ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“IMPLEMENTACIÓN DE LA INFRAESTRUCTURA DE NETWORKING PARA UNA INSTITUCIÓN PÚBLICA.”

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

MAGÍSTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

AUTOR

JOSÉ LUIS SALTOS MENDOZA

GUAYAQUIL-ECUADOR

SEPTIEMBRE 2021

AGRADECIMIENTO

A Dios por cada día en que me permitió despertar con vida, salud, fortaleza y empeño para seguir adelante en la culminación de este importante episodio en mi vida académica y a mi familia por ser el impulso que me motiva a seguir adelante en la búsqueda nuevos retos y logros.

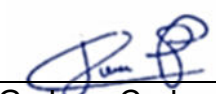
DEDICATORIA

Quiero dedicar este trabajo a mi familia y en especial a la memoria de mi padre, quien partió poco antes de empezar esta etapa de preparación académica y estoy seguro que desde el sitio en el que está, siempre me brindó su apoyo.

TRIBUNAL DE SUSTENTACIÓN

MSIG. Lenin Freire Cobo

CORDINADOR MSIG



MSIG. Juan Carlos García

PROFESOR MSIG

RESUMEN

Esta implementación tiene por objeto dotar a la institución de equipos de networking de última tecnología, diseñados y pensados para cumplir procesos de alta demanda en ancho de banda y altas velocidades de procesamiento, con estándares de calidad y seguridad en la transmisión de datos, los cuales serán los cimientos que sostengan a toda la infraestructura de comunicaciones que vaya adquiriendo para cumplir a cabalidad con las funciones para la cual ha sido creada.

La infraestructura implementada está conformada por equipos de la marca cisco, lo que garantiza su fiabilidad, y está compuesta por un switch de CORE ubicado en el centro de datos, este equipo se conecta a los switches de acceso que están ubicados en el mezzanine y en el primer piso mediante el enlace de fibra óptica instalado entre los pisos (MZ y P1) y el centro de datos (P1).

Esta infraestructura de red permitirá compartir de manera eficiente distintos recursos (aplicaciones, equipos, bases de datos, entre otros), además, proporciona una comunicación segura y de alta velocidad a los usuarios que utilizan los servicios de comunicaciones de datos, voz, video e internet.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ABREVIATURAS Y SIMBOLOGÍA

AP Access Point, dispositivos de capa 2 que permiten la integración de usuarios inalámbricos a la red cableada. Pueden operar en modo autónomo o liviano (lightweight).

AES Advanced Encryption Standard, algoritmo de encriptación a nivel corporativo basado en TKIP especificado por el estándar 802.11i. Encripta el contenido de la capa dos, adelanta una verificación integra del mensaje (MIC) en el paquete que está encriptado, garantizando la no afectación o alteración del mensaje. Utiliza información adicional del encabezado de la MAC que les permite a los hosts de destino reconocer si se alteraron los bits no encriptados. Además, agrega un número de secuencia al encabezado de información encriptada.

IOS Internetwork Operating System, es el sistema operativo que permite configurar los dispositivos Cisco.

LWAPP Lightweight Access Point Protocol, son access points que funcionan bajo la configuración de una WLC; es decir, no tienen inteligencia propia

Port Channel Protocolo que permite agrupar lógicamente múltiples interfaces físicas permitiendo que todas estén activas al mismo tiempo con la finalidad de proporcionar redundancia y, en consecuencia, incremento en el ancho de banda del enlace que comunica dos dispositivos de red. Cisco opera mediante dos protocolos: PAgP y LACP, siendo este último el estándar IEEE 802.3ad.

POST Power-on-self-test, revisión del hardware realizada por el switch o router. Si la revisión finaliza con éxito, el dispositivo carga el IOS desde su memoria flash.

PSK Pre-shared key, clave pre-compartida, es una contraseña compartida entre los access points y los usuarios de la red inalámbrica.

Router Dispositivo de capa tres del modelo OSI para interconexión de redes de ordenadores encargado de elegir las mejores rutas para entregar los paquetes basado en las direcciones de red de origen y destino.

SSID Service Set Identifier, un identificador de servicio compartido (SSID) es un identificador único que utilizan los dispositivos cliente para distinguir entre múltiples redes inalámbricas cercanas. Varios puntos de acceso en la red pueden compartir un SSID.

STP Spanning Tree Protocol, es un protocolo encargado de evitar lazos cuando existen caminos redundantes a nivel de capa dos del modelo OSI. Existen tres variaciones de STP estandarizados por la IEEE: 802.1D o Spanning Tree tradicional, cuyos tiempos de convergencia son muy elevados; 802.1w o Rapid Spanning Tree, una mejora notable con respecto a su predecesor pero que crea una sola instancia de STP; y, finalmente, 802.1s o Multiple Spanning Tree (MST), quien está basado en Rapid Spanning Tree pero permite crear varias instancias de Spanning Tree.

SVI Switch Virtual Interface, es la interface virtual a nivel de capa tres del modelo OSI de una vlan que permite, entre otras funciones, la comunicación entre varias vlans.

	Es el equivalente a la interface física de un router, quien a su vez sirve como Gateway de los dispositivos pertenecientes a la vlan.
Switch	Dispositivo de capa dos del modelo OSI que permite la comunicación entre dos o más equipos de una red local basado en las direcciones físicas (MAC address) de origen y destino.
Switch multicapa	Dispositivo similar al switch de capa dos pero con características de enrutamiento, normalmente utilizado en las capas de distribución y acceso.
Trunk	Interfaces que envían y reciben más de una vlan a través de ellas. Actualmente todos los dispositivos Cisco operan utilizando el protocolo de la IEEE 802.1q, permitiendo interoperatividad con otros fabricantes. A todas las vlans se añade una etiqueta a las tramas de capa 2 excepto a la vlan nativa.
VLAN	Virtual LAN, Red de área local virtual, grupo de dispositivos conectados físicamente a la red y que pertenecen de manera

lógica (virtual) a un mismo dominio de broadcast. Varias vlans pueden coexistir en un switch aumentando el número de dominios de broadcast y reduciendo el tamaño de los mismos, manteniendo el tráfico de una vlan dentro de ésta disminuyendo así la probabilidad de colisiones. Para que dos o más vlans se puedan comunicar entre sí se requiere un dispositivo de capa tres.

Vlan Nativa Única vlan que de acuerdo al protocolo 802.1q no se etiqueta a través de un puerto trunk.

VTP Virtual Trunking Protocol, es un protocolo propietario de Cisco que permite la replicación de las vlans configuradas en un switch evitando la necesidad de tener que configurarlas nuevamente en otros switches. Puede funcionar en tres modos: server, client y transparent. En modo server se pueden crear o eliminar vlans; en modo cliente solamente se pueden recibir vlans (no se puede editarlas). En modo transparente se pueden crear y eliminar vlans y replicarlas solamente entre switches que estén en modo transparente.

WLC Wireless LAN Controller, dispositivo que centraliza la configuración y administración de los access points. Para que los APs puedan registrarse a una WLC, éstos deben operar con un IOS lightweight.

WPA/WPA2 Wifi-Protected Acces, acceso protegido Wifi, es un protocolo de seguridad para conexiones inalámbricas. WPA surgió como una solución temporal para mejorar las vulnerabilidades de su predecesor WEP hasta que, finalmente, se llegó al WPA2.

