	10.20.50.0/24	10.20.50.254	250	GTC
	10.20.60.0/24	10.20.60.254	260	TICKETS
	10.20.70.0/24	10.20.70.254	270	CORPORATIVO
E3	10.30.10.0/24	10.30.10.254	310	CCTV
	10.30.20.0/24	10.30.20.254	320	SCA
	10.30.30.0/24	10.30.30.254	330	TELEFONÍA
	10.30.40.0/24	10.30.40.254	340	SONIDO
	10.30.50.0/24	10.30.50.254	350	GTC
	10.30.70.0/24	10.30.70.254	370	CORPORATIVO
E4	10.40.10.0/24	10.40.10.254	410	CCTV
	10.40.20.0/24	10.40.20.254	420	SCA
	10.40.30.0/24	10.40.30.254	430	TELEFONÍA
	10.40.40.0/24	10.40.40.254	440	SONIDO
	10.40.50.0/24	10.40.50.254	450	GTC
	10.40.60.0/24	10.40.60.254	460	TICKETS
	10.40.70.0/24	10.40.70.254	470	CORPORATIVO
	10.40.80.0/24	10.40.80.254	480	WIFI
	10.40.90.0/24	10.40.90.254	490	MULTICAM CABINAS

E5	10.50.10.0/24	10.50.10.254	510	CCTV
	10.50.20.0/24	10.50.20.254	520	SCA
	10.50.30.0/24	10.50.30.254	530	TELEFONÍA
	10.50.40.0/24	10.50.40.254	540	SONIDO
	10.50.50.0/24	10.50.50.254	550	GTC
	10.50.60.0/24	10.50.60.254	560	TICKETS
	10.50.70.0/24	10.50.70.254	570	CORPORATIVO

Tabla 1. Correspondencia VLANs, direcciones de red y sistemas de transporte.

Es importa mencionar que aparte del direccionamiento mostrado en la tabla anterior, también existe otro llamado de administración, el cual se usa para la gestión de la red en cuanto a configuración y monitoreo:

Localidad	Dirección de red	Máscara	Gateway	VLAN
CDC	10.0.1.1/26	255.255.255.192	10.0.1.1	1
E1	10.0.1.96/27	255.255.255.224	10.0.1.97	13
E2	10.0.1.128/27	255.255.255.224	10.0.1.129	14
E3	10.0.1.160/27	255.255.255.224	10.0.1.161	15
E4	10.0.1.192/27	255.255.255.224	10.0.1.193	16
E5	10.0.1.64/27	255.255.255.224	10.0.1.65	17

Tabla 2. Correspondencia VLANs, direcciones de red para gestión administrativa.

2.1.3 CONCEPTOS BÁSICOS

Virtual Chasis (VC)

Este es un grupo de switches que físicamente constituyen dispositivos separados pero que, previa habilitación de funciones y configuraciones, operan como entidades lógicas y administrativas únicas. Es decir, los dos switches en cada localidad del proyecto funcionan como un único switch, por lo cual se requiere una sola IP para su administración.

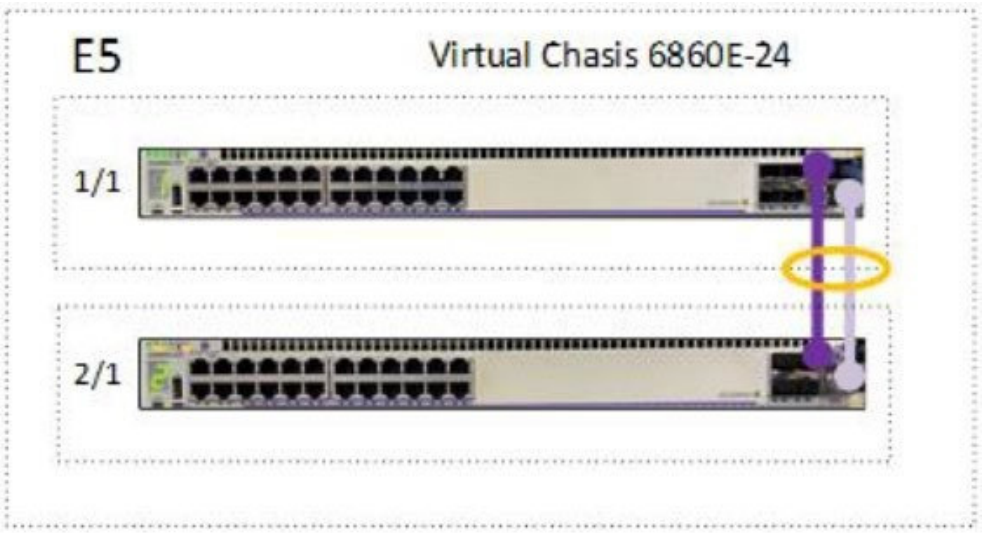

Figura 2.3. Virtual Chasis Localidad 5 (Nodo de acceso).

Fuente: Autor

En la figura 2.3 se puede observar la conformación de un Chasis virtual compuesto por dos switches. La administración y monitoreo de su comportamiento lógico se realizó a través de una única IP, para el ejemplo, fue la 10.0.1.65. La configuración en

este caso fue como de un chasis físico compuesto por dos slots identificados por la siguiente nomenclatura:

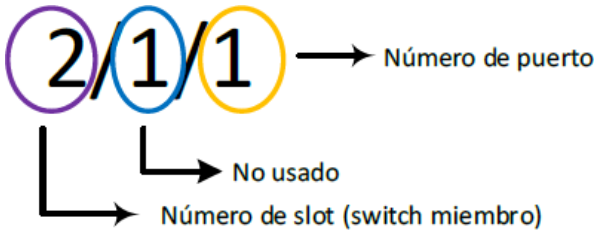

Figura 2.4. Nomenclatura puertos de Virtual Chasis.

Fuente: Autor

La unión de los switches individuales se realizó a través de puertos de alta conmutación Ethernet dedicados para el efecto. De tal manera que se utilizaron 2 puertos de 20 Gbps (40 Gbps FDX) cada uno, los cuales se interconectaron mediante cables llamados “Direct Attach Cables” que fueron fabricados para esta única función.

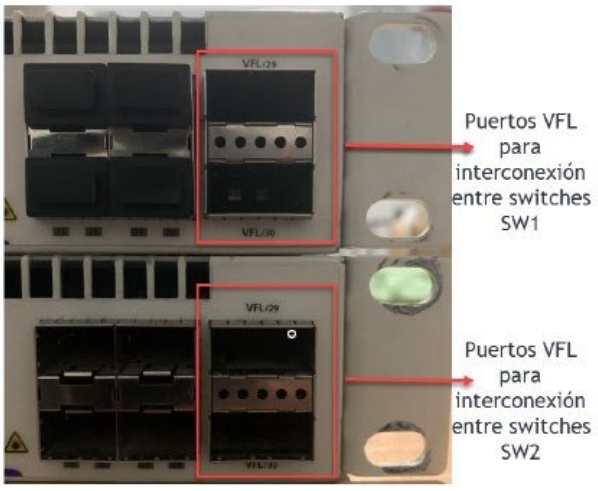

Figura 2.5. Puertos para conexión de DAC (Direct Attach Cables).

Fuente: Autor

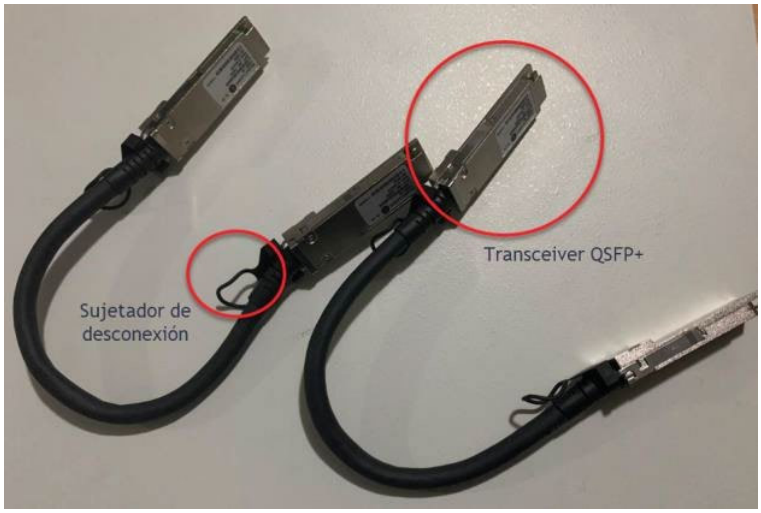

Figura 2.6. Direct Attach Cables (DAC).

Fuente: Autor

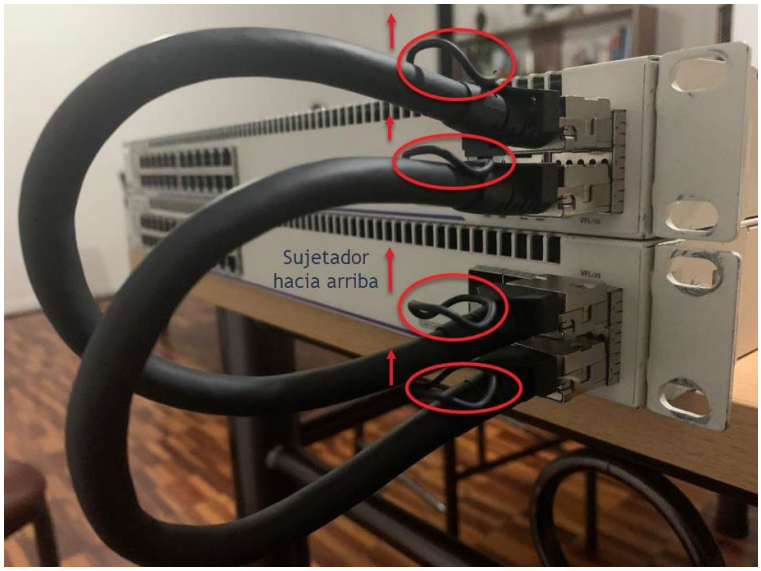

Figura 2.7. Conformación física de Virtual Chasis.

Fuente: Autor

Antes de abordar otros aspectos básicos del diseño, se explicará en esta sección la incorporación de redundancia a nivel eléctrico.

En los switches de nodo acceso, es posible interconectar una fuente adicional de poder. Esta fuente de poder adicional permite tener redundancia eléctrica de nivel N+N, es decir que al incorporar una nueva fuente, el switch podría soportar la pérdida total de una de sus fuentes y seguir funcionando a plena capacidad.

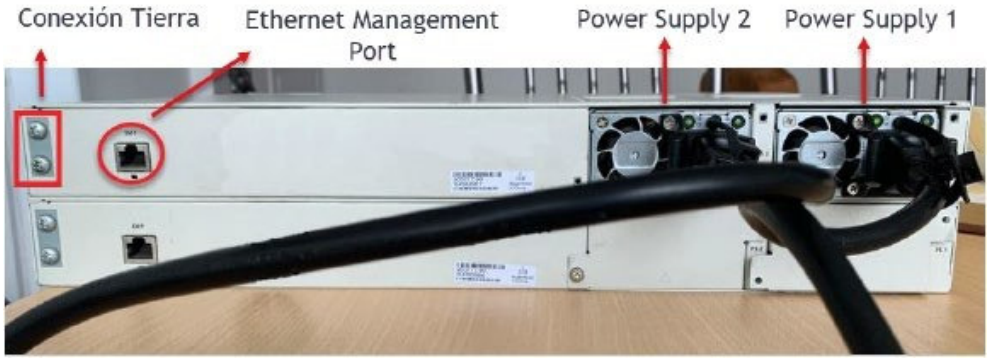

Figura 2.8. Conexiones eléctricas en Virtual Chasis.

Fuente: Autor

La figura anterior muestra la conexión de las fuentes de poder redundantes. En los data centers de cada localidad en el proyecto, los nodos de acceso tendrán redundancia completa al incorporar 4 fuentes de poder en todo el Virtual Chasis:

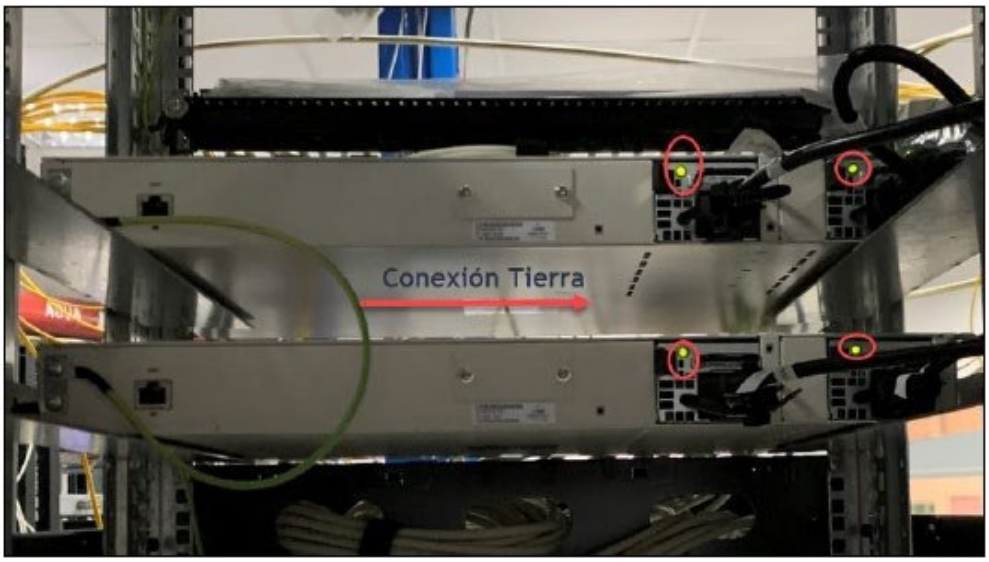

Figura 2.9. Fuentes de poder redundantes en Virtual Chasis.

Fuente: Autor

Es importante mencionar que la redundancia eléctrica es mucho más significativa e importante cuando las fuentes de poder se conectan a diferentes brakers o circuitos eléctricos de UPS, lo cual es de hecho implementado en la red.

Link Aggregation (LAG)

Esta es una funcionalidad en tecnología de Networking que permite multiplicar el ancho de banda disponible en una conexión entre dos dispositivos de red que se comunican a través de Ethernet. La idea fundamental es el balanceo de carga en el tráfico mediante enlaces redundantes entre dichos dispositivos.

En la aplicación, por ejemplo, se conectan dos switches a través de 2 enlaces Gigabit o 10 Gigabit Ethernet (podrían ser 4 o hasta 8 enlaces) redundantes. Los dispositivos extremos en lugar de censar un enlace de un Gigabit o 10 Gigabit Ethernet, establecen un enlace de 2 o 20 Gigabit Ethernet, dependiendo del número de conexiones agrupadas. Cada una de estas conexiones balancea la carga de tráfico y no constituyen un Bucle de capa 2.

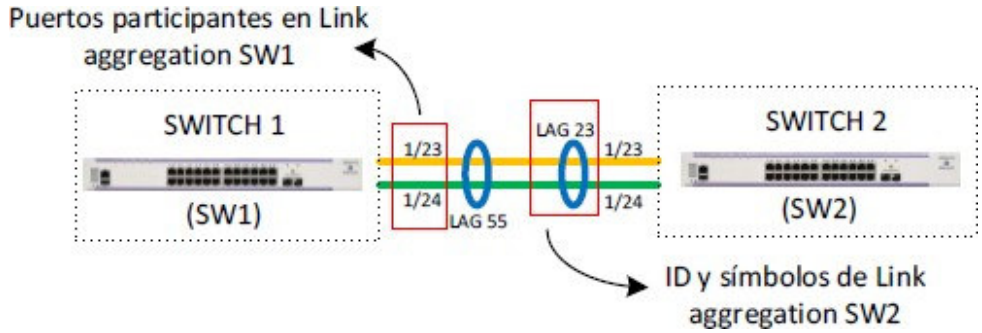

Figura 2.10. Representación y componentes Link Aggregation.

Fuente: Autor

2.1.4 CONFORMACIÓN DE TOPOLOGÍAS GLOBALES Y POR LOCALIDAD

Una vez conocido el hardware a utilizarse, el direccionamiento, los diferentes requerimientos y algunos conceptos básicos, se analizarán los diferentes diagramas topológicos que describen el estado actual de la configuración de la infraestructura a nivel global y por localidad.

A medida que se avance en la explicación se evidenciará y detallará el estado de las topologías luego de la configuración, por lo que se hallará información general relacionada con:

- **Puertos de fibra anillos:** Se identifica los puertos de fibra óptica utilizados para la conformación del anillo. Es de suma importancia que permanezcan conectados como en el diagrama presentado.
- **Direcciones IP de administración:** Cada Virtual Chasis, o switch de borde, tiene una dirección de administración, la cual será única y exclusivamente usada por el usuario administrador de manera remota, aquel con perfil root o súper usuario, como se lo suele identificar. No obstante, el switch de nodo acceso tendrá activado su EMP (Ethernet Management Port) para administración fuera de banda y de manera local, se lo mencionará oportunamente.
- **Identificación de ID de Agregados de Enlace:** Este dato es importante para poder gestionar la conectividad del anillo o de los switches de borde donde se conectan los sistemas de transporte. Es como conocer el número de puerto donde se conecta un enlace físico. Las posibles configuraciones futuras harán referencia a este ID y no al número de los puertos miembros del agregado de enlace.

Diagrama de red nodos de acceso

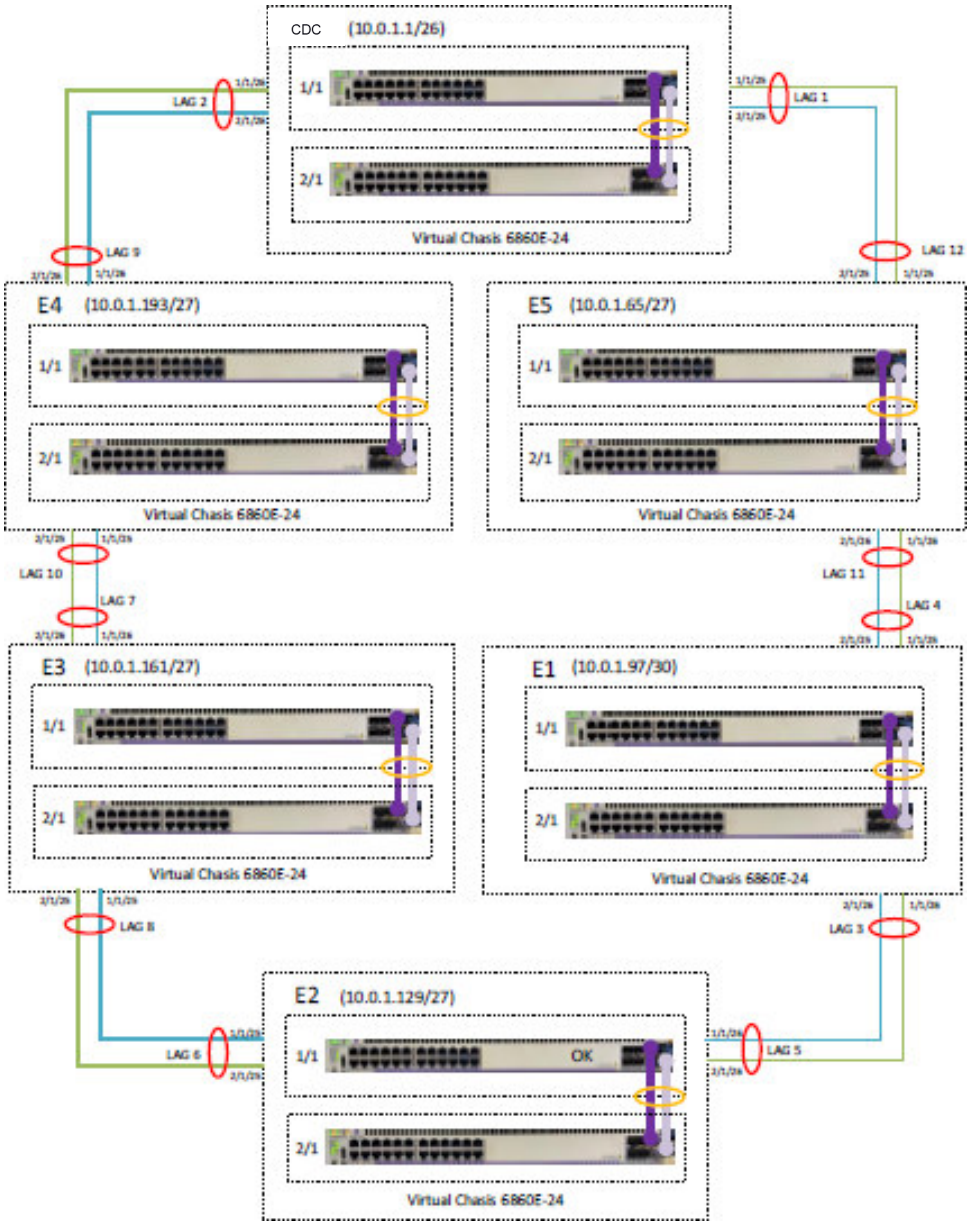

Figura 2.11. Topología nodos de acceso localidades.

Fuente: Autor

En el diagrama anterior también es visible lo peculiar de la ubicación de las localidades. Así, luego de CDC, en sentido horario, no está ubicado el nodo de acceso de la E1, sino el de E5. Luego de esta última se encuentra ubicado E1, y en lo posterior se sigue un orden lógico.

En la figura anterior es posible verificar que se cumplen los siguientes criterios de diseño en cuanto a redundancia:

- **Redundancia de Nodo:** ya que existen dos switches capa 3 en conformación de Virtual Chasis, los cuales estarán balanceando la carga recibida por los otros equipos de nodo acceso, debido a la configuración de redundancia de enlace.
- **Redundancia de Enlace:** existen dos enlaces de fibra que se usan para conformar un agregado de enlace para la interconexión entre localidades. Estos enlaces van conectados a ambos switches en el Virtual Chasis por lo que la carga se distribuye hacia los dos equipos.

En la siguiente sección se detallará cómo se realizó la conexión de la fibra de interconexión entre nodos de acceso en relación con el detalle mostrado en la figura anterior. Además de mencionar

las conexiones en agregado de enlace de los diferentes switches de borde que usan los sistemas de transporte.

Diagrama general de conexión de sistemas a nodos de acceso

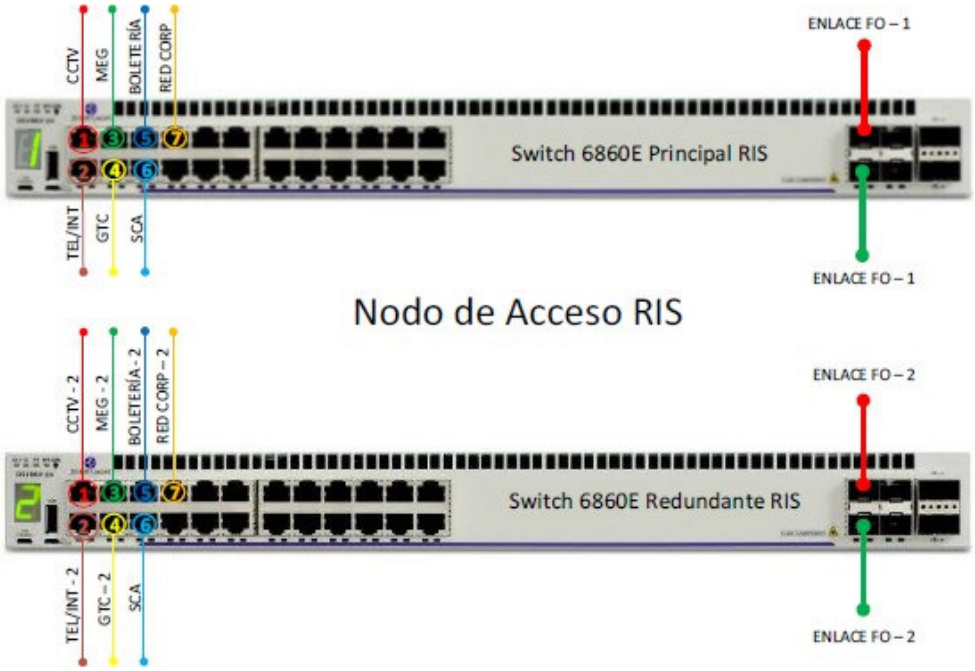

Figura 2.12. Conexiones en Agregado de Enlace de sistemas a nodo de acceso.

Fuente: Autor

Las observaciones generales necesarias al considerar las conexiones en los switches de nodo acceso son las siguientes:

- El switch de nodo acceso considerado como principal, es aquel designado con el número 1 en el display de la parte izquierda.

- El enlace hacia los respectivos switches de sistemas ocupa puertos de ambos switches de nodo de acceso, conformando de esta manera un agregado de enlace redundante. Por ejemplo, el agregado de enlace que conecta el switch de CCTV hacia el nodo de acceso está conformado por los puertos 1/1/1 y el 2/1/1; el de telefonía por los puertos 1/1/2 y el 2/1/2 y así sucesivamente.
- Es necesario mencionar que una secuencia similar se usó para la conexión por fibra óptica entre los nodos de acceso. Así, en la figura anterior, los llamados “ENLACE FO” de un color en particular conformaron un agregado de enlace que interconectaron los nodos de acceso vecinos.
- Los puertos que no se usen se encontrarán administrativamente deshabilitados y asociados a una VLAN llamada “PUERTOS_NO_USADOS”. Si se requiere habilitar algún servicio nuevo se debe habilitar el puerto y asociarlo a una VLAN válida.
- El gráfico anterior es referencial e indica la manera general en cómo es el patrón de conexiones, por lo cual, para una referencia exacta se debe verificar los diagramas de los numerales siguientes.

Diagrama de red Centro de Control (CDC)

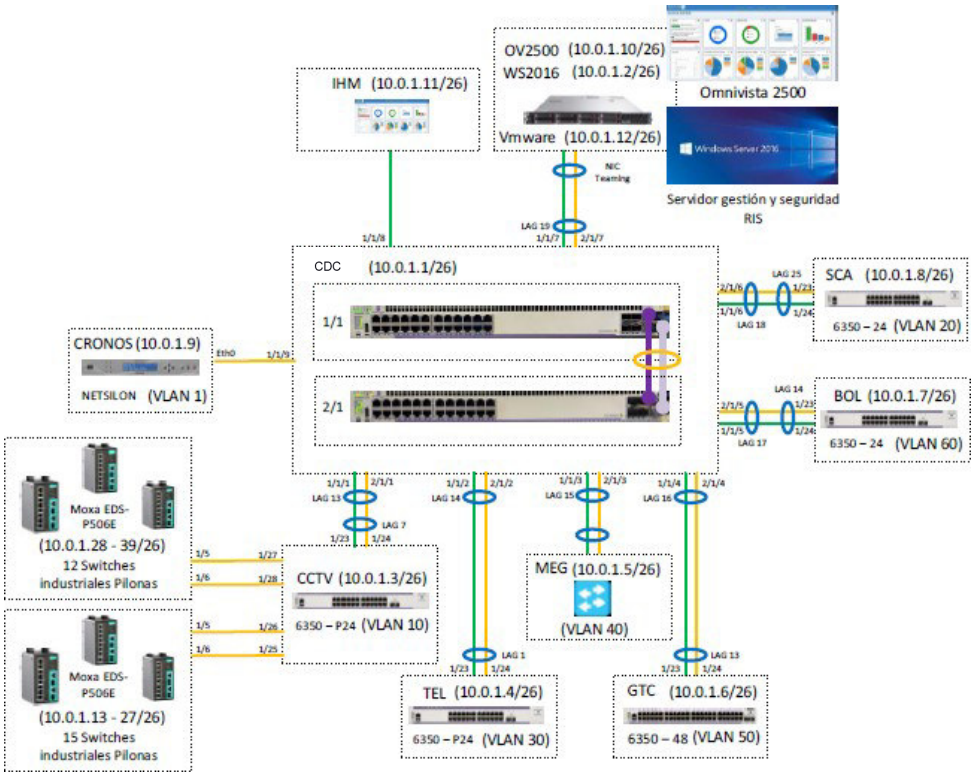

Figura 2.13. Diagrama de conexiones Centro de Control CDC.

Fuente: Autor

En el CDC existen las siguientes particularidades:

- Ubicado físicamente en el segundo piso del datacenter de la localidad 4. El Datacenter de la localidad 4 como tal se ubica en el primer piso.
- Los datos del segmento de red de la VLAN de administración para CDC son los siguientes:
  - Dirección de red: 10.0.1.0/26
  - Máscara de red: 255.255.255.192

- Primera dirección de Host: 10.0.1.1
- Última dirección de Host: 10.0.1.62

Las direcciones IP utilizadas para este rango se encuentran especificadas en cada uno de los equipos mostrados en la figura anterior. También existe una lista recopilatoria en un anexo del presente documento y obedece a la planificación mostrada en la tabla 2. Es importante mencionar que, este direccionamiento IP no solamente es utilizado por los switches, sino también por otros equipos complementarios de otros sistemas.

- En CDC se encuentran centralizados la mayoría de los servidores de los diferentes sistemas. Así por ejemplo se encuentran los servidores principales de la Central telefónica, el servidor de cronometría, los servidores para los NMS Omnivista y todos aquellos servidores principales de los otros sistemas de transporte.
- El único switch para las funcionalidades de Control de Acceso (SCA) se encuentra ubicado en el CDC. Las demás localidades no contemplan un switch de SCA. No obstante, como se observará en los gráficos posteriores, se ha dejado los puertos reservados del switch de nodo de acceso para la conexión de

estos equipos, pero no habrá reservado un Link Aggregation, sino solamente los puertos de manera independiente o normal.

- En CDC no existe un switch de red corporativa, para las demás localidades existen uno por cada localidad. Adicional, es importante mencionar que únicamente habrá salida a Internet a través de estos switches mediante los privilegios y restricciones que se asignarán oportunamente en el firewall de la Localidad 4.
- El switch de CCTV cumple un rol especial dentro de CDC. Como puede verse en la figura anterior, la totalidad de sus puertos de fibra es utilizado para la interconexión de dos grupos de switches industriales. Cada uno de estos grupos conforma un anillo cuya conexión regresa al switch de CCTV.

Así, para el primer grupo de 15 switches industriales se utiliza como salida el puerto 1/25 y como llegada el 1/26 del switch de CCTV. Los switches se interconectan uno a continuación del otro utilizando sus puertos 5 y 6. Algo similar sucede con el segundo grupo de 12 switches industriales utilizando los puertos 1/27 y 1/28 del switch de CCTV.

Adicionalmente, es importante mencionar que la IP de administración de los switches forma parte del segmento administrativo de CDC y se ubican en el rango 10.0.1.13 – 10.0.1.39.

Diagrama de red Localidad 5 (E5)

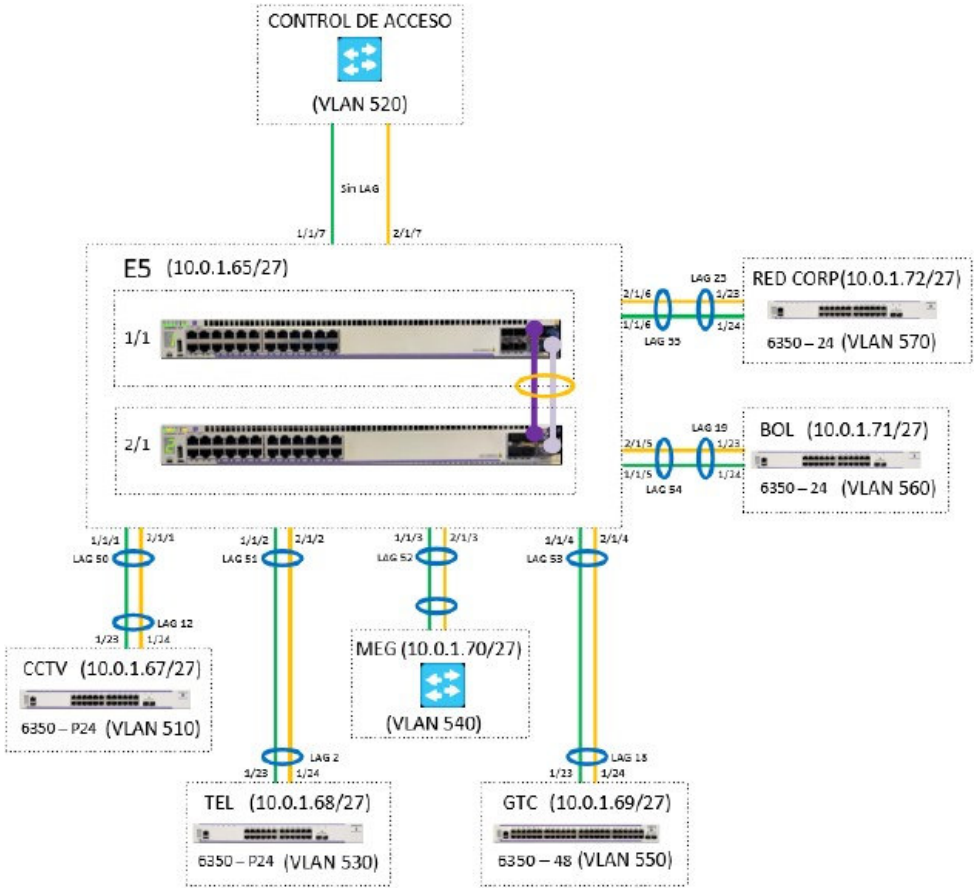

Figura 2.14. Diagrama de conexiones Localidad 5 – E5.

