UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

Estudio y diseño de una red corporativa de datos para la empresa Metalmax ubicada en la vía a Daule km 27,5 de la ciudad de Guayaquil

AUTOR:

Altamirano Maxi, Ronald Xavier

Trabajo de Titulación previo a la obtención del título de

INGENIERO EN TELECOMUNICACIONES

TUTOR:

Ing. Romero Rosero, Carlos Bolívar

Guayaquil, Ecuador

15 de septiembre del 2022

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Sr. **Altamirano Maxi, Ronald Xavier** como requerimiento para la obtención del título de **INGENIERO EN TELECOMUNICACIONES**.

TUTOR

Ing. Romero Rosero, Carlos Bolívar

DIRECTOR DE CARRERA

Msc. Bohórquez Escobar, Celso Bayardo

Guayaquil, a los 15 días del mes de septiembre del año 2022

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Altamirano Maxi, Ronald Xavier**

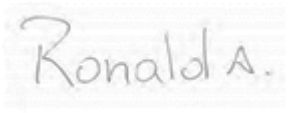
DECLARÓ QUE:

El trabajo de titulación, **Estudio y diseño de una red corporativa de datos para la empresa Metalmax ubicada en la vía a Daule km 27,5 de la ciudad de Guayaquil,** previo a la obtención del Título de **Ingeniero en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 15 días del mes de septiembre del año 2022

EL AUTOR



ALTAMIRANO MAXI, RONALD XAVIER

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Altamirano Maxi, Ronald Xavier**

Autorizó a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación: **Estudio y diseño de una red corporativa de datos para la empresa Metalmax ubicada en la vía a Daule km 27,5 de la ciudad de Guayaquil**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

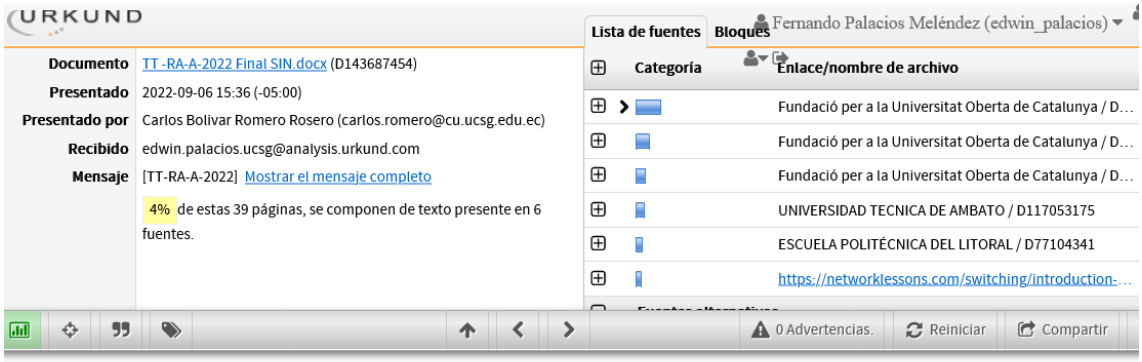
Guayaquil, a los 15 días del mes de septiembre del año 2022

EL AUTOR

ALTAMIRANO MAXI, RONALD XAVIER

REPORTE DE URKUND

Informe del Trabajo de Titulación de la Carrera de Ingeniería en Telecomunicaciones, con **4 %** de coincidencias perteneciente al estudiante ALTAMIRANO MAXI, RONALD XAVIER**.**



UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA: Estudio y diseño de una red corporativa de datos para la empresa Metalmax ubicada en la vía a Daule km 27,5 de la ciudad de Guayaquil

AUTOR: Altamirano Maxi, Ronald Xavier

Trabajo de Titulación previo a la obtención del título de INGENIERO EN TELECOMUNICACIONES

TUTOR: Ing. Romero Rosero, Carlos Bolivar

Guayaquil, Ecuador

15 de septiembre del 2022

Atentamente,

Ing. Carlos Romero Rosero.
Profesor Titular Principal
TUTOR

DEDICATORIA

A Dios por darme toda la fortaleza, sabiduría y resiliencia necesaria en todo momento para avanzar.

EL AUTOR

ALTAMIRANO MAXI, RONALD XAVIER

AGRADECIMIENTO

Agradezco a Dios por permitirme finalizar esta etapa de mi vida, en la cual he adquirido los conocimientos que me han servido para avanzar en mi vida profesional y personal.

EL AUTOR

ALTAMIRANO MAXI, RONALD XAVIER

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

M. Sc. ROMERO PAZ, MANUEL DE JESUS

DECANO/OPONENTE

f. _____

M. Sc. VELEZ TACURI, EFRAIN OLIVERIO

COORDINADOR DEL ÁREA

f. _____

M. Sc. CELSO BAYARDO BOHORQUEZ ESCOBAR

DIRECTOR DE CARRERA

ÍNDICE GENERAL

ÍNDICE DE FIGURAS ..... **XIV**

ÍNDICE DE TABLAS ..... **XVII**

RESUMEN ..... **XVIII**

CAPÍTULO 1: DESCRIPCIÓN GENERAL DEL TRABAJO DE TITULACIÓN **2**

1.1. Introducción. **2**

1.2. Antecedentes. **3**

1.3. Definición del Problema. **4**

1.4. Justificación del Problema. **4**

1.5. Objetivos del Problema de Investigación. **4**

1.5.1. Objetivo General. 4

1.5.2. Objetivos Específicos. 4

1.6. Hipótesis. **5**

1.7. Metodología de Investigación. **5**

CAPÍTULO 2: FUNDAMENTACIÓN TEÓRICA **6**

2.1. Descripción redes LAN **6**

2.2. Redes convergentes **6**

2.3. Aspectos de las redes conmutadas **7**

2.3.1. Acceso múltiple 7

2.3.2. Detección de colisiones. 7

2.3.3. Señal de congestión y postergación aleatoria. 7

2.3.4. Comunicaciones Ethernet. 7

2.3.5. Campos Preámbulo y Delimitador de inicio de trama. 8

2.4. Protocolos de enrutamiento IP **8**

2.5. Vector distancia y estado de enlace **9**

2.5.1. Vector Distancia. 9

2.5.2. Estado de enlace. 9

2.6. Distancia administrativa y métrica **9**

2.6.1. Métrica 10

2.7. VLAN 10

2.7.1. Tipos de VLAN. 11

2.7.1.1. VLAN de datos/usuario. 11

2.7.1.2. VLAN predeterminada. 11

2.7.1.3. VLAN nativa. 11

2.7.1.4. VLAN de administración. 11

2.7.1.5. VLAN de Voz. 11

2.7.2. VLAN de voz y datos. 11

2.7.3. VLAN Trunking Protocol (VTP). 12

2.7.3.1. Dominios de VTP 13

2.7.3.2. Modos de VTP. 13

2.7.3.3. Anuncios de VTP. 14

2.7.3.4. Configuración de VTP 16

2.7.3.5. VTP Pruning. 16

2.7.3.6. Encapsulamiento DOT1Q 17

2.8. Enrutamiento de un paquete IP 17

2.8.1. Enrutamiento Estático. 18

2.8.1.1. Tabla de enrutamiento. 19

2.8.2. Enrutamiento dinámico. 19

2.8.2.1. Open Shortest Path First (OSPF). 20

- Estados de Vecinos de OSPF 21
- OSPF: Intercambio de LSBD Entre Vecinos. 22
- OSPF: Tipos de Redes. 23
- OSPF Relaciones de Vecinos y Problemas. 23
- OSPF: Áreas. 25
- Áreas en OSPF 25

2.8.3. Enrutamiento Intra VLAN 25

2.8.4. Enrutamiento Inter VLAN 26

2.8.5. Intra VLAN vs Inter VLAN 26
2.8.6. Puerto de Enrutamiento 27
2.9. Modelo Jerárquico 29
2.9.1. Capa de acceso. 31
2.9.2. Capa de distribución. 31
2.9.2.1. Diseño de dos capas. 32
2.9.2.2. Diseño de tres capas. 33
2.9.3. Capa central. 33
2.10. Redes LAN inalámbricas 34
2.10.1. Topología de una Red LAN inalámbrica. 34
2.10.1.1. Conjunto de servicios básicos (BSS). 35
2.10.1.2. Sistema de distribución (DS). 36
2.10.1.3. Conjunto de servicios extendidos (ESS) 37
2.10.1.4. Conjunto de servicios básicos independientes (IBSS) 38
2.10.1.5. Repetidor. 39
2.10.1.6. Puente de grupo de trabajo (WGM). 39
2.10.1.7. Puente al Aire Libre (BO). 40
2.10.1.8. Red Mallada (Mesh Network). 41
2.10.2. Wireless LAN Controllers (WLC). 42
2.10.2.1. WLC Centralizado. 42
2.10.2.2. WLC en la nube. 43
2.10.2.3. WLC incrustado. 44
2.10.2.4. WLC movilidad rápida. 45
2.10.3. Puntos de Acceso Ligero. 46
2.10.3.1. Modo Local. 47
2.10.3.2. Modo Monitor. 47
2.10.3.3. Modo Flexconnect. 47
2.10.3.4. Modo Sniffer. 47
2.10.3.5. Modo Rogue Detector 48