INTRODUCCIÓN

El presente documento describe la necesidad que tiene una institución pública que demanda una infraestructura de red fiable y de alta velocidad, la implementación que se realizó para satisfacer su necesidad y las pruebas de funcionamiento de la solución implementada. El escrito se compone de tres partes resumidas a continuación. Capítulo 1 – Generalidades, en este apartado se describe la situación actual de la institución, la necesidad que se plantea satisfacer y se propone una solución que permita solventarla. Capítulo 2 – Metodología para el Desarrollo de la solución, se presenta desde la recolección de la información, el dimensionamiento del hardware y del software que se requieren, igualmente el diseño del plan de actividades, y por último, la aplicación de la solución propuesta. En el capítulo 3 – se presenta la Evaluación de los Resultados, donde se analiza el seguimiento de la operatividad de la implementación de la infraestructura de networking para una institución pública. Por último, se plantean las conclusiones y recomendaciones.

CAPÍTULO 1

GENERALIDADES

1.1 Descripción del problema

Por tratarse de una institución pública de reciente formación, la entidad no cuenta con infraestructura de red, encontrándose en la fase de adquisición de equipos de Networking, los cuales serán la base que sostengan a toda la infraestructura de comunicaciones adquirida para cumplir a cabalidad con las funciones para la cual ha sido creada, con el objetivo de “mejorar la continuidad del servicio, mejorar la utilización de los recursos, proteger la red, controlar cambios y actualizaciones” (Terán, 2020, p. 25)

La institución se encuentra en la etapa de planificación y diseño de una tecnología en hardware y software que le permitan digitalizar, catalogar y almacenar contenido de los medios de comunicación. Por lo cual, es necesario contar con una infraestructura de red dimensionada para el manejo de video y archivos de gran tamaño, con equipos diseñados y

pensados para cumplir procesos de alta demanda en ancho de banda y altas velocidades de procesamiento, con estándares de calidad y seguridad en la transmisión de datos.

1.2 SOLUCIÓN PROPUESTA

Como solución al problema descrito anteriormente, se propone la implementación de una infraestructura de networking cisco, compuesta por un switch de CORE ubicado en el centro de datos, este equipo se conectará a los switches de acceso que estarán ubicados en el mezzanine y el primer piso mediante el enlace de fibra óptica instalado entre los pisos (MZ y P1) y el centro de datos (P1), de tal forma que permita velocidades de transmisión de datos de mínimo 10GB, además se incluye la instalación, configuración y puesta en marcha de todo el equipamiento activo de networking.

Con la denominación Networking se identifica a aquellas soluciones de electrónica de red encargadas de suministrar a la red de datos de una empresa la eficacia, control, calidad y seguridad que demandan las comunicaciones de datos que transitan a través de ella (INSTEL, 2020).

CAPÍTULO 2

METODOLOGÍA PARA EL DESARROLLO DE LA SOLUCIÓN

2.1 SITUACIÓN ACTUAL DE LA RED

Por tratarse de una organización de reciente formación, la institución no cuenta con infraestructura de red, encontrándose precisamente en la fase de adquisición de equipos de Networking, los cuales serán los pilares que sostengan a toda la infraestructura de comunicaciones que vaya adquiriendo para cumplir a cabalidad con las funciones para la cual ha sido creada.

En la inspección previa a la implementación, se pudo constatar que:

- La institución ya tenía instalado el cableado estructurado.

• Los puntos de datos para conectar los access points ya habían sido fijados.

• Los únicos equipos que tenían en funcionamiento eran el router del proveedor de internet, switches y access points de gama baja, un servidor que tiene levantada una plataforma de firewall en linux.

La solución adquirida por la Institución cuenta con los dispositivos que se muestran en la tabla 1:

Tabla 1. Dispositivos adquiridos para la solución

Equipo	Modelo	Cantidad	# Puertos
Switch Core	Catalyst 4500X-16	1	16
Switch Acesso	WS-C3650-48PD	2	48
Access Points	AIR-CAP2702E	2	1
Transceiver SFP 1000Base-T	GLC-T	4	N/A
Transceiver SFP 10Gb (FO)	SFP 10G-SR	4	N/A

Elaboración propia

2.2 DIMENSIONAMIENTO DEL HARDWARE REQUERIDO

El proyecto de adquisición, instalación e implementación de una infraestructura de networking para la empresa pública, comprende poner

en marcha todo el diseño de red de datos, con la adquisición del equipamiento activo apropiado que asegure los distintos servicios de comunicación.

Al ser una institución pública que requiere gestionar continuamente información para brindar unos servicios a la comunidad en términos de calidad y oportunidad requiere adquirir, instalar y poner en marcha una Infraestructura integrada de equipos activos de networking y telecomunicaciones, que facilite la administración y gestión de la red de datos interna, además la institución se encuentra en el proceso de optar por tecnología de software para análisis de medios que requieren de procesos y manejo especial de la información, para lo cual se necesita comunicación veloz y fiable que cuente con altos estándares de calidad en la transmisión de datos y voz, por lo que se hace necesario contar con equipamiento activo de última tecnología.

La nueva infraestructura de red y comunicaciones permitirá compartir recursos (bases de datos, aplicaciones, impresiones, periféricos, etc., y servicios de videoconferencias), suministrando una comunicación segura, flexible y de alta velocidad entre los usuarios a los que presta servicio de comunicaciones de datos, voz, video e internet. De la misma forma, permitirá la capacidad necesaria para llevar a cabo una evolución en sus

comunicaciones respondiendo a una formación académica de calidad que actualmente lo demanda (Beneitez, 2020).

Seguidamente se puntualiza el alcance total para la realización del proyecto, el cual comprende lo siguiente:

Equipos activos:

- 1 Switch de core de 16 Puertos (Equipo Central con redundancia de fuente y tarjetas).
- 2 Switches de acceso de 48 Puertos con controladora Wireless.
- 2 Puntos de acceso (AP).

2.2.1 Consideraciones generales

Para este proyecto se deberá considerar lo siguiente:

- Toda la solución debe ser instalada, configurada y quedar operativa de acuerdo a las necesidades de la institución pública objeto del presente estudio.
- Las conexiones serán aseguradas de modo que no sean aflojadas por vibraciones, esfuerzos normales o algún otro factor que afecte a las mismas.

- Todas las instalaciones contarán con las partes necesarias para sujetar los equipos a los gabinetes de cada piso y data center.
- La instalación incluirá la organización y la conexión de todo el equipamiento; pasivo y activo.

2.2.2 Consideraciones específicas

Específicamente, el proyecto contempla los siguientes aspectos:

- Se instalarán los switches de acceso en cada piso, esta instalación incluye la puesta en marcha de toda la solución:
  - Configuración de VLANs
  - Configuración de Listas de Acceso.
  - Configuración de Puntos de Acceso.
  - Configuración de Políticas de Seguridad.
  - Todas las configuraciones necesarias para dejar operativa la solución.
- El equipo de CORE se instalará en el 1er Piso, deberá contar con todas las configuraciones:
  - Configuración de VLANs
  - Configuración de Access List.
  - Configuración de Puntos de Acceso.

2.2.3 Justificación

La empresa pública se encuentra en la etapa de planificación y diseño de una tecnología en hardware y software que le permitan realizar el monitoreo, almacenamiento, análisis e investigación de los medios de comunicación de dentro de su jurisdicción, conforme lo demanda la Ley Orgánica de Comunicación.

Siendo así, el diseño de networking del Área de Tecnologías de la Información y Comunicación de la institución, debe ser conceptualizado desde el punto de vista del manejo de video y archivos de gran tamaño, mismos que serán colocados en sistemas de almacenamiento, esta información deberá estar disponible para que cualquier usuario autorizado, que desde cualquier ubicación, en cualquier momento y sin importar el dispositivo, disponga de esta información, sin poner en riesgo la seguridad de la información, es así, que estos equipos han sido diseñados y pensados para que cumplan procesos de alta demanda en ancho de banda y altas velocidades de procesamiento, con estándares de calidad y seguridad en la transmisión de datos, por lo que, se hace necesario contar con equipamiento activo de última tecnología.