Fuente: Autor

Las particularidades para la localidad cinco son las siguientes:

- Ubicado físicamente en el datacenter de la localidad 5.
- Los datos del segmento de red de la VLAN de administración para E5 son los siguientes:
  - Dirección de red: 10.0.1.64/27
  - Máscara de red: 255.255.255.224
  - Primera dirección de Host: 10.0.1.65
  - Última dirección de Host: 10.0.1.94

  Las direcciones IP utilizadas para este rango se encuentran especificadas en cada uno de los equipos mostrados en la figura anterior. También existe una lista recopilatoria en un anexo del presente documento y obedecen a la planificación mostrada en la tabla 2. Es importante mencionar que, este direccionamiento IP no solamente es utilizado por los switches, sino también por otros equipos complementarios de otros sistemas.
- En esta localidad no existe un switch de control de acceso o SCA. No obstante, en la figura anterior puede notarse que se reservan los puertos 1/1/7 y 2/1/7 para la conexión de equipos de este sistema. Es importante mencionar que estos puertos no conforman un agregado de enlace y se los debe usar de manera independiente.

Diagrama de red Localidad 1 (E1)

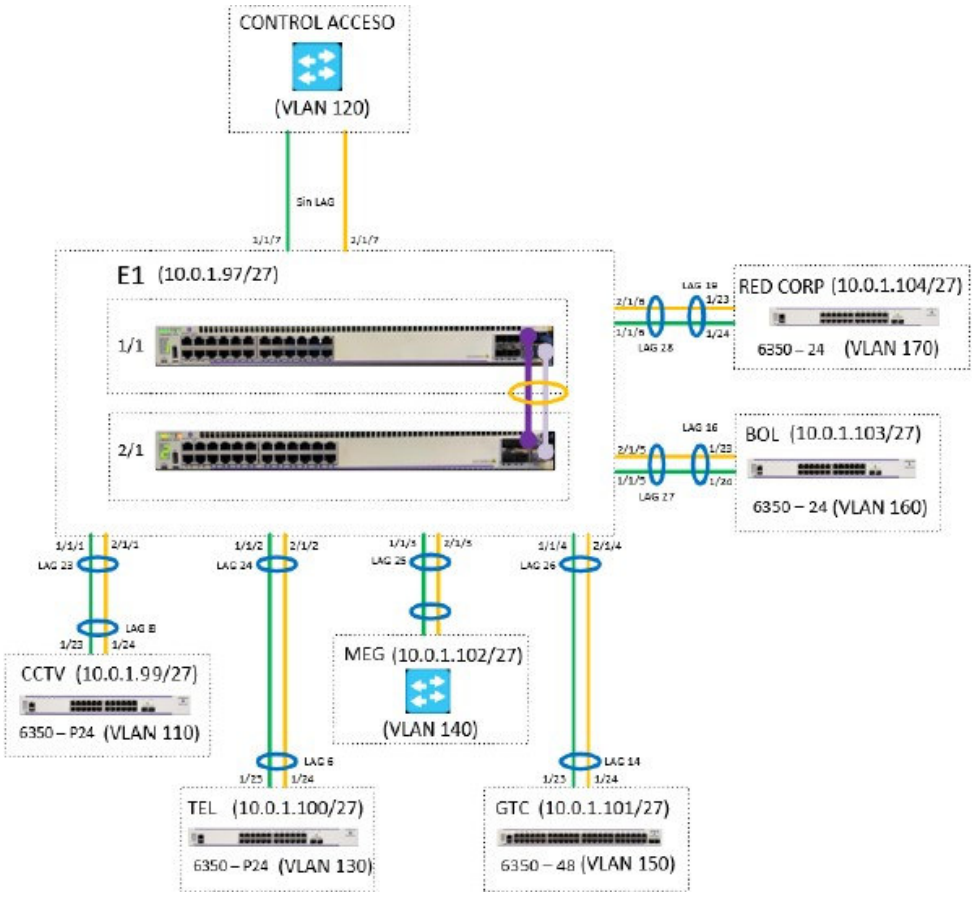

Figura 2.15. Diagrama de conexiones Localidad 1 – E1.

Fuente: Autor

En la Localidad se pueden evidenciar las siguientes particularidades:

- Ubicado físicamente en el datacenter de la localidad 1.
- Los datos del segmento de red de la VLAN de administración para E1 son los siguientes:
  - Dirección de red: 10.0.1.96/27

- Máscara de red: 255.255.255.224
- Primera dirección de Host: 10.0.1.97
- Última dirección de Host: 10.0.1.126

Las direcciones IP utilizadas para este rango se encuentran especificadas en cada uno de los equipos mostrados en la figura anterior. También existe una lista recopilatoria en un anexo del presente documento y obedecen a la planificación mostrada en la tabla 2. Es importante mencionar que, este direccionamiento IP no solamente es utilizado por los switches, sino también por otros equipos complementarios de otros sistemas.

- En esta localidad no existe un switch de control de acceso o SCA. No obstante, en la figura anterior se puede observar que se reservan los puertos 1/1/7 y 2/1/7 para la conexión de equipos de este sistema. Cabe destacar que estos puertos no conforman un agregado de enlace y se los debe usar de manera independiente.

Diagrama de red Localidad 2 (E2)

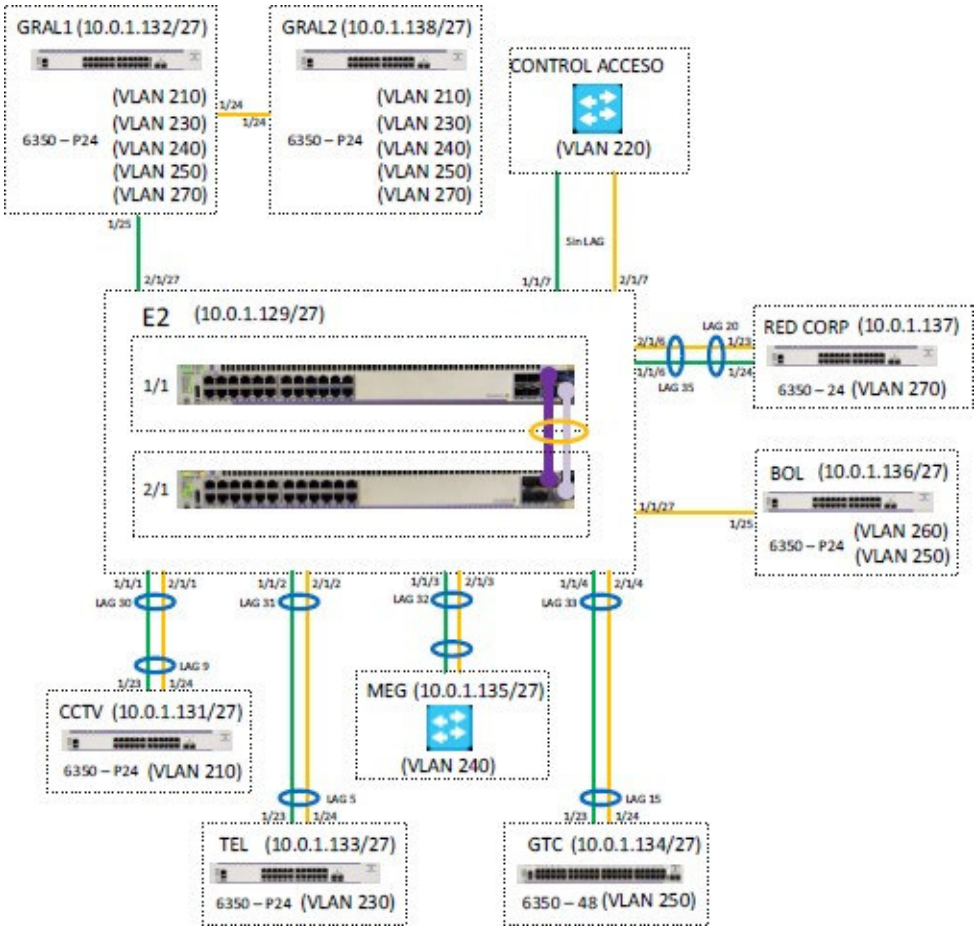

Figura 2.16. Diagrama de conexiones Localidad 2 – E2.

Fuente: Autor

En la Localidad Dos existen las siguientes particularidades:

- Ubicado físicamente en el datacenter de la localidad 2.
- Los datos del segmento de red de la VLAN de administración para E2 son los siguientes:
  - Dirección de red: 10.0.1.128/27
  - Máscara de red: 255.255.255.224

- Primera dirección de Host: 10.0.1.129
- Última dirección de Host: 10.0.1.158

- Las direcciones IP utilizadas para este rango se encuentran especificadas en cada uno de los equipos mostrados en la figura anterior. También existe una lista recopilatoria en un anexo del presente documento y obedecen a la planificación mostrada en la tabla 2. Es importante mencionar que, este direccionamiento IP no solamente es utilizado por los switches, sino también por otros equipos complementarios de otros sistemas.
- Existe un par de switches diferentes, al que se los ha llamado GRAL1 y GRAL 2 respectivamente. Estos presentan la particularidad de que tienen configuradas varias VLANs, las que pueden verse en la figura anterior, y es que puede conectar equipos finales tanto de CCTV, Telefonía, red corporativa Sonido y GTC.
- De manera adicional, por superar la distancia de los 100 metros, el switch GRAL 1 se conecta al nodo de acceso a través de un puerto de fibra óptica del mismo (1/1/27). El switch GRAL 2 está en cascada con el primero. El objetivo en el futuro es conformar un solo switch GRAL a través de la implementación de un stack.

- En esta localidad no existe un switch de control de acceso o SCA. No obstante, en la figura anterior se puede observar que se reservan los puertos 1/1/7 y 2/1/7 para la conexión de equipos de este sistema. Es necesario aclarar que estos puertos no conforman un agregado de enlace y se los debe usar de manera independiente.
- De manera similar al switch GRAL1, el enlace del switch de Tickets al nodo de acceso supera los 100 m por lo que se usa fibra óptica para su conexión, la cual se establece a través del puerto 2/1/27.

Diagrama de red Localidad 3 (E3)

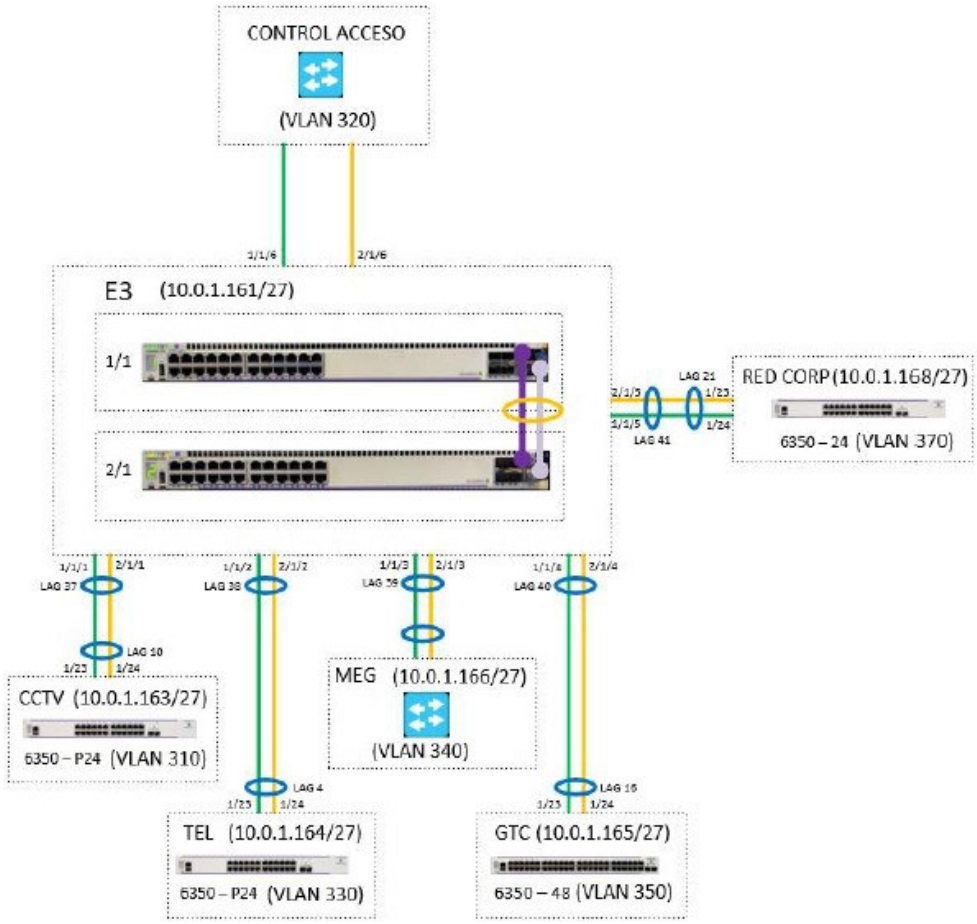

Figura 2.17. Diagrama de conexiones Localidad 3 – E3.

Fuente: Autor

En la Localidad Tres se tiene las siguientes particularidades:

- Ubicada físicamente en el datacenter de la localidad 3.
- Los datos del segmento de red de la VLAN de administración para E3 son los siguientes:
  - Dirección de red: 10.0.1.160/27
  - Máscara de red: 255.255.255.224

- Primera dirección de Host: 10.0.1.161
- Última dirección de Host: 10.0.1.190

Las direcciones IP utilizadas para este rango se encuentran especificadas en cada uno de los equipos mostrados en la figura anterior. También existe una lista recopilatoria en un anexo del presente documento y obedecen a la planificación mostrada en la tabla 2. Es importante mencionar que, este direccionamiento IP no solamente es utilizado por los switches, sino también por otros equipos complementarios de otros sistemas.

- Esta localidad no posee un switch de Tickets.
- Esta localidad no tiene un switch de control de acceso o SCA. No obstante, en la figura anterior se puede observar que se reservan los puertos 1/1/7 y 2/1/7 para la conexión de equipos de este sistema. Es importante mencionar que estos puertos no conforman un agregado de enlace y se los debe usar de manera independiente.

Diagrama de red Localidad 4 (E4)

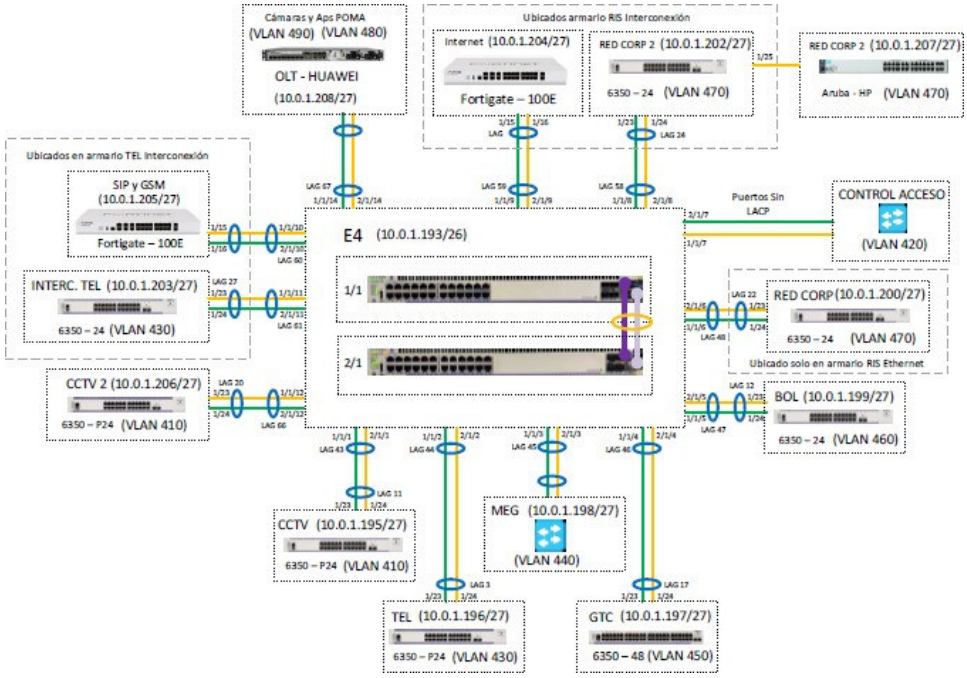

Figura 2.18. Diagrama de conexiones Localidad 4 – E4.

Fuente: Autor

La Localidad Cuatro tiene las siguientes particularidades:

- Ubicada físicamente en el datacenter de la localidad 4 planta baja.
- Los datos del segmento de red de la VLAN de administración para E4 son los siguientes:
  - Dirección de red: 10.0.1.192/27
  - Máscara de red: 255.255.255.224
  - Primera dirección de Host: 10.0.1.193
  - Última dirección de Host: 10.0.1.222

Las direcciones IP utilizadas para este rango se encuentran especificadas en cada uno de los equipos mostrados en la figura anterior. También existe una lista recopilatoria en un anexo del presente documento y obedecen a la planificación mostrada en la tabla 2. Es importante mencionar que, este direccionamiento IP no solamente es utilizado por los switches, sino también por otros equipos complementarios de otros sistemas.

- A esta localidad llegan los proveedores de servicio de Internet, troncales SIP y red GSM. Es decir, estos servicios se encuentran centralizados en la localidad 4.
- El Virtual Chasis de la Localidad Cuatro tiene previsto la conexión a través de un Link Aggregation con dos firewalls, el primero se utilizará como UTM de Datos y el segundo como UTM de voz. Estos equipos tendrán conexión directa con los CPEs de los servicios mencionados en el anterior punto. En la siguiente página se muestra una imagen con los detalles de las conexiones y rutas configuradas.
- Se tiene adicionalmente dos switches llamados “Red Corp 2” e “Interc. Tel” en la figura anterior, cuya conexión también se tiene contemplada a través de los enlaces pertinentes.

- El switch de nodo acceso provee también la interconexión de un OLT marca Huawei, el cual permite la interconexión de las llamadas cámaras móviles y de Access Points para la provisión de servicio WiFi. Estos al considerarse servicios de transporte se conectan directamente al nodo de acceso a través de dicho OLT. La IP de administración del OLT está en el mismo segmento administrativo designado para la E4.
- No obstante, para los servicios proporcionados por las cámaras móviles y los Access Points, se crearon dos VLANs adicionales, la 490 y la 480. La primera fue asignada para la administración de las cámaras y posee el segmento de red 192.168.0.0/24 y la última para la administración de los Access Points en el segmento 10.40.80.0/24, cuyas IPs fueron asignadas dinámicamente por el switch de nodo acceso.
- Los usuarios Wifi toman su direccionamiento IP directamente desde el ISP. El Acceso a Internet se hizo a través de un enlace distinto que el de red corporativa.
- Esta localidad no posee un switch de control de acceso o SCA. No obstante, en la figura anterior puede notarse que se reservan los puertos 1/1/7 y 2/1/7 para la conexión de equipos de este sistema. Es importante mencionar que estos puertos

no conforman un agregado de enlace y se los debe usar de manera independiente.

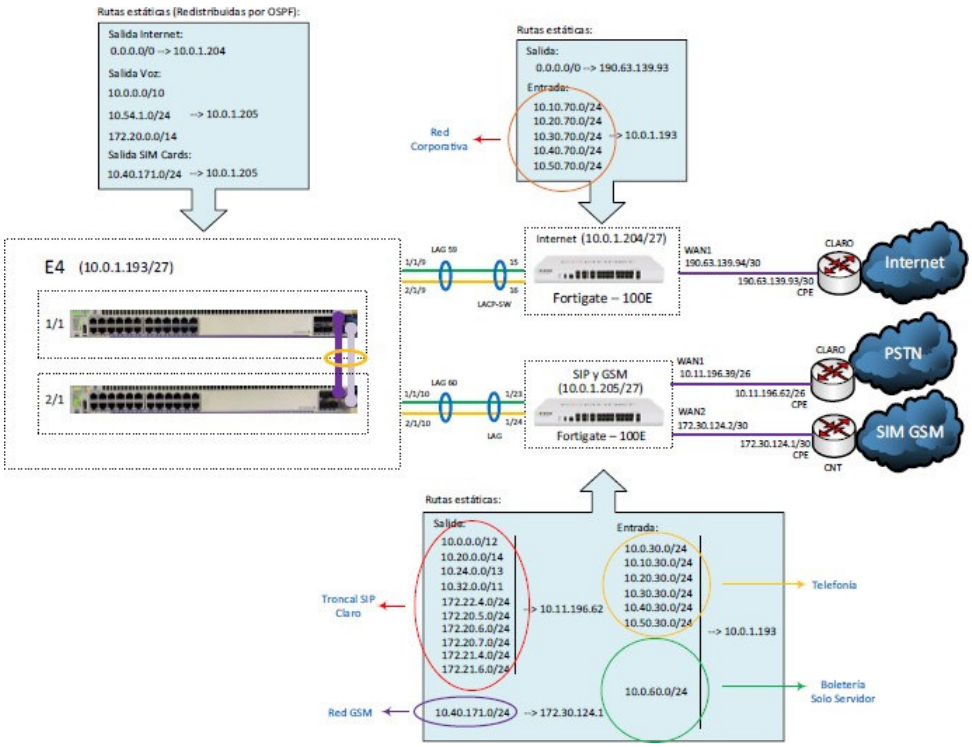

Figura 2.19. Diagrama de conexiones proveedores externos Localidad 4 – E4.

Fuente: Autor

2.2 IMPLEMENTACIÓN

En esta sección se describirán las tareas principales de configuración que, en su conjunto, proporcionan el funcionamiento de acuerdo con las expectativas del proyecto. Es objetivo de esta sección es detallar, paso a paso, cómo se procedió en las diferentes tareas de configuración.

Muchas de estas tareas se aplican a varios equipos de la infraestructura de red, por lo cual en esta fase se lo explicará solamente una vez y se mencionará a qué partes de la red aplica.

2.2.1 CONFIGURACIONES DE RED

En esta sección se abarcarán las configuraciones relacionadas con el transporte, segmentación y organización del tráfico de la red, ya que más adelante se especificarán aspectos de seguridad, monitoreo, control, complementarios, entre otros.

VLANs

Para describir esta sección, se considera los criterios de diseño del numeral 4.2, que hacen referencia a la ID de VLAN y direccionamiento IP, al configurar las VLANs en los switches de nodo de acceso y aplicar el comando “show vlan”, se verá la creación de VLANs como se muestra en la figura 2.20.

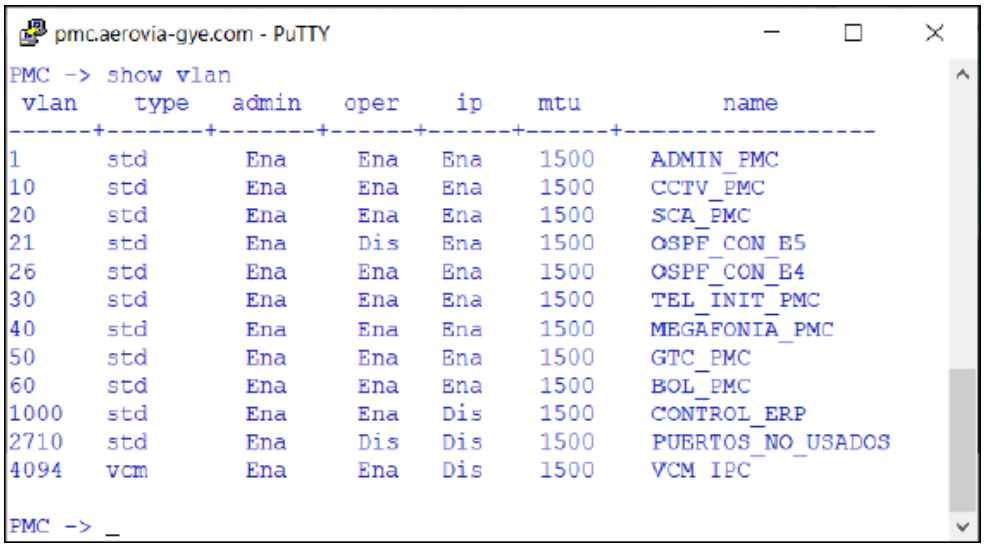

Figura 2.20. VLANs creadas en switch de nodo acceso CDC.

Fuente: Autor

La figura 2.20, muestra VLANs adicionales como son:

- VLAN 1000, que es destinada una VLAN de control, exclusiva del uso de ERP.
- VLAN 21 y 26, de uso exclusivo para la formación del OSPF.
- VLAN 2710, usada para asignar puertos no utilizados, se desvincula puertos no usados por seguridad.
- Los SW de acceso están configurados con dos VLANs, por ejemplo, el SW CCTV de CDC tendrá configurado las VLANs:
- VLAN 1, VLAN por defecto y será utilizada para la administración del equipo.
- VLAN10, VLAN asignada para equipos de CCTV.

La creación de VLANs, para los otros switches que forman los nodos de acceso y switch de acceso se basan en el mismo criterio mostrado anteriormente.

Agregados de Enlace LACP

El agregado de enlace provee mayor ancho de banda y también redundancia. Además, el anillo que une los nodos de acceso y la comunicación desde los switches de borde de los sistemas de transporte hacia el nodo de acceso, usan un agregado de enlace. A continuación, la figura 2.21, muestra los LACP existentes en el switch nodo de acceso de CDC.

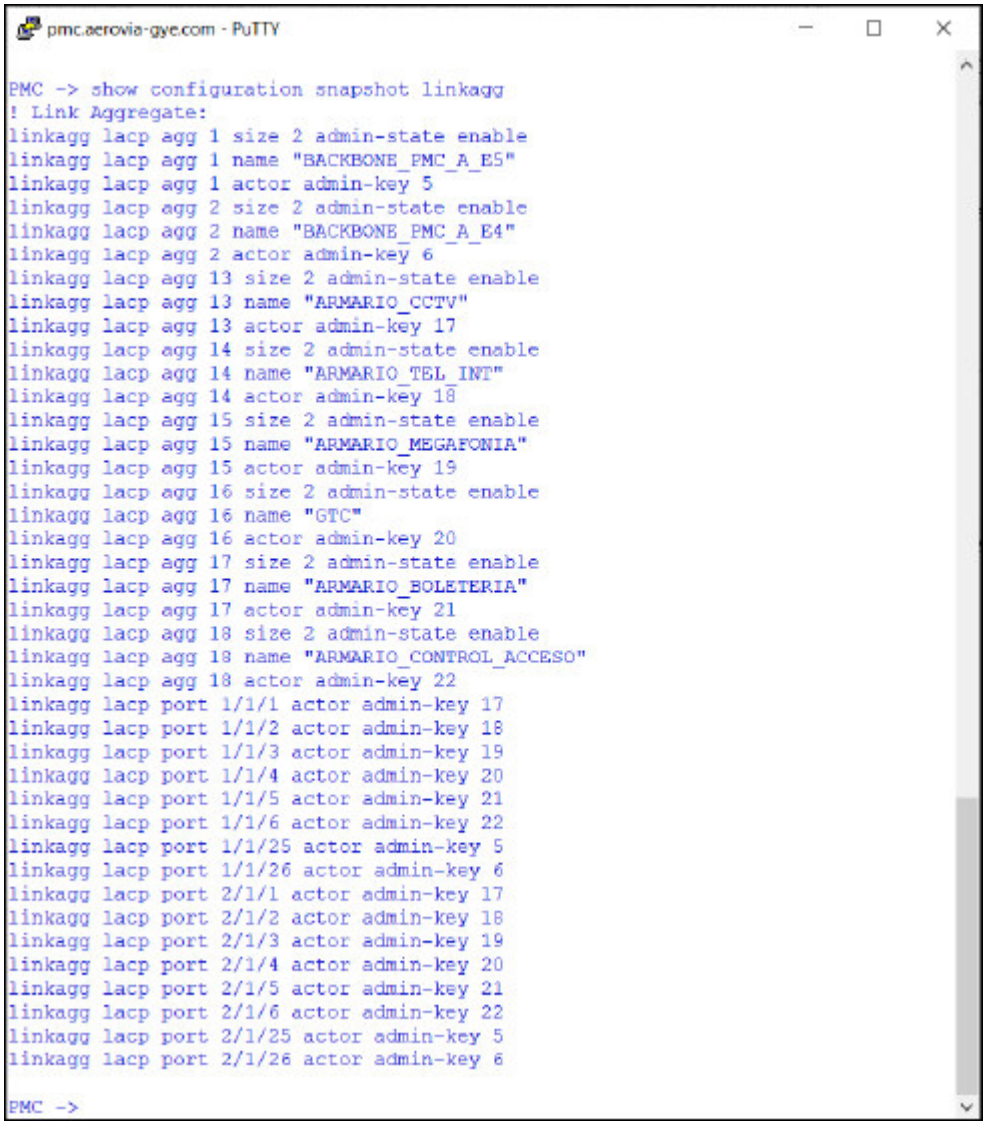

Figura 2.21. Agregados de enlace switch nodo acceso CDC.

Fuente: Autor

Los parámetros importantes en los LACP a considerar son:

- ID del agregado: “linkagg lacp agg X” permite identificar el agregado de enlace de manera unívoca.

- Size 2: es el número de enlaces o conexiones que el agregado de enlace va a agrupar e identificar como uno solo. Estos modelos de switches pueden ser de 2, 4 y 8 enlaces del mismo medio y velocidad.
- Admin-key “Y”: es un número aleatorio que el administrador le asigna al agregado de enlace y que se asocia al ID del agregado. Con este admin-key se puede asociar el puerto al ID del agregado.

Para verificar el estado de un LACP y puertos asociados, se utiliza un comando show, referirse a la figura 2.22.

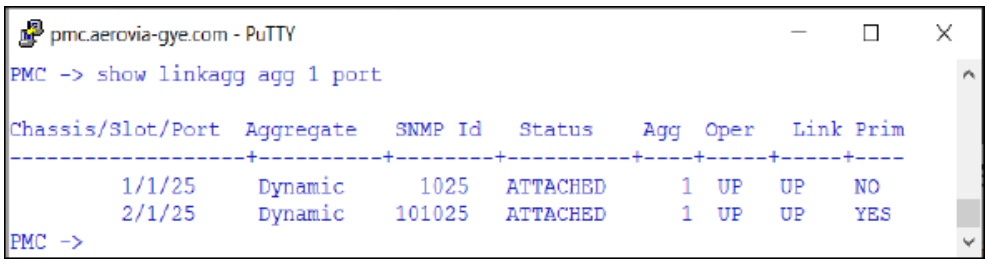

Figura 2.22. Verificación de estado de agregado de enlace.

Fuente: Autor

Para los switches de borde existe una lógica similar, solo que existe un único agregado de enlace hacia el switch de nodo acceso, ver figura 2.23.

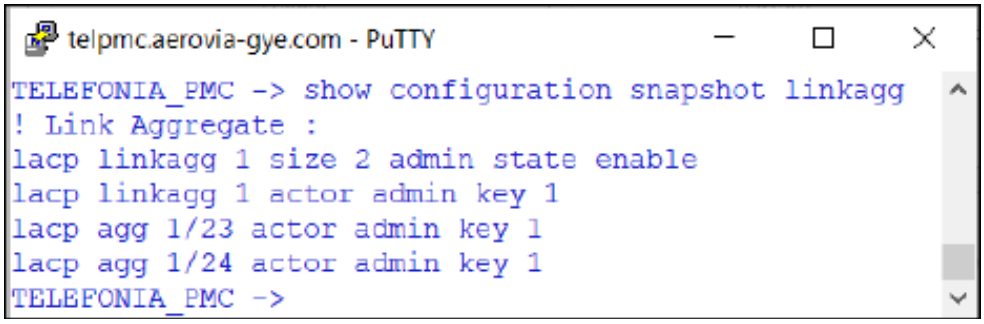

Figura 2.23. Agregados de enlace switch de borde.