2.10.3.6. Modo Bridge. 48
2.10.3.7. Modo Flex+Bridge. 48
2.10.3.8. Modo SE-Connect. 48
2.11. Servidores y servicios 49
2.11.1. Servidor DNS. 49
2.11.2. Servidor HTTP. 49
2.11.3. Servidor Mail. 49
2.11.4. Servidor FTP y SFTP. 49
2.11.5. Servidor IoT. 49
CAPÍTULO 3: DISEÑO, SIMULACIÓN Y RESULTADOS. 50
3.1. Descripción general y territorial de la empresa Metalmax 50
3.2. Distribución de departamentos 50
3.3. Distribución de VLANs 51
3.4. Distribución de los segmentos de red 52
3.5. Diseño de la red de datos 52
3.5.1. Descripción del diseño de las capas. 54
3.6. Configuraciones propuestas para los equipos principales. 58
3.6.1. Configuración router principal. 58
3.6.2. Configuración de conmutador para distribución LAN. 62
3.6.3. Configuración de conmutador para distribución de servicios. 63
3.6.4. Configuración de conmutadores clientes. 65
3.7. Simulación en Packet Tracer 67
3.8. Características técnicas de los equipos para la propuesta de implementación de la red de datos. 75
3.8.1. Conmutadores para distribución. 75
3.8.2. Conmutadores para departamentos. 75
3.8.3. Controladoras inalámbricas. 76
3.8.4. Puntos de acceso ligero. 76
3.8.5. Puntos de acceso. 77

3.8.6. Router central. 78

3.8.7. Servidores. 78

3.9. Costos aproximados 80

CONCLUSIONES 82

RECOMENDACIONES 83

Bibliografía 84

ÍNDICE DE FIGURAS

Capítulo 2:

Figura 2.1: Redes convergentes. 6
Figura 2.2: Interconexión de VLANs. 10
Figura 2.3: VLAN de voz y datos. 12
Figura 2.4: VLAN trunking protocol. 13
Figura 2.5: Modos VTP. 14
Figura 2.6: Dominio VTP. 16
Figura 2.7: VTP difusión-componentes. 17
Figura 2.8: Enrutamiento IP. 18
Figura 2.9: Link State Database. 20
Figura 2.10: Paquetes Hello en OSPF. 21
Figura 2.11: Estados de vecinos. 22
Figura 2.12: Subinterfaces en un enrutador. 25
Figura 2.13: Enrutamiento Inter-VLAN. 26
Figura 2.14: Intra VLAN vs Inter VLAN. 27
Figura 2.15: Puerto de Enrutamiento. 28
Figura 2.16: Estados de vecinos. 29
Figura 2.17: Modelo de red jerárquico. 30
Figura 2.18: Escalabilidad de 2 capas a 3 capas. 30
Figura 2.19: Capa de acceso. 31
Figura 2.20: Diseño de dos capas. 32
Figura 2.21: Diseño de tres capas. 33
Figura 2.22: Modelo de red malla sin núcleo. 34
Figura 2.23: Modelo de red con núcleo. 34
Figura 2.24: Conjunto de servicios básicos (BSS). 35
Figura 2.25: Sistema de distribución. 36
Figura 2.26: Múltiples SSIDs. 37
Figura 2.27: Conjunto de servicios extendidos. 38
Figura 2.28: Repetidores inalámbricos. 39
Figura 2.29: Puente de grupo de trabajo. 40
Figura 2.30: Puente al aire libre. 41
Figura 2.31: Red mesh. 41
Figura 2.32: WLC centralizado. 43
Figura 2.33: WLC en la nube. 44

Figura 2.34: WLC incrustado. 45
Figura 2.35: WLC movilidad rápida. 46
Figura 2.36: WLC esquema ejemplo.....47

Capítulo 3:

Figura 3.1: Ubicación geográfica de la empresa Metalmax.....50
Figura 3.2: Diagrama del diseño de la red. 53
Figura 3.3: Referencia de colores usados para las VLAN en el diagrama.....54
Figura 3.4: Conmutador para distribución LAN. 55
Figura 3.5: WLC para LAN.....55
Figura 3.6: Punto de accesos ligeros. 55
Figura 3.7: Conmutador para distribución de servicios.....56
Figura 3.8: Clúster de servidores. 56
Figura 3.9: Conmutadores departamentales. 57
Figura 3.10: Conmutadores departamentales. 57
Figura 3.11: Conmutador para distribución de servicios.....57
Figura 3.12: Configuración del router principal - Configuración de interfaz 0. Parte 1/2 58
Figura 3.13: Configuración del router principal - Configuración de interfaz 0. Parte 2/2 59
Figura 3.14: Configuración del router principal - Configuración de interfaz 1. 60
Figura 3.15: Configuración del router principal - Configuración de DHCP. 61
Figura 3.16: Configuración del conmutador para distribución LAN. Parte 1/2. 62
Figura 3.17: Configuración del conmutador para distribución LAN. Parte 1/2. 63
Figura 3.18: Configuración del conmutador para distribución de servicios. Parte 1/2. 63
Figura 3.19: Configuración del conmutador para distribución de servicios. Parte 2/2. 64
Figura 3.20: Configuración de los conmutadores clientes. Parte 1/2. 65
Figura 3.21: Configuración de los conmutadores clientes. Parte 2/2. 66
Figura 3.22: Redes disponibles en el WLC. 67
Figura 3.23: Redes aprovisionadas en los LWAPs. 68
Figura 3.24: Disponibilidad de redes vista desde los dispositivos finales. 68
Figura 3.25: Dispositivos finales usando DHCP. 68
Figura 3.26: PC siendo provisionada de IP por DHCP. 69
Figura 3.27: PC haciendo uso de HTTP. 69

Figura 3.28: PC0 haciendo uso del servicio MAIL. 70
Figura 3.29: PC1 haciendo uso del servicio MAIL. 71
Figura 3.30: Sección con dispositivos IoT. 72
Figura 3.31: Portal del servicio IoT. 72
Figura 3.32: Panel de control de dispositivos IoT. 73
Figura 3.33: Simulación de la red con dispositivos finales y servicios. 74
Figura 3.34: Especificaciones técnicas del conmutador de distribución. 75
Figura 3.35: Especificaciones técnicas del conmutador departamental 76
Figura 3.36: Especificaciones técnicas del WLC. 76
Figura 3.37: Especificaciones técnicas del LWAP. 77
Figura 3.38: Especificaciones técnicas del AP. 77
Figura 3.39: Especificaciones técnicas del router central. 78
Figura 3.40: Especificaciones técnicas del servidor. 79

ÍNDICE DE TABLAS

Capítulo 2:

Tabla 2.1: Funciones de los modos VTP. 14
Tabla 2.2: Tipos de redes OSPF.....23
Tabla 2.3: Requerimientos para comunicación OSPF.....24

Capítulo 3:

Tabla 3.1: Distribución de los segmentos de red.....52
Tabla 3.2: Costos aproximados de dispositivos. 80

RESUMEN

El presente trabajo de titulación aborda el “Estudio y diseño de una red corporativa de datos para la empresa Metalmax ubicada en la vía a Daule km 27,5 de la ciudad de Guayaquil”. El documento brinda información sobre la importancia del diseño de redes acorde a las necesidades, tanto como redes alámbricas como inalámbricas, pero siguiendo un modelo que abarque todas las necesidades. En el Capítulo 1 se presenta la descripción general del trabajo de titulación. El Capítulo 2 describe a las redes, sus fundamentos, modelos existentes, tecnologías disponibles y las aplicaciones en los diversos casos de la industria. El capítulo 3 presenta el diseño de la red propuesto, mediante la descripción del (1) sector o empresa a intervenir, (2) análisis técnico de los requerimientos empresariales, (3) características de los equipos necesarios para la implementación, (4) diseño de la red en el software “Packet Tracer” y (5) presupuesto de la implementación.

Palabras claves: REDES, INALÁMBRICO, ALÁMBRICO, MODELO JERÁRQUICO, REDES CONVERGENTES, PACKET TRACER.

CAPÍTULO 1: DESCRIPCIÓN GENERAL DEL TRABAJO DE TITULACIÓN

En este capítulo, se presenta la descripción general del proyecto de titulación.

1.1. Introducción.

El mundo de las tecnologías de la información se encuentra en constante evolución buscando cada vez opciones que sean capaces de cumplir a cabalidad con las necesidades de los usuarios de distintas áreas, lo cual conlleva a la existencia o desarrollo de distintos tipos de redes, con características que buscan satisfacer necesidades específicas. Además, estas deben ser capaces de crecer y adaptarse a los cambios sin afectar el rendimiento o funcionamiento. Por lo cual no basta con tener un buen diseño de la red sino también seleccionar los dispositivos que serán la base de esta, para que sea capaz de solventar todas las solicitudes de los múltiples servicios que se encuentra funcionando y que todas las personas hagan uso de esto sin tener la mínima preocupación de que la red colapse.

Cuando se hablaba de tipos de redes, comenzaba la comparación y extenuante batalla sobre que, si una red cableada es mejor que una inalámbrica, hoy en día se dejó esa discusión a un lado para juntar los dos tipos de redes. De tal manera que en el mismo ecosistema coexistan ambas, aprovechando los beneficios a la par y compensando sus falencias o desventajas entre sí. Pero para que eso sea posible debe cumplirse que el diseño de la red se adapte a las necesidades, obteniendo como resultado una red flexible que le permita buena movilidad a el empleado en la empresa mediante el acceso total a la red desde cualquiera de sus dispositivos móviles. (Almentero Arrieta & Mieles Montes, 2008)

Hoy en día las redes convergentes son base en infraestructura tecnológica, siendo un método muy eficiente y flexible para la expansión tecnológica en una empresa u organización, porque puede tener múltiples servicios operando en la misma red, sin necesidad de invertir en una infraestructura adicional. Sin embargo, para que todo esto suceda exitosamente se necesita una red resiliente y flexible, ya que al operar múltiples servicios se deberá asegurar el funcionamiento de estos con técnicas avanzadas de calidad de servicios en red, tipos de servicios, entre otros. (Zhang & Liu, 2018)

Siendo así que cualquier análisis para realizar una expansión de infraestructura tecnológica tiene como uno de sus objetivos el diseñar o modelar una red empresarial que siga un modelo jerárquico, para que esta sea tolerante y flexible. Brindando la

capacidad de soportar muchos servicios operando al mismo tiempo, tal como debe de ser una red convergente.