La nueva infraestructura de red permitirá la compartición de recursos (bases de datos, aplicaciones, impresiones, periféricos, etc.), proporcionando una comunicación segura, flexible y de alta velocidad entre los usuarios a los que presta servicio de comunicaciones de datos, voz, video e internet. Así mismo permitirá la capacidad necesaria para llevar a cabo una evolución en sus comunicaciones respondiendo a las exigencias demande su misión institucional.

2.2.4 Alcance

Se procura la interconexión entre los diferentes pisos de la institución hacia el centro de datos (DATACENTER) y la comunicación con las diferentes zonales a nivel nacional mediante el enlace de datos.

El proyecto comprende la instalación de un switch de CORE con redundancia, este equipo se conectará a los switches de acceso ubicados en el mezzanine y el primer piso mediante el enlace de fibra óptica instalado entre los pisos (MZ y P1) y el centro de datos (P1), de tal forma que permita velocidades de transmisión de datos de mínimo 10GB, además se incluye la instalación, configuración y puesta en marcha de todo el equipamiento activo de networking y comunicaciones unificadas en redundancia.

2.2.5 Equipamiento

Actualmente el acceso a la red debe poder realizarse tanto alámbrica como inalámbricamente. Es por esto que, para una efectiva solución de tecnología, el equipamiento de los dispositivos de Networking debe incluir los siguientes dispositivos

- Un switch de core
- Dos switches de acceso
- Wireless LAN Controller
- Access Points

A continuación, en la tabla 2, se presentan las características de los equipos requeridos

Tabla 2. Características de los equipos requeridos

Equipo	Características
Switch de core	• Switch de capa 3 • Puertos Ethernet 10G o 1G de fibra o cobre (SFP+/SFP) • Módulo de expansión de 8 puertos 10G • Puerto de administración por consola 10/100/1000 Mbps • Redundancia en fuente de poder • MTBF: 209,330 • Throughput: >=800 Gbps • Routing IPv4 en Hardware: >=250Mpps • Routing IPv6 en Hardware: >=125Mpps • Bridging Capa 2 en Hardware: >=250Mpps • Media Access Control Entries: >=55K • Flexible Netflow Entries: >=128K • Total VLANs: >=4094 • Total SVIs: >=4094 • Grupos IGMP: >=32K

	• DHCP Snooping Entries: >=12K • ARP Entries: >=47K • Instancias STP: >=10K • Soporte de Jumbo Frames: >=9216 bytes • Alta disponibilidad mediante VSS • Número de switches stackeables: >=2 • Throughput VSS: >=1.6Tbps • Soporte de Virtual Switch Link: 1GE o 10GE • Máximo número de VSL: >=8 • Memoria SRAM DDR-II • Port Buffers: Memoria compartida de 32MB • CPU: Dual Core 1.5GHz • NVRAM: >=2GB • Colas de puertos: 8 colas / puerto • Colas de CPU: 64 • Entradas de QoS: 128K • Class of Service (CoS) • Port Security • IEEE 802.1x and 802.1x Extensions • VLAN, Router, and Port ACLs • Security ACL Entries (1K=1024): >=128K • Unicast Reverse Path Forwarding (uRPF) Check en Hardware • VLAN privadas • Control Plane Policing (CoPP) for Multicast • ACL Labels • Port ACL • Control de tormenta de tráfico • Escalabilidad VRF-Lite: >=64 • Escalabilidad Easy Virtual Network: >=32 • **Ethernet: IEEE 802.3:** 10 Gigabit Ethernet: IEEE 802.3ae EEE 802.3ad LACP • IEEE 802.1p CoS Prioritization • IEEE 802.1Q VLAN • IEEE 802.1X User Authentication • IEEE 802.1x-Rev • RMON I and II standards • USGv6 and IPv6 Gold Logo certified • IEEE 802.1D Spanning Tree Protocol • IEEE 802.1w Rapid Reconfiguration of Spanning Tree • IEEE 802.1s Multiple VLAN Instances of Spanning Tree.
Switches de acceso	• Switch de capa 3 con controladora inalámbrica embebida. • Puertos Ethernet a 10G SFP: >= 2 • Puerto RJ-45 para administración por consola • Capacidad de Switching >= 176Gbps • Ancho de Banda de Stacking >= 160 Gbps • Número total de MAC Addresses >=32000

	• Número total de Rutas IPv4 >=24000 • Entradas FNF >= 480000 flujos • DRAM >= 4Gb • FLASH >= 2Gb • Manejo mínimo de 4096 VLAN IDs • Jumbo Frame: 9198 bytes • SVIs: 1000 • Soporte número de puntos de acceso por switch / stack • Número de clientes wireless por switch / stack • Ancho de Banda Wireless por switch >= 40 Gbps • Soporte de los switches solicitados • Licencias para access point • Redundancia de fuente de alimentación • **Cumplimiento de normas:** • IEEE 802.1D Spanning Tree Protocol • IEEE 802.1p CoS Prioritization • IEEE 802.1Q VLAN • IEEE 802.1s • IEEE 802.1w • IEEE 802.1X • IEEE 802.1ab (LLDP) • IEEE 802.3ad (LACP) • IEEE 802.3af y IEEE 802.3at • IEEE 802.3ah (100BASE-X single/multimode fiber only) • IEEE 802.3x full duplex para 10BASE-T, 100BASE-TX, y 1000BASE-T ports • IEEE 802.3 10BASE-T • IEEE 802.3u 100BASE-TX • IEEE 802.3ab 1000BASE-T • IEEE 802.3z 1000BASE-X • RMON I and II standards • SNMP v1, v2c, and v3 • IEEE 802.3az • IEEE 802.3ae 10Gigabit Ethernet • IEEE 802.1ax • Listas de control de acceso para IPv4 e IPv6 • Listas de control de acceso para VLANs • Listas de control de acceso para puertos • Autenticación TACACS+ y RADIUS • Notificación de MAC Address • Seguridad multinivel en consola • Spanning Tree Root Guard • Filtrado IGMP • Asignación dinámica de VLANs • Calidad de servicio SRR, 802.1p class of service, Cross-stack QoS, Rate limiting
Access Points	Administración centralizada vía WLC. Radio dual (2.4 GHz y 5GHz)

Capacidad 802.11n Version 2.0:

- Tecnología MIMO 3x4 con soporte para múltiples entradas y múltiples salidas con tres espectros de transmisión.
- 802.11n and 802.11a/g beamforming
- Canales de 20 y 40 Mhz
- Mínimo 450 Mbps de transmisión (40-MHz con 5 GHz)
- Selección dinámica de frecuencia (DFS)

Capacidad 802.11ac Capacidad de Onda 1:

- Tecnología MIMO 3x4 con soporte para múltiples entradas y múltiples salidas con tres espectros de transmisión
- MRC
- 802.11ac beamforming
- Canales 20, 40, 80 MHz
- 801. DFS
- Soporte CSD
- Tasa de datos >= 1.3 Gbps (80 MHz en 5 GHz)

Capacidad de transmisión de datos

- 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps
- 802.11bg: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps
- 802.11n data rates (2.4 GHz1 and 5 GHz

Potencia máxima de transmisión a 2.4 Ghz

- 802.11b
- 22 dBm: 3 Antennas
- 802.11g
- 22 dBm: 3 Antennas
- 802.11n (HT20)
- 22 dBm: 3 Antennas

Potencia máxima de transmisión a 5 Ghz

- 802.11a
- 23 dBm: 4 Antennas
- 802.11n (HT20)
- 23 dBm: 4 Antennas
- 802.11n (HT40)
- 23 dBm: 4 Antennas

Soporte de antenas hasta de 3 dBi/2.4 GHz y 5 dBi/5 GHz Low profile

Memoria RAM: >= 512 MB

Memoria FLASH: >= 64 MB

Interface de administración por consola e interface Ethernet PoE.