Fuente: Autor

Se aplicó el mismo procedimiento para la creación, verificación y estado de los LACPs para los demás switches nodos de acceso y switches de borde.

Asignación de puertos y 802.1q (Troncalización)

La troncalización de puertos está asociada al concepto de VLANs, con la troncalización (802.1q) se logra que por un mismo enlace circulen varias VLANs, por lo general las configuraciones de enlaces troncales están aplicados a los LACP de los switches que forman los nodos de acceso y los switches de borde, la figuras 2.24 y 2.25 muestran la configuración de un LACP como puerto troncal. En ella se puede apreciar la existencia de una VLAN default o nativa y una VLAN qtagged troncalizada.

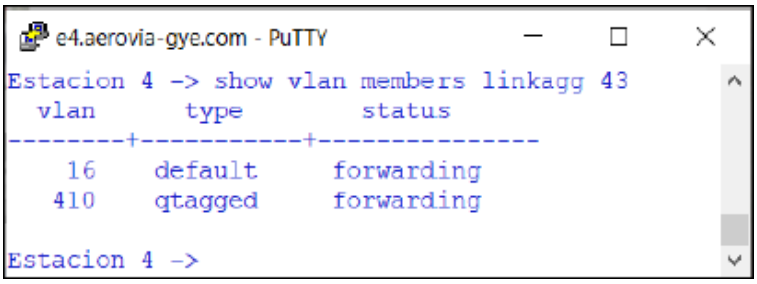

Figura 2.24. VLANs asignadas a un agregado de enlace switch nodo acceso E4.

Fuente: Autor

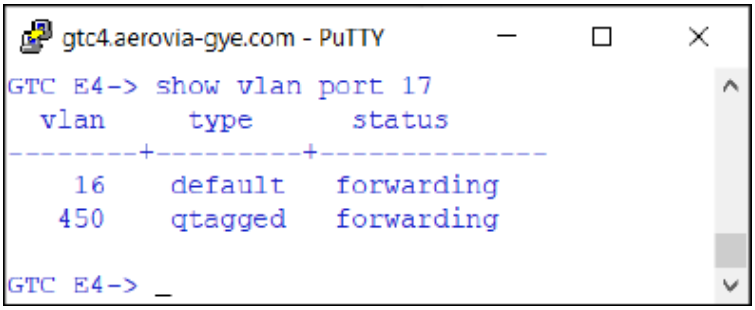

Figura 2.25. VLANs asignadas a un agregado de enlace en switch de borde GTC.

Fuente: Autor

ERP (Ethernet Ring Protection).

ERP es un protocolo ligero diseñado para topologías en anillo, sin mucho “overhead” en cuanto a la trama. Sin embargo, con él se logra vigilar constantemente la integridad del anillo y reaccionar rápidamente ante una eventual “ruptura” de manera que la comunicación esté permanentemente activa.

El ERP basa su funcionamiento en la configuración de una VLAN de servicio y un puerto llamado RPL (Ring Protection Link), en la implementación del anillo se configuró la VLAN 1000 en los switches que forman los nodos de acceso y se la asoció a todos los LACP que forman el anillo. Adicional a eso, el puerto RPL se definió en el LACP que une a la localidad de CDC con la localidad E5. Es importante destacar que LACP pertenece a la localidad CDC el RLP owner, ver la figura 2.26.

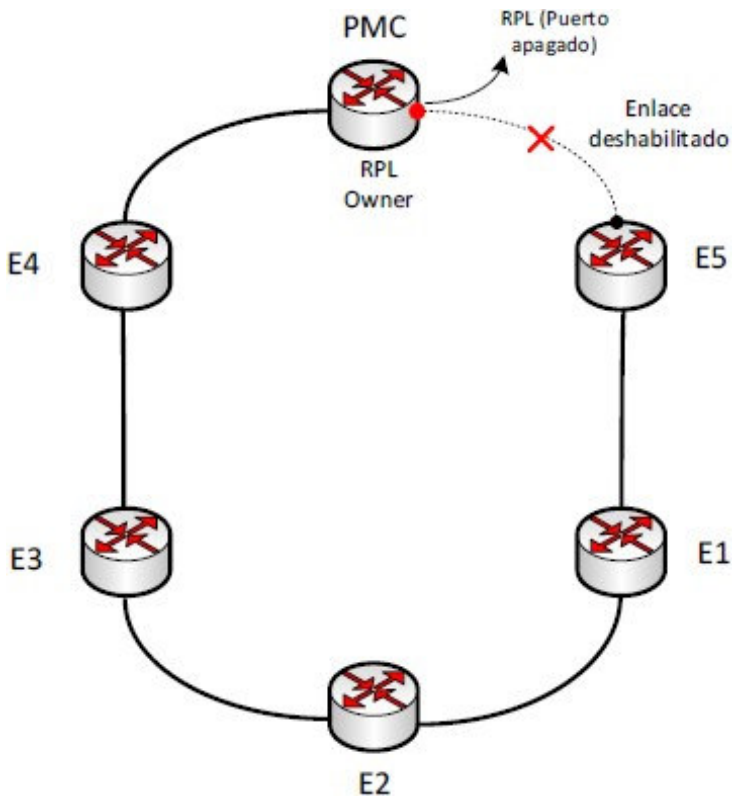

Figura 2.26. Funcionamiento normal en modo “Idle” de ERP.

Fuente: Autor

Por lo tanto, al presentarse una falla en cualquier sección del anillo, en hasta 50 ms el protocolo reacciona y habilita el puerto RPL permitiendo que en dicho tiempo la comunicación se restablezca. Esto se lo puede comprobar de manera contundente mediante una llamada de VoIP entre localidades, la cual no se interrumpe en su audio pese al paso de un modo de ERP al otro, la figura 2.27, muestra un evento de falla de enlace entre las localidades E3 y E2 y la forma en que actúa el puerto RPL.

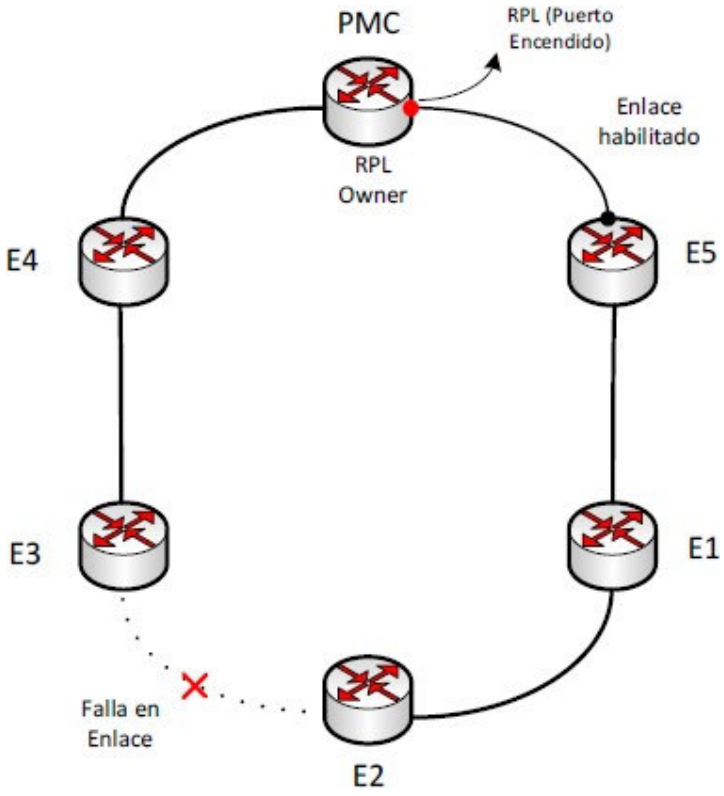

Figura 2.27. Funcionamiento emergente en modo “Protection” de ERP.

Fuente: Autor

Un aspecto fundamental que se debe considerar es el tiempo de resiliencia llamado WTR Timer (Wait to restore), el cual es una protección contra enlaces inestables. Cuando un enlace sube nuevamente, se pone en marcha este timer y si al finalizar el mismo se comprueba que el enlace en cuestión sigue funcionando normalmente se pasa de modo protection a idle. De esta manera se evita que ERP cambie de modo constantemente debido a la inestabilidad de un enlace. El tiempo mínimo configurable para WTR es de 1 minuto, el cual fue considerado y configurado en la red.

A continuación, se muestran las configuraciones aplicadas en los VC (virtual chasis) de los switches de nodo que forman la red, primero se observan las configuraciones aplicadas en la localidad CDC y su comportamiento.

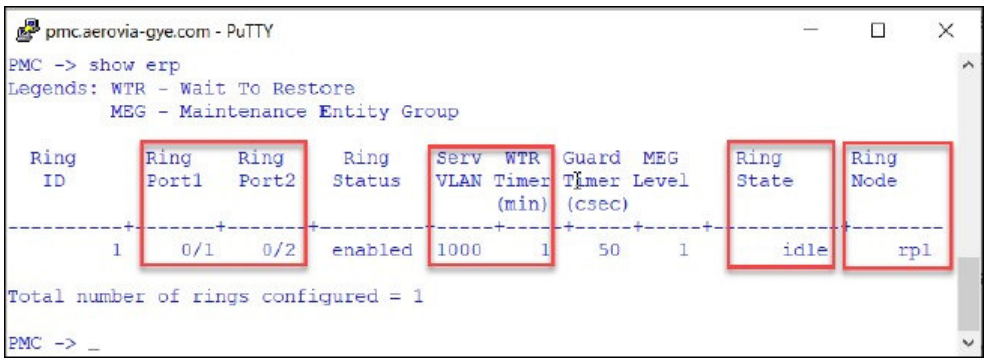

Figura 2.28. Configuración y estado de ERP en nodo RPL CDC.

Fuente: Autor

La figura 2.230 muestra las configuraciones de ERP realizadas en la localidad de CDC, esta contiene el puerto RPL. Además, se observa que en los enlaces LACP 1 y 2 está configurada la VLAN de servicio 1000, su WTR está configurada en 1 minuto y el estado del anillo es idle. Es decir que no ha habido eventos de caídas de enlaces en el anillo.

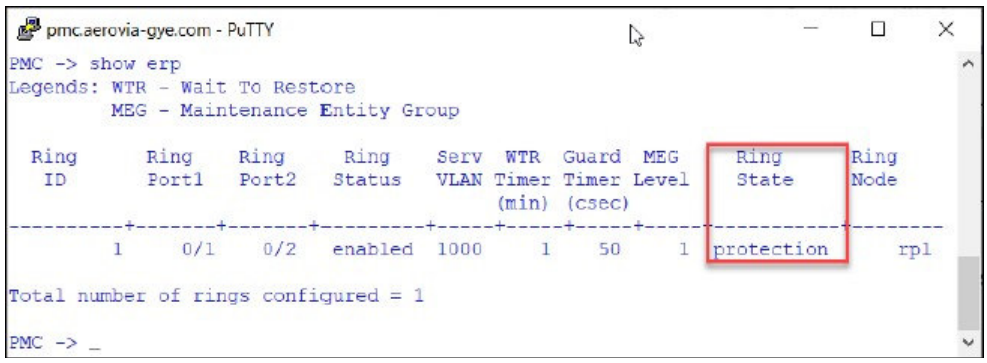

Figura 2.29. Modo protección de ERP.

Fuente: Autor

La figura 2.30 muestra la existencia de un cambio en el comportamiento del anillo, el ring state, ha cambiado de idle a protection, lo que significa que algún segmento del anillo ha perdido conectividad.

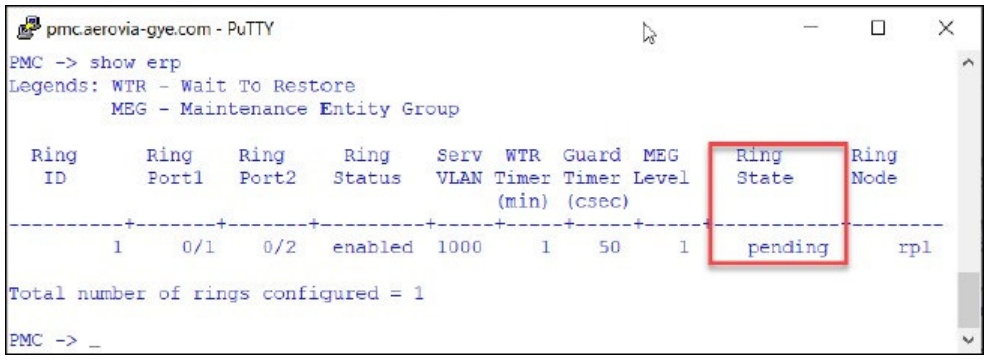

Figura 2.30. Modo pending de ERP.

Fuente: Autor

La figura 2.30 muestra el ring state en pending, lo cual implica que el anillo ha recuperado el estado de sus enlaces y está próximo a recuperar su estado original, se verificará los estados de los enlaces durante el periodo configurado en WTR, un minuto, luego de ese tiempo (1 minuto), el ring state volverá a su estado original idle.

A continuación, se muestran las configuraciones realizadas a otros nodos del anillo que no contienen el RPL owner, para ello se tomó como ejemplo a la localidad 3, pues las configuraciones son similares.

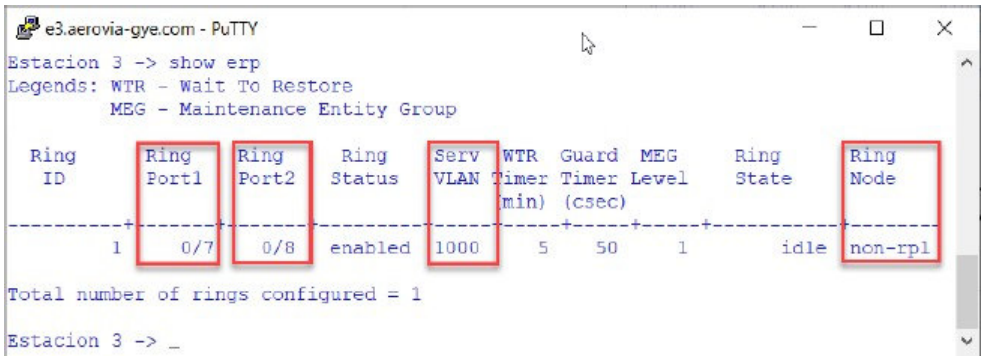

Figura 2.31. Configuraciones ERP en un nodo no RPL.

Fuente: Autor

La figura 2.31 muestra las configuraciones de ERP realizadas en la localidad E3, esta no contiene un puerto RPL, pero sí se encuentra configurada la VLAN de servicio 1000 en los enlaces LACP 7 y 8, el WTR está configurada en 5 minutos, no tiene peso. El WTR siempre hará referencia al que ha sido configurado en el nodo que contiene el RPL owner, en este caso al configurado en la localidad de CDC, que es de 1 minuto.

Servidor DHCP

Como se ha mencionado en secciones precedentes, por diseño el direccionamiento IP en la red se otorga de forma manual, es decir que no existe DHCP. Esta premisa es cierta excepto para el servicio Wifi configurado al otro lado del OLT Huawei en localidad 4.

La dirección IP del direccionamiento para los Access Points que proveen de este requerimiento es otorgada por un servicio proporcionado por el switch de nodo acceso de la localidad 4. Los parámetros especificados para dicha instancia de servidor DHCP son los siguientes:

- Red: 10.40.80.0/24
- Rango del direccionamiento: 10.40.80.10 – 10.40.80.200
- Gateway: 10.40.80.254
- DNS: 8.8.8.8
- Lease time: 30000 sec.

A continuación, se muestra una imagen en el que se evidencia el funcionamiento de este servicio exclusivo del switch de nodo acceso de la localidad 4:

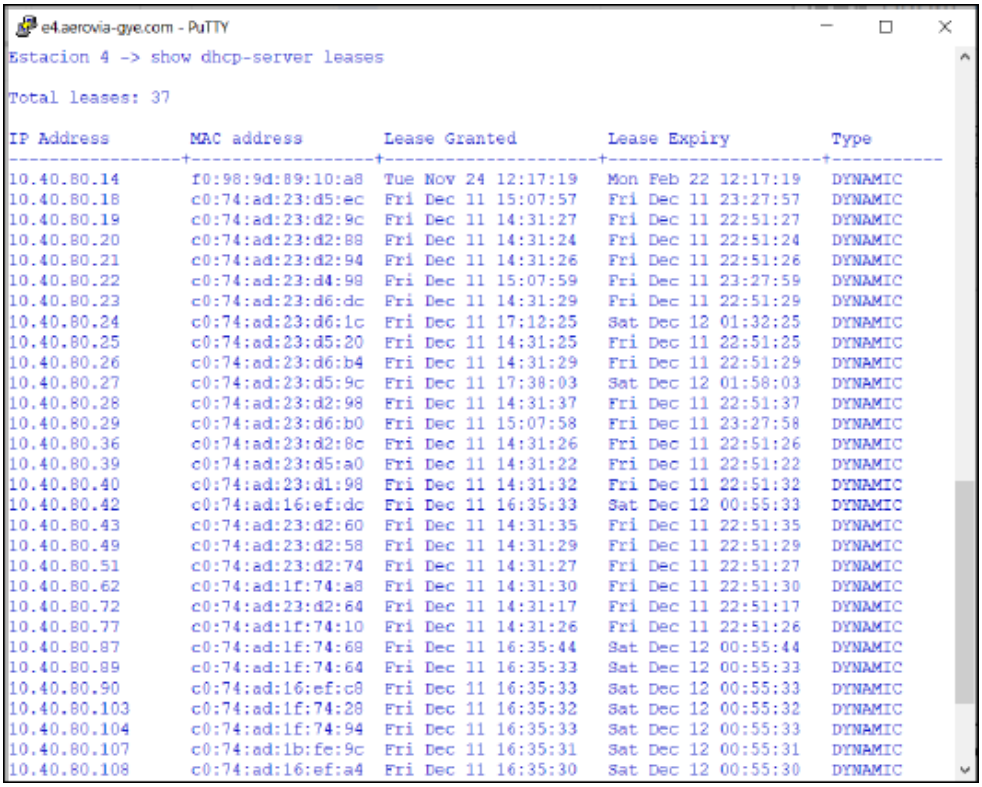

Figura 2.32. Servidor DHCP en Switch nodo acceso E4

Fuente: Autor

Interfaces de Red (Gateway del Sistema)

En los switches de nodos de acceso, se configuran interfaces IP que vienen a constituir los gateways de las diferentes redes que son asociadas en VLANs, esto gateways o interfaces IP participan activamente en conjunto con los protocolos de enrutamiento unicast y multicast.

Para los switches de borde, donde se conectan los diferentes sistemas de transporte, la interfaz IP se configura solamente para

dar una dirección IP válida de host en el segmento de direccionamiento administrativo.

Las figuras 34 y 35 muestran las configuraciones de las interfaces IP de algunas VC de nodo de acceso, la localidad CDC y localidad 4 respectivamente.

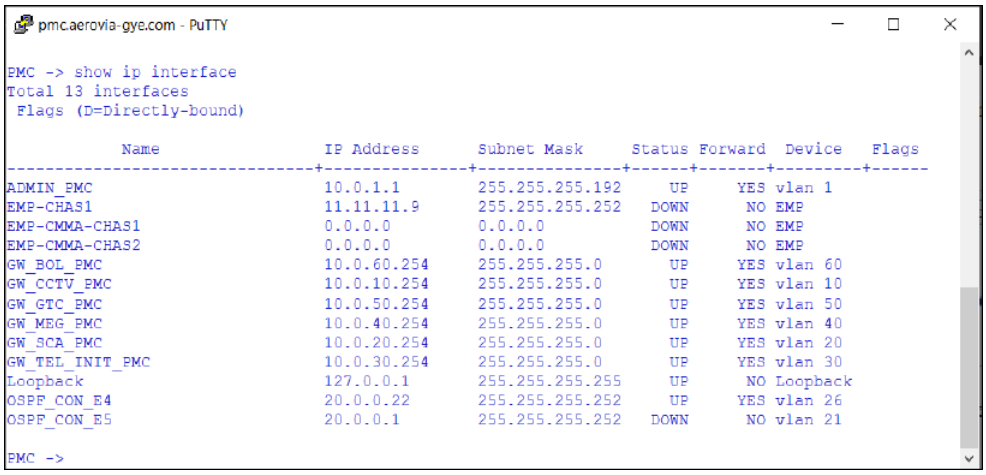

Figura 2.33. Direcciones IP de interfaz en switch nodo acceso CDC.

Fuente: Autor

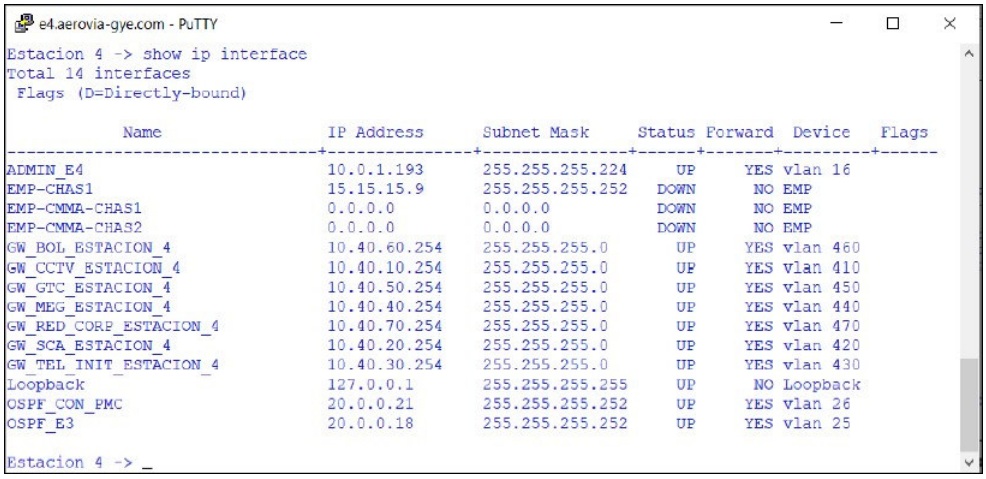

Figura 2.34. Direcciones IP de interfaz en switch nodo acceso E4.

Fuente: Autor

Para los demás switches de nodo acceso, el resultado es muy similar al mostrado en las figuras anteriores. El direccionamiento empleado es aquel que se describió en la tabla 2 de la sección 4.2. Nótese además que se ha dado un nombre descriptivo y en mayúsculas a la respectiva interfaz IP, con la finalidad de hacer más fáciles las tareas de configuración, así como también los procesos posibles de troubleshooting.

Ahora para los switches de borde donde se conectan los equipos de los diferentes sistemas de transporte se configuró una única dirección IP para la administración y configuración del switch, ver figura 2.35.

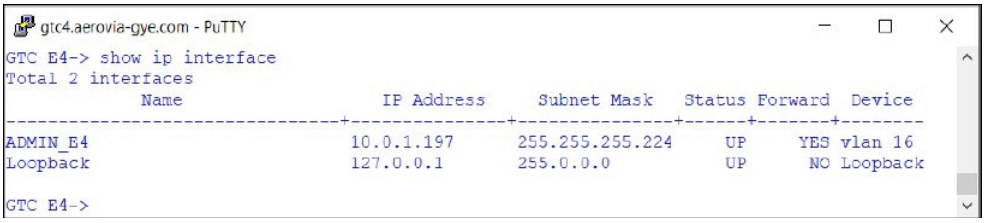

Figura 2.35. Dirección IP interfaz en switch de borde.

Fuente: Autor

OSPF (Open Shortest Path First).

OSPF es un protocolo de enrutamiento dinámico unicast que permite la convergencia de tablas de enrutamiento dentro de un sistema autónomo (AS), de tal manera que todos los nodos capa 3 sepan cómo alcanzar cualquier otra red dentro de los límites de dicho sistema autónomo.

El protocolo crea adyacencias entre los nodos habilitados con OSPF que permite comunicarse con sus vecinos y dar origen a un árbol de estado de enlace, con lo cual cada nodo conoce las direcciones IP de siguientes saltos para continuar la ruta óptima hacia una red de destino en particular. Es imperativo mencionar que, se entiende por óptima a toda ruta que sea más corta o rápida.

OSPFv2 es un protocolo de tipo IGP (Interior Gateway Protocol), al igual que los protocolos de vector distancia como RIP (Routing Information Protocol), pero a diferencia de estos últimos, OSPF toma en consideración otras variables como velocidad, costo y congestión de las posibles rutas para construir su árbol de rutas preferentes a cada destino. RIP solo toma en consideración el número de saltos hasta llegar al destino.

Adicional a las ventajas mostradas en el párrafo anterior, OSPF tiene tiempos de convergencia más rápidos que todos los algoritmos de enrutamiento de vector distancia.

Por lo tanto, lo descrito anteriormente sobre la existencia de una topología de anillo de la red y la necesidad del proyecto de tener nodos de acceso enrutables independientes, fue lo que llevó a tomar la decisión de implementar sobre el ERP, un protocolo de enrutamiento dinámico como es el OSPF. En las configuraciones de OSPF se toma en cuenta lo siguiente:

- Los enlaces que conforman el anillo entre nodos pueden considerarse punto a punto.
- Las interfaces IP participantes en el algoritmo de distribución de rutas o construcción de árboles de estado de enlace, son

aquellas que constituyen los gateways de los sistemas y redes de administración.

- Tiempo de convergencia menor a 5 segundos.

A continuación, se muestra un gráfico descriptivo, a partir del cual se puede entender la configuración de OSPF en la red:

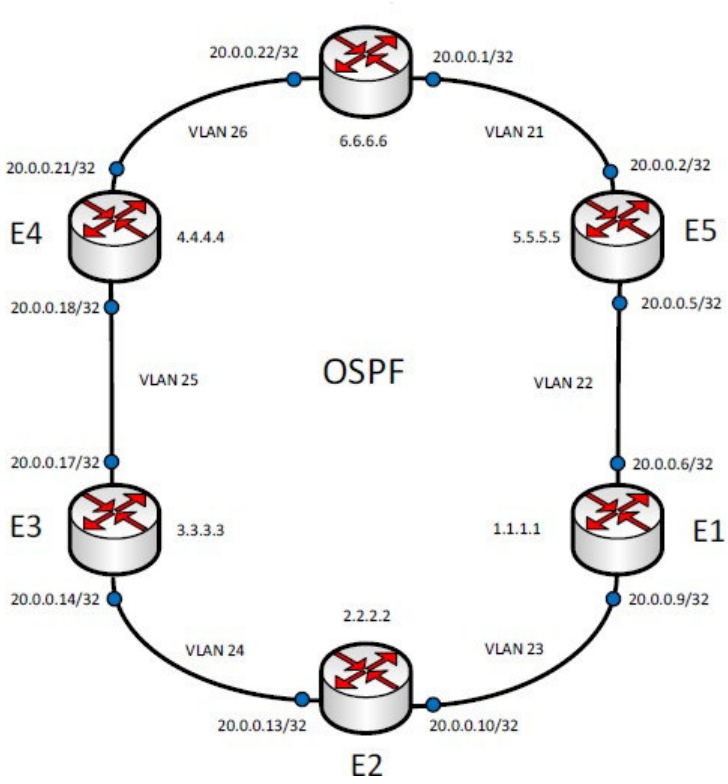

Figura 2.36. Topología OSPF.

Fuente: Autor

En la figura 2.36 se explica que las configuraciones de OSPF se basan en la disponibilidad de enlaces punto a punto entre cada uno de los nodos de acceso. Dichos enlaces se identifican y

conforman a través de una VLAN en particular. A continuación, se mostrará un ejemplo para CDC:

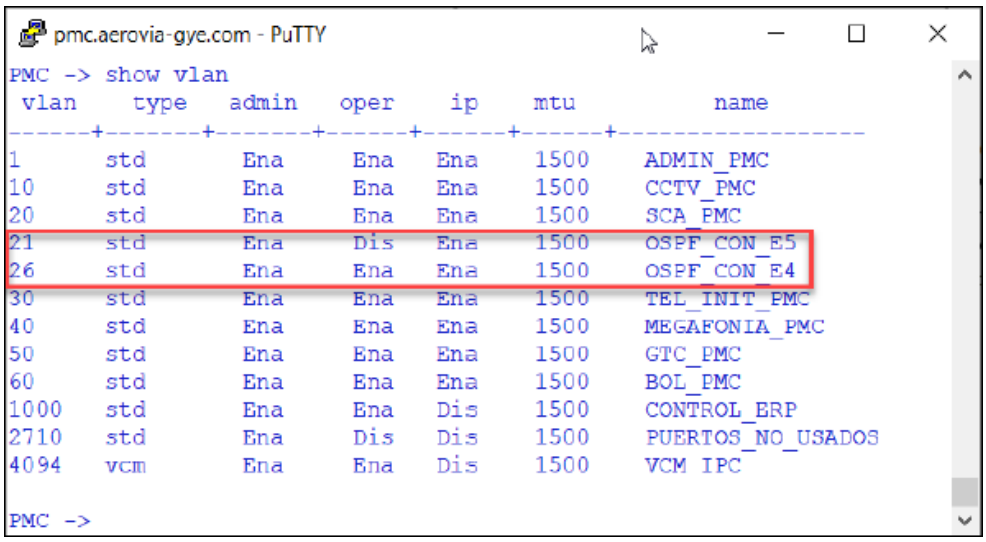

Figura 2.37. VLANs exclusivas para enlaces punto a punto OSPF - CDC.

Fuente: Autor

Cada switch de nodo de acceso contó con sus propias VLANs para OSPF, en las cuales también se asociaron IPs de interfaz. Estas direcciones IP fueron exclusivas para el enlace punto a punto, por lo cual su máscara de red es de prefijo 32. Es decir, solamente hubo dos direcciones para la conformación del enlace porque fue lo necesario, referirse a la figura 2.37, que es un ejemplo de las configuraciones de las interfaces IP utilizadas que permitieron unir la localidad de CDC, E4 y E5.

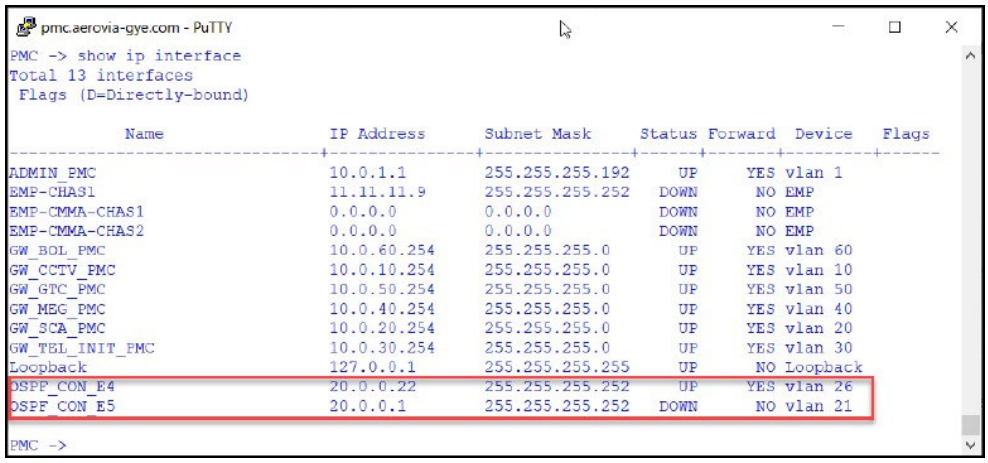

Figura 2.38. Interfaces IP de enlace punto a punto OSPF CDC.

Fuente: Autor

Es importante observar que en esta sección se está hablando de un diseño de capa 3, por lo que no es necesario troncalizar los LACPs con las diferentes VLANs, solo debe cursarse la VLAN de enlace (21 y 26) y la VLAN de servicio 1000 del ERP en el caso de la localidad de CDC, ver figura 2.38.

Para las otras localidades el procedimiento se repitió, considerar la figura 2.38 como referencia, para profundizar en los aspectos mencionados.