1.2. Antecedentes.

El uso de servicios y aplicativos en red ya no es una opción, sino una necesidad por parte de cualquier empresa que tenga visión, por lo cual el diseño técnico de una red debería ser considerado primordial para el desarrollo de la empresa. Lamentablemente, muchas compañías ven esto como algo sin importancia y continúan invirtiendo dinero en otros aspectos que también son relevantes para el desarrollo, avanzando hasta llegar a un punto en el cual notan que su red o infraestructura de TI es precaria y está afectando los procesos de la empresa, ya que estos son más exigentes que al inicio. Analizando la situación obtienen como resultado que para corregir ese problema se debe rediseñar toda la infraestructura, labor que no se puede ejecutar sin tomar en cuenta que muchos procesos se tendrían que detener provocando pérdidas para la empresa.

Hoy en día la cantidad de servicios en red que necesita una empresa para operar eficientemente son innumerables, comenzando desde sistemas de facturación hasta servidores de almacenamiento. Resaltando que todo esto debe operar de forma simultánea mientras muchos usuarios internos de la empresa acceden, por lo cual la red debe tener un diseño capaz de tolerar toda la carga sin colapsar. Actualmente la empresa Metalmax ubicada en la vía a Daule km 27,5 de la ciudad de Guayaquil no posee una red que sustente estos escenarios, por lo cual surge la necesidad de diseñar una red capaz de tolerar fallos y expandirse sin problemas, requerimientos que actualmente no se pueden cumplir porque todo está conectado a un solo dispositivo.

1.3. Definición del Problema.

Actualmente la empresa Metalmax no cuenta con una red que siga el modelo jerárquico que asegure un buen funcionamiento de esta. Por lo cual el problema de investigación es:

¿Cómo afecta la falta del diseño de una red de datos corporativa con modelo jerárquico para el uso de internet en la empresa Metalmax ubicada en la vía a Daule km 27,5 de la ciudad de Guayaquil?

1.4. Justificación del Problema.

La principal beneficiaria será la empresa Metalmax, la cual no posee capacidad de red para expandir e implementar nuevos servicios. A su vez se beneficiarían los usuarios y trabajadores de la empresa que gozarán de una excelente conectividad en los dispositivos que usen, sin tener preocupaciones de perder conectividad en alguno de ellos.

El aporte académico de este trabajo del presente estudio determinará que estudiantes de la facultad puedan asegurar el funcionamiento de una red empresarial teniendo como pilar principal el modelo jerárquico de red.

Este trabajo tiene relevancia para mejorar la información que les permite a las nuevas empresas y/o emprendedores conectarse con empresas de esta última década.

1.5. Objetivos del Problema de Investigación.

1.5.1. Objetivo General.

Realizar el estudio y diseño de una red corporativa de datos, mediante una simulación en Packet Tracer para la empresa Metalmax ubicada en la vía a Daule km 27,5 de la ciudad de Guayaquil.

1.5.2. Objetivos Específicos.

1. Describir los fundamentos teóricos del modelo jerárquico en diseño de redes corporativas y sus aplicaciones.
2. Identificar ubicación geográfica de la empresa Metalmax, generando un estudio técnico sobre los requerimientos físicos y dispositivos necesarios para el despliegue de la red.

3. Modelar el diseño de la propuesta de la red mediante el software Packet Tracer para la empresa Metalmax ubicada en la vía a Daule km 27,5 de la ciudad de Guayaquil.
4. Elaborar un presupuesto económico aproximado para la futura implementación de la red diseñada.

1.6. Hipótesis.

Con este proyecto de graduación se resolverá la falta de una red corporativa que satisfaga los requerimientos de la empresa Metalmax.

1.7. Metodología de Investigación.

En el presente trabajo se usarán tres métodos de investigación que son: inductivo, de análisis y de síntesis. Análisis para descomponer toda la información obtenida, pasando al método inductivo donde se podrá generar una conclusión con los datos y/o requerimientos analizados. Y síntesis para reunir todos estos elementos dispersos.

CAPÍTULO 2: FUNDAMENTACIÓN TEÓRICA.

En este capítulo, se presentará la investigación sobre los principios, características y definiciones de las redes y sus aplicaciones.

2.1. Descripción redes LAN

Una LAN es la interconexión de redes que permite el acceso a los diversos servicios en red y recursos para los usuarios y sus dispositivos. La red de un campus se crea mediante un grupo de redes LAN que se encuentran interconectadas en un área. Los conceptos de diseño de red de campus o redes pequeñas son simples de entender, y la guía de diseño de redes LAN te dicta que la red no solo debe proporcionar una base de acceso a los servicios sino también que debe brindar: conectividad LAN entre todas las capas, acceso a la red por cable a los empleados, multidifusión IP para la distribución eficiente de los datos y una infraestructura cableada adecuada y lista para todos los servicios multimedia. (CISCO, 2014)

2.2. Redes convergentes

La tecnología ha avanzado tanto que está en un punto en el cual se tiene muchos servicios que viajan usando la misma red, ya sea para almacenamiento, streaming, servicios de voz IP, servicios de videos o más avanzados para procesamiento de datos. Es decir que la necesidad de crear y mantener redes separadas fue erradicada. Resaltando que en una red convergente existirán muchos tipos dispositivos desde computadores hasta facturadoras, todo interconectado entre sí tal como se ilustra en la figura 2. 1. (Cervantes, 2015)

Figura 2.1: *Redes convergentes.*
Fuente: **(Cervantes, 2015)**

2.3. Aspectos de las redes conmutadas

A continuación, se dará una breve explicación de los aspectos de las redes conmutadas y sus funciones.

2.3.1. Acceso múltiple.

Si la latencia (suma de retardos dentro de una red), entre un par de dispositivos es muy alta, al realizar en envío de datos por parte de uno el otro no detectará dicha señal y replicará una acción de envío. Ambas señales que fueron enviadas por este par de dispositivos colisionaran, mezclándose la señal y propagándose. (Cervantes, 2015)

2.3.2. Detección de colisiones.

Cualquier dispositivo que se encuentre en modo escucha podrá detectar cuando se produzca una colisión debido al aumento en la amplitud en las señales. (Cisco, 2020)

2.3.3. Señal de congestión y postergación aleatoria.

Al detectar la colisión en la red los dispositivos generan una señal de congestión lo cual tendrá como fin invocar el algoritmo de postergación logrando que todos los dispositivos detengan su transmisión durante un período de tiempo aleatorio. Reduciendo las señales de colisión. (Cervantes, 2015) (Cisco, 2020)

2.3.4. Comunicaciones Ethernet.

Existen tres formas en que ocurra la comunicación en las redes conmutadas.

- ***Unicast.***

  En este modo un host envía la trama a un host específicos.

- ***Broadcast.***

  Un host envía la trama hacia todos hosts disponibles en dicha red o segmento.

- ***Multicast.***

  En este modo existen grupos, y las tramas se envían hacía dichos grupos específicos de host. Un claro ejemplo de esto son las reuniones en Zoom.

2.3.5. Campos Preámbulo y Delimitador de inicio de trama.

Son identificadores únicos que son usados para que el emisor y receptor se comuniquen correctamente.

- ***Campo Dirección MAC destino.***

  Identificador usado en la capa 2 para determinar si el contenido está dirigido para ese dispositivo.

- ***Campo Dirección MAC origen.***

  Identificador usado en la capa 2 para determinar el origen del contenido y agregar la información a las tablas de búsqueda.

2.4. Protocolos de enrutamiento IP

Los protocolos de enrutamiento IP cumplen muchos propósitos entre los principales se tiene:

- Llenar y mantener la tabla de enrutamiento con una o más rutas por subred.
- En caso de tener más de una ruta para llegar a una subred, el protocolo de enrutamiento es el encargado de elegir la mejor ruta.
- Notificar y modificar en la tabla de enrutamiento cuando una ruta ya no se encuentra disponible.
- Gestionar y agregar en la tabla de enrutamiento nuevas rutas, con la finalidad de remplazar las rutas que se pierden o ya no están disponibles.
- Prevenir los bucles en la red.

En la actualidad existen muchos protocolos de enrutamiento, pero todos funcionan de manera similar, por esa razón se definirá una serie de pasos generalizados que describen la funcionalidad de los protocolos de enrutamiento:

- Cada router se responsabiliza de agregar las rutas que están conectadas a él directamente a la tabla de enrutamiento.
- Cada router notifica a su router vecino acerca de las rutas que contiene su tabla de enrutamiento.
- A través de la notificación del paso 2, el router agrega la ruta aprendida a su tabla de enrutamiento junto a la del router del siguiente salto que habitualmente es el router por donde aprendió la ruta.

2.5. Vector distancia y estado de enlace

Generalmente existen 2 tipos protocolos de enrutamiento, ambos basados en algoritmos distintos, pero que comparten un propósito común, el de poder elegir la mejor línea de salida para trasmitir un paquete.

2.5.1. Vector Distancia.

Los protocolos de enrutamiento que usan vector distancia se basan en el algoritmo Bellan-Ford para calcular la distancia entre rutas para determinar el mejor camino para llegar a la red.