Elaboración propia

Descripción de la nomenclatura de identificación de equipos

A continuación, en la figura 1, se presenta una simbología gráfica de los equipos propuestos para la solución.

Figura 2.1. Simbología de los equipos
Elaboración propia

2.3 Generación del plan de acción

Para ejecutar el proyecto de adquisición, instalación e implementación de una infraestructura de networking para la istitución pública se requieren los siguientes plazos que se contemplan en la tabla 3:

Tabla 3. Plan de acción

Nombre de tarea	Duración	Fecha inicio	Fecha culminación
Portoviejo	**6.81 días**	**04/12/14**	**12/12/14**
Actividades de implementación	**6.81 días**	**04/12/14**	**12/12/14**
Inspección	1 hora	04/12/14	12/12/14
Levantamiento de información	1 hora	04/12/14	12/12/14

Entrega de equipos	8 horas	04/12/14	05/12/14
Instalación y configuraciones	**5 días**	**08/12/14**	**12/12/14**
Montajes	4 horas	08/12/14	12/12/14
Configuración de switches y acceso	2 días	08/12/14	12/12/14
Acces point	1 días	08/12/14	12/12/14
Acces point	1 día	08/12/14	12/12/14

Elaboración propia

En tal sentido, los recursos del proyecto se muestran en la tabla 4:

Tabla 4. Recursos del proyecto.

Responsable	Tipo de recursos	Disponibilidad	Observación
Empresa	Equipos	Fabricante Cisco e Importaciones	Depende del stock del fabricante.
	Económicos	Inmediata	Cobertura de eventualidades y riesgos.
	Recurso Humano	Inmediata	Personal certificado y con experiencia en networking.
Institución	Recurso Humano	Inmediata	Conocimiento de las necesidades de la empresa y definiciones.
	Ambiente	Inmediata	Áreas definidas de instalación y requerimientos preliminares listos.
	Económicos	De acuerdo al Contrato	Conforme a las formas de pago del contrato.

Elaboración propia

Por tanto, los hitos del proyecto y que son determinantes para el plan de acción se indica en la tabla 5:

Tabla 5. Hitos del proyecto

Responsable	Hito	Fecha
Institución	Definiciones para configuraciones	03/12/2014
Empresa	Equipos	04/12/2014
Empresa	Implementación Terminada	07/12/2014
Empresa	Documentos para cierre	09/12/2014

Elaboración propia

2.4. Esquema de red propuesto por la solución

2.4.1 Modelo jerárquico

La arquitectura de una LAN que responda a los requerimientos corporativos tiene mayores posibilidades de éxito si se adopta un prototipo diseñado jerárquicamente. Comparado con diferentes proyectos de redes, una de orden jerárquica se gestiona y difunde más fácilmente de modo que los contratiempos se solventan más rápidamente (Castro, 2020).

El bosquejo y formulación de una red jerárquica involucra la segmentación de la misma en capas autónomas. Por tanto, cada capa desempeña funciones determinadas y diferenciadas definiendo su actuación adentro de la red completa. La diferenciación de las

diversas funciones de una red permite que su diseño se torne modular facilitando su escalabilidad y desempeño, (Vaca, 2021) tal como lo indica la figura 2.

Cisco recomienda utilizar un diseño jerárquico en una red LAN que incluya las siguientes capas:

- Capa de acceso
- Capa de distribución
- Capa de núcleo (core)

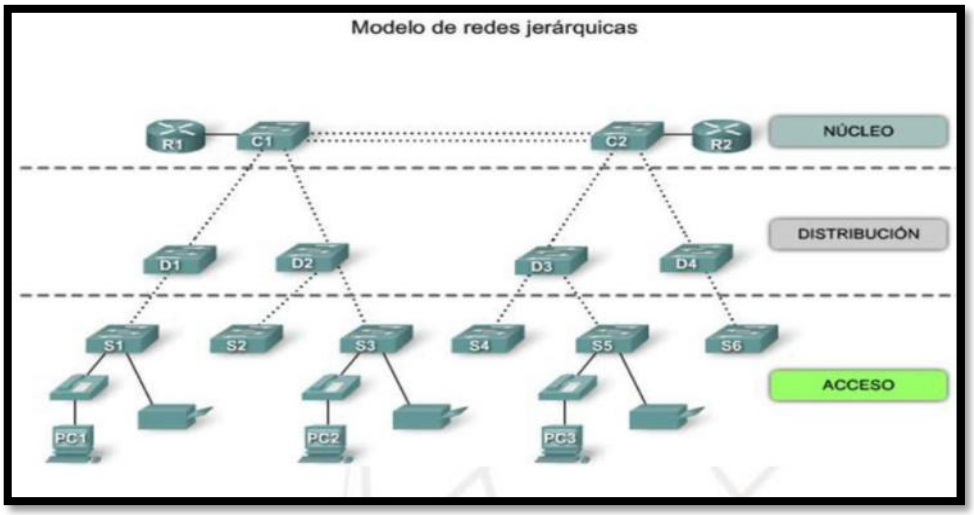


Figura 2.2. Modelo de redes jerárquicas
Elaboración propia

Para redes pequeñas o medianas, el uso de una capa de distribución resulta innecesario, por tanto, suele usarse el modelo “colapsado”, en donde las capas de distribución y núcleo se fusionan.

2.4.1.1 VLANs

Las VLANs configuradas en el switch de core para los diferentes usuarios, lo indica la tabla 6:

Tabla 6. Configuración de VLANs

VLan ID	Nombre
10	RTP
11	Servidores
12	Datos
13	TV-Monitoreo
14	Impresoras
15	Tecnología
16	Vigilancia y Control
17	Autoridades
18	General
19	Invitados
20	Financiero
99	Administración

Elaboración propia

2.4.1.2 VTP

Aprovechando la facilidad que brinda el protocolo VTP propietario de Cisco, las vlans se configuran únicamente en el switch de core, en tanto que ambos switches de acceso aprendieron las vlans sin que se requiera ninguna configuración en ellos (Bueno, 2021).

Los roles de los switches quedan configurados como lo indica la tabla 7:

Tabla 7. Roles de los switches

Switch	MODO VTP
Core	Sever
Acceso a 48 puertos	Client
Acceso a 48 puertos	Client

Elaboración propia.

2.4.1.3 Direccionamiento ip de la solución

Según el direccionamiento IP proporcionado por la Institución, tal como lo indica la tabla 8, las siguientes interfaces de capa 3 (SVI) se configuraron en el switch de core para cada una de las vlans respectivas.

Tabla 8. Direccionamiento IP de la solución

VLAN	SVI	VLAN ID
RTP	10.40.10.1/24	10
SERVIDORES	10.40.11.1/24	11
DATOS	10.40.12.1/24	12
TELEVISORES y MONITOREO	10.40.13.1/24	13
IMPRESORAS	10.40.14.1/24	14
TECNOLOGIA	10.40.15.1/24	15
VIGILANCIA Y CONTROL	10.40.16.1/24	16
AUTORIDADES	10.40.17.1/2	17
GENERAL	10.40.18.1/24	18
INVITADOS	10.40.19.1/24	19
FINANCIERO	10.40.20.1/24	20
ADMINISTRACION	10.40.99.254/24	99

Elaboración propia

2.4.1.4 Puertos trunk y port channel

La comunicación entre los switches se efectúa a través de puertos en modo trunk (Fajardo, 2020), tal como lo indica la tabla 9, y aprovechando la disponibilidad de los SFPs de 10G, se crean grupos de agregación mediante el estándar 802.3ad para generar caminos activos compartidos desde los switches de acceso hacia el core. La vlan nativa para dichos puertos es la vlan 99.