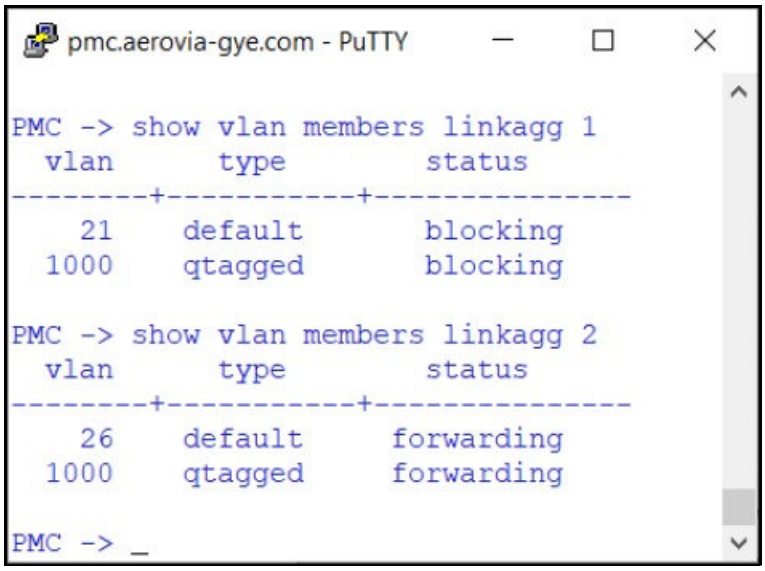

Figura 2.39. Asignación de VLANs a enlace punto a punto CDC.

Fuente: Autor

Cuando se realizaron todas las configuraciones y se levantó el anillo de la red, se continuó con las configuraciones del protocolo de enrutamiento dinámico OSPF, a continuación, se describen los pasos a seguir:

- Cargar OSPF en la memoria del switch de nodo acceso.
- Habilitar OSPF de manera global.
- Designar un router ID para el switch de nodo acceso
- Declarar el área de OSPF.
- Declarar las interfaces IP que participarán en el algoritmo OSPF y asociarlas con el área OSPF anterior.

La figura 2.40, muestra el resultado de la configuración del protocolo de enrutamiento dinámico OSPF aplicado al VC de CDC.

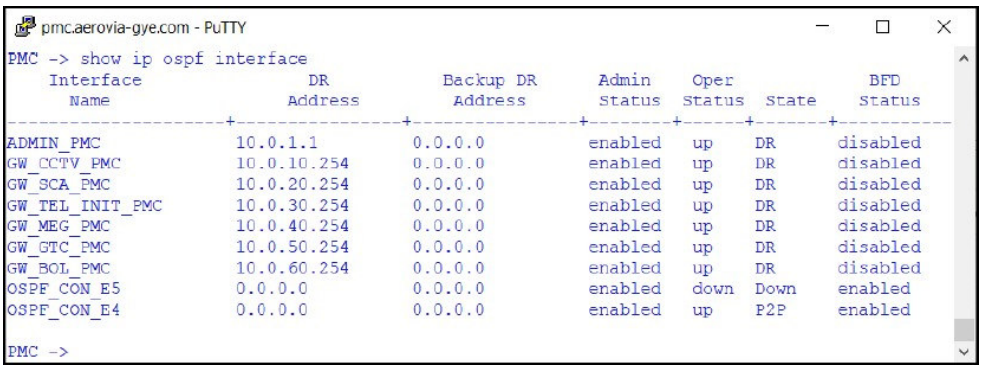

Figura 2.40. Interfaces OSPF en CDC.

Fuente: Autor

En la figura 2.40 se pudieron evidenciar todas las interfaces IP del nodo CDC que participaron en el algoritmo OSPF. Nótese que para habilitar una interfaz IP como Interfaz válida en OSPF se tuvo que usar el mismo nombre que se registró cuando se la creó. Por otra parte, hay dos tipos de interfaces OSPF:

- Interfaces de punto a punto: son aquellas que intervienen en la conformación del enlace punto apunto entre nodos de acceso.
- Interfaces no punto a punto: son aquellas que pertenecen a los gateways de los sistemas de transporte o a la interfaz administrativa.

Cuando se realizaron las configuraciones de OSPF en todos los VC formados por los SW en los nodos del anillo, se pudo ver que el backbone, área del OSPF, estaba levantado e interactuando con sus router OSPF vecinos, lo descrito se puede ver en la figura 2.41.

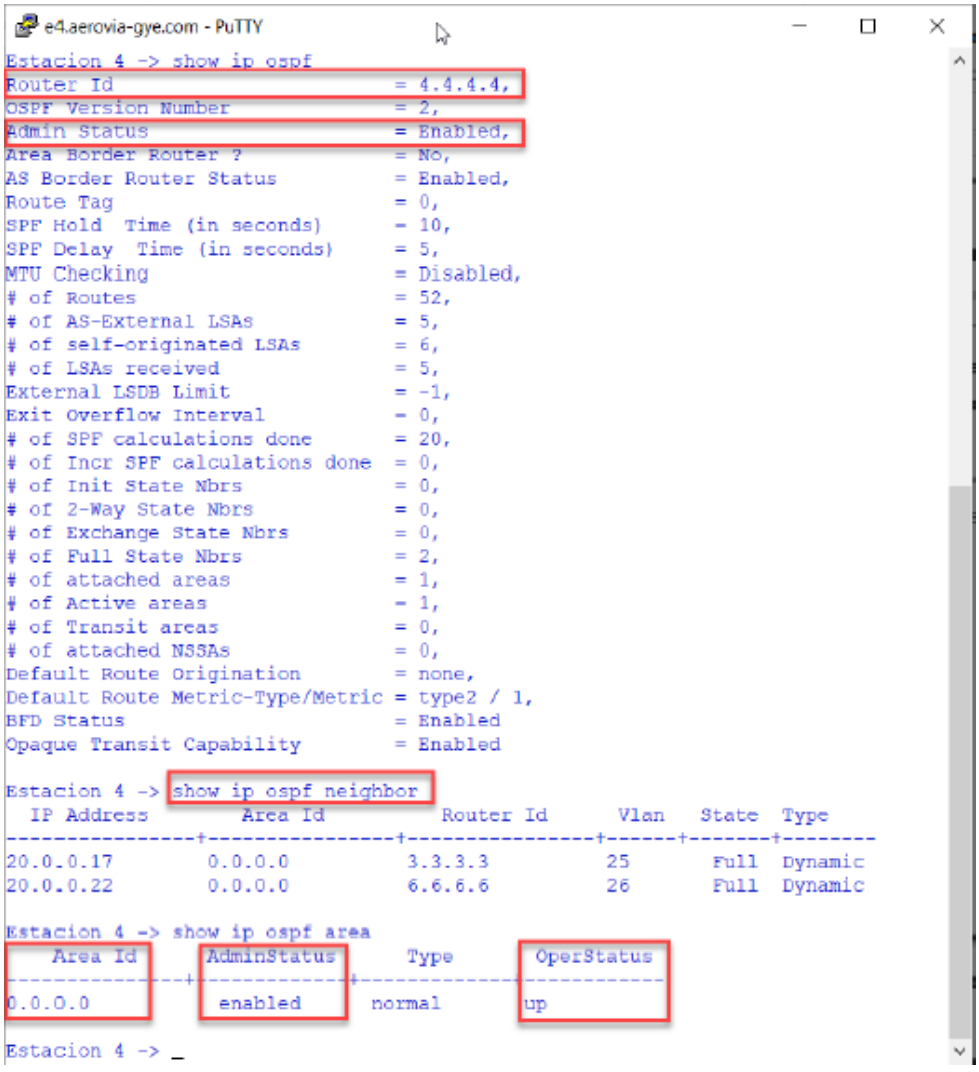

Figura 2.41. Verificación de parámetros OSPF – E4.

Fuente: Autor

La figura 2.42 muestra la existencia de intercambio de información vía algoritmo de OSPF, en este caso se actualizaron rutas que le permitieron a la localidad E4 alcanzar redes externas.

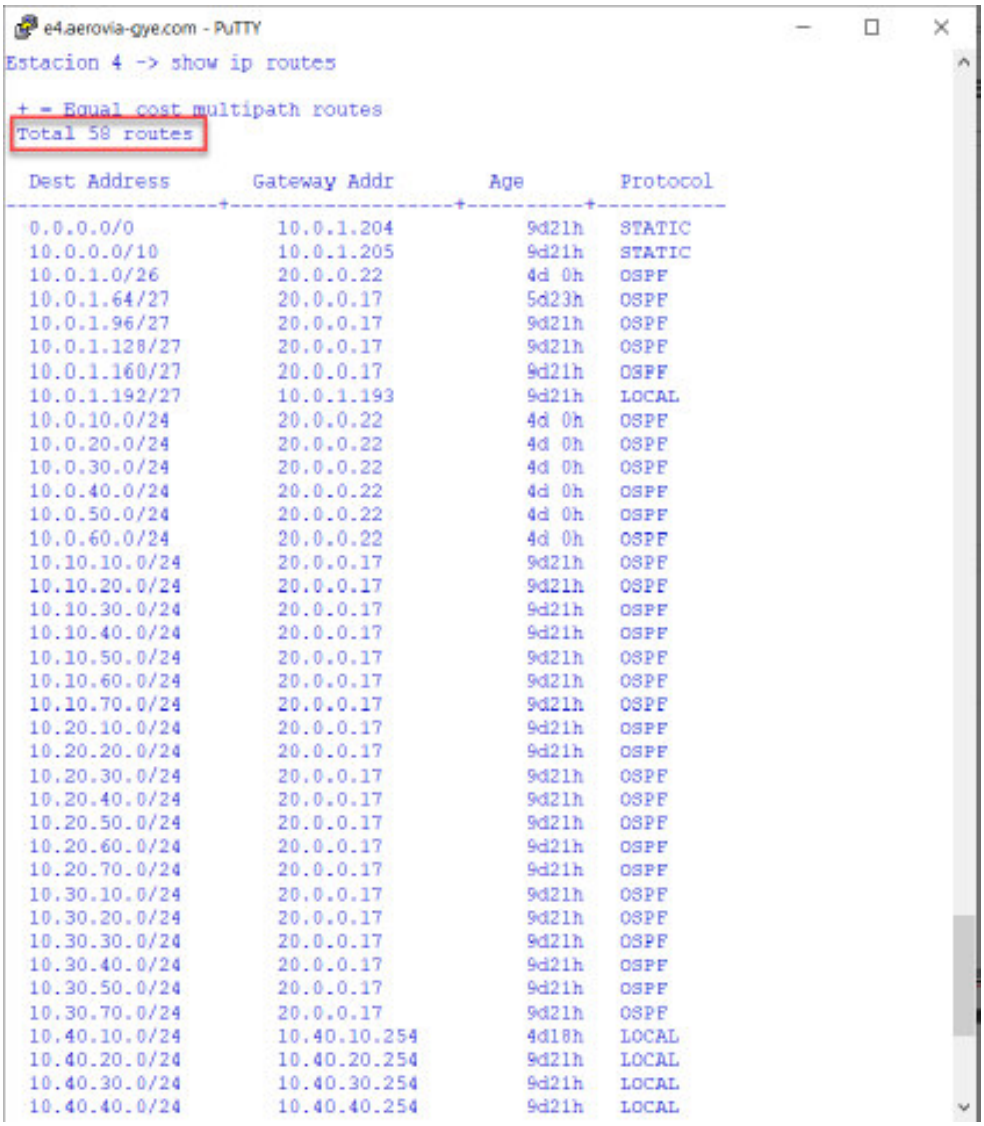

Figura 2.42. Verificación de parámetros OSPF – E4(2).

Fuente: Autor

PIM-SM (Protocol Independient Multicast – Sparte Mode).

PIM – SM es un protocolo de enrutamiento exclusivamente diseñado para tráfico multicast, ya que los protocolos de enrutamiento dinámico clásicos como RIP, OSPF, ISIS, entre otros, no pueden lidiar con las características específicas de este tipo de tráfico y solamente operan a nivel unicast.

Por lo tanto, es necesario analizar los protocolos de enrutamiento multicast, entre los cuales se tiene: DVMRP (Distance Vector Multicast Routing Protocol) y PIM (Protocol Independent Multicast).

DVMRP construye su propia tabla de enrutamiento, mientras que PIM utiliza el protocolo de enrutamiento unicast subyacente a la tabla de enrutamiento generada para hacer llegar los paquetes.

A continuación, se profundizará en el protocolo de enrutamiento PIM, ya que este fue implementado en el proyecto.

PIM puede ser implementado en dos versiones: DM (Dense Mode) y SM (Sparse Mode). A continuación, se especificarán las características de cada uno:

- El PIM DM implementa un mecanismo de Flood and Pruning, lo cual quiere decir que
- inicialmente el tráfico multicast se envía hacia todos los rincones de la topología (Flooding) sin que se lo haya pedido explícitamente, de no haber receptores en alguna parte de la topología el router de borde de aquella parte rechaza el flujo (Pruning). Eventualmente solo queda un árbol de trasmisión multicast constituido por el origen y aquellos routers que aceptaron el flujo. Este procedimiento se repite cada cierto período, flood and pruning.
- El PIM SM se basa en las solicitudes de los clientes finales, de manera que el tráfico no inunda toda la red, ya que se establecen árboles SPF (Shortest Path Firts) a destinos específicos.
- Por lo tanto, en PIM SM, se tiene una estructura de funcionamiento más compleja en la cual una de las entidades más importantes es un punto intermedio llamado RP (Rendezvous Point). De manera que el servidor de contenido tiene contacto solamente con el RP y este último con los routers finales que soliciten el flujo multicast, las figuras 44 y 45 muestran la suscripción y flujo multicast del PIM SM.

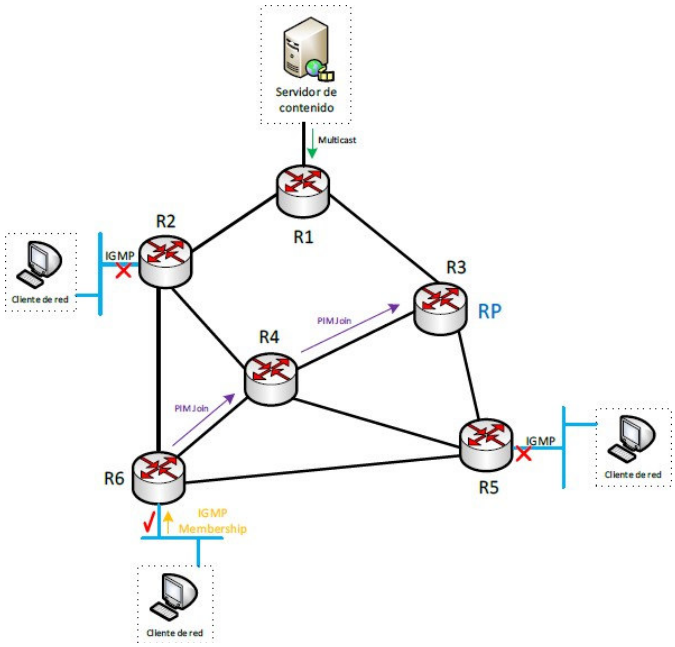

Figura 2.43. Suscripción a un grupo multicast PIM SM.

Fuente: Autor

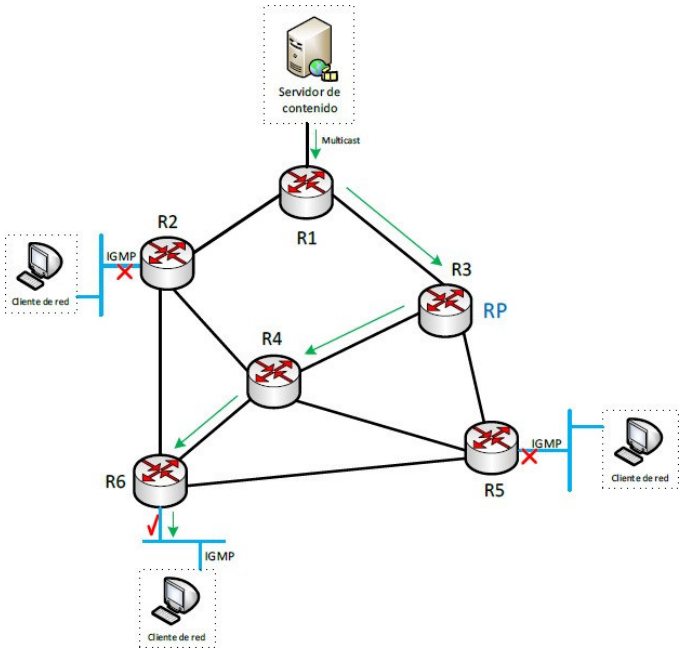

Figura 2.44. Flujo multicast en PIM SM.

Fuente: Autor

Después de haber conocido de manera muy general los aspectos básicos del funcionamiento de multicast y su protocolo de enrutamiento PIM, se procede a analizar su adaptación con lo requerido en el proyecto. En la sección 3.4 del presente documento se mencionó que el sistema de transporte Sonido tiene como requisito el uso de multicast.

Es importante mencionar que Sonido no es más que un sistema de sonido avanzado y en alta definición para todas las localidades del proyecto. El servidor de contenido, que origina las emisiones de sonido se encuentra en CDC.

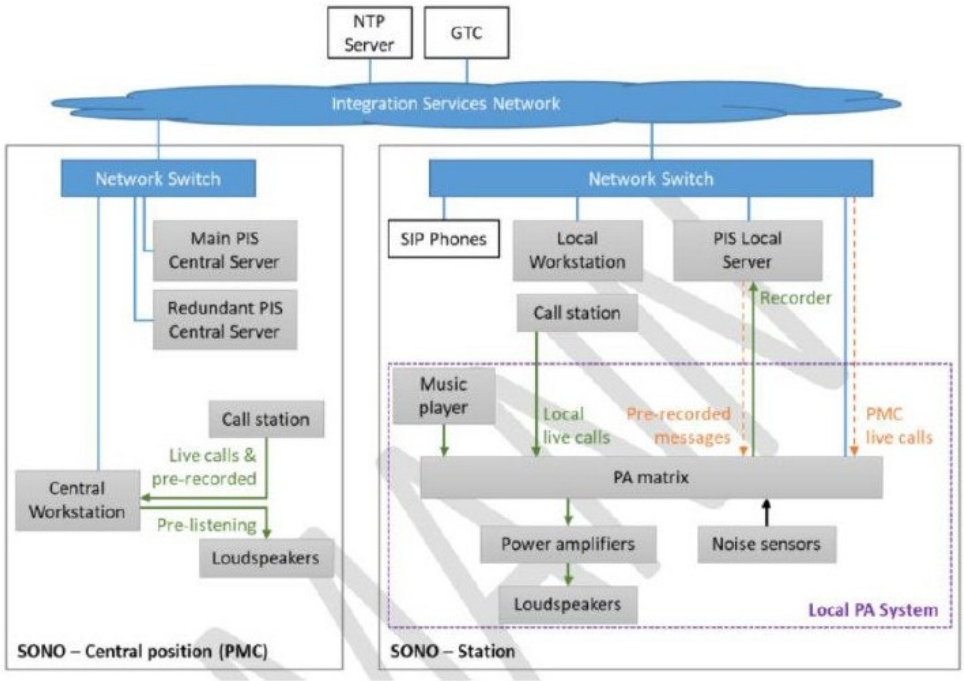

Figura 2.45. Estructura general sistema de Sonido.

Fuente: Autor

Al servidor de contenido se lo denominó PIS, este y su correspondiente redundancia solamente existen en CDC y no en alguna otra localidad. Esta particularidad, y los comentarios de los encargados de aquel sistema, indicaron que no habrá transmisiones multicast desde alguna localidad que no sea CDC. PIM se encuentra configurado para que cualquier localidad pueda iniciar una transmisión de difusión.

Con estos datos se ha realizado la siguiente planificación para el funcionamiento de PIM – SM en la infraestructura de red:

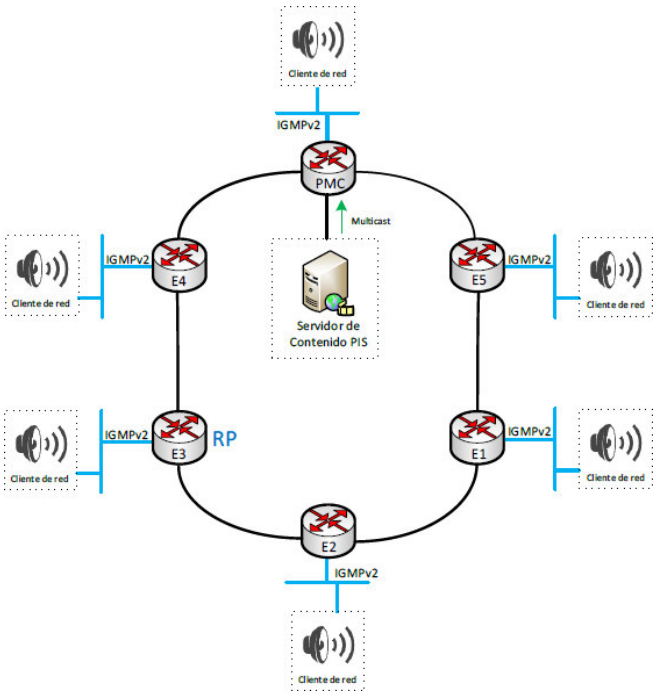

Figura 2.46. Elementos multicast PIM SM.

Fuente: Autor

Se ha designado de manera arbitraria al switch de nodo acceso de E3 como el RP, que como se ha visto, es el encargado de difundir el tráfico multicast hacia las demás localidades desde CDC.

Para configurar PIM-SM, se deben realizar las siguientes tareas:

- Cargar PIM en la memoria del switch.
- Habilitar PIM en las interfaces respectivas del anillo y aquella relacionada con Sonido.

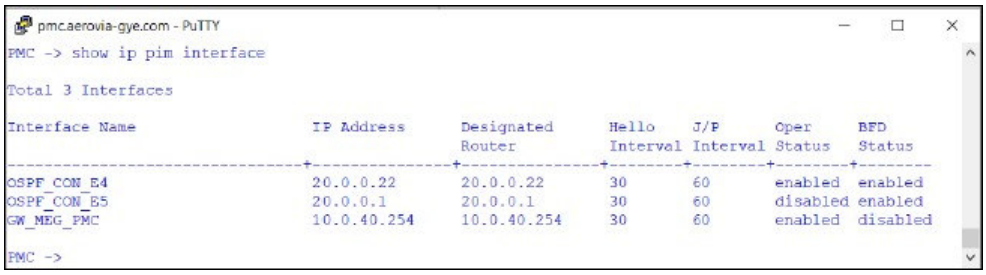

Figura 2.47. Interfaces PIM CDC.

Fuente: Autor

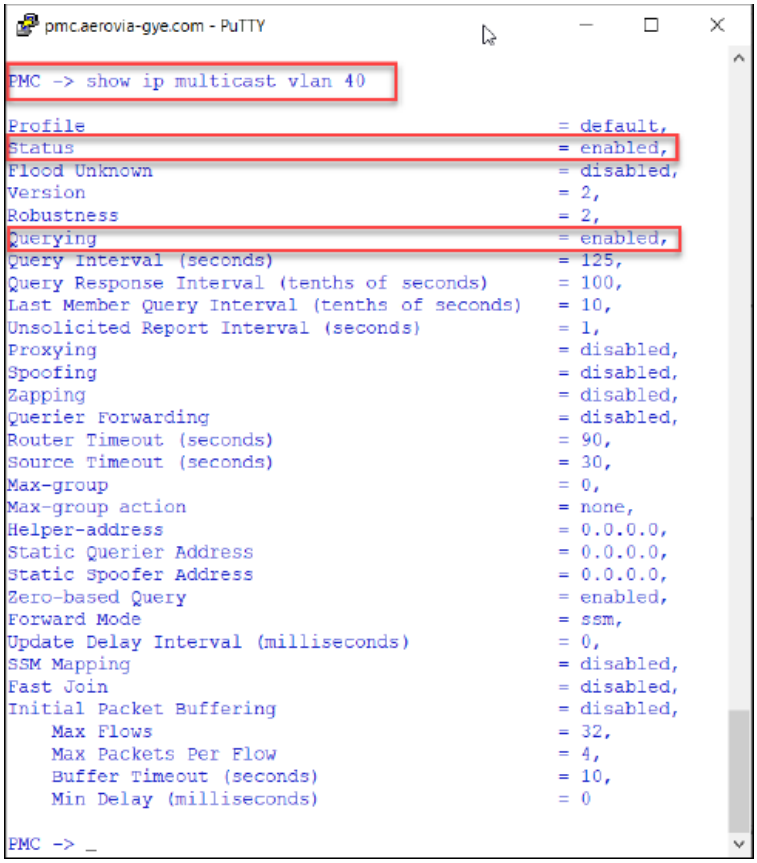

Figura 2.48. IPMS habilitado por defecto en VLAN 40 (MEG).

Fuente: Autor

- Habilitar el modo SM de PIM.

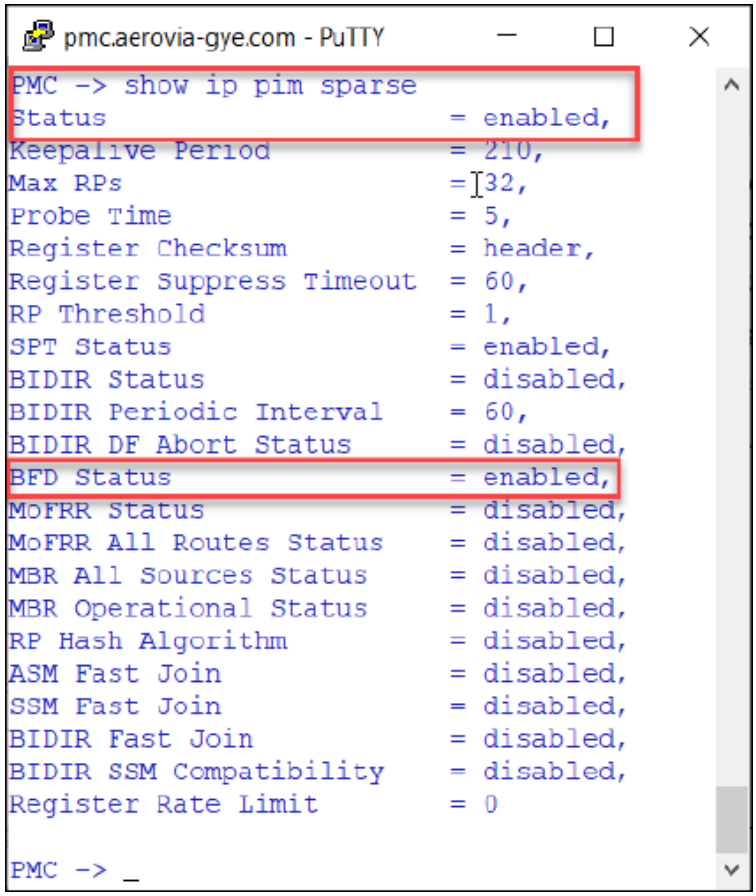

Figura 2.49. PIM SM habilitado en CDC.

Fuente: Autor

- Configurar un C-BSR.

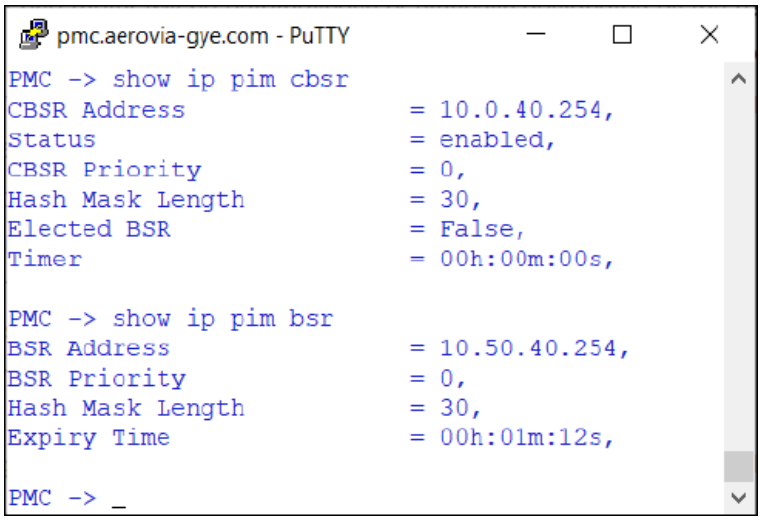

Figura 2.50. CBSR y BSR en PIM SM en CDC.

Fuente: Autor

Ahora bien, la configuración mostrada con anterioridad obedece a las realizadas en CDC y es importante mencionar que es la misma para el resto de las localidades, con excepción de la E3 cuyo nodo de acceso tiene asignado el rol de RP (Rendezvous Point). Para esta localidad la secuencia de configuración fue la siguiente:

- Cargar PIM en la memoria del switch.
- Habilitar PIM en las interfaces respectivas del anillo y aquella relacionada con Sonido.
- Habilitar el modo SM de PIM
- Configurar un C-BSR

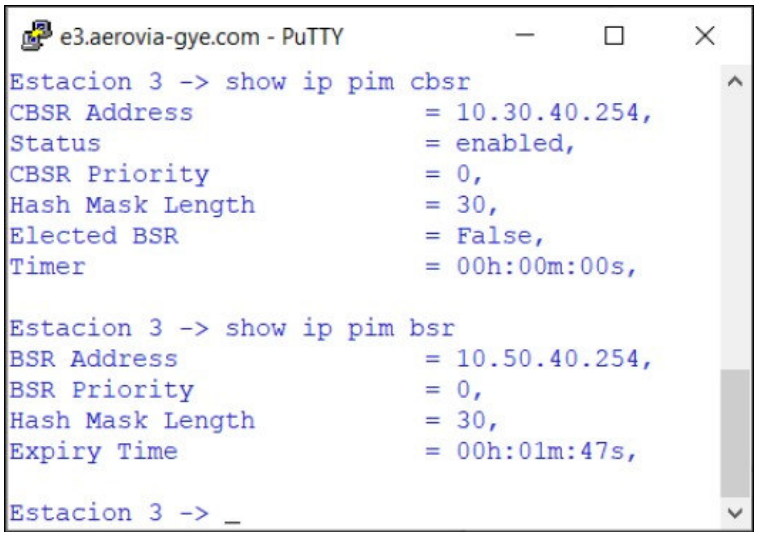

Figura 2.51. CBSR y BSR en PIM SM en E3.

Fuente: Autor

- Declarar el RP para grupos de difusión multicast específicos.

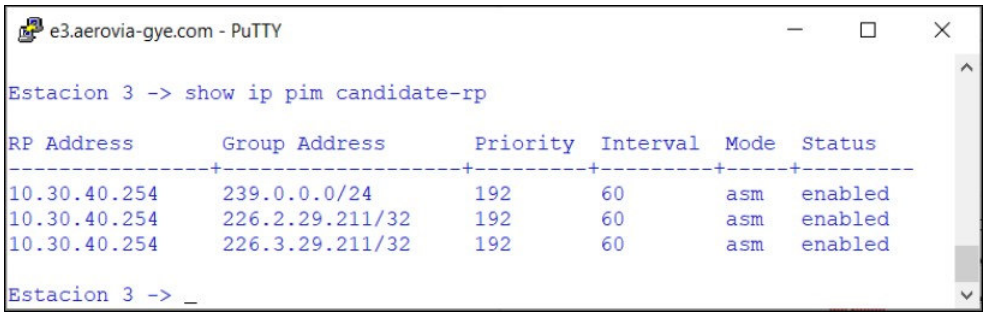

Figura 2.52. Flujos multicast asignado al RP E3.

Fuente: Autor

Mediante la configuración de todos los switches de nodo acceso según lo mencionado, es posible transmitir flujo multicast desde CDC hacia cualquier otra localidad. Esto último fue confirmado por los responsables del sistema de transporte de Sonido. No

obstante, algunos comandos para verificar el funcionamiento de multicast mientras se esté transportando un flujo son:

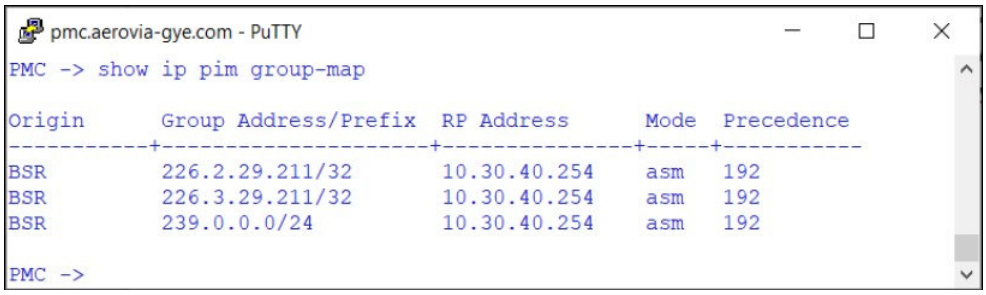

Figura 2.53. Flujos multicast.