Cuando un router aprende una ruta por un protocolo de enrutamiento vector distancia, debe contener tres factores importantes: La red de destino, La distancia (Métrica), El vector (enlace y el router del siguiente salto a usar como parte de la ruta), generalmente este tipo de protocolo envía la tabla de enrutamiento completa a cada vecino conectado directamente al router que ejecute el mismo protocolo. (Cisco, 2020)

2.5.2. Estado de enlace.

Los protocolos de enrutamiento que usan estado de enlace en cambio se basan en el algoritmo Dijkstra, este protocolo no comparte la tabla de enrutamiento completa, sino que, a través de actualizaciones referentes a los cambios en la topología, los routers llegan a tener una imagen completa de la red. (Cisco, 2020)

Cuando se utiliza este protocolo de enrutamiento el router debe crear tres tablas fundamentales para la implementación de este:

- Tabla de Vecinos: esta contiene los routers vecinos con el mismo protocolo de enrutamiento.
- Tabla de Topología: esta contiene todos los detalles referentes a la topología de la red.
- Tabla de Enrutamiento: es la tabla que tiene todo router donde guarda las mejores rutas.

2.6. Distancia administrativa y métrica

En los escenarios en donde el router es configurado con más de un protocolo de enrutamiento para alcanzar la misma subred, la distancia administrativa permite elegir la mejor ruta, bajo el criterio de: que la ruta del protocolo que tenga la distancia administrativa más baja será la escogida. En el caso que la distancia administrativa

sea 225, el router no agrega la ruta a la tabla de enrutamiento por que la considera poca confiable. (Cisco, 2020)

2.6.1. Métrica.

La métrica es la medida usada para decidir la mejor ruta en caso de que existan dos caminos diferentes para la misma red con el mismo protocolo de enrutamiento, cada protocolo define su propia métrica, en el caso de OSPF usa el costo, en cambio RIP usa el conteo de saltos. (Cisco, 2020)

2.7. VLAN

VLAN es el acrónimo de virtual LAN, básicamente es un método que permite agrupar de manera lógica dispositivos en un mismo dominio de broadcast, creando así distintas redes lógicas como si fueran redes físicas. (Cisco, 2020)

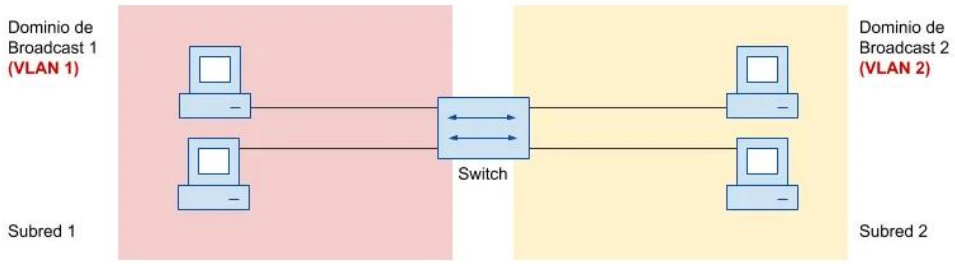


Figura 2.2: *Interconexión de VLANs.*
Fuente: **(Cisco, 2020)**

Varias VLAN pueden coexistir en un único Switch o red física, tal como se visualiza en la figura 2.2, ya que como se mencionó antes estas son configuradas para agrupar interfaces físicas en un mismo dominio de broadcast/difusión para que las tramas se interconecten en la red por medio de las VLAN.

La implementación de VLAN en una red trae consigo múltiples beneficios como:

- Reducir la sobrecarga del CPU al segmentar el número de dispositivos que recibirán una trama broadcast.
- Evitar riesgos al reducir el número de clientes que reciben copias de la trama.
- Mejorar la seguridad al separar los dominios de los clientes manteniendo así los datos sensibles en una VLAN especifica.
- Permite tener redes más flexibles al agrupar usuarios por departamentos sin importar la localización física.
- Permite que la red sea más resistente a fallos, ya que en caso de presentarse un problema normalmente la zona de falla se encuentra en el mismo dominio de broadcast.

- Reduce significativamente la carga de trabajo del dispositivo ya que el uso de las VLAN limita la funcionalidad del protocolo STP (capa 2).

2.7.1. Tipos de VLAN.

2.7.1.1. VLAN de datos/usuario.

Esta VLAN es usada para enviar únicamente tráfico de datos generados por el usuario.

2.7.1.2. VLAN predeterminada.

Esta VLAN no se puede eliminar ya que por medio de ella pasa el tráfico de control de la capa 2, en cisco la VLAN 1 es la VLAN predeterminada, una vez encendido el switch todos los dispositivos por default se encuentra en la VLAN predeterminada.

2.7.1.3. VLAN nativa.

Esta VLAN es la encargada de conectar un puerto configurado como Trunk 802.1Q con otra VLAN, en ella se maneja el tráfico no etiquetado.

2.7.1.4. VLAN de administración.

Esta VLAN es configurada para acceder a la gestión el switch.

2.7.1.5. VLAN de Voz.

Esta VLAN es para uso de servicios de telefonía de Voz sobre IP, con la finalidad de mantener la calidad del servicio, ya que el tráfico enviado a través de VLAN de Voz es catalogado como prioritario frente a otros.

2.7.2. VLAN de voz y datos.

En la actualidad la mayoría de las oficinas tienen un único cable UTP, conectado desde el rack hasta cada escritorio, por lo que si se tiene dos dispositivos (PC y Teléfono), se necesitaría instalar dos cables por cada escritorio, además implicaría ocupar muchos puertos en switch principal, por lo que podría resultar muy caro. (Cisco, 2020)

Con la finalidad de dar solución a esta problemática cisco incorpora un pequeño switch con tres puertos en los teléfonos IP, logrando así necesitar un único cable conectado desde el rack hasta el teléfono IP y así la PC se conectaría a un puerto del switch-teléfono IP, tal como se puede visualizar en la figura 2.3, para esto se necesita configurar dos VLANs en un único puerto físico. (Cisco, 2020)

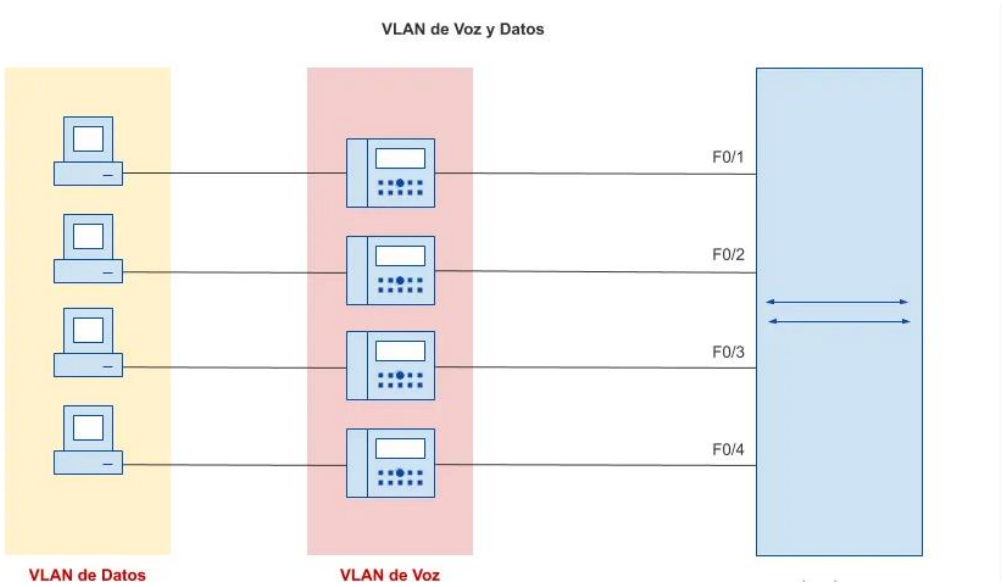


Figura 2.3: *VLAN de voz y datos.*
Fuente: **(Cisco, 2020)**

2.7.3. VLAN Trunking Protocol (VTP).

Si bien la configuración de VLAN se puede administrar fácilmente en una red o entorno pequeño, en entornos grandes, configurar todas las VLAN en todos los conmutadores puede ser muy complejo y potencialmente costoso. Podría ser fácil que una VLAN no esté configurada en uno de los conmutadores, especialmente si se usa un diseño de VLAN de extremo a extremo. En caso de que se tenga una red de tamaño considerable y se quiera mantener la consistencia en las VLAN creadas, es muy recomendable que se tenga un mecanismo que permita sincronizar todos los circuitos de Switches bajo la red VLAN. (Collado, 2018)

Un protocolo que permite sincronizar todos los Switches en la red sobre las VLAN disponibles en la red es VTP - VLAN Trunking Protocol. VTP es un protocolo de capa 2 propietario de Cisco que permite intercambiar información de VLAN entre troncales para que los Switches de la red tengan una base de datos de VLAN sincronizada en todo momento desde un punto central de la red, tal como se ilustra en la figura 2.4. En caso de que no se use Switches Cisco o se quiera conectar Switches Cisco a otros Switches de otros fabricantes, no se puede usar VTP y se tendrá que usar otro protocolo abierto como GVRP, tiene funciones muy similares a VTP, pero es un protocolo abierto. protocolo, a diferencia de VTP. VTP permite crear VLAN, modificarlas o eliminarlas de un conmutador central en todos los conmutadores de la red. (Collado, 2018)