Tabla 9. Puertos en modo trunk y port channel

Switch	Interface	Port channel ID	Modo LACP
CORE	Te1/15	1	Active
	Te1/16	1	Active
Acceso 48	Te1/1/3	1	Passive
Acceso 48	Te1/1/3	2	Passive

Elaboración propia

2.4.1.5 IPs de administración

En la tabla 10, se presentan las direcciones IP de administración de los switches propuestas por la institución:

Tabla 10. Direcciones IP propuestas por la institución

Dispositivo	Hostname	IP Administración
Switch core	CORE_SUPER	10.40.99.254
Switch acceso 48	SWITCH_PISO1	10.40.99.4
Switch acceso 48	SWITCH_MZ	10.40.99.1
Acess Point *	AP_Piso1	10.40.99.3
	AP_Mz	10.40.99.2

Elaboración propia

2.4.1.6 DHCP

Como la empresa pública no cuenta con un servidor DHCP, esta funcionalidad fue configurada en el switch core. Las subredes no incluidas en la tabla 11, tendrán asignación manual en los dispositivos finales que operen en dicha vlan. Las IPs no mencionadas en el rango de IPs dinámicas quedan reservadas para ser asignadas de forma manual.

Tabla 11. Subredes

Subred	Nombre Pool	Rango		Gateway
		IP Inicial	IP Final	
10.80.10.0/24	RTP	10.40.10.100	10.40.10.200	10.80.10.1
10.80.12.0/24	DATOS	10.40.12.100	10.40.12.200	10.80.12.1
10.80.15.0/24	TECNOLOGIA	10.40.15.100	10.40.15.200	10.80.15.1
10.80.16.0/24	VIGILANCIA_ Y_CONTROL	10.40.16.100	10.40.16.200	10.80.16.1
10.80.17.0/24	AUTORIDADE S	10.40.17.100	10.40.17.200	10.80.17.1
10.80.18.0/24	GENERAL	10.40.18.100	10.40.18.200	10.80.18.1
10.80.19.0/24	INVITADOS	10.40.19.100	10.40.19.200	10.80.19.1
10.80.20.0/24	FINANCIERO	10.40.20.100	10.40.20.200	10.80.20.1
10.80.99.0/24	APs	10.40.99.8	10.40.99.10	10.80.99.254

Elaboración propia

2.4.1.7 WLC

Los SSIDs proporcionados por la institución se asociaron en la WLC a las siguientes vlans. Indicadas en la tabla 12**:**

Tabla 12. SSIDs proporcionados por la institución

Nombre SSID	**Vlan Asociada**
DESPACHO	17
GENERAL	18
INVITADOS	19

Elaboración propia.

El switch de acceso de 48 puertos contiene las configuraciones de la WLC embebida que permite la conectividad inalámbrica mediante los APs livianos. Hay que recordar que:

- Los APs no contienen ninguna configuración (por ser lightweight).

- Al no contener ninguna configuración, tampoco se puede acceder remotamente a los APs

2.4.1.8 Enrutamiento y topología de la solución

Se configuraron las siguientes rutas en el core con la finalidad de tener conectividad con todas las zonales:

ip route 0.0.0.0 0.0.0.0 10.40.11.2 10 name INTERNET

ip route 10.0.0.0 255.0.0.0 10.40.0.1 name DATOS

ip route 192.168.10.0 255.255.255.0 10.40.0.1

Siguiendo las recomendaciones del fabricante, la figura 3, muestra la topología final de la implementación realizada:

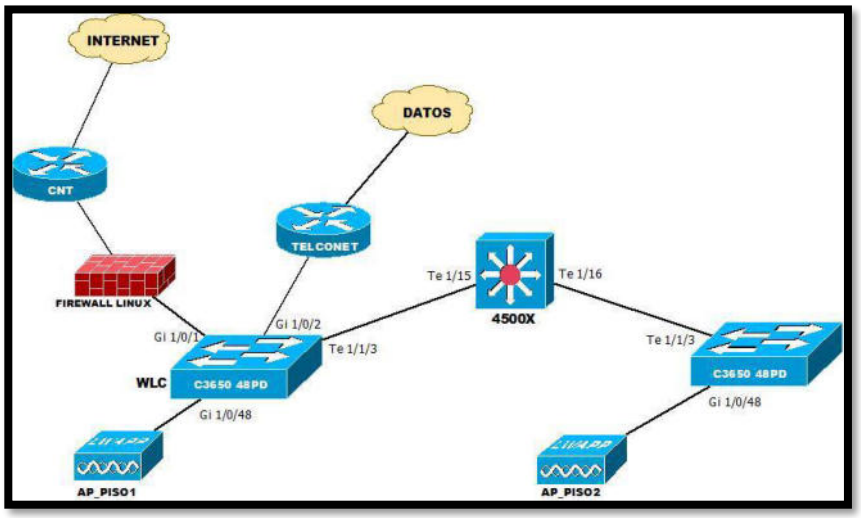


Figura 2.3. Topología final de la implementación
Elaboración propia basada en las recomendaciones del proveedor

2.4.1.9 Políticas implementadas por la solución

Para los usuarios y contraseñas de administración:

- Por facilidad y agilizar la implementación, se configuró un usuario y contraseña provisional sin grados de complejidad para todos los switches.

- Tanto el usuario como la contraseña provisional fueron proporcionados por el administrador de red.

- El único protocolo de acceso remoto a los switches habilitado es SSH. No se puede acceder remotamente usando telnet.

De acceso a la red: a la red LAN se puede acceder mediante un punto de datos o por medio de cualquiera de los SSIDs inalámbricos configurados en la WLC.

Access Points: a nivel de conexiones inalámbricas, la única política de seguridad implementada es la contraseña de acceso a los distintos SSIDs, información que la institución proporcionó para poder implementar el proyecto.

CAPÍTULO 3

EVALUACIÓN DE RESULTADOS

3.1. Beneficios del diseño de la red jerarquica asumida en la solución propuesta.

La construcción de una LAN asumida para satisfacer las necesidades de la empresa pública objeto de estudio, alcanzó el éxito esperado originalmente pues se utilizó un modelo de diseño jerárquico. Esto en virtud de la comprobación con diferentes diseños de redes, por tanto una red jerárquica se gestiona y difunde más fácilmente y los inconvenientes son resueltos más expeditamente.

El diseño de la red jerárquica asumida para la solución fue el “colapsado”, funcionando las capas de distribución y núcleo, lo que implicó la segmentación de la red en 2 capas completamente autónomas. Por tanto, en la actualidad cada capa desempeña actividades determinadas definiendo su papel en el marco de la red global. La segmentación de las

capas presentes en la red favorece su diseño modular permitiendo con éxito la escalabilidad y el rendimiento. El modelo jerárquico que se asumió fue el de separar la red en dos capas diferenciadas:

- Capa de acceso
- Capa de distribución y núcleo (core)

La capa de acceso planteada favorece positivamente la interfaz con unidades finales tales como las PC, impresoras y teléfonos IP, proveyendo el acceso al resto de la red. Esta capa comprende 2 switches, y 2 puntos de acceso inalámbricos, lo cual permite la conectividad de los dispositivos a la red y regula propiciamente cuáles de estos están facultados para comunicarse a través de la red.

La capa de distribución y núcleo constituye el backbone de alta velocidad de la internetwork, agrega los datos que se reciben de los switches de la capa de acceso, controlando el flujo de tráfico entre las LAN virtuales (VLANs) definidas en la capa de acceso y el enrutamiento de grandes volúmenes de datos muy rápidamente hacia su destino final.

Resulta importante señalar como resultado del presente proyecto los beneficios resultantes asociados con los diseños de la red jerárquica asumidas para la solución. A continuación, se presentan estos beneficios observados y monitoreados.