Fuente: Autor

Figura 2.54. Interfaces vecinas PIM desde E3.

Fuente: Autor

DNS (Domain Name Server).

DNS es una base de datos que asocia direcciones IP con nombres de dominio.

En el proyecto el servicio DNS se utiliza para resolver principalmente nombres de dominio para los servidores de los sistemas de transporte de Tickets, control de acceso y CCTV.

Adicional a estas correspondencias, también se ha configurado lo que se conoce como nombres canónicos en DNS.

El proyecto tiene un servidor DNS que se encuentra funcionando en el firewall (10.0.1.205) designado como UTM de voz y los registros de las dos tablas anteriores se encuentran configuradas en dicho equipo.

En el firewall, las configuraciones de las entradas de DNS pueden ser, una correspondencia simple entre un nombre y una IP o un nombre Canónico (CNAME). A continuación, se muestra un ejemplo de ambos en la figura 2.55 y 2.56 respectivamente.

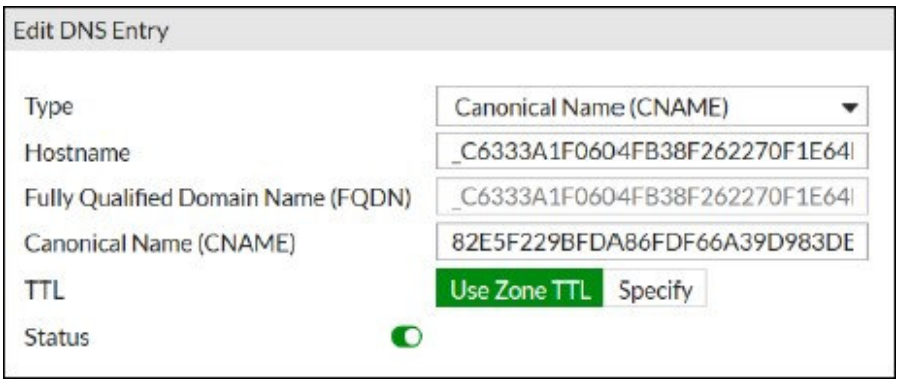

Figura 2.55. Ingreso de registro DNS simple.

Fuente: Autor

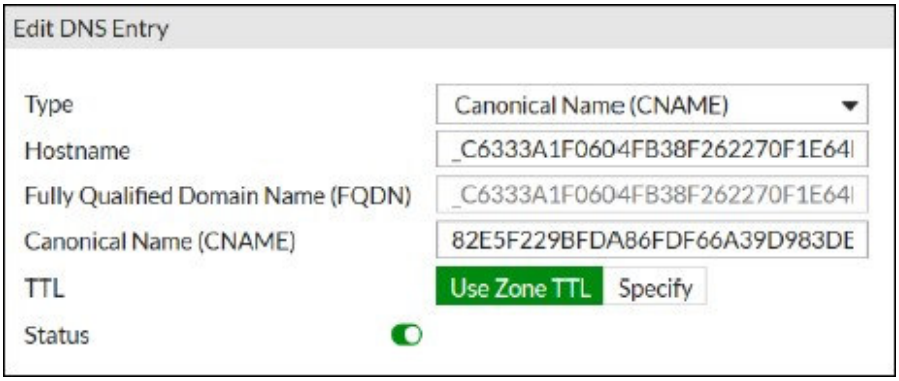

Figura 2.56. Ingreso de registro CNAME.

Fuente: Autor

NTP (Network Time Protocol).

El protocolo NTP es muy útil cuando se trata de la verificación de logs, correlación de eventos pasados y otras funcionalidades para tener una única referencia de tiempo.

El NTP es un servicio, por lo tanto, habrá clientes y un servidor, los primeros tomarán los registros temporales del segundo.

En el proyecto, la sincronización de tiempo la provee un único equipo ubicado en CDC, es decir es un appliance dedicado para el efecto, su marca es NETSILON BODET. Este dispositivo tiene la capacidad de tomar la referencia de tiempo desde el servicio GPS, Internet, o ser su propia referencia. A este último modo se le denomina freerun y es el que fue escogido para proveer la referencia de tiempo a cualquier otro equipo dentro de la red.

Los equipos clientes constituyen todos los switches, tanto de nodo acceso como aquellos de borde para la conexión de sistemas de transporte. Además de todas las instancias de servidores para Omnivista 2500, Omnivista 8770, Vmware EXSi y Windows Server 2019. Es posible que los servidores de transporte también sincronicen sus relojes desde el NETSILON.

A continuación, la figura 2.58, muestra la interfaz gráfica del servidor NTP NETSILON, que permitirá su configuración, ajustándose a las necesidades del cliente.

Para iniciar la configuración del NTP NETSILON, se siguieron los pasos que se describen a continuación:

- Definir sincronización, en este caso se elige la freerun.

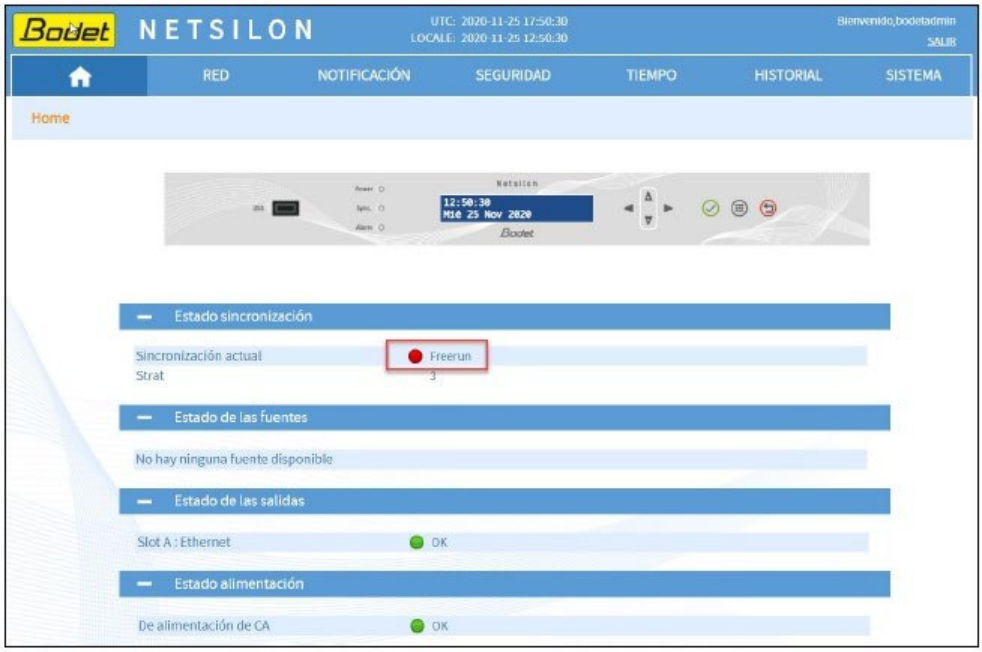

Figura 2.57. Pantalla inicial NTP Server Netsilon.

Fuente: Autor

- Asignar una IP al NTP NETSILON, la asignada es la 10.0.1.9/27.

Figura 2.58. Sección de parámetros IP Netsilon NTP Server.

Fuente: Autor

- Habilitar en la red el servicio de Time Protocol.

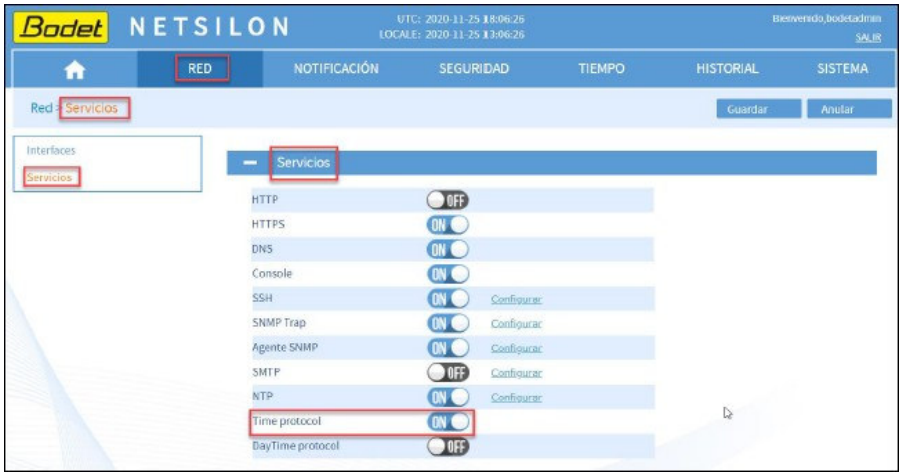

Figura 2.59. Time Protocol habilitado.

Fuente: Autor

- Configuración de parámetros de tiempo.

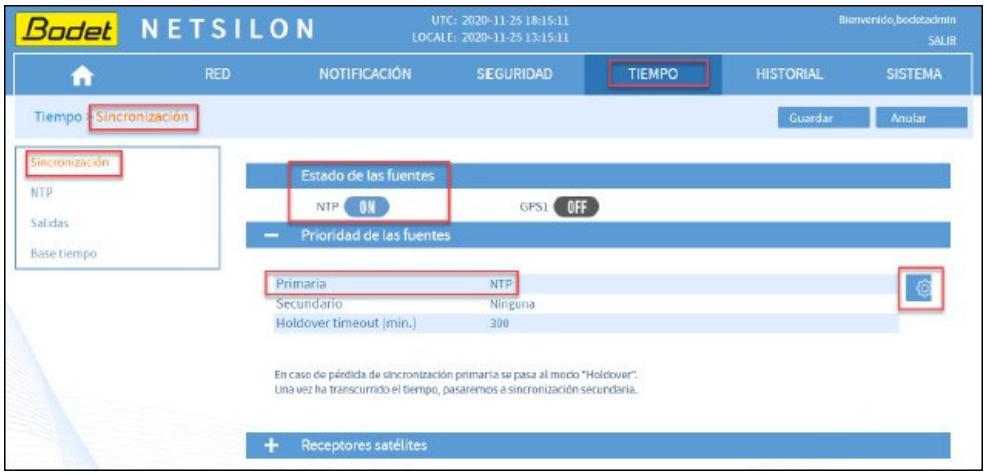

Figura 2.60. Configuración y habilitación de parámetros.

Fuente: Autor

Figura 2.61. Habilitación del servicio NTP.

Fuente: Autor

- Configuración de zona horaria.

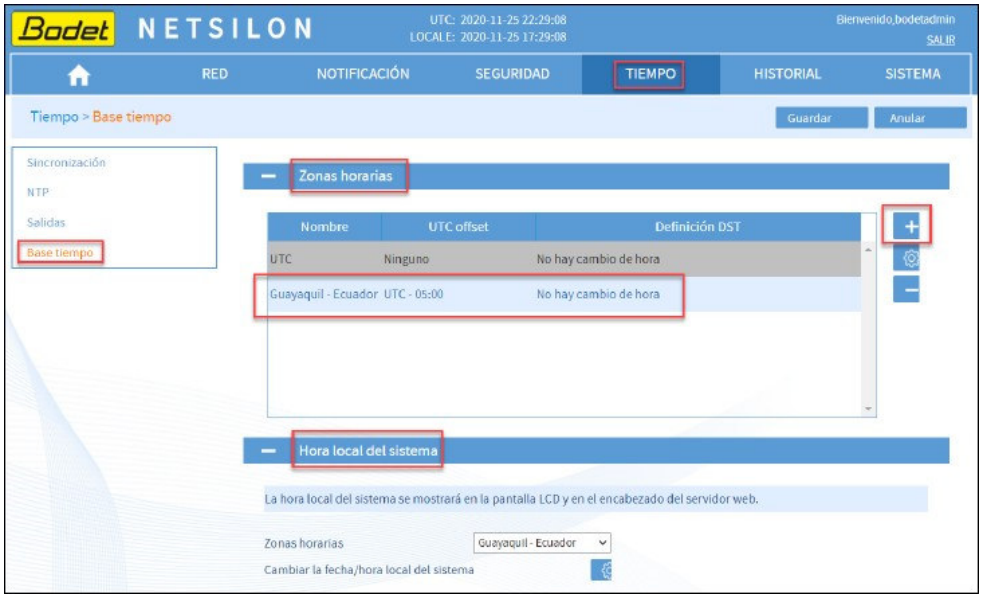

Figura 2.62. Configuración de zonas horarias NTP Server.

Fuente: Autor

Estas fueron las configuraciones necesarias en el NTP Server para lograr la sincronización de tiempo de todos los equipos de red. Lo siguiente fue indicar la configuración de los clientes NTP.

- Switches de nodo acceso

  En los VC, se tuvo que configurar tanto la IP del servidor NTP (10.0.1.9) como la zona horaria, siendo este último paso el más importante para disponer de los parámetros de tiempo correctos.

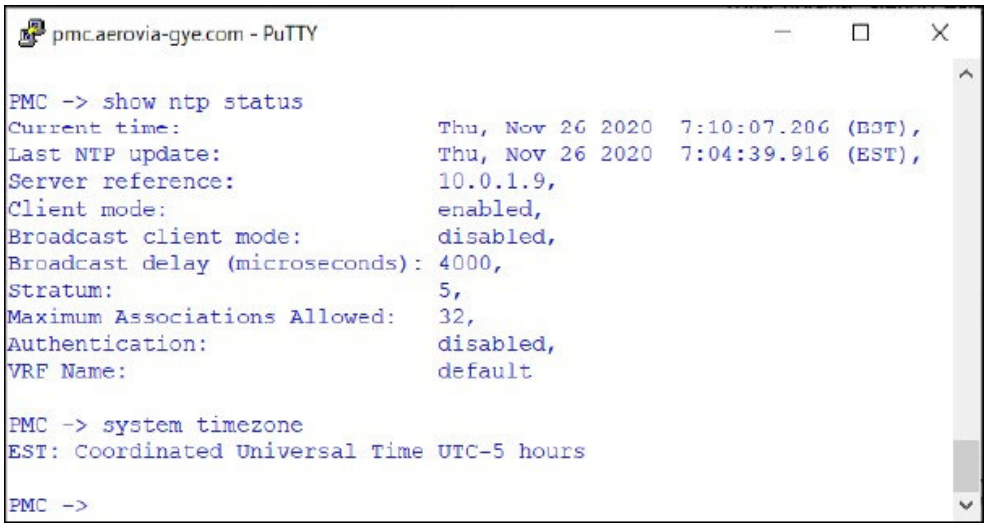

Figura 2.63. Estado cliente NTP nodo acceso CDC.

Fuente: Autor

- Switches de borde

  En los switches de borde la lógica de funcionamiento fue la misma.

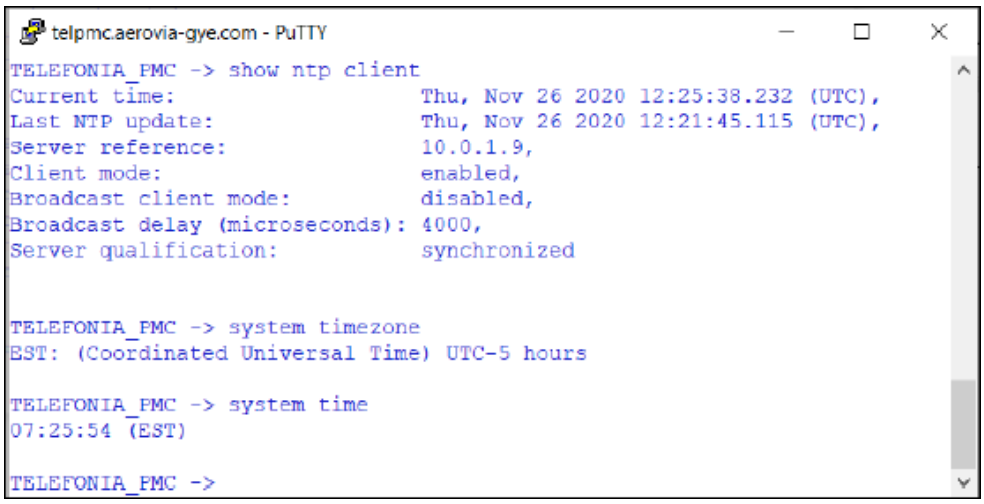

Figura 2.64. Estado cliente NTP switch de borde.

Fuente: Autor

Es importante mencionar que cuando se configuró la funcionalidad NTP la sincronización no se dio de inmediato, pues esta tarda unos minutos hasta que se tomen los datos.

- Servidor Omnivista 2500

  En Omnivista 2500 la configuración del NTP fue igual de sencilla y también se la realizó a través de la interfaz de línea de comandos.

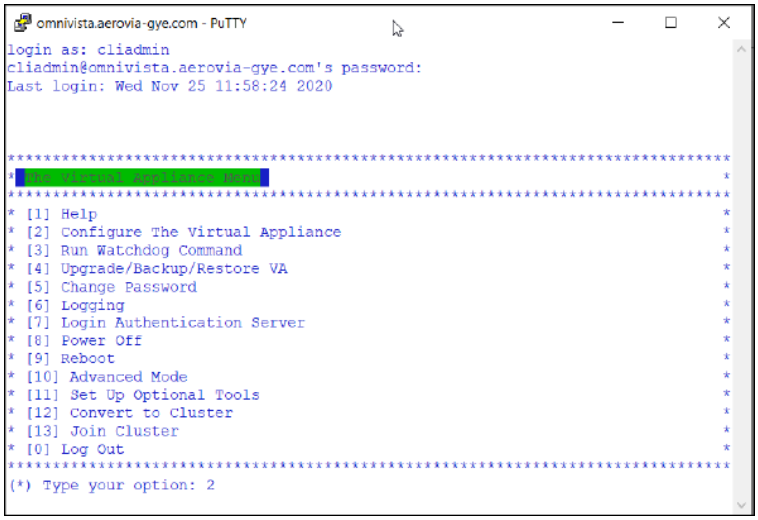

Figura 2.65. Menú principal OV2500 CLI.

Fuente: Autor

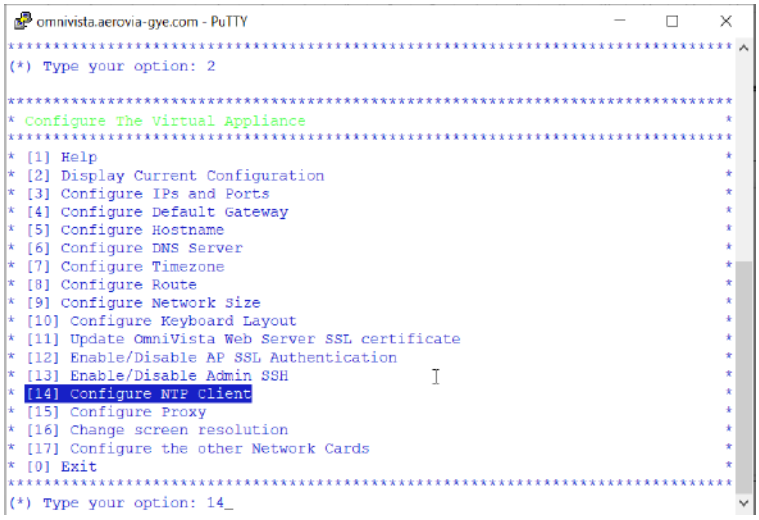

Figura 2.66. Menú configuración de Virtual Appliance OV2500.

Fuente: Autor

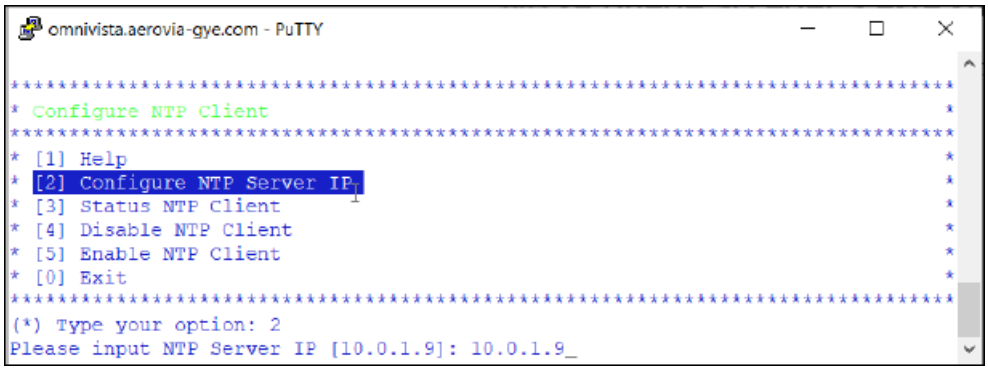

Figura 2.67. Configuración de NTP OV2500.

Fuente: Autor

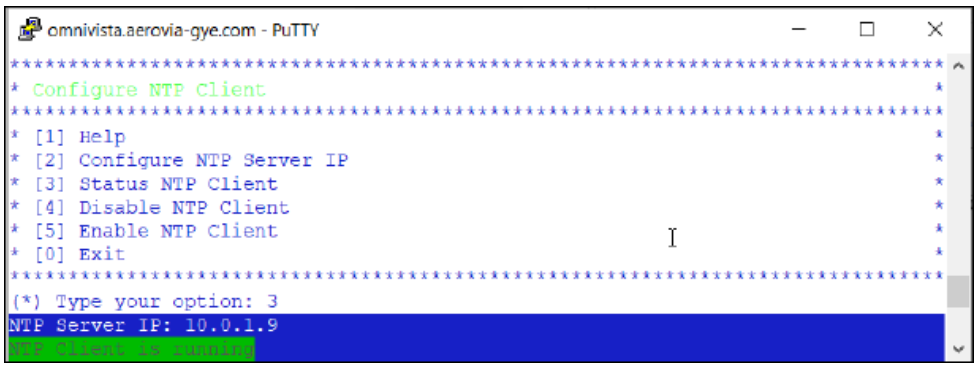

Figura 2.68. Verificación servicio NTP OV2500.

Fuente: Autor

Es imperativo recalcar la importancia que tuvo la buena configuración del NTP server en OV2500, la misma que fue necesaria para el módulo llamado notificaciones, el cual presenta todas las alarmas en tiempo real respecto de lo que va sucediendo con la topología de la red y evidentemente, los eventos de este módulo tienen la hora exacta y precisa.

- VMware ESXi

  Este es el sistema operativo del servidor donde residen las máquinas virtuales del Omnivista 2500, Omnivista 8770 y Servidor de gestión de seguridad de la red. En vista de esto, también tiene su cliente NTP sincronizado para cualquier correlación de eventos. A continuación, se muestra la forma de configurarlo.

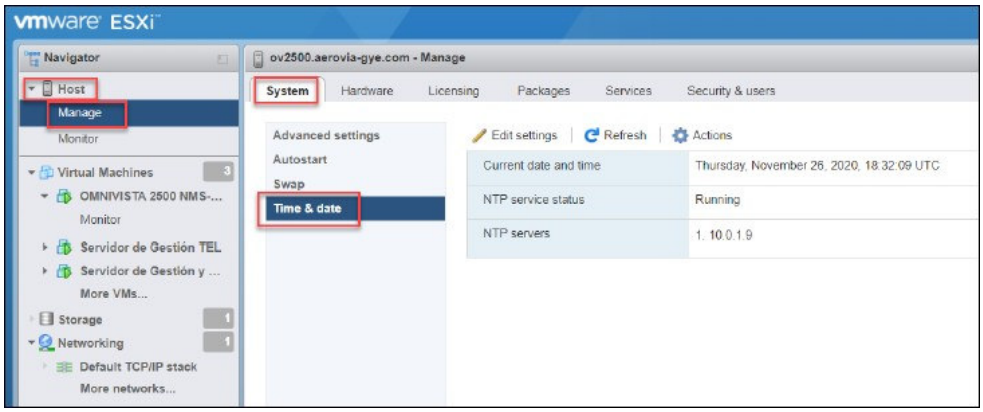

Figura 2.69. Administración Host Vmware ESXi.

Fuente: Autor

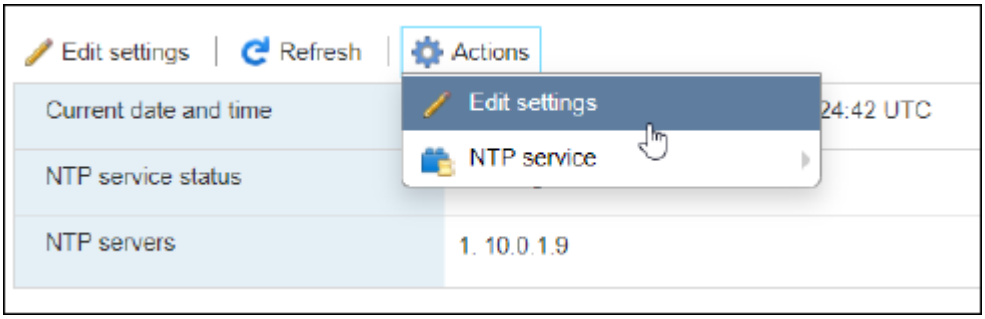

Figura 2.70. Editar configuraciones NTP en Vmware ESXi.

Fuente: Autor

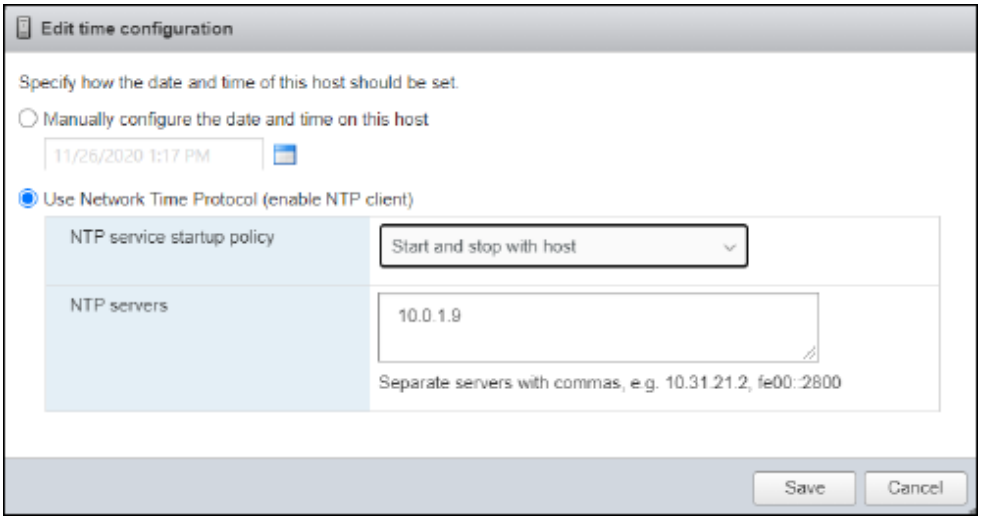

Figura 2.71. Configuración NTP en Vmware ESXi 6.7.

Fuente: Autor

2.2.2 SEGURIDAD

En el diseño de seguridad de la infraestructura de red, física y lógica, se trató de tomar en consideración todas las aristas posibles. Se partió de la premisa en la que todas las comunicaciones debían estar cerradas y se tenía que abrir aquello que era estrictamente necesario.

En los siguientes tópicos se abordarán temas relacionados con seguridad física, de administración, de comunicación, protección contra eventos de red inesperados, entre otros.

Gestión

Garantizar la administración de toda la infraestructura de red, en cualquier circunstancia, durante la operación es de suma importancia. Esta permite mantener el control del desempeño de la red y dar el soporte requerido por los diferentes sistemas de transporte en todo momento. Es debido a esto, que el tráfico de configuración y monitoreo debe tener reservado sus propios recursos para que pueda ser cursado inclusive durante una tormenta de broadcast en red, lo cual se logra, entre otras estrategias, al asignar una VLAN separada con un segmento de red dedicado.

Localidad	Dirección de red	Máscara	Gateway	VLAN ID
CDC	10.0.1.1/26	255.255.255.192	10.0.1.1	1
E1	10.0.1.96/27	255.255.255.224	10.0.1.97	13
E2	10.0.1.128/27	255.255.255.224	10.0.1.129	14
E3	10.0.1.160/27	255.255.255.224	10.0.1.161	15
E4	10.0.1.192/27	255.255.255.224	10.0.1.193	16
E5	10.0.1.64/27	255.255.255.224	10.0.1.65	17

Tabla 3. Direccionamiento de administración por localidad.

El espacio en direcciones para cada segmento de red en la tabla anterior está dimensionado para tratar de ajustarse al mínimo necesario. Ahora bien, no solamente los switches ocupan estas direcciones IP sino también otros que conforman la

infraestructura de red en su totalidad. Por ejemplo, se puede evidenciar que el segmento de administración para CDC tiene un prefijo 26, lo cual le permite tener hasta 62 hosts, parte de los cuales serán usados por 27 switches industriales para las pilonas, así como también por los equipos en las localidades.

Localidad	Servicio	IP ADMIN SW	VLAN
CDC	ADMIN	10.0.1.1	1
	CCTV	10.0.1.3	
	SCA	10.0.1.8	
	TEL	10.0.1.4	
	MEG	10.0.1.5	
	GTC	10.0.1.6	
	BOL	10.0.1.7	
	VMWARE	10.0.1.12	
	OV2500	10.0.1.10	
	IHM OV2500	10.1.1.10	
	CRONOS	10.0.1.9	
	OV8770	10.0.1.50	
E1	ADMIN	10.0.1.97	13
	CCTV	10.0.1.99	
	SCA	N/A	
	TEL	10.0.1.100	
	MEG	10.0.1.102	
	GTC	10.0.1.101	
	BOL	10.0.1.103	
	CORP	10.0.1.104	
E2	ADMIN	10.0.1.129	14

	CCTV	10.0.1.131	
	SCA	N/A	
	TEL	10.0.1.133	
	MEG	10.0.1.135	
	GTC	10.0.1.134	
	BOL	10.0.1.136	
	CORP	10.0.1.137	
	GRAL2	10.0.1.132	
E3	ADMIN	10.0.1.161	15
	CCTV	10.0.1.163	
	SCA	N/A	
	TEL	10.0.1.164	
	MEG	10.0.1.166	
	GTC	10.0.1.165	
	CORP	10.0.1.168	
E4	ADMIN	10.0.1.193	16
	CCTV	10.0.1.192	
	CCTV2	10.0.1.206	
	SCA	N/A	
	TEL	10.0.1.196	
	MEG	10.0.1.198	
	GTC	10.0.1.197	
	BOL	10.0.1.199	
	CORP	10.0.1.200	
	FW-INTERNET	10.0.1.204	
	CORP2	10.0.1.202	
	FW-TELEFONÍA	10.0.1.205	
	TEL2	10.0.1.203	

	OFICINAS	10.0.1.207	
	OLT	10.0.1.208	
E5	ADMIN	10.0.1.65	12
	CCTV	10.0.1.67	
	SCA	N/A	
	TEL	10.0.1.68	
	MEG	10.0.1.70	
	GTC	10.0.1.69	
	BOL	10.0.1.71	
	CORP	10.0.1.72	

Tabla 4. Direccionamiento de administración equipos.

Las direcciones mostradas anteriormente son aquellas que tienen únicamente abierto los puertos de administración remota. Esto último puede ser a través de SSH, SFTP o HTTPS.

Es importante mencionar que no existe forma de acceder a la administración, a través de las IPs de la tabla 7, de manera local. Es decir, no existen puertos físicos en las VLANs de administración para acceder de manera convencional, las únicas formas son las siguientes:

- Conexión remota vía VPN (Virtual Private Network) configurada en el firewall de localidad 4.

- Conexión local a través de un puerto no convencional llamado EMP (Ethernet Management Port) con un direccionamiento especial.

EMP (Ethernet Management Port) Switches nodo acceso

Los puertos EMP o llamados también puertos para administración fuera de banda, ofrecen un método para la administración de los equipos de red de manera segura. Es decir, los puertos EMP pueden estar aún disponibles cuando, por alguna razón, la red se ha caído o no es funcional. En conclusión, el puerto EMP sirve para reiniciar los equipos y sacarlos de un estado de inhibición.

En el caso de este proyecto, a más de beneficiarse de las virtudes mencionadas en el punto anterior, se utilizan los puertos EMP para patrocinar el acceso de los técnicos en sitio hacia una administración segura de la red. De hecho, al utilizar el puerto EMP los técnicos no tendrán que:

- Desconectar ningún cable asociado a la comunicación de los sistemas de transporte.
- Utilizar ninguna IP en ninguna red de administración o red de un sistema de transporte.

Los puntos anteriores implican algunos riesgos obvios e inherentes que son totalmente eliminados al usar este puerto.

El direccionamiento exclusivo de los puertos EMP para cada una de las localidades fueron descritos en la tabla 7.