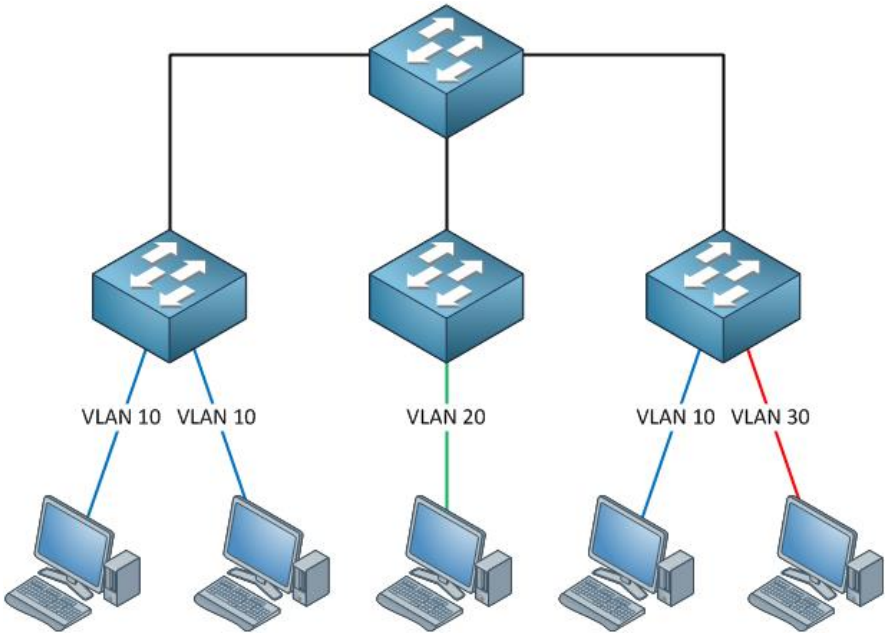


Figura 2.4: *VLAN trunking protocol.*
Fuente: **(Network Lessons, 2022)**

2.7.3.1. Dominios de VTP.

VTP usa dominios para agrupar switches que compartirán la misma información de VLAN. En dominios VTP, la siguiente información se intercambia mediante mensajes VTP:

- Dominios
- Versión VTP
- Lista de VLAN
- Configuración específica para cada VLAN

2.7.3.2. Modos de VTP.

Los Switches en el dominio VTP pueden operar de tres formas diferentes:

- Modo Servidor: El servidor es responsable de crear y mantener información para todas las VLAN en la red, y es responsable de transmitir la información al resto de los Switches. De forma predeterminada, los conmutadores de Cisco están en modo servidor. (Collado, 2018)
- Modo cliente: un conmutador en modo cliente no puede realizar cambios en la VLAN y retiene la información de la VLAN a través de los mensajes enviados desde el servidor. (Collado, 2018)
- Modo transparente: los Switches en modo transparente no participan en el proceso VTP y no transmiten mensajes VTP, pero varían según la versión VTP. Si es la versión 1 del VTP, solo se transmitirán los mensajes del VTP

que tengan la versión 1 y coincidan con el nombre de dominio configurado. Sin embargo, en la versión 2 del VTP, un conmutador transparente puede reenviar mensajes del VTP incluso si no coinciden con la versión que el conmutador ha configurado o el dominio de conmutación incluido en el modo transparente tal como se muestra en la figura 2.5. (Collado, 2018)

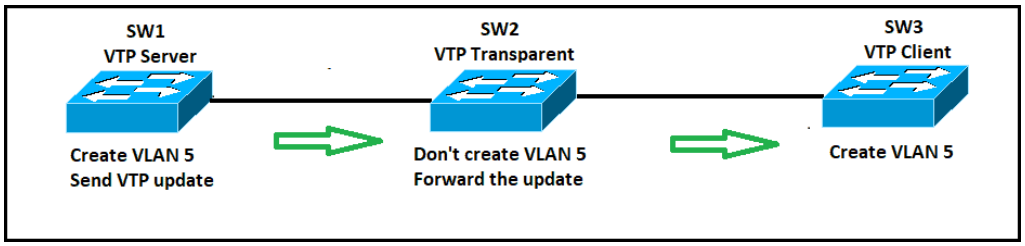


Figura 2.5: *Modos VTP.*
Fuente: **(CCNA, 2022)**

Dependiendo del modo en el que opere el conmutador este podrá realizar operaciones con la base de datos de VLANs, dichas operaciones se detallan a continuación en la tabla 2.1.

Tabla 2.1: *Funciones de los modos VTP.*

	VTP Server	**VTP Client**	**VTP Transparent**
Create/Modify/Delete VLANs	Yes	No	Only local
Synchronizes itself	Yes	Yes	No
Forwards advertisements	Yes	Yes	Yes

Fuente: (Network Lessons, 2022).

2.7.3.3. Anuncios de VTP.

Los Switches que usan VTP versión 1 o versión 2 anuncian VLAN (solo del 1 al 1005), números de versión de configuración y ajustes para cada VLAN sobre el enlace troncal para comunicar esta información al resto de la red. multidifusión, la versión 3 de VTP permitía el uso de VLAN en el rango 1-4096, lo que haría que VTP fuera compatible con el estándar IEEE 802.1Q. Es importante tener en cuenta que el número de versión de configuración siempre comienza con 0 y con cada cambio,

el número de versión de configuración se incrementa en 1 y el mensaje con el número de versión de configuración más alto se considera una notificación, por lo que finalmente se sincronizarán las notificaciones. (Collado, 2018)

Y también cabe señalar que, por defecto, los mensajes VTP se transmiten de forma clara y sin contraseña, es decir, sin encriptación, por lo que la comunicación segura no se realiza mediante el intercambio de contraseña. (Collado, 2018)

Después de comentar esto, queda un problema muy serio. Teniendo en cuenta que Cisco utiliza el modo de servidor de forma predeterminada y que el cliente VTP almacenará la información con el número de versión de configuración más alto, es posible utilizar un conmutador integrado desde otro lugar con una versión de configuración alta y el modo de servidor predeterminado, es posible que esto El nuevo conmutador integrado en la red anulará la configuración de todos los conmutadores de la red, eliminará y/o creará VLAN y, por lo tanto, modificará la configuración y dará como resultado un error. Por supuesto, si este conmutador está configurado en modo cliente y tiene un número de versión de configuración superior al del servidor, omitirá las actualizaciones y eso significa que el conmutador no actualizará su configuración. (Collado, 2018)

Por lo tanto, es extremadamente importante antes de incorporar un nuevo conmutador a la red para asegurarse de que el número de versión de configuración esté establecido en 0, pero dado que no se tiene ningún comando que haga esto directamente, se tiene que hacer lo siguiente indirectamente: Cambiar el modo cambia a transparente y luego vuelve al servidor o cambie el dominio VTP a uno que no se use y vuelva a configurar el dominio VTP correcto. Después de tomar estas precauciones, se pudo instalar el nuevo interruptor. (Collado, 2018)

En cuanto a los anuncios VTP, hay que tener en cuenta que se crean de tres formas diferentes:

- Resumen de anuncios: el servidor genera estos anuncios cada 300 segundos o cada vez que hay un cambio en la base de datos de VLAN.
- Notificaciones de subconjunto: estos mensajes se generan cada vez que se realiza un cambio en una VLAN.
- Notificaciones solicitadas por el cliente: este tipo de notificación se genera cada vez que un cliente necesita actualizar su configuración, como después de reiniciar la computadora.

Los conmutadores que funcionan en modo servidor no necesitan cambiar la configuración después del restablecimiento porque almacenan la información de VTP y VLAN en el archivo vlan.dat en Flash, por lo que el restablecimiento no implica la

pérdida de material de información, en la figura 2.6 se puede observar el envío de información desde el servidor al cliente. (Collado, 2018)

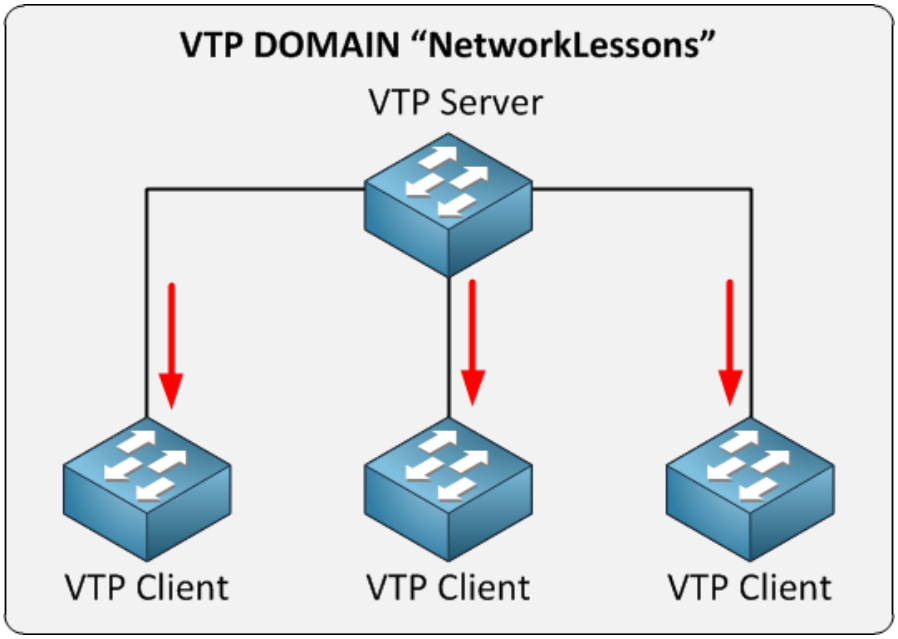


Figura 2.6: *Dominio VTP.*
Fuente: **(Network Lessons, 2022)**

2.7.3.4. Configuración de VTP.

Configurar VTP en Switches Cisco con IOS es bastante sencillo ya que lo único que se debe configurar es el dominio y modo VTP, opciones de versión, contraseña, etc. De forma predeterminada, el perfil se utilizará cuando la configuración de VTP sea la versión 1, aunque la versión 2 tiene las siguientes ventajas sobre la versión 1:

En un cambio de modo transparente, la versión 2 dará permiso para reenviar los anuncios de VTP recibidos independientemente de su versión o su dominio

La versión 2 realiza una verificación de coherencia al ingresar comandos a través de CLI o SNMP, pero no realizará esta verificación en los anuncios recibidos de otros conmutadores.