3.1.1. Escalabilidad

La red jerárquica asumida para la institución púbica escala adecuadamente. La modularidad del diseño representa exactamente sus componentes en la medida que la red lograse mayor crecimiento. En virtud de que las instancias del módulo son coherentes, se facilita la planificación e implementación del crecimiento. Está diseñada para que al agregarse más switches en la capa de acceso, puedan adicionarse más switches a la capa de distribución y núcleo para gestionar la carga añadida.

3.1.2. Redundancia

El diseño adoptado posibilita que mientras la red observe un crecimiento, la disponibilidad adquiera importancia. Puede ampliarse fundamentalmente la disponibilidad por medio de implementaciones abundantes fáciles como la red jerárquica. Los switches de la capa de acceso se enlazan comunicándose a través de dos switches distintos de la capa de distribución y núcleo garantizando la redundancia de la ruta. En tal sentido, al fallar alguno de los switches de la capa de distribución y núcleo, el switch de la capa de acceso conmuta a un diferente switch de la capa de distribución y núcleo. Únicamente la capa donde está restringida la redundancia es la capa de acceso. Generalmente, las unidades de nodo final, tales como PC, impresoras y teléfonos IP, no alcazan a conectarse con los

numerosos switches de la capa de acceso para conseguir la redundancia. En una eventualidad debida al deterioro de un switch de la capa de acceso, únicamente se afectarían por la discontinuidad los dispositivos acoplados a ese switch particularmente. El remanente de la red permanecería trabajando sin ningún tipo de alteración.

3.1.3. Rendimiento

El rendimiento de la comunicación es mejorada al evitarse la transmisión de datos por medio de switches intermediarios de poco rendimiento. Los datos son remitidos por intermedio de empalmes del puerto del switch adicionado desde la capa de acceso a la capa de distribución y núcleo aproximadamente a la velocidad de cable en casi la totalidad de los casos. Posteriormente, la capa de distribución y núcleo emplea sus potenciales de compensar el alto rendimiento para enrutarse hacia su trayectoria terminal. En virtud de que las capas núcleo y de distribución efectúan sus procedimientos a altas velocidades, no hay limitación para el ancho de banda de la red. Como consecuencia, la red jerárquica adoptada alcanza aproximadamente la velocidad de cable entre la totalidad de los dispositivos.

3.1.4. Seguridad

La seguridad aumentó y es sencillamente gestionable. Es viable establecer los switches de la capa de acceso con diversas alternativas de seguridad del puerto que proporcionan control sobre a cuáles dispositivos se les concede la conexión a la red. Asimismo, se cuenta con la flexibilidad de emplear medidas de seguridad de mayor avance en la capa de distribución. Pueden aplicarse las medidas de control de acceso que precisan qué protocolos de comunicación se establecen en su red y a dónde se les permite encaminarse. Un ejemplo de ello, si se aspira restringir el empleo de HTTP a una determinada agrupación de usuarios enlazada a la capa de acceso, cabría aplicarse una serie de medidas que bloqueen el tráfico de HTTP en la capa de distribución. La limitación del tráfico basada en protocolos de capas más prominentes, como IP y HTTP, demanda que sus switches logren procesar las medidas asumidas en esa capa. Ciertos switches de la capa de acceso aceptan la operatividad de la capa 3, sin embargo, generalmente es trabajo de los switches de la capa de distribución el procesamiento de los datos de la capa 3, por su mayor eficacia en este sentido.

3.1.5. Facilidad de administración

La facilidad de administración es comparativamente sencilla en esta red jerárquica. Cada capa del diseño jerárquico desempeña

maniobras determinadas que son coherentes en dicha capa. En consecuencia, si se requiere alternar la funcionalidad de un switch de la capa de acceso, valdría reproducir dicho cambio en cada switch de la capa de acceso en la red porque probablemente desempeñan iguales funciones en su capa. El empleo de switches nuevos igualmente se facilita porque pueden reproducirse las alineaciones del switch entre los dispositivos con pocas transformaciones. La solidez y coherencia entre los switches en cada capa admite un recobro expedito y la reducción de la solución de complicaciones.

3.1.6. Capacidad de mantenimiento

Debido a que la red jerárquica asumida es naturalmente modular y escala con suficiente claridad, se hace fácil su mantenimiento. Con diferentes esquemas de la topología de la red, la gestión se vuelve muy compleja mientras que la red se desarrolla. Asimismo, en ciertos modelos de diseños de red, hay un término referido a la ampliación del incremento de la red antes de que se transforme en compleja y onerosa en su mantenimiento. En el modelo jerárquico es definido el desempeño de los switches en cada capa permitiendo que la elección del switch apropiado sea más simple. El incremento de switches a una capa no precisamente estipula que se impedirá un cuello de botella u otra restricción en otra capa.

3.2. Pruebas y certificación de la funcionalidad-conectividad de la solución

A continuación, desde la figura 4 a la figura 10, se presentan las capturas de pantalla de las pruebas realizadas una vez concluida la implementación de la solución.