Localidad	Dirección IP EMP	máscara de red	Dirección usable para conexión
CDC	11.11.11.9	255.255.255.252	11.11.11.10
E1	12.12.12.9	255.255.255.252	12.12.12.10
E2	13.13.13.9	255.255.255.252	13.13.13.10
E3	14.14.14.9	255.255.255.252	14.14.14.10
E4	15.15.15.9	255.255.255.252	15.15.15.10
E5	16.16.16.9	255.255.255.252	16.16.16.10

Tabla 5. Direccionamiento exclusivo interfaces EMP nodos acceso.

La figura 2.73 muestra la posición del puerto EMP en los switches. Para ingresar a la administración del switch basta configurar la dirección IP válida en la NIC conforme a lo descrito en la tabla 7, tener las credenciales de administración y conocer los comandos necesarios y adecuados para proceder a interactuar con el switch.

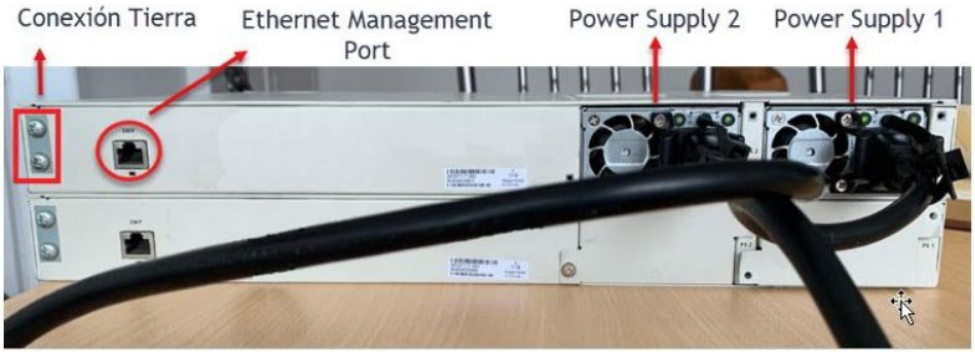

Figura 2.72. Ubicación de puerto EMP switches.

Fuente: Autor

La configuración del puerto EMP es sencilla y se la realiza de manera idéntica a fijar una dirección IP más, pues en lugar de estar asociada a una VLAN, ahora se asocia directamente al puerto EMP, ver la figura 2.74. En ella se observa cómo se configuró el EMP para el VC de la localidad E1.

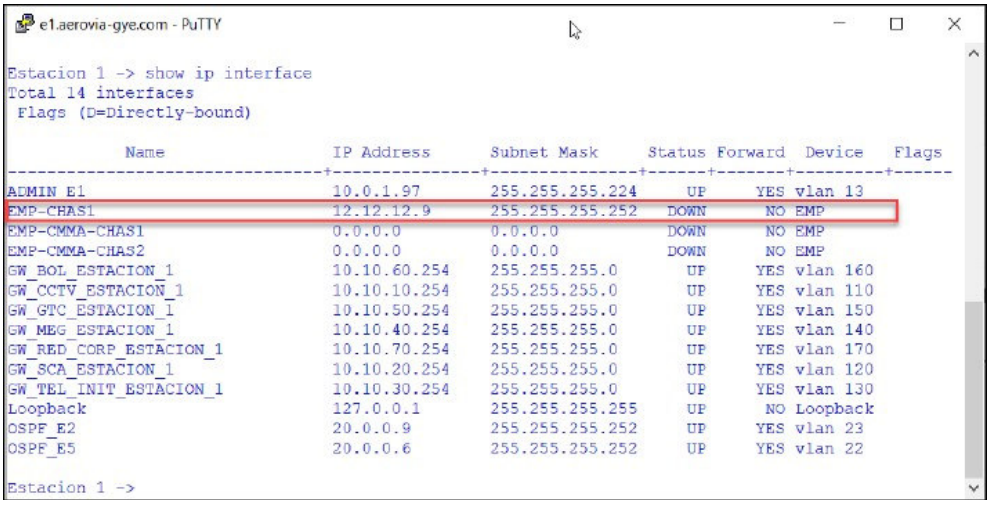

Figura 2.73. Ubicación de puerto EMP switches.

Fuente: Autor

La interfaz EMP se encuentra en estado DOWN, esto es normal y se debe a que no hay actividad en el puerto, pero el momento en el que se conecte a un adaptador de red se activa y permite la conexión.

Los switches de borde no disponen de un puerto EMP, por lo que, la conexión y administración, se debe realizar a través de un nodo de acceso.

Authenticated Switch Acess (ASA)

El ASA está basado en un conjunto de protocolos AAA (Authentication, Authorization and Accounting) que permiten autenticar y autorizar a los usuarios que desean ingresar, administrar y monitorear a los switches, ya sea de nodo de acceso o los switches de borde.

La autenticación se refiere al procedimiento mediante el cual se verifica la identidad de la persona que intenta acceder a algún recurso cuyo acceso es restringido. La autorización, le da al usuario el nivel de acceso requerido.

El accounting es complementario a las funcionalidades descritas anteriormente, y permite saber las actividades realizadas por el usuario autenticado y autorizado en los pasos anteriores.

Por lo tanto, el ASA viene a ser un caso particular del NAC (Network Access Control), donde se autentica y autoriza usuarios para acceder a múltiples recursos de red. En el caso de los switches de nodo de acceso y switches de borde se permite la configuración y el monitoreo.

La más sencilla de las topologías de NAC incluye los siguientes elementos:

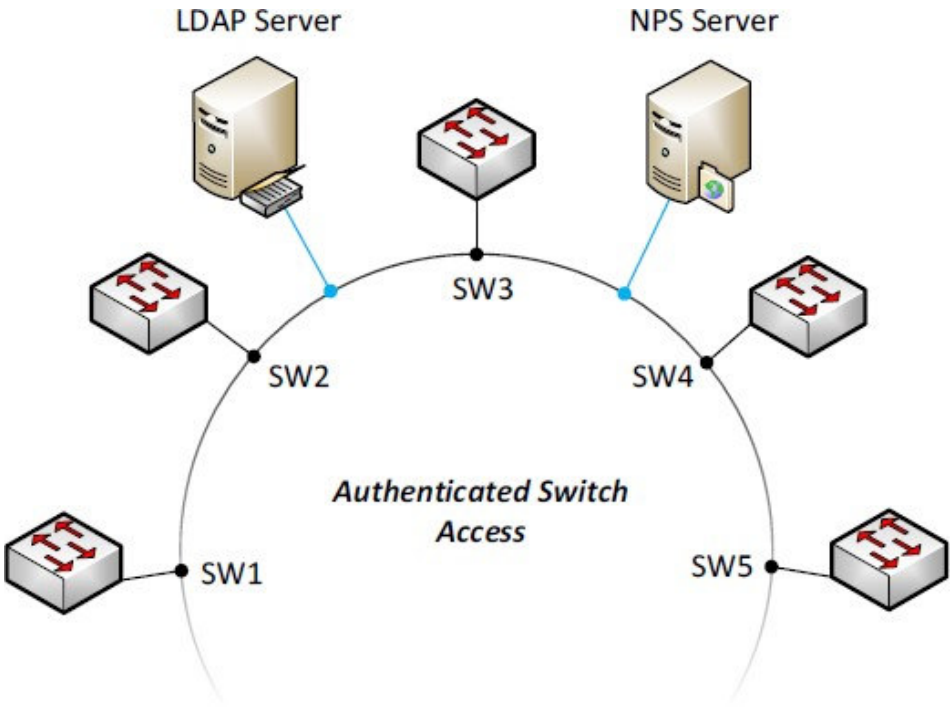

Figura 2.74. Topología NAC - ASA.

Fuente: Autor

Donde se pueden describir los siguientes elementos:

- NPS (Network Policy Server): es la estructura que permite la autenticación y autorización de usuarios que intentan conectarse. Utiliza a RADIUS como protocolo para el efecto.
- Directorio LDAP (Típicamente Directorio Activo de Microsoft): es la estructura que contiene la definición de usuarios y sus contraseñas, es decir sus credenciales. Se integra con el NPS.

Las principales ventajas son:

- Seguridad, los usuarios que pueden ingresar a la configuración y monitoreo pueden tener diferentes niveles de autorización.
- Facilidad en cambio de contraseña, al depender la autenticación y autorización de un solo servidor de identidad, las credenciales pueden ser actualizadas en un solo registro, por ejemplo, en AD (Active Directory), y afectar el modo en que se validan credenciales en muchos switches.

En este proyecto hay una necesidad inherente de asegurar la red desde todas las perspectivas y formas posibles, ya que dicha red posibilita la prlocalidad de un servicio público. En este sentido, el acceso a los switches de nodo acceso y a los switches de borde, no constituyen una excepción.

En la topología de implementación se puede notar que existen 76 equipos que constituyen la red principal:

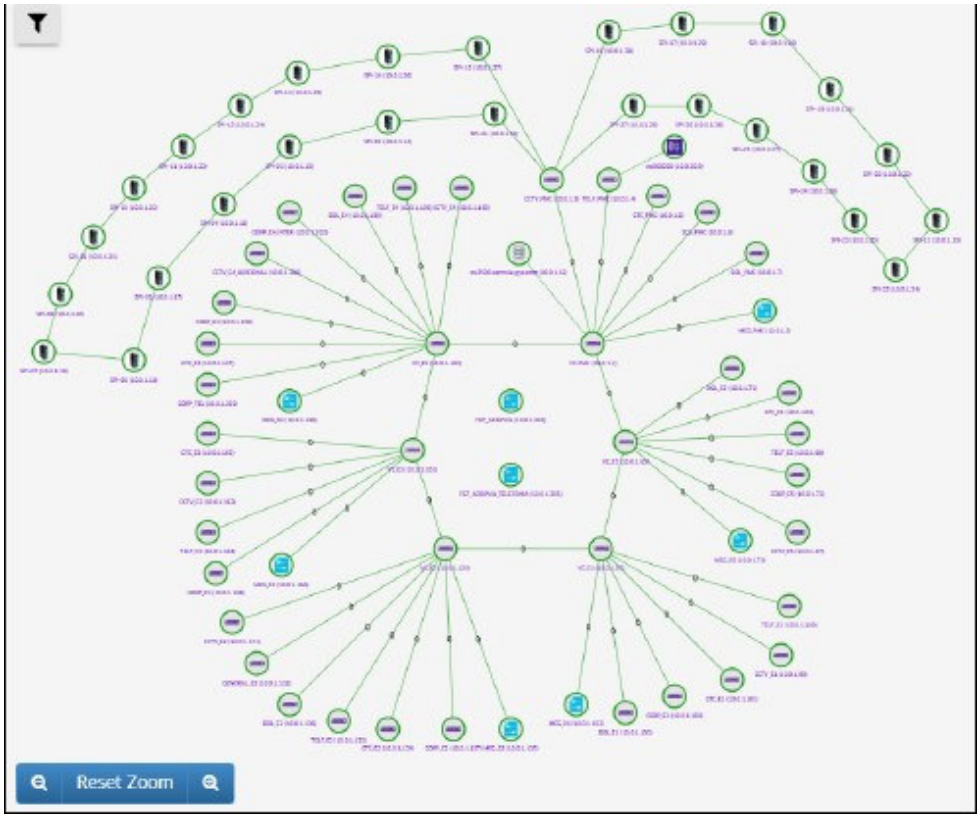

Figura 2.75. Número de equipos de red.

Fuente: Autor

En cuanto a la implementación para lograr el ASA, se tuvieron que crear los roles de NPS y LDAP (AD), incluidos como roles en un Windows Server que reside en el servidor de gestión y seguridad de la red, a continuación, se ve la situación física de dicho equipo en CDC:

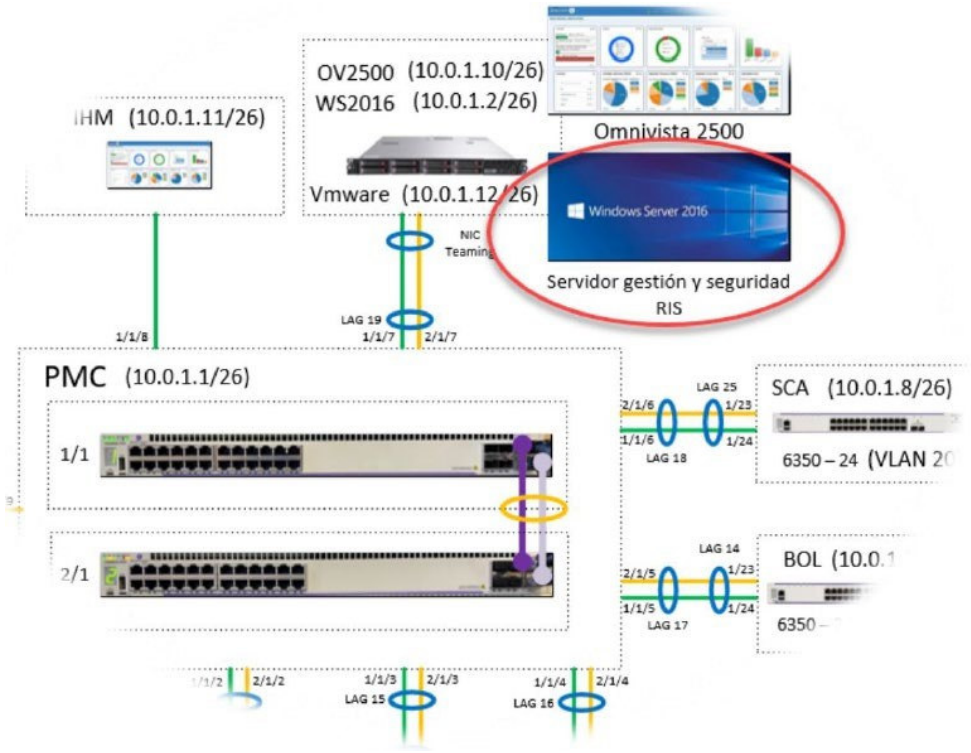

Figura 2.76. Situación de servidor de gestión y seguridad.

Fuente: Autor

Si el servidor Windows no está disponible, el acceso a los switches del nodo y de borde, tiene una segunda fuente de autenticación que es su misma base de datos local.

A continuación, se indica de manera explícita los nombres de usuarios y contraseñas al momento de la entrega del proyecto para los equipos de conmutación y enrutamiento:

Las configuraciones aplicadas en los switches de nodo de acceso y switches de borde son las que se pueden observar en las figuras 80 y 81 respectivamente.

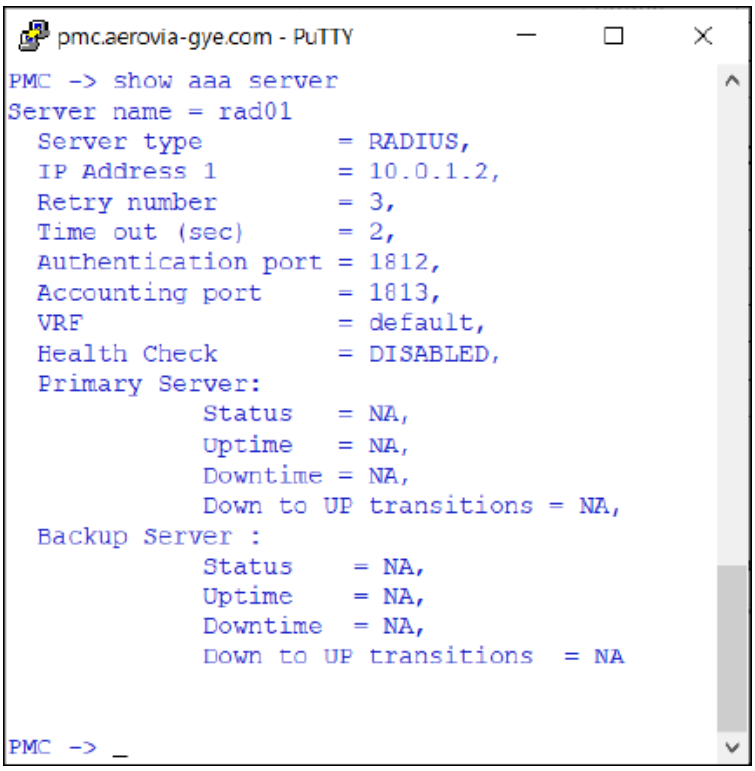

Figura 2.77. Servidor Radius declarado en switch nodo acceso.

Fuente: Autor

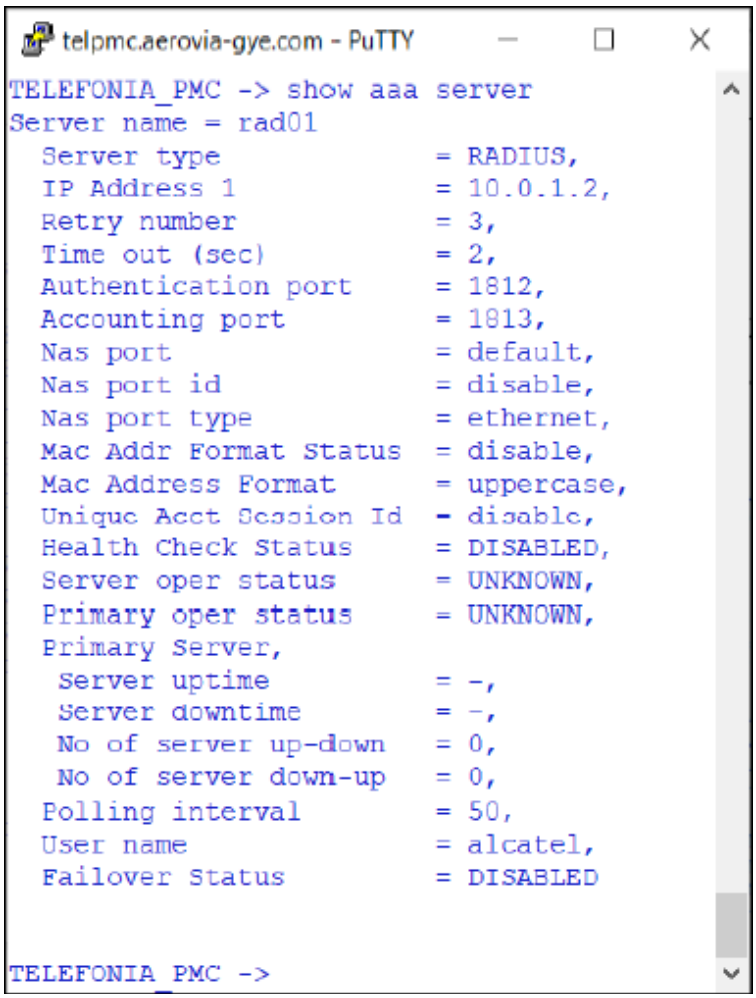

Figura 2.78. Servidor Radius declarado en switch de borde.

Fuente: Autor

A continuación, se muestra el orden de las fuentes de autenticación que fueron programadas en los switches de nodo de acceso y de borde.

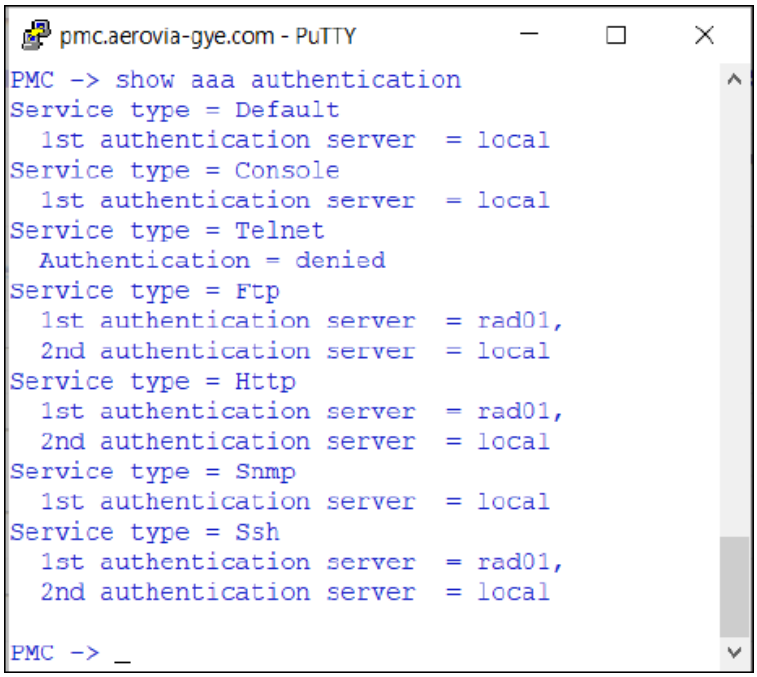

Figura 2.79. Fuentes de autenticación declaradas para cada tipo de conexión.

Fuente: Autor

LPS (Lean Port Security)

La seguridad a nivel de capa 2 es importante, ya que permite controlar de manera efectiva cómo el switch aprende direcciones MAC, pudiendo existir en este proceso vulnerabilidades que pueden ser aprovechadas para generar ataques como MAC Flooding (Switch se comporta como un Hub), suplantación de identidad, ataques de DHCP, denegación de servicio, entre otros.

Una solución para muchos de estos ataques es el control sobre la forma en que el switch aprende las direcciones MAC que

intentan comunicarse a través de sus puertos. Para esto existe la funcionalidad de LPS, la cual puede brindar las siguientes facilidades:

- Período de tiempo limitado de aprendizaje de MAC.
- Máximo número de MACs por puerto.
- Configuración estática de MACs.
- Posibilidad de escoger la acción ante una violación a una regla.

En este proyecto se tienen switches de borde que permiten la conexión de los diferentes sistemas de transporte como CCTV, Telefonía, Red Corporativa, GTC, Sonido y Tickets etc. Muchos de estos sistemas permiten la conexión de dispositivos finales al otro lado del cableado horizontal donde puede haber contacto con muchos usuarios finales, y no solo dentro del datacenter, esto implica un riesgo de seguridad. Por ese motivo fue necesario configurar en los switches de borde el LPS con ciertos parámetros mínimos, los cuales se describen a continuación:

- Se permite el aprendizaje de MACs sin límite de tiempo.
- Se permite el aprendizaje de máximo cuatro direcciones MAC, de las cuales solamente se permite el curso de tráfico de una, las otras tres si bien son aprendidas, pero su tráfico es

bloqueado. Esto se efectuó con el objetivo de obtener un seguimiento y monitoreo del comportamiento.

- La disposición en caso de violación fue la de bloquear el tráfico no permitido. Por ejemplo, si hay una quinta MAC en uno de los puertos, esta no se aprende y por tanto su tráfico se descarta.

La figura 2.81 muestra un ejemplo del estado de los puertos configurados con LPS en el switch de telefonía del CDC.

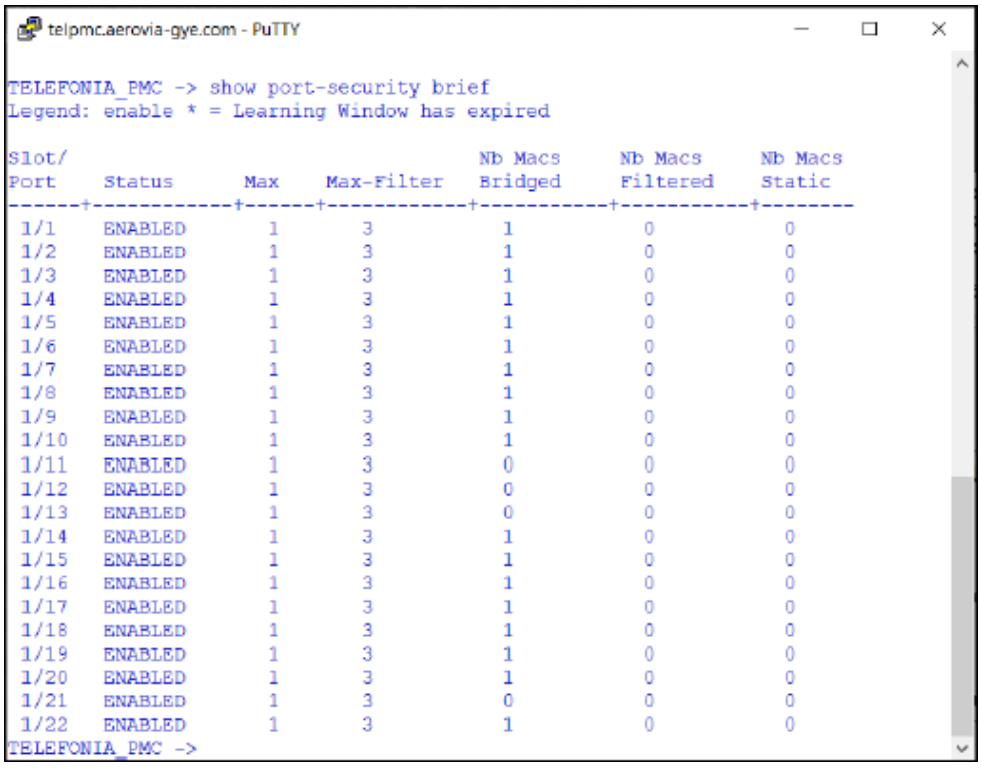

Figura 2.80. Configuración de puertos LPS en switch Telefonía CDC.

Fuente: Autor

En la figura 2.82 se puede apreciar el estado del LPS en un puerto determinado, adicionalmente también se ven los parámetros de configuración específicos para ese puerto.

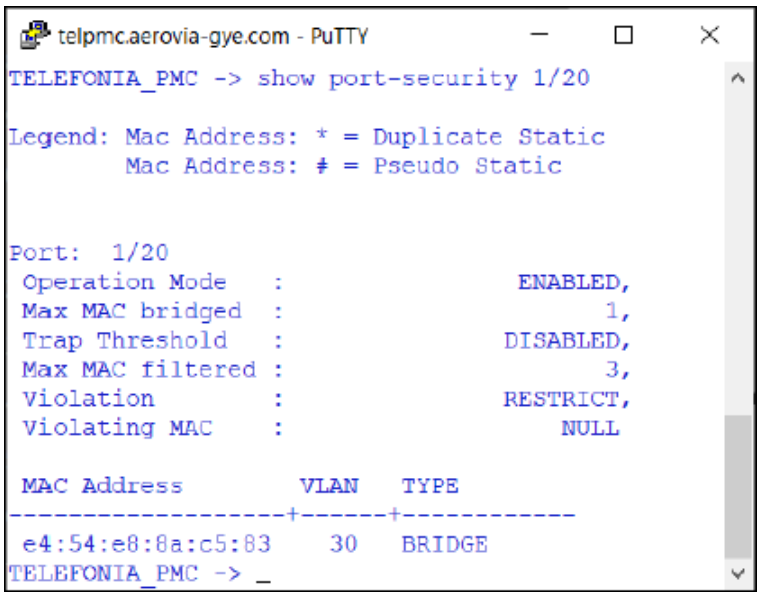

Figura 2.81. Información de LPS en puerto específico.

Fuente: Autor

Todos los switches de los sistemas tienen configurado LPS, excepto el de Sonido porque este no estuvo contemplado dentro del alcance de configuración.

DHCP Snooping

Su funcionalidad es garantizar que en todo momento solamente haya servidores DHCP autorizados. Las opciones que tiene el DHCP Snooping son:

- Solamente cliente: en este modo, los puertos aceptan solamente el tráfico DHCP relacionado con clientes.
- Confiable: ningún tipo de paquete DHCP tiene restricción. Este modo está reservado para los puertos donde efectivamente se ha conectado un servidor DHCP autorizado.
- Bloqueado: no se acepta ningún paquete DHCP en el puerto.

En el proyecto no existe servicio DHCP para clientes finales, por lo que no caben en ninguna parte de la red, la conexión de servidores con esta capacidad. Todos los equipos tienen asignado su direccionamiento IP de manera estática. En este sentido, la configuración de DHCP Snooping para el proyecto debe incluir el modo de bloqueo total, como se muestra en la figura 2.83.

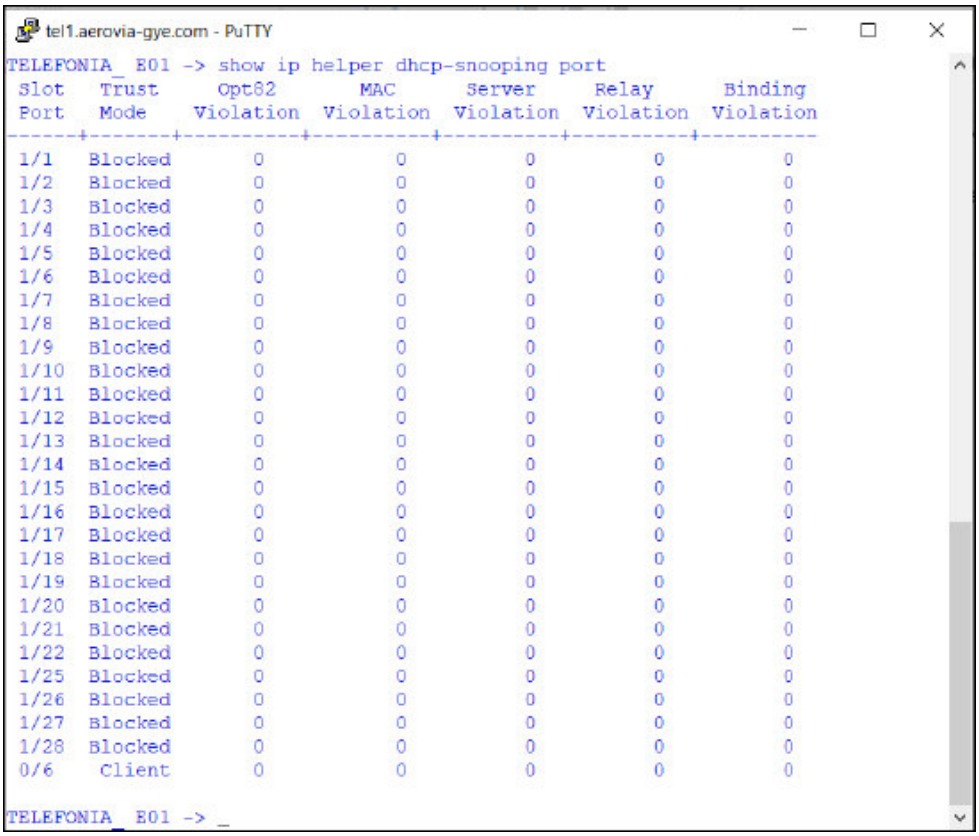

Figura 2.82. Puertos configurados en DHCP Snooping en modo Blocked.

Fuente: Autor

Comunicación entre VLANs

En este proyecto existen diversos sistemas de transporte tales como CCTV, Telefonía, GTC, Sonido, SCA, Red Corporativa, entre otros. Previamente, se mencionó que cada uno de estos sistemas tiene asignado una VLAN y un segmento de red específico, por lo que cada sistema es independiente y en principio no deben comunicarse entre ellos. Obviamente hay excepciones y GTC es una de ellas, ya que este sistema

monitorea a otros, por lo que se debe garantizar que haya comunicación entre este y los demás.

La idea es partir de la premisa en la cual ninguno de los sistemas debe comunicarse entre sí e ir añadiendo las respectivas excepciones conforme se las solicite. Es importante aclarar que, por el diseño de red, un mismo sistema de red posee varias VLANs en las diferentes localidades. Esta comunicación está garantizada.

El siguiente cuadro muestra el punto de partida para la comunicación entre VLANs de todo el proyecto:

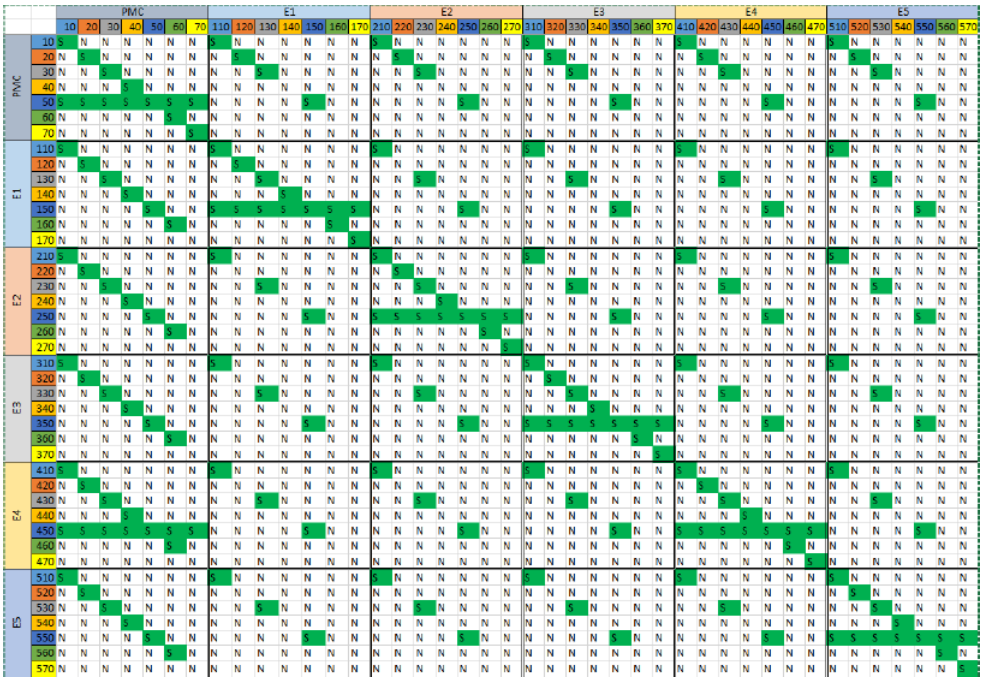

Tabla 6. Comunicación entre VLANs; S es aceptado; N negado.