2.7.3.5. VTP Pruning.

Es un método que evita que las actualizaciones de VTP se propaguen a través de todos los puertos troncales, de esta manera se puede limitar la transmisión de VTP a una parte bien definida de la red, reduciendo así el tráfico y el procesamiento de información innecesarios para los cruces. De tal manera que solo se propague la información necesaria, tal cual se muestra en la figura 2.7. Recuerde que VTP usa

mensajes de multidifusión y que estos mensajes, como las transmisiones predeterminadas, se transmiten a través de todos los puertos de la VLAN excepto el que se recibió. La configuración de eliminación de VTP no es demasiado pesada, lo único que debe tener en cuenta es que está deshabilitada de forma predeterminada y deberá habilitarse. (Collado, 2018)

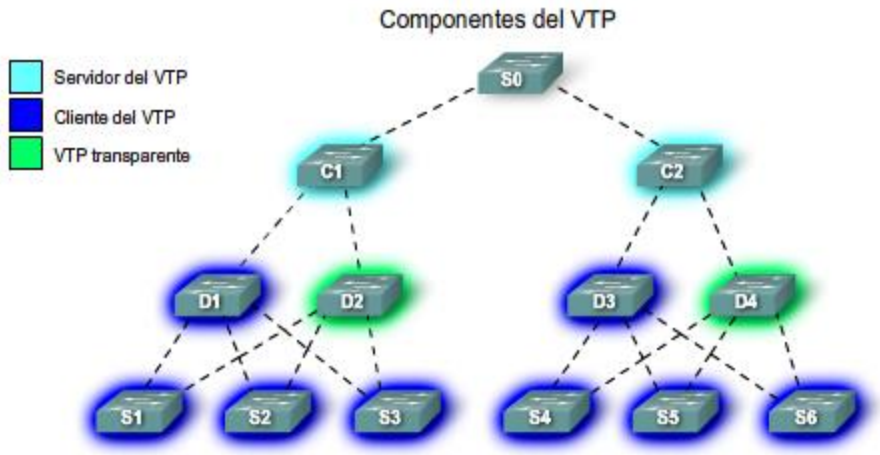


Figura 2.7: *VTP difusión-componentes.*
Fuente: **(Cisco, 2020)**

2.7.3.6. Encapsulamiento DOT1Q

DOT1Q (nombre real 802.1q) es un protocolo que transmite información de VLAN con tramas de Ethernet, conocidas como tramas "etiquetadas", porque cada trama lleva una etiqueta de VLAN que le dice al dispositivo receptor "esta trama pertenece a la VLAN. X"; hay otros protocolos que pueden hacer cosas similares, pero DOT1Q es el más utilizado. En los dispositivos Cisco, esto se maneja a través de subinterfaces: tiene una sola interfaz Ethernet, como FastEthernet 0, luego se crean subinterfaces, como FastEthernet 0.1 y FastEthernet 0.2. La interfaz principal (física) está configurada para encapsulación y enlace troncal de VLAN, a cada subinterfaz se le asigna una VLAN diferente y el enrutador puede enrutar el tráfico entre estas interfaces "virtuales" como si fueran "reales".

2.8. Enrutamiento de un paquete IP

Para entender este mecanismo se utilizará la figura 2.8, donde se analizará que pasos sigue un paquete IP a través de la red para llegar a su destino.

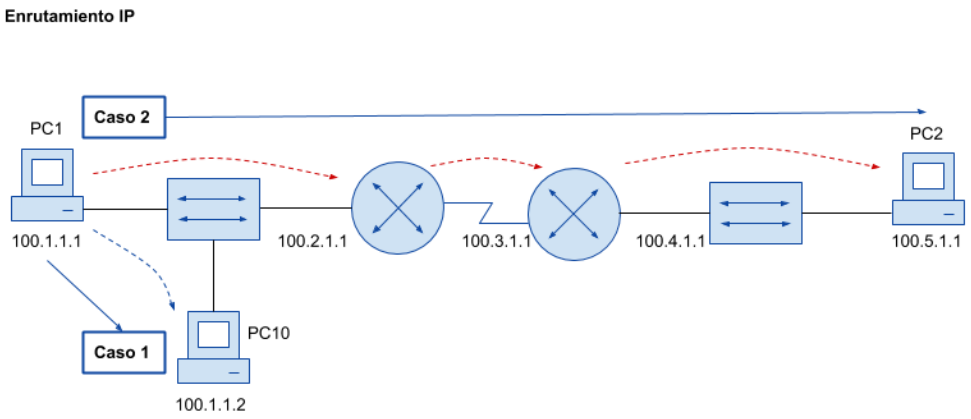


Figura 2.8: *Enrutamiento IP.*
Fuente: **(Cisco, 2020)**

Caso 1: Enrutamiento IP dentro de una misma subred - **PC1 → PC10**

- La dirección IP de destino está en la misma subred IP del paquete, por lo tanto, él envió es directo.
- Otra forma seria enviar el paquete a la ruta por defecto (default gateway), ya que esta tiene una interfaz en la misma subred que el host destino.

Caso 2: Enrutamiento IP en diferentes subredes - **PC1 → PC2**

Para este caso el paquete IP tendrá que salir de la subred a través del router, este debe procesar el contenido de la trama efectuado la siguiente lógica:

- Verifica el campo FCS de la trama, que sirve para detectar errores, en caso de estar defectuosa se descarta la trama.
- Asumiendo que la trama no fue descartada en el paso 1, lo siguiente es quitar el encabezado y la cola de la trama para obtener solo el paquete IP.
- Luego compara la dirección IP de destino del paquete con su tabla de enrutamiento, con la finalidad de buscar la ruta que mejor se correlaciona con la dirección IP de destino, una vez encontrada la ruta debe identificar la interfaz de salida del router y posiblemente la dirección IP del siguiente salto/Router.
- El último paso es encapsular el paquete IP dentro de una nueva trama que contenga los datos necesarios para reenviar el paquete hacia una nueva interfaz de salida.

Esta lógica de procesamiento se repite hasta que el paquete IP alcanza la dirección de destino.

2.8.1. Enrutamiento Estático.

Enrutamiento estático es un método en donde el administrador de la red es el encargado de configurar manualmente las rutas por las que se transmiten los datos

en una red, normalmente se utilizan los protocolos de enrutamiento para aprender rutas automáticamente (rutas dinámicas), pero para ciertos escenarios es necesario prescindir de estos protocolos y agregar rutas de manera estática. (Cisco, 2020)

2.8.1.1. Tabla de enrutamiento.

La tabla de enrutamiento es básicamente un documento electrónico que tiene cada router, esta almacena las rutas a los diferentes nodos en una red, así como las reglas para determinar cuál es el mejor camino para enviar los paquetes. En caso de que exista más de una opción de camino para la misma ruta, el router debe considerar un valor numérico llamado Distancia Administrativa que sirve para saber que ruta es más importante y fiable, de acuerdo con cómo fue configurada (conexión directa, ruta dinámica, ruta estática). (Cisco, 2020)

También existe la ruta por defecto (default route), el sistema operativo de cisco permite configurar una ruta por defecto en la tabla de direccionamiento, que sirve para las ocasiones en las que el router no es capaz de hacer coincidir una red destino con ninguna entrada en la tabla de enrutamiento, para si llegar al Gateway como último esfuerzo por enviar el paquete. (Cisco, 2020)

2.8.2. Enrutamiento dinámico.

Básicamente en el enrutamiento dinámico se usa los protocolos de enrutamiento para crear rutas de forma dinámica, en cuento a la funcionalidad del enrutamiento dinámico, esta dependerá del protocolo que utilices, pero en esencia realizan las siguientes actividades:

- Leen la información de enrutamiento de las subredes IP de los routers vecinos.
- Notifican sobre la información de enrutamiento de las subredes IP a los routers vecinos.
- En caso de tener más de un camino para alcanzar una subred, esta es elegida basándose en el concepto de la métrica de los protocolos de enrutamiento.
- Reacciona a los cambios en la red.

Si bien todos los protocolos de enrutamiento comparten lo anterior, difieren en cuanto al modo de realizar las tareas. Existen dos categorías principales de los protocolos de enrutamiento IP:

- Protocolo interior/ Interior Gateway Protocol (IGP): Como su nombre lo indica es un protocolo diseñado para trabajar dentro de un sistema autónomo (AS) único.

- Protocolo Exterior/ External Gateway Protocol (EGP): En cambio, este protocolo fue diseñado para trabajar entre diferentes sistemas autónomos.

Aclarando un poco más los conceptos anteriores, con sistemas autónomos (AS) se refiere a las redes administradas por una sola organización, ahora bien, conociendo todas estas definiciones, es importante que, al momento de elegir un protocolo de enrutamiento se considere las siguientes características:

- El algoritmo que utiliza.
- La métrica.
- Velocidad de convergencia.
- El estándar del protocolo Public/Private.

2.8.2.1. Open Shortest Path First (OSPF).

OSPF (Open Shortest Path First) es un protocolo de enrutamiento dinámico interior que usa el algoritmo de estado de enlace, este tipo de protocolos crean rutas IP enviando información sobre los enlaces entre los routers, para así por medio de actualizaciones mantener una imagen de la red completa.