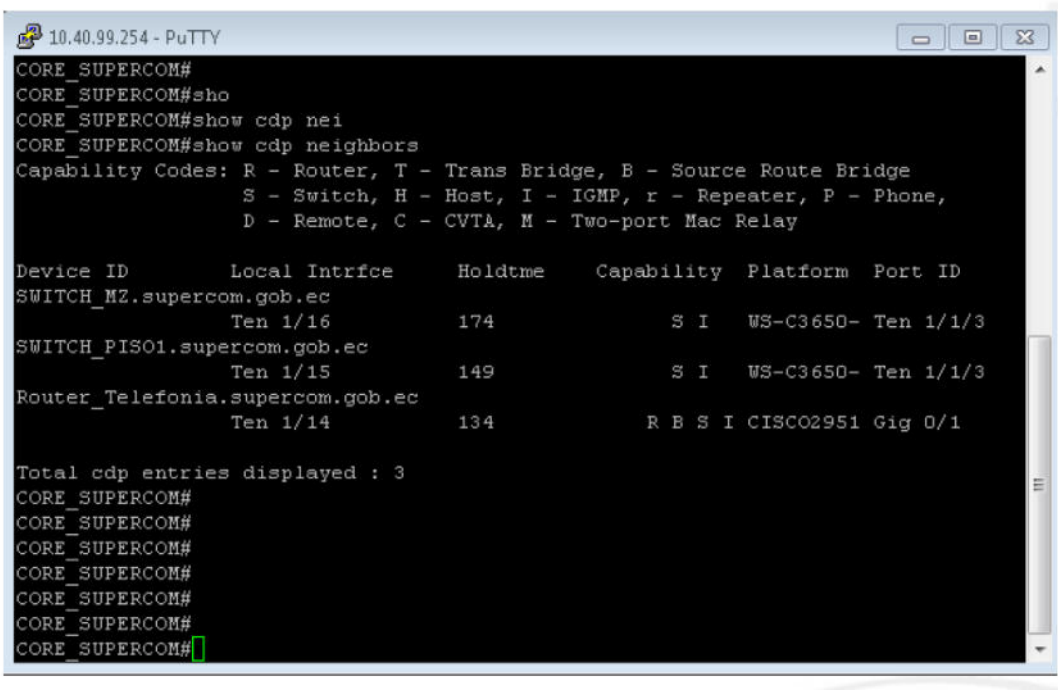


Figura 3.4**.** Equipos Cisco directamente conectados al switch de core

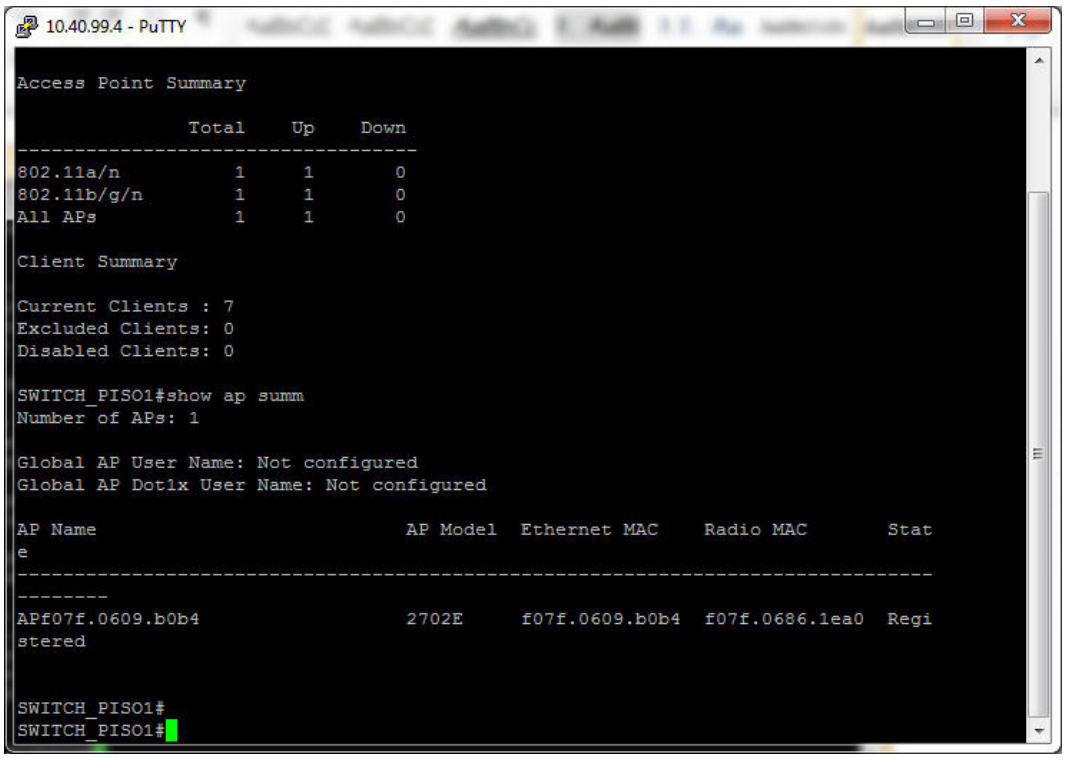


Figura 3.5. APs Cisco conectados al SWITCH_PISO1 puertos registrados en la WL

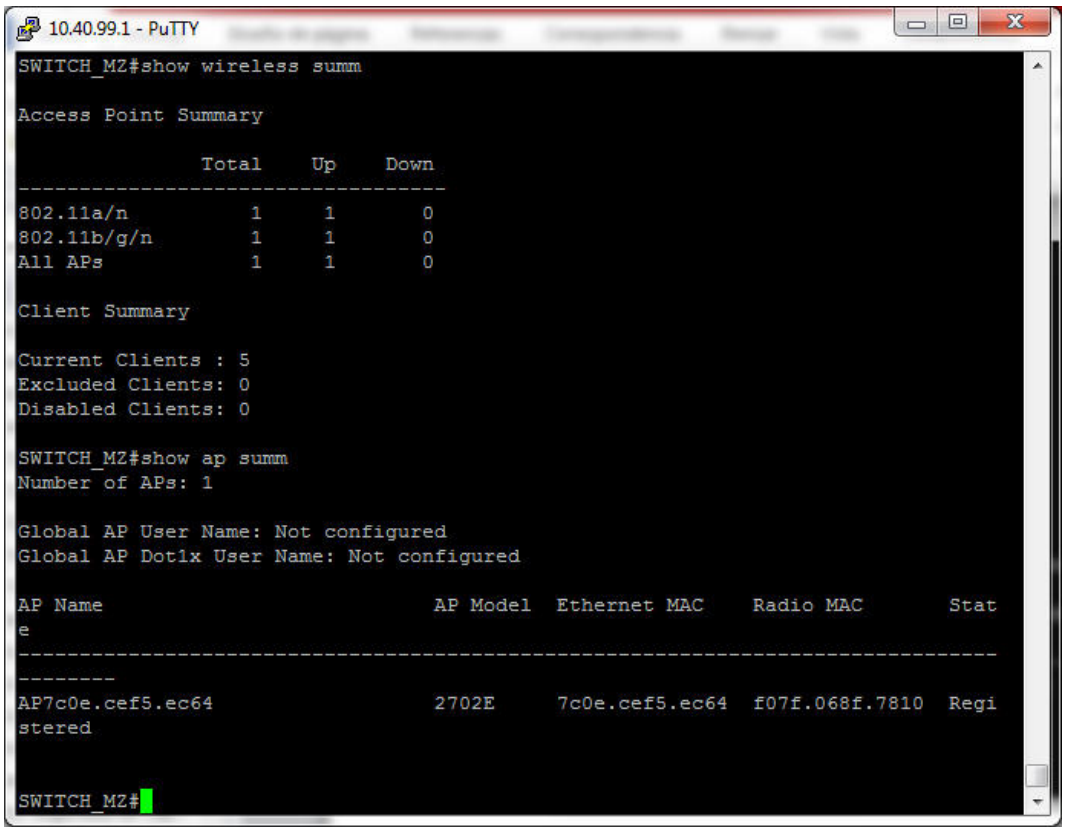


Figura 3.6. APs Cisco conectados al SWITCH_MZ puertos registrados en la WLC.

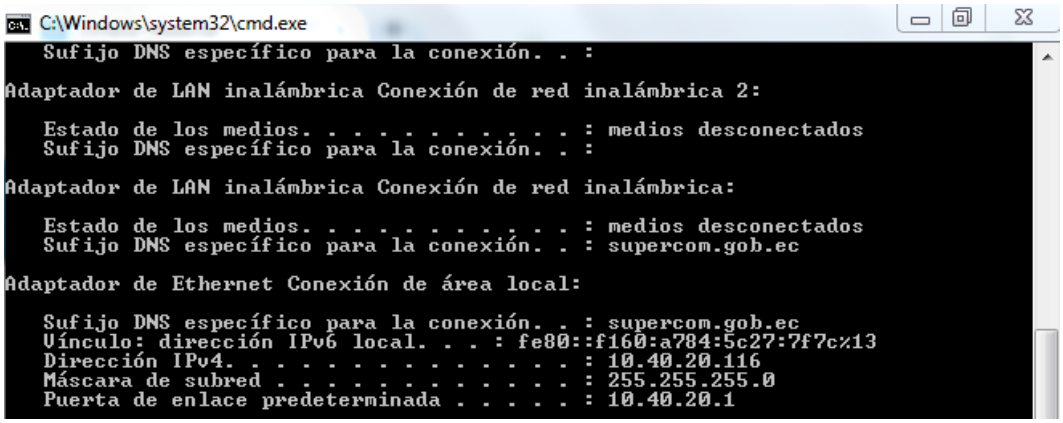


Figura 3.7. Dirección IP recibida por el servidor DHCP (del switch core)