La tabla 9 muestra aproximadamente cómo se encuentra la comunicación entre VLANs, y es un buen punto de partida. A continuación, se detalla equipo a equipo las redes o hosts de las cuales acepta comunicación:

Centro de Control (CDC)							
SW	Redes Permitidas			Host Permitidos			
CCTV	10.0.10.0/24 10.10.10.0/24 10.20.10.0/24 10.30.10.0/24 10.40.10.0/24 10.50.10.0/24			10.0.20.1 10.0.50.2 10.0.50.3 10.0.50.81 10.0.50.82 10.0.50.109 10.40.50.2			
TELEFONÍA	10.0.30.0/24 10.10.30.0/24 10.20.30.0/24 10.30.30.0/24 10.40.30.0/24 10.50.30.0/24			10.0.40.1 10.0.40.2 10.0.40.3 10.0.50.2 10.0.50.3 10.10.40.1	10.10.40.2 10.10.40.3 10.20.40.1 10.20.40.2 10.20.40.3 10.30.40.1	10.30.40.2 10.30.40.3 10.40.40.1 10.40.40.2 10.40.40.3 10.50.40.1	10.50.40.2 10.50.40.3
GTC	10.0.10.0/24 10.10.10.0/24 10.20.10.0/24 10.30.10.0/24 10.40.10.0/24 10.50.10.0/24	10.0.50.0/24 10.10.50.0/24 10.20.50.0/24 10.30.50.0/24 10.40.50.0/24 10.50.50.0/24	10.0.60.0/24 10.10.60.0/24 10.20.60.0/24 10.30.60.0/24 10.40.60.0/24 10.50.60.0/24	10.0.10.1 10.0.10.2 10.0.20.1 10.0.30.1 10.0.30.2 10.0.30.3 10.0.30.9 10.0.40.1 10.0.40.2 10.0.40.3	10.10.30.1 10.10.30.2 10.10.30.3 10.10.40.1 10.10.40.2 10.10.40.3 10.20.30.1 10.20.30.2 10.20.30.3 10.20.40.1	10.20.40.2 10.20.40.3 10.30.30.1 10.30.30.2 10.30.30.3 10.30.40.1 10.30.40.2 10.30.40.3 10.40.30.1 10.40.30.2	10.40.30.3 10.40.40.1 10.40.40.2 10.40.40.3 10.50.30.1 10.50.30.2 10.50.30.3 10.50.40.1 10.50.40.2 10.50.40.3

SCA	N/A			10.0.10.1 10.0.10.2 10.0.50.2 10.0.50.3 10.0.50.81 10.0.50.82	10.10.10.45 10.10.10.46 10.10.10.47 10.10.10.48 10.10.10.49 10.10.10.50	10.10.10.51 10.10.10.52 10.10.10.53 10.10.50.2 10.20.50.2 10.30.50.2	10.40.50.2 10.40.50.80 10.50.50.2 10.50.50.80
TICKETS	10.0.60.0/24 10.10.60.0/24 10.20.60.0/24	10.40.60.0/24 10.50.60.0/24 10.0.50.0/24 10.10.50.0/24	10.20.50.0/24 10.30.50.0/24 10.40.50.0/24 10.50.50.0/24 10.40.171.0/24	N/A			

Tabla 7. Comunicaciones permitidas switches de borde CDC.

Localidad 1 (E1)							
SW	Redes Permitidas			Host Permitidos			
CCTV	10.0.10.0/24 10.20.10.0/24 10.40.10.0/24	10.10.10.0/24 10.30.10.0/24 10.50.10.0/24		10.0.20.1 10.0.20.2 10.0.50.2 10.0.50.3 10.10.50.2			
TELEFONÍA	10.0.30.0/24 10.10.30.0/24 10.20.30.0/24 10.30.30.0/24 10.40.30.0/24 10.50.30.0/24			10.0.40.1 10.0.40.2 10.0.40.3 10.0.50.2 10.0.50.3 10.10.40.1	10.10.40.2 10.10.40.3 10.10.50.2 10.20.40.1 10.20.40.2 10.20.40.3	10.30.40.1 10.30.40.2 10.30.40.3 10.40.40.1 10.40.40.2 10.40.40.3	10.50.40.1 10.50.40.2 10.50.40.3
GTC	10.0.10.0/24 10.10.10.0/24 10.20.10.0/24 10.30.10.0/24	10.40.10.0/24 10.50.10.0/24 10.0.50.0/24 10.10.50.0/24	10.20.50.0/24 10.30.50.0/24 10.40.50.0/24 10.50.50.0/24 10.10.60.0/24		10.0.20.1 10.10.30.1 10.10.30.2 10.10.30.3	10.10.40.1 10.10.40.2 10.10.40.3	
CORP	10.10.70.0/24 192.168.0.0/24			N/A			

TICKETS	10.0.60.0/24 10.10.60.0/24 10.20.60.0/24	10.40.60.0/24 10.50.60.0/24 10.0.50.0/24 10.10.50.0/24	10.20.50.0/24 10.30.50.0/24 10.40.50.0/24 10.50.50.0/24 10.40.171.0/24	N/A

Tabla 8. Comunicaciones permitidas switches de borde E1.

Localidad 2 (E2)							
SW	Redes Permitidas			Host Permitidos			
CCTV	10.0.10.0/24 10.20.10.0/24 10.40.10.0/24	10.10.10.0/24 10.30.10.0/24 10.50.10.0/24		10.0.50.2 10.0.50.3 10.20.50.2			
TELEFONÍA	10.0.30.0/24 10.10.30.0/24 10.20.30.0/24 10.30.30.0/24 10.40.30.0/24 10.50.30.0/24			10.0.40.1 10.0.40.2 10.0.40.3 10.0.50.2 10.0.50.3 10.10.40.1	10.10.40.2 10.10.40.3 10.20.50.2 10.20.40.1 10.20.40.2 10.20.40.3	10.30.40.1 10.30.40.2 10.30.40.3 10.40.40.1 10.40.40.2 10.40.40.3	10.50.40.1 10.50.40.2 10.50.40.3
GTC	10.0.10.0/24 10.10.10.0/24 10.20.10.0/24 10.30.10.0/24	10.40.10.0/24 10.50.10.0/24 10.0.50.0/24 10.10.50.0/24	10.20.50.0/24 10.30.50.0/24 10.40.50.0/24 10.50.50.0/24 10.20.60.0/24		10.0.20.1 10.20.30.1 10.20.30.2 10.20.30.3	10.20.40.1 10.20.40.2 10.20.40.3	
CORP	10.20.70.0/24 192.168.0.0/24			N/A			
TICKETS	10.0.60.0/24 10.10.60.0/24 10.20.60.0/24	10.40.60.0/24 10.50.60.0/24 10.0.50.0/24 10.10.50.0/24	10.20.50.0/24 10.30.50.0/24 10.40.50.0/24 10.50.50.0/24 10.40.171.0/24	10.20.50.6			

Tabla 9. Comunicaciones permitidas switches de borde E2.

Localidad 3 (E3)							
SW	Redes Permitidas			Host Permitidos			
CCTV	10.0.10.0/24 10.20.10.0/24 10.40.10.0/24	10.10.10.0/24 10.30.10.0/24 10.50.10.0/24		10.0.50.2 10.0.50.3 10.30.50.2			
TELEFONÍA	10.0.30.0/24 10.10.30.0/24 10.20.30.0/24 10.30.30.0/24 10.40.30.0/24 10.50.30.0/24			10.0.40.1 10.0.40.2 10.0.40.3 10.0.50.2 10.0.50.3 10.10.40.1	10.10.40.2 10.10.40.3 10.30.50.2 10.20.40.1 10.20.40.2 10.20.40.3	10.30.40.1 10.30.40.2 10.30.40.3 10.40.40.1 10.40.40.2 10.40.40.3	10.50.40.1 10.50.40.2 10.50.40.3
GTC	10.0.10.0/24 10.10.10.0/24 10.20.10.0/24 10.30.10.0/24	10.40.10.0/24 10.50.10.0/24 10.0.50.0/24 10.10.50.0/24	10.20.50.0/24 10.30.50.0/24 10.40.50.0/24 10.50.50.0/24		10.0.20.1 10.30.30.1 10.30.30.2 10.30.30.3	10.30.40.1 10.30.40.2 10.30.40.3	
CORP	10.30.70.0/24 192.168.0.0/24			N/A			

Tabla 10. Comunicaciones permitidas switches de borde E3.

Localidad 4 (E4)							
SW	Redes Permitidas			Host Permitidos			
CCTV / CCTV2	10.0.10.0/24 10.20.10.0/24 10.40.10.0/24	10.10.10.0/24 10.30.10.0/24 10.50.10.0/24		10.0.50.2 10.0.50.3 10.40.50.2			
TELEFONÍA	10.0.30.0/24 10.10.30.0/24 10.20.30.0/24 10.30.30.0/24 10.40.30.0/24 10.50.30.0/24			10.0.40.1 10.0.40.2 10.0.40.3 10.0.50.2 10.0.50.3 10.10.40.1	10.10.40.2 10.10.40.3 10.40.50.2 10.20.40.1 10.20.40.2 10.20.40.3	10.30.40.1 10.30.40.2 10.30.40.3 10.40.40.1 10.40.40.2 10.40.40.3	10.50.40.1 10.50.40.2 10.50.40.3

GTC	10.0.10.0/24 10.10.10.0/24 10.20.10.0/24 10.30.10.0/24	10.40.10.0/24 10.50.10.0/24 10.0.50.0/24 10.10.50.0/24	10.20.50.0/24 10.30.50.0/24 10.40.50.0/24 10.50.50.0/24 10.40.60.0/24		10.0.20.1 10.40.30.1 10.40.30.2 10.40.30.3	10.40.40.1 10.40.40.2 10.40.40.3	
CORP	10.40.70.0/24 192.168.0.0/24			N/A			
TICKETS	10.0.60.0/24 10.10.60.0/24 10.20.60.0/24	10.40.60.0/24 10.50.60.0/24 10.0.50.0/24 10.10.50.0/24	10.20.50.0/24 10.30.50.0/24 10.40.50.0/24 10.50.50.0/24 10.40.171.0/24	10.40.50.6			

Tabla 11. Comunicaciones permitidas switches de borde E4.

Localidad 5 (E5)							
SW	Redes Permitidas			Host Permitidos			
CCTV	10.0.10.0/24 10.20.10.0/24 10.40.10.0/24	10.10.10.0/24 10.30.10.0/24 10.50.10.0/24		10.0.50.2 10.0.50.3 10.50.50.2			
TELEFONÍA	10.0.30.0/24 10.10.30.0/24 10.20.30.0/24 10.30.30.0/24 10.40.30.0/24 10.50.30.0/24			10.0.40.1 10.0.40.2 10.0.40.3 10.0.50.2 10.0.50.3 10.10.40.1	10.10.40.2 10.10.40.3 10.50.50.2 10.20.40.1 10.20.40.2 10.20.40.3	10.30.40.1 10.30.40.2 10.30.40.3 10.40.40.1 10.40.40.2 10.40.40.3	10.50.40.1 10.50.40.2 10.50.40.3
GTC	10.0.10.0/24 10.10.10.0/24 10.20.10.0/24 10.30.10.0/24	10.40.10.0/24 10.50.10.0/24 10.0.50.0/24 10.10.50.0/24	10.20.50.0/24 10.30.50.0/24 10.40.50.0/24 10.50.50.0/24 10.50.60.0/24		10.0.20.1 10.50.30.1 10.50.30.2 10.50.30.3	10.50.40.1 10.50.40.2 10.50.40.3	
CORP	10.40.70.0/24 192.168.0.0/24			N/A			

TICKETS	10.0.60.0/24 10.10.60.0/24 10.20.60.0/24	10.40.60.0/24 10.50.60.0/24 10.0.50.0/24 10.10.50.0/24	10.20.50.0/24 10.30.50.0/24 10.40.50.0/24 10.50.50.0/24 10.40.171.0/24	10.50.50.6

Tabla 12. Comunicaciones permitidas switches de borde E5.

Las reglas que permitieron la configuración de privilegios y restricciones en la comunicación entre redes se denominan QoS – ACL. Estas fueron configuradas en los switches de borde para contener el tráfico lo más cercanamente posible al origen y evitar un consumo de ancho de banda innecesario en tráfico que se tiene que descartar por no estar permitido.

A continuación, se explica la lógica usada por estos modelos de switches para la gestión del tráfico a través de QoS – ACLS:

- Establecer una condición para la identificación de tráfico. Para esto se identifica el direccionamiento IP (red o host) sobre el cual se aplica una acción.
- Definir una acción en particular. Esta puede ser permitir o denegar.
- Declarar una regla que asocie la condición del paso a con la acción del b. Es importante mencionar que las reglas poseen un número de precedencia, el cual sirve para establecer un

orden de evaluación. Además, se aplica la primera regla que haga un match en la condición.

La figura 2.84 muestra un ejemplo de las reglas de las cuales se habló en el paso c anterior.

Se puede evidenciar que en letras mayúsculas se encuentran los nombres de las instancias Regla, Condición y Acción respectivamente. Por ejemplo, la regla "ACCEPT_IPs_PERMITIDAS" asocia la condición "ID_IPs_PERMITIDAS" con la acción "PERMITIR". La regla tiene la más alta precedencia del grupo (3125), por lo cual se evalúa primero.

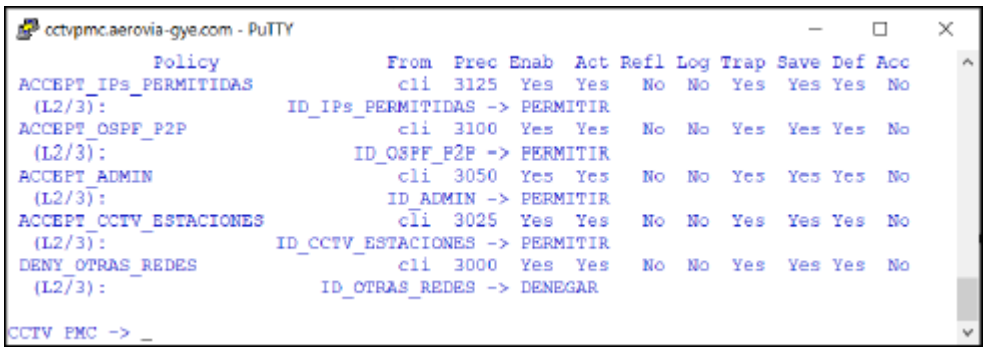

Figura 2.83. Ejemplo reglas QoS - ACL en switch de borde.

Fuente: Autor

La figura 2.85 muestra que para una ACL existen solamente dos tipos de acciones, permitir o denegar, pero lo switches pueden

aplicar otras acciones que están fuera del alcance para esta situación en particular.

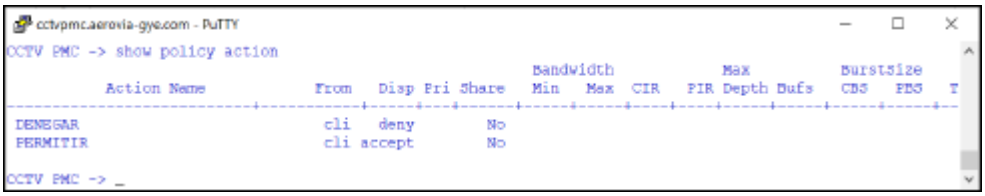

Figura 2.84. Ejemplo de acciones para reglas QoS – ACL en switch de borde.

Fuente: Autor

La figura 2.86 muestra las condiciones que forman parte de las reglas, una condición establece un patrón a buscar en el tráfico. Por ejemplo, la condición llamada “ID_CCTV_LOCALIDADES” establece busca un patrón en el tráfico que tenga como origen las IPs de un grupo llamado “CCTV_LOCALIDADES”.

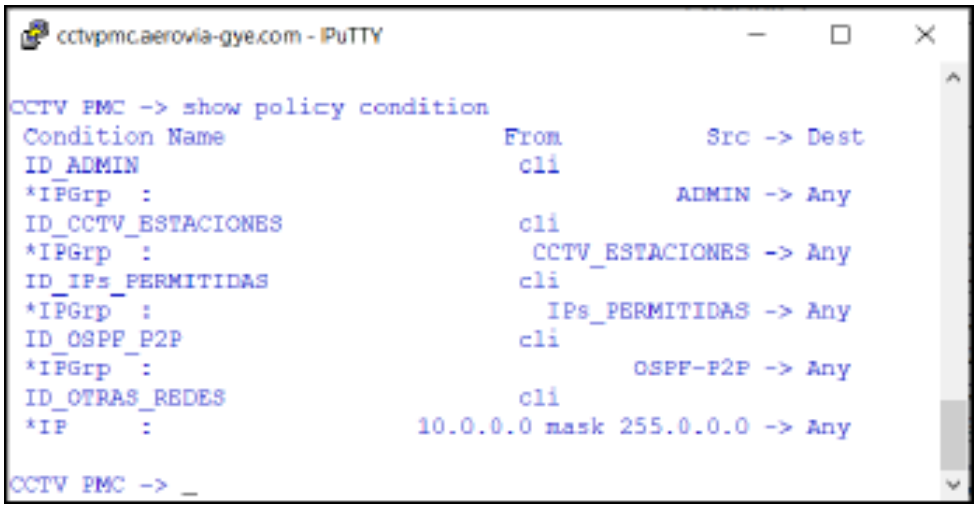

Figura 2.85. Ejemplo de condiciones para reglas QoS – ACL en switch de borde.

Fuente: Autor

Para facilitar la elaboración de las condiciones, se puede establecer un grupo de redes o hosts IP que al darle un nombre puede ser invocado en dichas condiciones, con lo cual se evita el tener que elaborar una condición diferente por IP, pese a que se ejecutará una misma acción para dichas IPs. La figura 2.87 muestra un ejemplo de lo anteriormente descrito.

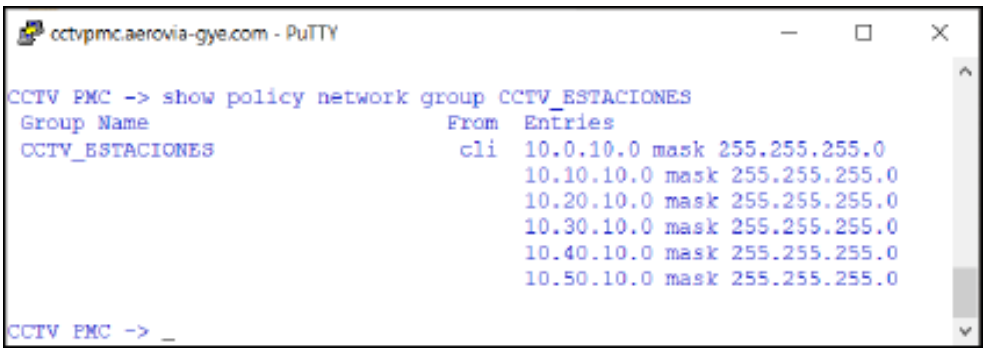

Figura 2.86. Ejemplo de grupo de red para condiciones QoS – ACL en switch de borde.

Fuente: Autor

Una vez examinada la lógica general de configuración se puede explicar la lógica particular de las ACLs en los switches de borde, por lo que se considera nuevamente la figura 2.88.

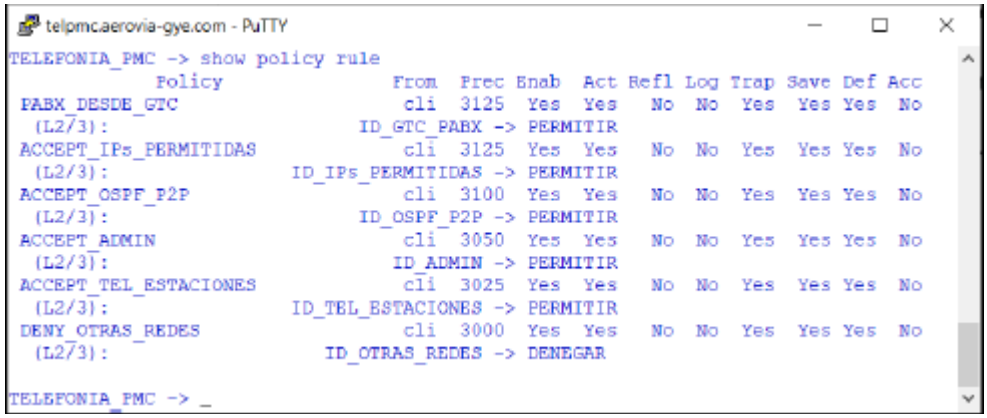

Figura 2.87. Ejemplo reglas QoS - ACL en switch de borde Telefonía.

Fuente: Autor

Para empezar, se parte del hecho de que todas las redes 10.0.0.0/8 (ID_OTRAS_REDES) están denegadas. Es importante recalcar que todas las redes, por diseño, utilizan el esquema de red 10.x.x.x. Por ello esta regla se la configura con menor precedencia para que sea tratada como una opción por defecto.

Sobre la regla por defecto vendrán todas aquellas que permitan el tráfico específico. En el ejemplo de la figura 2.91 se muestran las reglas para un switch de Telefonía, por lo que una regla específica fue permitir el tráfico de todas las redes de telefonía a nivel de todas las localidades (ID_TEL_LOCALIDADES), similar lógica se aplica para las redes administrativas (ID_ADMIN), que permiten administrar el equipo en todo momento, y para cualquier otra regla específica de precedencia superior.

Una regla que permite flexibilidad en la configuración, al permitir o denegar IPs, es la llamada “ACCEPT_IPs_PERMITIDAS”, que engloba un network group que se puede editar para permitir IPs de otros sistemas de ser el caso.

Una observación crítica de reglas QoS – ACL hace referencia sobre conservar y aplicar los cambios que se vayan realizando. Cada vez que se cree una condición, acción, regla o grupo de red es necesario aplicar el comando qos apply, con esto los cambios se aplican al tráfico cursado en tiempo real, pero de manera adicional hay que guardar los cambios en el archivo de configuración con write memory flash-synchro.

Seguridad Perimetral

Previamente, se mencionó el rol especial de la localidad 4 al integrar servicios externos a la infraestructura de red, servicios como Internet, troncales SIP para telefonía y SIMs GSM se acoplan a la red a través de los firewalls. En esta sección se explicará cómo dichos servicios se integran a la red.

Los firewalls se encuentran ubicados en armarios especiales dentro del centro de datos de la localidad 4:

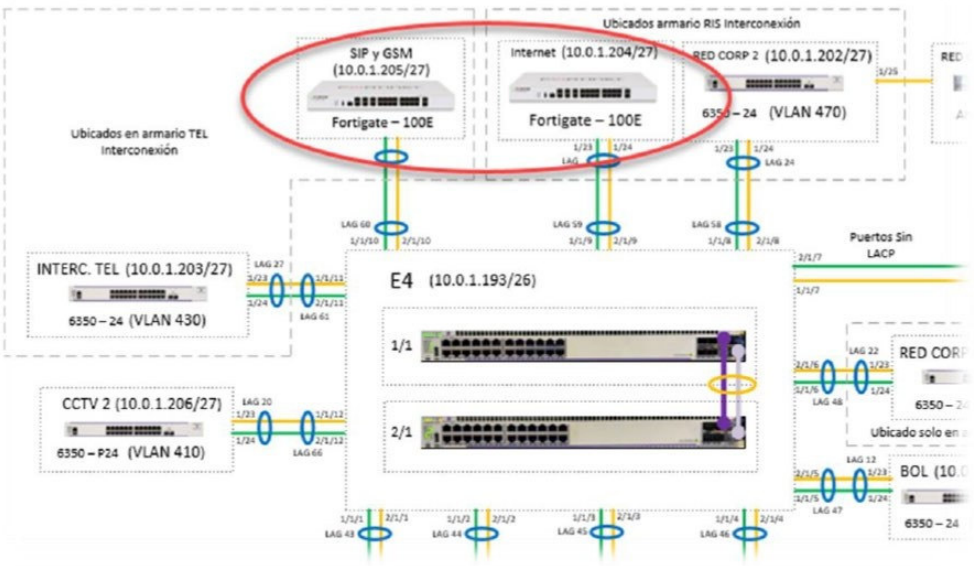

Figura 2.88. Situación topológica firewalls para Datos y Telefonía.

Fuente: Autor

La figura 2.90 muestra la integración de los servicios externos con la red:

- Conexiones de LACP desde y hacia los firewalls.
- Rutas estáticas para la provisión de servicios en switch de nodo acceso y en firewalls.
- Direccionamiento IP proporcionado por los diferentes proveedores de servicios para sus CPE (Customer Premises Equipment).

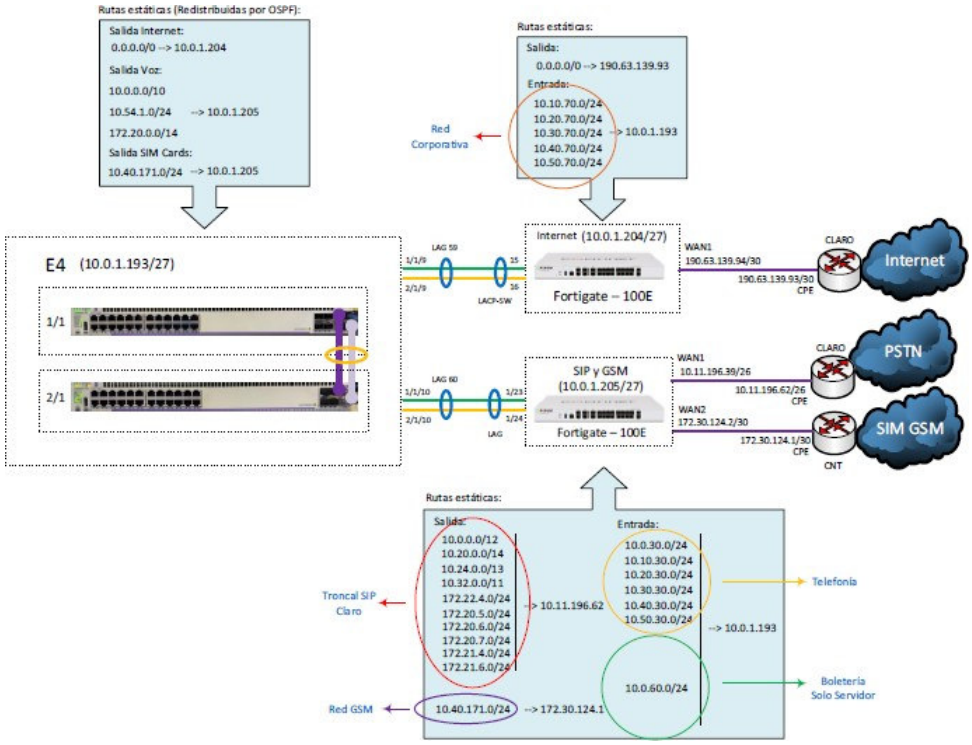

Figura 2.89. Topología de integración de servicios externos.

Fuente: Autor

El servicio de Internet es proporcionado por el ISP, cuyos datos para activar la salida pueden verificarse en la figura 2.90. En el proyecto, solamente debe tener acceso a internet el sistema de transporte denominado Red Corporativa, es por ello que solamente existen rutas de regreso para las siguientes redes:

- 10.10.70.0/24 – VLAN 170 – Red Corporativa Localidad 1.
- 10.20.70.0/24 – VLAN 270 – Red Corporativa Localidad 2.
- 10.30.70.0/24 – VLAN 370 – Red Corporativa Localidad 3.
- 10.40.70.0/24 – VLAN 470 – Red Corporativa Localidad 4.

Es de vital importancia proteger a los internautas de visitar páginas peligrosas o que potencial malware pueda acceder a las PCs. En este sentido, y por defecto, se configuraron las protecciones de buena práctica contra estas amenazas:

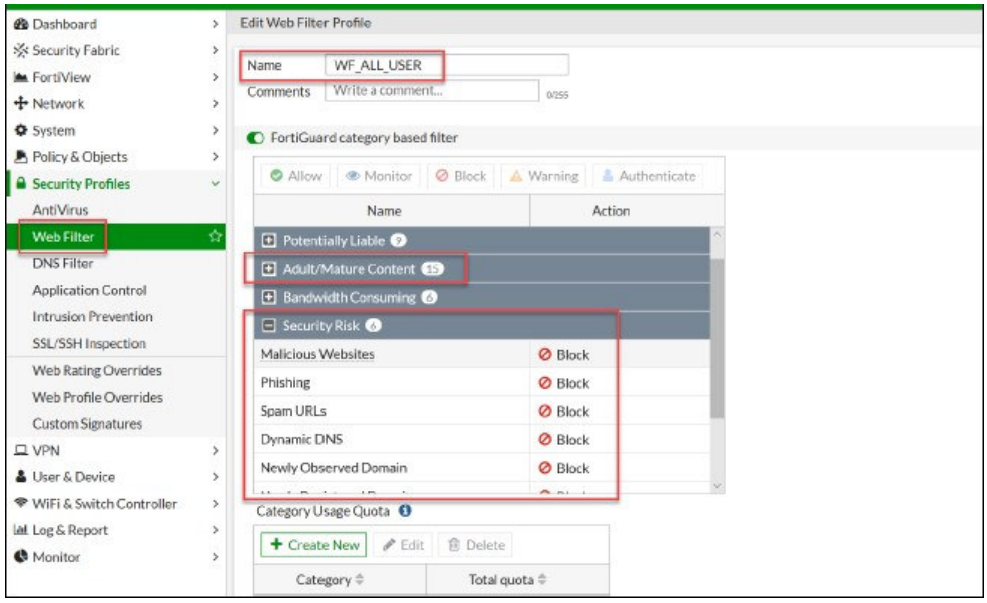

Figura 2.90. Perfil de WebFiltering aplicado a navegación a Internet

Fuente: Autor

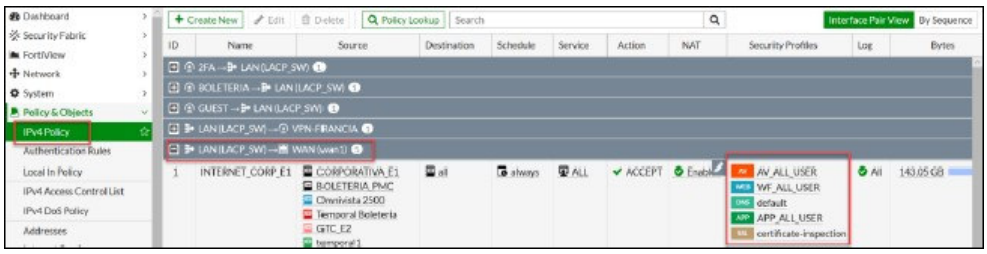

Figura 2.91. Ejemplo de perfiles de seguridad asociados a políticas de salida a Internet

Fuente: Autor

La troncal SIP que permite que el sistema de transporte Telefonía del proyecto pueda acceder a la PSTN (Red pública Conmutada) se encuentra conectado en el segundo firewall (Aquel de IP 10.0.1.205).

Como es conocido, el ISP entrega una serie de rutas hacia redes de su infraestructura para lograr que tanto señalización de llamadas como voz puedan coexistir con éxito. En la figura 2.90 se puede ver cuáles son dichas rutas, las cuales son declaradas tanto en el firewall y redistribuidas a través de OSPF hacia todas las localidades.

Además, solamente las redes de telefonía, 10.X.30.H/24, pueden acceder hacia estas rutas de la PSTN.