OSPF utiliza los bloques funcionales (LSA) de la base de datos de estado de enlace (LSDB) para organizar la información de la tipología de la red, estos bloques contienen información específica sobre la tipología de la red y son almacenados en la LSDB tal como se puede visualizar en la figura 2.9. (Cisco, 2020)

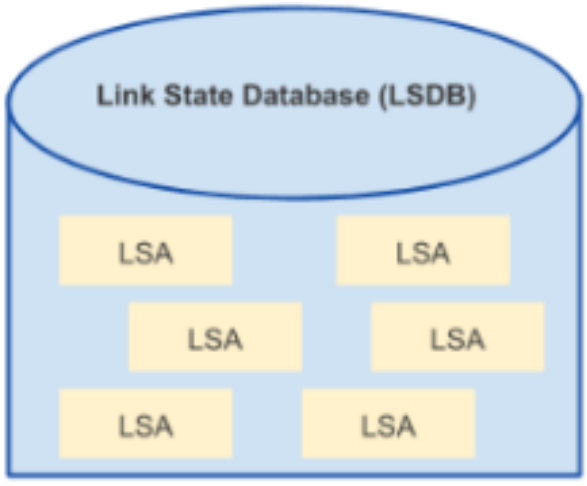


Figura 2.9: *Link State Database.*
Fuente: **(Cisco, 2020)**

Todos los protocolos tienen su algoritmo matemático para poder escoger la mejor ruta hacia una subred, en caso de OSPF se tiene Dijkstra que se encarga de

procesar la LSDB para construir las rutas que el router local debe añadir a su tabla de enrutamiento. (Cisco, 2020)

Es importante saber que los routers con OSPF antes de intercambiar actualizaciones de enrutamiento con sus vecinos, estos deben ser descubiertos dinámicamente a través del envío de mensajes *Hello* a cada interfaz habilitada para OSPF en el router, la figura 2.10 muestra el concepto:

Figura 2.10: *Paquetes Hello en OSPF.*
Fuente: **(Cisco, 2020)**

- *Estados de Vecinos de OSPF.*

Los routers con OSPF deben pasar por varios cambios de estado antes de establecer una relación vecina, estos serán explicados en 6 puntos e ilustrados en la figura 2.11 a continuación:

a) Inicio: En este estado el router ha recibido un mensaje Hello de otro router OSPF.
b) 2-Way: En este estado el vecino recibió el mensaje Hello y respondió con un mensaje Hello propio.
c) Exstart: En este estado empieza el intercambio de información sobre el estado de enlace entre ambos routers.
d) Exchange: En este estado se intercambian paquetes DBD, estos contienen encabezados de LSA y con esa información los routers pueden ver que LSA debe enviarse.
e) Carga: En este estado un vecino envía un paquete LSRs que es una solicitud de estado de enlace para cada router que no conoce, el otro vecino debe responder con un LSU, que es una actualización del estado de enlace, esta contiene información sobre el estado de la red solicitada.
f) Full: En este estado ambos routers tienen la base de datos sincronizada y completamente adyacentes entre sí.

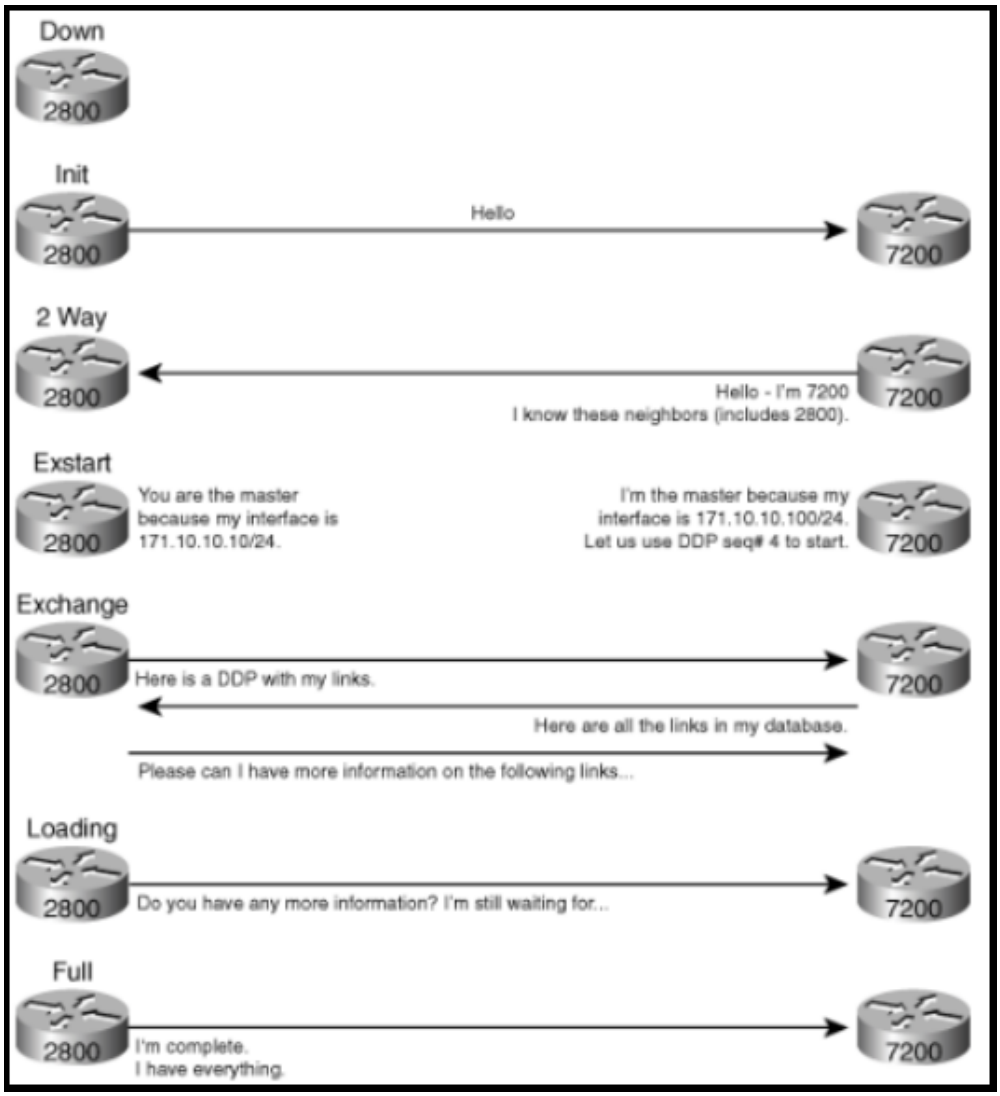


Figura 2.11: *Estados de vecinos.*
Fuente: **(Cisco, 2020)**

- *OSPF: Intercambio de LSBD Entre Vecinos.*

Cuando dos routers vecinos alcanzan el estado Full, se creería que todo el proceso de sincronización esta completo, sin embargo, los routers deben realizar algunas tareas continuas para mantener la relación con los vecinos. (Cisco, 2020)
La siguiente lista enumera las tres tareas de mantenimiento básicas:

a) OSPF incorpora dos temporizadores relacionados: el intervalo Hello y el Intervalo Dead. Los routers envían mensajes Hello cada intervalo Hello a cada vecino, en caso de que un vecino no responda durante un intervalo Dead, significara que el vecino ha fallado.
b) Cuando exista un cambio en el estado de enlace, uno o más routers modificaran los LSA necesarios para especificar estos cambios,

posteriormente se inundarán las rutas hacia los vecinos con los LSA para que estos puedan actualizar su LSDB.

c) Las LSA tienen un temporalizador independiente que reduce su vida útil a 30 min, por lo que los routers están obligados a regenerar los LSA cada 30min, cabe recalcar que este valor es configurable.

- *OSPF: Tipos de Redes.*

En la actualidad existen dos tipos de redes OSPF, Point-to-Point y broadcast, esta configuración le permite al router saber si debe descubrir o no de manera dinámica a los vecinos de la red y si debe usar un router Designado (DR) para ello, en la tabla 2.2 se puede observar la principal diferencia entre estos dos tipos de redes**.**

Tabla 2.2: *Tipos de redes OSPF.*

Palabra Clave del Network Type	**Descubre Vecinos Dinámicamente**	**Usa un DR/BDR**
Broadcast	Si	Si
Point-To-Point	Si	No

Fuente**:** (Cisco, 2020)

a) Red OSPF de Broadcast: Es el tipo de red por defecto que usa OSPF en las interfaces, para facilitar el descubrimiento automático de vecinos se usa la ventaja de que en las redes Ethernet se puede hacer broadcast, donde un solo paquete trasmitido por un dispositivo se puede retrasmitir a todos los puertos conectados en la misma subred.

b) Red OSPF Point-to-Point: Una red punto a punto es mucho más simple, un paquete enviado siempre tendrá exactamente un destinatario en el enlace local.