Figura 3.8. Conectividad exitosa desde la subred 10.40.20.0/24 hacia el internet

Figura 3.9. Pruebas de conexión wifi desde dispositivo móvil

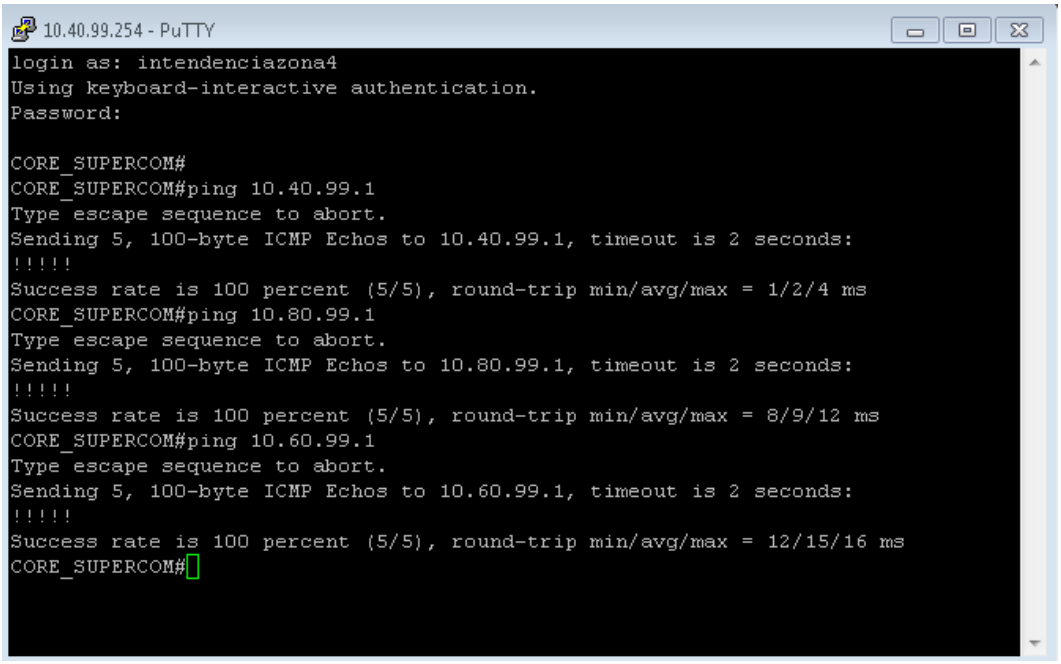


Figura 3.10. Túnel de datos operativo

Como puede observarse, la solución resultó viable operativamente generando la conectividad esperada en términos de oportunidad y calidad.

CONCLUSIONES Y RECOMENDACIONES

1. La solución generada a través de una implementación de la infraestructura de networking para una institución pública se basó en la construcción de una LAN diseñada para satisfacer las necesidades de la empresa y alcanzó los resultados esperados pues se utilizó un modelo de diseño jerárquico “colapsado”. Por tanto, la solución suministra mayor velocidad de datos, mejor rendimiento y mejor cobertura en comparación con los estándares anteriores.
2. La nueva infraestructura de red permitió la compartición de recursos (bases de datos, aplicaciones, impresiones, periféricos, etc.), proporcionando una comunicación segura, flexible y de alta velocidad entre los usuarios a los que presta servicio de comunicaciones de datos, voz, video e internet. Además, usa un canal más amplio y un esquema de modulación mejorado que admite más clientes.
3. Los beneficios observados y monitoreados permiten concluir que la solución tiene una buena Escalabilidad, pues el diseño modular permite reproducir exactamente los elementos del diseño en la medida que la red vaya creciendo, y que en virtud de que cada instancia del módulo es consistente, resulta con mucha facilidad la planificación e implementación de cualquier expansión requerida.

4. Igualmente se observa una aceptable y buena Redundancia pues el diseño asumido para la solución, permite incrementar radicalmente la disponibilidad a través de implementaciones redundantes fáciles en este tipo de red jerárquica. En este mismo sentido, el Rendimiento de la comunicación es optimizado evadiendo la transferencia de datos mediante switches intermediarios de poco rendimiento. Los datos son transferidos a través de conexiones del puerto del switch adicionado desde la capa de acceso a la capa de distribución aproximadamente a la velocidad de cable en la mayoría de los casos.
5. Otro beneficio observado es la Seguridad, pues es factible la configuración de switches de la capa de acceso con diversas medidas de seguridad del puerto que facilitan el seguimiento y monitoreo a aquellos dispositivos que se les permite conectarse a la red. De esta forma, se permite el uso flexible de medidas avanzadas de seguridad en la capa de distribución. La solución implementada brinda mayor facilidad de administración, porque en cada capa del diseño jerárquico adoptado se desempeñan funciones específicas estables y sólidas en dicha capa. Por último, referente a la capacidad de mantenimiento se considera que en virtud del diseño modular de la red jerárquica asumida en la solución y que esta escala muy bien su mantenimiento se facilita por estas causas.

6. Al observar las pruebas de conectividad de la solución a través de las capturas de pantalla de las pruebas realizadas concluida la implementación de la solución, esta resultó viable operativamente generando la conectividad esperada en términos de oportunidad y calidad.

Las recomendaciones sugeridas con respecto a la solución, instalados los equipos y capacitados los integrantes de la empresa encargados de la gestión de esta, están orientadas a la observación de los índices de seguridad y operatividad de los nuevos equipos para notificar en el periodo de garantía cualquier situación que amerite la intervención del fabricante y el proveedor a través del servicio técnico acordado en los lapsos establecidos en las garantías del proyecto.

En cuanto a las políticas implementadas para el acceso a la red, para los usuarios y contraseñas de administración se han acordado y propuesto las siguientes recomendaciones:

1. Cambiar la contraseña de acceso ssh.
2. Utilizar combinaciones que refuercen la seguridad de la contraseña elegida, usando caracteres alfanuméricos y especiales.
3. Evitar el uso de contraseñas tales como cisco, password1, etc.

4. Se requiere la implementación de seguridad perimetral, ya que la red está expuesta a ataques cibernéticos, dado a que el servidor que tienen en la actualidad no les brinda las garantías necesarias de acuerdo a la importancia de la institución.
5. Cualquier switch de acceso que se vaya añadiendo a la red debe ir conectado directamente al switch core evitando el uso de cascadas.
6. Las contraseñas de los SSIDs solamente deben conocerlas los administradores de IT.
7. Es altamente recomendable que se realicen respaldos periódicos de los archivos de configuración.

BIBLIOGRAFÍA

Beneitez, D. (2020). *Infraestructura IT*. Recuperado el 04 de Marzo de 2021, de https://www.icot.es/infraestructura-it/

Bueno, C. (2021). *Solución de dos escenarios presentes en entornos corporativos bajo el uso de tecnología CISCO.* Bucaramanga: UNAD-Escuela de Ciencias Básicas,Tecnología e Ingenieria.

Castro, L. (2020). *Diseño de una red administrable entre elcentro de datos y la facultad de ciencias económicas para mejorar el acceso a los servicios informáticos mediante fibra óptica en la Universidad Estatal del Sur de Manabí.* Jipijapa, Manabí, Ecuador: Universidad Estatal el Sur de Manabí-Facultad de Ciencias Técnicas.

Fajardo, C. (2020). *Diseño de una VPN sitio a sitio para proteger los datos transmitidos entre la sede principal en Bogotá D.C. y la planta de producción ubicada en La Calera Cundinamarca de la empresa manantiales de los andes S.A.S.* Bogotá: Universidad Cooperativa de Colombia, Facultad de Ingeniería.

Fernández, J. (2021). *Red, infraestructura, software y bases de datos: un equipo ganador para innovar*. Recuperado el 03 de Marzo de 2021, de https://www.e-dea.co/blog/red-infraestructura-software-y-bases-de-datos

INSTEL. (2020). *Networking*. Recuperado el 03 de Marzo de 2021, de ¿Qué es?: https://instel.es/productos/comunicaciones-corporativas/networking/

Terán, J. (2020). *Sistema de gestión de configuración para la infraestructura de networking de la empresa pública Yachay E.P.* Ibarra: Universidad Técnica del Norte - Facultad de Ingeniería en Ciencias Aplicadas.

Vaca, J. (2021). *Diseño de cambios estructurales para mejorar la operación de la red LAN que conecta los usuarios y servidores a nivel nacional, basado en un modelo de red LAN eficiente y redundante, en la empresa Unifianza S.A.* Bogotá: Universidad Cooperativa de Colombia-Facultad de Ingeniería.