Existe un servicio adicional externo que permite accededr a un servicio de conectividad hacia una red GSM para uso exclusivo de Tickets. Este servicio es proporcionado por la red 10.40.171.0/24, la cual se ha configurado para que sea accedida solamente por la red de Tickets de CDC (10.0.60.0/24).

Monitoreo

La red consta de muchos equipos, por lo que no resulta práctico realizar actividades de vigilancia y monitoreo por cada uno de ellos. Es necesario entonces aplicar otras herramientas que permitan estar pendientes de la topología total de manera masiva a través de notificaciones dinámicas, gestión gráfica y aprovisionamiento masivo. Tales herramientas constituyen los llamados NMS (Network Management System) que se apoyan de protocolos subyacentes como SNMP para su funcionamiento.

El NMS que se utilizó para este proyecto fue el Omnivista 2500, el cual es una aplicación que basa su funcionamiento en el modelo cliente – servidor y su interfaz puede ser accedida desde cualquier parte de la red a través de un navegador.

SNMP es un protocolo que permite la administración de la red, entendiéndose por administración todo aquello relacionado con la configuración y monitoreo de esta. En esta sección se detallarán las configuraciones subyacentes en SNMP para el funcionamiento del Omnivista 2500 y del software de monitoreo implementado por el sistema de transporte GTC.

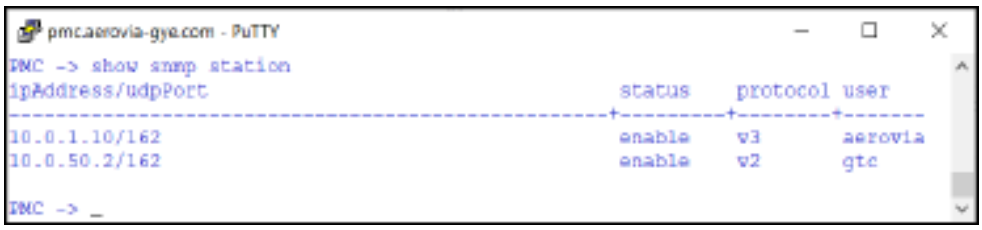

Figura 2.92. Localidades para destino de traps SNMP CDC.

Fuente: Autor

Es el software NMS (Network Management System) es el encargado fundamental del monitoreo del desempeño de la infraestructura de red, lo cual incluye los nodos de acceso que conforman el anillo principal y los switches de borde, los cuales permiten la interconexión de los diferentes sistemas de transporte.

Omnivista 2500 es una aplicación que basa su funcionamiento en el modelo cliente – servidor y su interfaz puede ser accedida desde cualquier parte de la red a través de un navegador invocando su nombre DNS (o dirección IP).

La aplicación servidor del Omnivista 2500 se ejecuta como una máquina virtual sobre el sistema operativo Vmware ESXi 6.7 en un servidor Dell R440 en CDC:

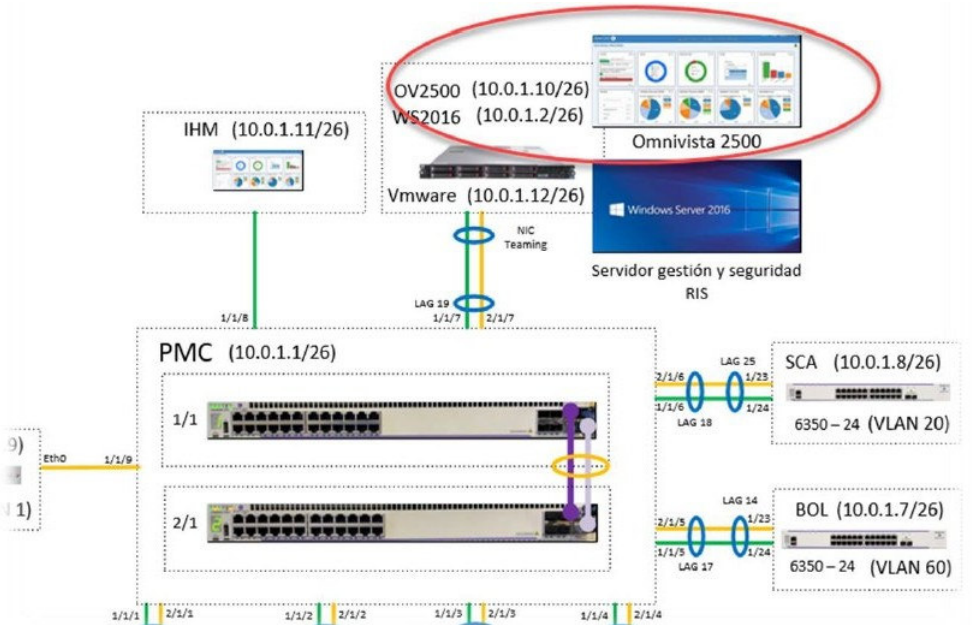

Figura 2.93. Situación topológica Omnivista 2500 en CDC.

Fuente: Autor

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 PRUEBAS SAT

Las pruebas SAT o Pruebas de Aceptación en Sitio (Site Aceptance Test) son pruebas que se realizan en la ubicación final de las instalaciones del cliente, también puede referirse a las pruebas de puesta en marcha del funcionamiento de un sistema. Estas pruebas tienen como objetivo demostrar el correcto funcionamiento del sistema, verificando que se cumple con los requisitos funcionales y las especificaciones técnicas del proyecto.

Estas pruebas fueron realizadas junto con la fiscalización del proyecto. A continuación, se listan cada una de las pruebas que se realizaron:

Lista de pruebas de Protocolo SAT-E1	
Ítem	**Descripción de la prueba**
1.	Verificar que el recorrido de FO forme un anillo, interconectando el CDC y las localidades, donde las terminaciones del cable lleguen al cuarto COM.
2.	Verificar que los ODF del armario ART del cuarto COM tengan al menos 4 puertos LC, conectados con patchcords monomodo hacia el Switch de nodo de acceso.
3.	Verificar que exista una reserva del cableado de FO en los cuartos donde existan fusiones de FO.
4.	Verificar que la distancia máxima de cableado entre armarios y equipos con armarios no deberá superar los 90 metros. Dicho cable debe ser de categoría 5e o superior.
5.	Verificar que todos los sistemas se interconecten con el armario de FO con sus respectivos puertos asignados.
6.	Verificar que las conexiones eléctricas estén reguladas por un UPS y aterrizadas de acuerdo con lo requerido por los equipos.
7.	Verificar que el cableado dentro de los armarios esté peinado en organizadores, bandejas y patch panel.

8.	Verificar que exista comunicación con el armario de GTC a través del punto de conexión de armarios.
9.	Verificar que exista comunicación con el armario de CCTV a través del punto de conexión de armarios.
10.	Verificar que exista comunicación con el armario de MEG a través del punto de conexión de armarios.
11.	Verificar que exista comunicación con el armario de TEL a través del punto de conexión de armarios.
12.	Verificar que exista comunicación con el armario de BOL a través del punto de conexión de armarios.
13.	Verificar que exista comunicación con el armario de SCA a través del punto de conexión de armarios.
14.	Verificar que exista comunicación con el armario de RED CORPORATIVA a través del punto de conexión de armarios.
15.	Verificar que exista comunicación desde el punto PCR-201 hacia el CDC y hacia Internet.
16.	Verificar que exista comunicación desde el punto PCR-202 hacia el CDC e Internet.

17.	Verificar que exista comunicación desde el punto PCR-203 hacia el CDC e Internet.
18.	Verificar que exista comunicación desde el punto PCR-204 hacia el CDC e Internet.
19.	Verificar que exista comunicación desde el punto PCR-205 hacia el CDC e Internet.
20.	Verificar que exista comunicación desde el punto PCR-206 hacia el CDC e Internet.
21.	Verificar que exista comunicación desde el punto PCR-207 hacia el CDC e Internet.
22.	Verificar que exista comunicación desde el punto PCR-208 hacia el CDC e Internet.
23.	Verificar VLANs de sistemas asignadas en los switches de nodo de acceso.
24.	Configurar un cliente NTP para sincronizarse con el switch de cronometría.
25.	Verificación de recuperación de comunicación en menos de 5 segundos.
26.	Verificación de operación de equipos en modo emergente.

27.	Prueba de hot swap en fuentes redundantes: Verificación de funcionalidad de alta disponibilidad eléctrica en switches.
28.	Verificación de redundancia en enlaces de comunicación de F.O.
29.	RED CORPORATIVA: Verificar redundancia y disponibilidad de comunicación entre switch de nodo de acceso y switch de RED CORPORATIVA. Se debe desconectar un enlace (cable) entre el switch de nodo de acceso y el switch de RED CORPORATIVA.
30.	Pruebas de balanceo de carga: se comprueba que los dos enlaces de FO conforman un backbone redundante a 40 Gbps FDX. Es posible que en esta etapa aún se conserve activo el STP.
31.	RED CORPORATIVA: prueba de velocidad de enlace de datos hacia nodo de acceso con link aggregation. (2Gbps).
32.	Verificar disponibilidad de puertos mayor al 40% en los switches de nodo de acceso.
33.	Prueba de aislamiento de VLANS. Conectar dos dispositivos (PCs) en diferentes localidades y verificar que NO exista comunicación entre localidades.
34.	Gestión y administración del sistema: acceso a Omnivista 2500 mediante vía web.

35.	Gestión y administración del sistema: pruebas de configuración inicial.
36.	Gestión y administración del sistema: prueba de niveles de usuario.
37.	Gestión y administración del sistema: histórico de alarmas.
38.	Gestión y administración del sistema: reportes de tráfico.
39.	Verificación en estación de trabajo de sistema, los estados de switches en Omnivista 2500.

Tabla 13. Lista de pruebas Protocolo SAT –E1

Lista de pruebas de Protocolo SAT- E2	
Ítem	**Descripción de la prueba**
1.	Verificar que el recorrido de FO forme un anillo, interconectando el CDC y las localidades, donde las terminaciones del cable lleguen al cuarto COM.
2.	Verificar que los ODF del armario ART del cuarto COM tengan al menos 4 puertos LC, conectados con patchcords monomodo hacia el Switch de nodo de acceso.
3.	Verificar que exista una reserva del cableado de FO en los cuartos donde existan fusiones de FO.

4.	Verificar que la distancia máxima de cableado entre armarios y equipos con armarios no deberá superar los 90 metros. Dicho cable debe ser de categoría 5e o superior.
5.	Verificar que todos los sistemas se interconecten con el armario de FO con sus respectivos puertos asignados.
6.	Verificar que las conexiones eléctricas estén reguladas por un UPS y aterrizadas de acuerdo con lo requerido por los equipos.
7.	Verificar que el cableado dentro de los armarios esté peinado en organizadores, bandejas y patch panel.
8.	Verificar que exista comunicación con el armario de GTC a través del punto de conexión de armarios.
9.	Verificar que exista comunicación con el armario de CCTV a través del punto de conexión de armarios.
10.	Verificar que exista comunicación con el armario de MEG a través del punto de conexión de armarios.
11.	Verificar que exista comunicación con el armario de TEL a través del punto de conexión de armarios.
12.	Verificar que exista comunicación con el armario de BOL a través del punto de conexión de armarios.

13.	Verificar que exista comunicación con el armario de BOL a través del punto de conexión de armarios.
14.	Verificar que exista comunicación con el armario de SCA a través del punto de conexión de armarios.
15.	Verificar que exista comunicación con el armario de RED CORPORATIVA a través del punto de conexión de armarios.
16.	Verificar que exista comunicación desde el punto PCR-001 hacia el CDC e Internet.
17.	Verificar que exista comunicación desde el punto PCR-002 hacia el CDC e Internet.
18.	Verificar que exista comunicación desde el punto PCR-003 hacia el CDC e Internet.
19.	Verificar que exista comunicación desde el punto PCR-104 hacia el CDC e Internet.
20.	Verificar que exista comunicación desde el punto PCR-105 hacia el CDC e Internet.
21.	Verificar que exista comunicación desde el punto PCR-206 hacia el CDC e Internet.

22.	Verificar que exista comunicación desde el punto PCR-207 hacia el CDC e Internet.
23.	Verificar que exista comunicación desde el punto PCR-208 hacia el CDC e Internet.
24.	Verificar VLANs de sistemas asignadas en los switches de nodo de acceso.
25.	Configurar un cliente NTP para sincronizarse con el switch de cronometría.
26.	Se debe aislar una localidad, desconectando ambos cables de fibra.
27.	Verificación de recuperación de comunicación en menos de 5 segundos.
28.	Verificación de operación de equipos en modo emergente.
29.	Prueba de hot swap en fuentes redundantes: verificación de funcionalidad de alta disponibilidad eléctrica en switches.
30.	Verificación de redundancia en enlaces de comunicación de F.O.
31.	RED CORPORATIVA: Verificar redundancia y disponibilidad de comunicación entre switch de nodo de acceso y switch de RED

	CORPORATIVA. Se debe desconectar un enlace (cable) entre el switch de nodo de acceso y el switch de RED CORPORATIVA.
32.	Verificar disponibilidad de puertos mayor al 40% en los switches de nodo de acceso.
33.	Prueba de aislamiento de VLANS. Conectar dos dispositivos (PCs) en diferentes localidades y verificar que NO exista comunicación entre localidades.
34.	Gestión y administración del sistema: acceso a Omnivista 2500 mediante vía web.
35.	Gestión y administración del sistema: pruebas de configuración inicial.
36.	Gestión y administración del sistema: prueba de niveles de usuario.
37.	Gestión y administración del sistema: Histórico de Alarmas.
38.	Gestión y administración del sistema: reportes de tráfico.
39.	Verificación en estación de trabajo de sistema, los estados de switches en Omnivista 2500.
40.	Verificar VLANs de sistemas asignadas en los switches de nodo de acceso.

Tabla 14. Lista de pruebas Protocolo SAT –E2

Lista de pruebas de Protocolo SAT- E3	
Ítem	**Descripción de la prueba**
1.	Verificar que el recorrido de FO forme un anillo, interconectando el CDC y las localidades, donde las terminaciones del cable lleguen al cuarto COM.
2.	Verificar que los ODF del armario ART del cuarto COM tengan al menos 4 puertos LC, conectados con patchcords monomodo hacia el Switch de nodo de acceso.
3.	Verificar que exista una reserva del cableado de FO en los cuartos donde existan fusiones de FO.
4.	Verificar que la distancia máxima de cableado entre armarios y equipos con armarios no deberá superar los 90 metros. Dicho cable debe ser de categoría 5e o superior.
5.	Verificar que todos los sistemas se interconecten con el armario de FO con sus respectivos puertos asignados.
6.	Verificar que las conexiones eléctricas estén reguladas por un UPS y aterrizadas de acuerdo con lo requerido por los equipos.
7.	Verificar que el cableado dentro de los armarios esté peinado en organizadores, bandejas y patch panel.

8.	Verificar que exista comunicación con el armario de GTC a través del punto de conexión de armarios.
9.	Verificar que exista comunicación con el armario de CCTV a través del punto de conexión de armarios.
10.	Verificar que exista comunicación con el armario de MEG a través del punto de conexión de armarios.
11.	Verificar que exista comunicación con el armario de TEL a través del punto de conexión de armarios.
12.	Verificar que exista comunicación con el armario de SCA a través del punto de conexión de armarios.
13.	Verificar que exista comunicación con el armario de RED CORPORATIVA a través del punto de conexión de armarios.
14.	Verificar que exista comunicación desde el punto PCR-101 hacia el CDC e Internet.
15.	Verificar que exista comunicación desde el punto PCR-102 hacia el CDC e Internet.
16.	Verificar que exista comunicación desde el punto PCR-103 hacia el CDC e Internet.

17.	Verificar que exista comunicación desde el punto PCR-204 hacia el CDC e Internet.
18.	Verificar que exista comunicación desde el punto PCR-205 hacia el CDC e Internet.
19.	Verificar que exista comunicación desde el punto PCR-206 hacia el CDC e Internet.
20.	Verificar VLANs de sistemas asignadas en los switches de nodo de acceso.
21.	Configurar un cliente NTP para sincronizarse con el switch de cronometría.
22.	Se debe aislar una localidad, desconectando ambos cables de fibra.
23.	Verificación de recuperación de comunicación en menos de 5 segundos.
24.	Verificación de operación de equipos en modo emergente.
25.	Prueba de hot swap en fuentes redundantes: Verificación de funcionalidad de alta disponibilidad eléctrica en switches.
26.	Verificación de redundancia en enlaces de comunicación de F.O.

27.	RED CORPORATIVA: Verificar redundancia y disponibilidad de comunicación entre switch de nodo de acceso y switch de RED CORPORATIVA. Se debe desconectar un enlace (cable) entre el switch de nodo de acceso y el switch de RED CORPORATIVA.
28.	Pruebas de balanceo de carga: se comprueba que los dos enlaces de FO conforman un backbone redundante a 40 Gbps FDX. Es posible que en esta etapa aún se conserve activo el STP.
29.	RED CORPORATIVA: Prueba de velocidad de enlace de datos hacia nodo de acceso con link aggregation. (2Gbps).
30.	Probar velocidad entre nodos de acceso (20GBps).
31.	Verificar velocidad de transmisión entre localidades y CDC. (2 Gbps). Se debe enviar un archivo entre una localidad y CDC.
32.	Verificar disponibilidad de puertos mayor al 40% en los switches de nodo de acceso.
33.	Prueba de aislamiento de VLANS. Conectar dos dispositivos (PCs) en diferentes localidades y verificar que NO exista comunicación entre localidades.
34.	Apagado seguro de equipos: demostración de funcionalidad en el caso de aplicación de una ventana de mantenimiento.

35.	Reinicio seguro de equipos: demostración de reinicio de equipos y entrada en modo normal de funcionamiento.
36.	Gestión y administración del sistema: acceso a Omnivista 2500 mediante vía web.
37.	Gestión y administración del sistema: pruebas de configuración inicial.
38.	Gestión y administración del sistema: prueba de niveles de usuario.
39.	Gestión y administración del sistema: histórico de alarmas.
40.	Gestión y administración del sistema: reportes de tráfico.
41.	Verificación en de sistema, los estados de switches en Omnivista 2500.

Tabla 15. Lista de pruebas Protocolo SAT –E3

Lista de pruebas de Protocolo SAT- E4	
Ítem	**Descripción de la prueba**
1.	Verificar que el recorrido de FO forme un anillo, interconectando el CDC y las localidades, donde las terminaciones del cable lleguen al cuarto COM.

2.	Verificar que los ODF del armario ART del cuarto COM tengan al menos 4 puertos LC, conectados con patchcords monomodo hacia el Switch de nodo de acceso.
3.	Verificar que exista una reserva del cableado de FO en los cuartos donde existan fusiones de FO.
4.	Verificar que la distancia máxima de cableado entre armarios y equipos con armarios no deberá superar los 90 metros. Dicho cable debe ser de categoría 5e o superior.
5.	Verificar que todos los sistemas se interconecten con el armario de FO con sus respectivos puertos asignados.
6.	Verificar que las conexiones eléctricas estén reguladas por un UPS y aterrizadas de acuerdo con lo requerido por los equipos.
7.	Verificar que el cableado dentro de los armarios esté peinado en organizadores, bandejas y patch panel.
8.	Verificar que exista comunicación con el armario de GTC a través del punto de conexión de armarios.
9.	Verificar que exista comunicación con el armario de CCTV a través del punto de conexión de armarios.

10.	Verificar que exista comunicación con el armario de MEG a través del punto de conexión de armarios.
11.	Verificar que exista comunicación con el armario de TEL a través del punto de conexión de armarios.
12.	Verificar que exista comunicación con el armario de BOL a través del punto de conexión de armarios.
13.	Verificar que exista comunicación con el armario de SCA a través del punto de conexión de armarios.
14.	Verificar que exista comunicación con el armario de RED CORPORATIVA a través del punto de conexión de armarios.
15.	Verificar que exista comunicación con el armario de INTERCONEXIÓN CON RED PÚBLICA a través del punto de conexión de armarios.
16.	Verificar que exista comunicación con el armario de INTERCONEXIÓN CON RED PÚBLICA a través del punto de conexión de armarios.
17.	Verificar que exista comunicación con el armario de GTC a través del punto de conexión de armarios.

18.	Verificar que exista comunicación con el armario de CCTV a través del punto de conexión de armarios.
19.	Verificar que exista comunicación con el armario de MEG a través del punto de conexión de armarios.
20.	Verificar que exista comunicación con el armario de TEL a través del punto de conexión de armarios.
21.	Verificar que exista comunicación con el armario de BOL a través del punto de conexión de armarios.
22.	Verificar que exista comunicación con el armario de SCA a través del punto de conexión de armarios.
23.	Verificar que exista comunicación con la estación de trabajo a través del puerto de red del switch de nodo de acceso.
24.	Verificar que exista comunicación con el SWITCH de CRONOMETRÍA a través del puerto de red de nodo de acceso.
25.	Verificar que exista comunicación desde el punto PCR-001 hacia el CDC e Internet.
26.	Verificar que exista comunicación desde el punto PCR-002 hacia el CDC e Internet.

27.	Verificar que exista comunicación desde el punto PCR-003 hacia el CDC e Internet.
28.	Verificar que exista comunicación desde el punto PCR-004 hacia el CDC e Internet.
29.	Verificar que exista comunicación desde el punto PCR-005 hacia el CDC e Internet.
30.	Verificar que exista comunicación desde el punto PCR-106 hacia el CDC e Internet.
31.	Verificar que exista comunicación desde el punto PCR-107 hacia el CDC e Internet.
32.	Verificar que exista comunicación desde el punto PCR-108 hacia el CDC e Internet.
33.	Verificar que exista comunicación desde el punto PCR-109 hacia el CDC e Internet.
34.	Verificar que exista comunicación desde el punto PCR-110 hacia el CDC e Internet.
35.	Verificar que exista comunicación desde el punto PCR-111 hacia el CDC e Internet.

36.	Verificar que exista comunicación desde el punto PCR-112 hacia el CDC e Internet.
37.	Verificar que exista comunicación desde el punto PCR-113 hacia el CDC e Internet.
38.	Verificar que exista comunicación desde el punto PCR-114 hacia el CDC e Internet.
39.	Verificar que exista comunicación desde el punto PCR-115 hacia el CDC e Internet.
40.	Verificar que exista comunicación desde el punto PCR-116 hacia el CDC e Internet.
41.	Verificar que exista comunicación desde el punto PCR-117 hacia el CDC e Internet.
42.	Verificar que exista comunicación desde el punto PCR-118 hacia el CDC e Internet.
43.	Verificar que exista comunicación desde el punto PCR-119 hacia el CDC e Internet.
44.	Verificar que exista comunicación desde el punto PCR-120 hacia el CDC e Internet.

45.	Verificar que exista comunicación desde el punto PCR-121 hacia el CDC e Internet.
46.	Verificar que exista comunicación desde el punto PCR-122 hacia el CDC e Internet.
47.	Verificar que exista comunicación desde el punto PCR-123 hacia el CDC e Internet.
48.	Verificar que exista comunicación desde el punto PCR-124 hacia el CDC e Internet.
49.	Verificar que exista comunicación desde el punto PCR-125 hacia el CDC e Internet.
50.	Verificar que exista comunicación desde el punto PCR-226 hacia el CDC e Internet.
51.	Verificar que exista comunicación desde el punto PCR-227 hacia el CDC e Internet.
52.	Verificar VLANs de sistemas asignadas en los switches de nodo de acceso.
53.	Configurar un cliente NTP para sincronizarse con el switch de cronometría.

54.	Se debe aislar una localidad, desconectando ambos cables de fibra.
55.	Verificación de recuperación de comunicación en menos de 5 segundos.
56.	Verificación de operación de equipos en modo emergente.
57.	Prueba de hot swap en fuentes redundantes: verificación de funcionalidad de alta disponibilidad eléctrica en switches.
58.	Verificación de redundancia en enlaces de comunicación de F.O.
59.	RED CORPORATIVA: verificar redundancia y disponibilidad de comunicación entre switch de nodo de acceso y switch de RED CORPORATIVA. Se debe desconectar un enlace (cable) entre el switch de nodo de acceso y el switch de RED CORPORATIVA.
60.	Pruebas de balanceo de carga: se comprueba que los dos enlaces de FO conforman un backbone redundante a 40 Gbps FDX. Es posible que en esta etapa aún se conserve activo el STP.
61.	RED CORPORATIVA: prueba de velocidad de enlace de datos hacia nodo de acceso con link aggregation. (2Gbps).
62.	Probar velocidad entre nodos de acceso (20GBps).

63.	Verificar velocidad de transmisión entre localidades y CDC. (2 Gbps). Se debe enviar un archivo entre una localidad y CDC.
64.	Verificar disponibilidad de puertos mayor al 40% en los switches de nodo de acceso.
65.	Prueba de aislamiento de VLANS. Conectar dos dispositivos (PCs) en diferentes localidades y verificar que NO exista comunicación entre localidades.
66.	Apagado seguro de equipos: demostración de funcionalidad en el caso de aplicación de una ventana de mantenimiento.
67.	Reinicio seguro de equipos: demostración de reinicio de equipos y entrada en modo normal de funcionamiento.
68.	Gestión y administración del sistema: acceso a Omnivista 2500 mediante vía web.
69.	Gestión y administración del sistema: pruebas de configuración inicial.
70.	Gestión y administración del sistema: prueba de niveles de usuario.
71.	Gestión y administración del sistema: histórico de alarmas.
72.	Gestión y administración del sistema: reportes de tráfico.

73.	Verificación en estación de trabajo de sistema, los estados de switches en Omnivista 2500.

Tabla 16. Lista de pruebas Protocolo SAT –E4

Lista de pruebas de Protocolo SAT- E5	
Ítem	**Descripción de la prueba**
1.	Verificar que el recorrido de FO forme un anillo, interconectando el CDC y las localidades, donde las terminaciones del cable lleguen al cuarto COM.
2.	Verificar que los ODF del armario ART del cuarto COM tengan al menos 4 puertos LC, conectados con patchcords monomodo hacia el Switch de nodo de acceso.
3.	Verificar que exista una reserva del cableado de FO en los cuartos donde existan fusiones de FO.
4.	Verificar que la distancia máxima de cableado entre armarios y equipos con armarios no deberá superar los 90 metros. Dicho cable debe ser de categoría 5e o superior.
5.	Verificar que todos los sistemas se interconecten con el armario de FO con sus respectivos puertos asignados.

6.	Verificar que las conexiones eléctricas estén reguladas por un UPS y aterrizadas de acuerdo con lo requerido por los equipos.
7.	Verificar que el cableado dentro de los armarios esté peinado en organizadores, bandejas y patch panel.
8.	Verificar que exista comunicación con el armario de GTC a través del punto de conexión de armarios.
9.	Verificar que exista comunicación con el armario de CCTV a través del punto de conexión de armarios.
10.	Verificar que exista comunicación con el armario de MEG a través del punto de conexión de armarios.
11.	Verificar que exista comunicación con el armario de TEL a través del punto de conexión de armarios.
12.	Verificar que exista comunicación con el armario de BOL a través del punto de conexión de armarios.
13.	Verificar que exista comunicación con el armario de SCA a través del punto de conexión de armarios.
14.	Verificar que exista comunicación con el armario de RED CORPORATIVA a través del punto de conexión de armarios.

15.	Verificar que exista comunicación desde el punto PCR-001 hacia el CDC e Internet.
16.	Verificar que exista comunicación desde el punto PCR-002 hacia el CDC e Internet.
17.	Verificar que exista comunicación desde el punto PCR-003 hacia el CDC e Internet.
18.	Verificar que exista comunicación desde el punto PCR-004 hacia el CDC e Internet.
19.	Verificar que exista comunicación desde el punto PCR-005 hacia el CDC e Internet.
20.	Verificar que exista comunicación desde el punto PCR-006 hacia el CDC e Internet.
21.	Verificar que exista comunicación desde el punto PCR-007 hacia el CDC e Internet.
22.	Verificar que exista comunicación desde el punto PCR-008 hacia el CDC e Internet.
23.	Verificar que exista comunicación desde el punto PCR-009 hacia el CDC e Internet.

24.	Verificar que exista comunicación desde el punto PCR-010 hacia el CDC e Internet.
25.	Verificar que exista comunicación desde el punto PCR-011 hacia el CDC e Internet.
26.	Verificar VLANs de sistemas asignadas en los switches de nodo de acceso.
27.	Configurar un cliente NTP para sincronizarse con el switch de cronometría.
28.	Se debe aislar una localidad, desconectando ambos cables de fibra.
29.	Verificación de recuperación de comunicación en menos de 5 segundos.
30.	Verificación de operación de equipos en modo emergente.
31.	Prueba de hot swap en fuentes redundantes: verificación de funcionalidad de alta disponibilidad eléctrica en switches.
32.	Verificación de redundancia en enlaces de comunicación de F.O.
33.	RED CORPORATIVA: Verificar redundancia y disponibilidad de comunicación entre switch de nodo de acceso y switch de RED

	CORPORATIVA. Se debe desconectar un enlace (cable) entre el switch de nodo de acceso y el switch de RED CORPORATIVA.
34.	Pruebas de balanceo de carga: Se comprueba que los dos enlaces de FO conforman un backbone redundante a 40 Gbps FDX. Es posible que en esta etapa aún se conserve activo el STP.
35.	RED CORPORATIVA: Prueba de velocidad de enlace de datos hacia nodo de acceso con link aggregation. (2Gbps).
36.	Probar velocidad entre nodos de acceso (20GBps).
37.	Verificar velocidad de transmisión entre localidades y CDC. (2 Gbps). Se debe enviar un archivo entre una localidad y CDC.
38.	Verificar disponibilidad de puertos mayor al 40% en los switches de nodo de acceso.
39.	Prueba de aislamiento de VLANS. Conectar dos dispositivos (PCs) en diferentes localidades y verificar que NO exista comunicación entre localidades.
40.	Apagado seguro de equipos: demostración de funcionalidad en el caso de aplicación de una ventana de mantenimiento.
41.	Reinicio seguro de equipos: demostración de reinicio de equipos y entrada en modo normal de funcionamiento.

42.	Gestión y administración del sistema: acceso a Omnivista 2500 mediante vía web.
43.	Gestión y administración del sistema: pruebas de configuración inicial.
44.	Gestión y administración del sistema: prueba de niveles de usuario.
45.	Gestión y administración del sistema: histórico de alarmas.
46.	Gestión y administración del sistema: reportes de tráfico.
47.	Verificación en estación de trabajo de sistema, los estados de switches en Omnivista 2500.

Tabla 17. Lista de pruebas Protocolo SAT –E5

CONCLUSIONES Y RECOMENDACIONES

A continuación, se detallará las conclusiones y recomendaciones del proyecto, estas se establecen por lo que se realizó y desarrolló en la implementación.

Conclusiones

1. Se finalizó con éxito la implementación de la infraestructura Integral de red. Desplegando en anillo los diferentes switches de nodo acceso que constituyeron la columna vertebral comunicacional que permitieron el funcionamiento óptimo de los diferentes sistemas de transporte.
2. Parte de esta infraestructura de red está conformada por switches de borde, los que permiten la conexión de los diferentes elementos de los sistemas de transporte en una topología Top of the Rack.
3. Integrante esencial de dicha infraestructura de red es un NMS moderno y con funcionalidades según el estado del arte de la tecnología, permitiendo una administración (monitoreo y configuración) sencilla e intuitiva.
4. La implementación se caracterizó por el uso de mejores prácticas en Networking y seguridad en redes de datos.

Recomendaciones

1. Es importante que se regularicen aquellos accesos a internet otorgados de manera temporal, debido a la necesidad de la implementación.
2. Se debe revisar los accesos a VPN proporcionados, debido a necesidades de implementación. Habría que eliminar aquellos accesos que no se usen.
3. Es necesario que se creen diversos perfiles de navegación para los diferentes tipos de usuarios que acceden al internet. Por ejemplo, cuotas de ancho de banda, acceso a redes sociales, streaming, etc.
4. Los usuarios de internet de la red Wifi de localidades usan, de momento, el mismo acceso a Internet que aquellos de red corporativa. Se sugiere independizar dicho acceso.
5. En la infraestructura de localidad 2, para los switches GRAL, se recomienda implementar un stack que permita manejar a los dos switches como uno solo. Al momento hay una cascada entre los dos switches.
6. La infraestructura de red es de funcionamiento crítico y su seguridad de vital importancia, por lo cual se sugiere cambiar la contraseña de administración de sus componentes cada mes. La disponibilidad de un servidor de autenticación hace esta actividad más sencilla.

ANEXOS