- *OSPF Relaciones de Vecinos y Problemas.*

Durante el proceso intercambiar información de la topología y estado de la red, el router debe lograr relacionase con sus vecinos, por esa razón el protocolo de enrutamiento examina la información en el saludo del vecino y la compara con la propia configuración del router local, en caso de que no coincida no se concreta la sincronización, en la tabla 2.3 se enlistan una serie de requerimientos necesarios para establecer la vecindad. (Cisco, 2020)

Tabla 2.3: *Requerimientos para comunicación OSPF.*

Requerimientos	**Requerido para OSPF**	**Vecindad Perdida si es incorrecto**
Las interfaces deben estar levantadas, en estado up/up.	Si	Si
La lista de control de acceso no debe filtrar los mensajes del protocolo de enrutamiento.	Si	Si
Las interfaces deben estar en la misma subred.	Si	Si
Deben pasar la autenticación de vecino del protocolo de enrutamiento (si está configurado).	Si	Si
Los temporizadores de *Hello* y *hold/dead* deben coincidir.	Si	Si
El router IDs (RID) debe ser único.	Si	Si
Deben estar en la misma área.	Si	Si
El proceso OSPF no debe estar apagado.	Si	Si
Las interfaces entre vecinos deben tener la misma configuración de MTU.	Si	No
Las interfaces entre vecinos deben usar el mismo tipo de red OSPF	Si	No

Fuente: (Cisco, 2020)

La columna denominada «Requerido para OSPF» significa que el elemento debe estar funcionando correctamente para que la relación de vecino funcione correctamente. Ten en cuenta que todos los elementos de esta columna muestran un «sí», lo que significa que todos deben ser correctos para que la relación de vecino funcione correctamente. (Cisco, 2020)

- *OSPF: Áreas.*

El concepto de trabajar con áreas en OSPF surgió de la necesidad de solucionar las limitantes que trae consigo el diseño de área única, básicamente la base de datos LSDB se divide en varias LSDB más pequeñas con la finalidad de segmentar las complicadas matemáticas por áreas. (Cisco, 2020)

- *Áreas en OSPF.*

En el diseño del área de OSPF se recomienda seguir las siguientes reglas:

a) Colocar todas las interfaces conectadas a la misma subred dentro de la misma área.
b) Un área debe ser contigua.
c) Algunos routers son internos en el área, es decir todas sus interfaces están asignadas a esa única área.
d) Algunos routers deben ser de Borde de Área (ABR), porque algunas interfaces se conectan con el área de “backbone” (área 0) y otras no.
e) Todas las áreas que no son de “backbone” deben tener un camino para alcanzar al área de área 0, teniendo al menos un ABR conectado hacia el área de “backbone” y el área que no es de “backbone”.

2.8.3. Enrutamiento Intra VLAN

Dado que una interfaz solo puede tener una IP y se tiene varias subredes con sus VLAN a las que se quiere llegar, entonces se tiene que crear subinterfaces y vincular IP a ellas. Esto se puede lograr usando el protocolo 802.1Q.

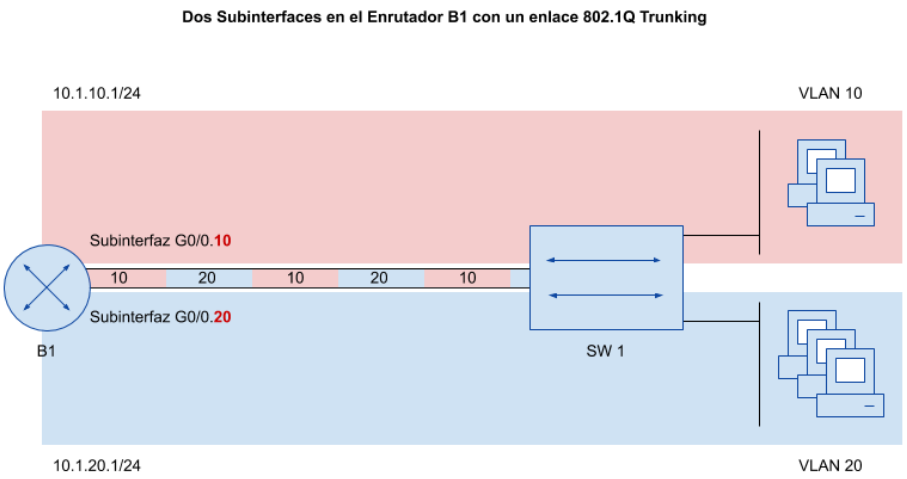


Figura 2.12: *Subinterfaces en un enrutador.*
Fuente: **(Cisco, 2020)**

El ejemplo anterior ilustrado en la figura 2.12 muestra la configuración de red troncal 802.1Q requerida por el enrutador B1. Ahora que el router ha configurado las subinterfaces, funcionará con ellas como si fueran interfaces normales, y con IPv4 configurado, el router podrá enrutar paquetes a través de las subinterfaces.

2.8.4. Enrutamiento Inter VLAN

En el enrutamiento Inter VLAN se tiene distribuida VLAN por puertos físicos independientes tal como se muestra en la figura 2.13.

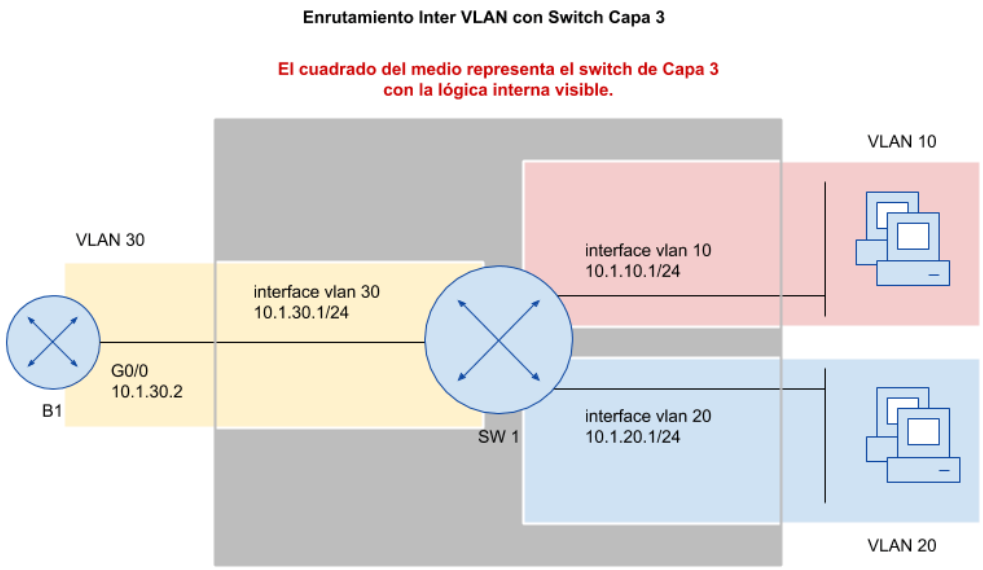


Figura 2.13: *Enrutamiento Inter-VLAN.*
Fuente: **(Cisco, 2020)**

2.8.5. Intra VLAN vs Inter VLAN

El enrutamiento entre VLAN puede ser Intra VLAN o Inter VLAN y se utiliza para comunicarse entre diferentes subredes en diferentes VLAN.

- Intra VLAN: interfaz física de estilo troncal que se utiliza para conectar varias VLAN juntas y enrutar entre ellas.
- Inter VLAN: un conmutador de capa 3 está realizando el enrutamiento entre las VLAN.

Hay tres opciones para conectar un enrutador a cada subred de una VLAN:

Opción 1 (VLAN interna): enrutar una VLAN con un enlace troncal 802.1Q en el enrutador: Utilice un enrutador con una conexión troncal a la LAN del conmutador de capa 2. El enrutador es responsable del enrutamiento con el conmutador que crea las VLAN. Esta función se denomina Enrutamiento en VLAN troncal y también se conoce como Enrutador en clave (ROAS). (Cisco, 2020)

Opción 2 (Inter VLAN): enrutamiento de VLAN con conmutadores de capa 3 (SVI): Utilice un conmutador que admita tanto la capa 2 como la capa 3 (llamado conmutador de capa 3 o conmutador multicapa). Para el enrutamiento, la configuración del conmutador de capa 3 utiliza la denominada interfaz virtual de conmutación (SVI). (Cisco, 2020)

Opción 3: enrutamiento de VLAN con reenvío de puertos en un conmutador de capa 3: Una alternativa a la opción 2 de Inter VLAN, o SVI, es la denominada puerta de enlace de enrutamiento donde los puertos físicos del conmutador se hacen actuar como si fueran la interfaz del enrutador. Esta sección también presenta el concepto de EtherChannel, que es una característica denominada Layer 3 EtherChannel y se utiliza en una puerta de enlace de tipo enrutamiento. (Cisco, 2020)

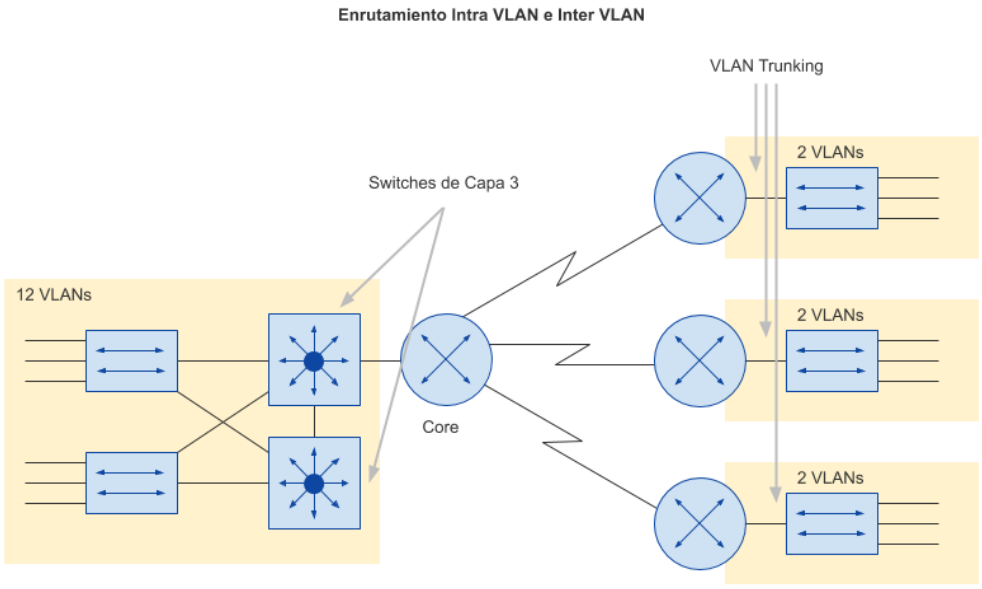


Figura 2.14: *Intra VLAN vs Inter VLAN.*
Fuente: **(Cisco, 2020)**

En la figurar 2.14 se muestra una topología conformada por enrutamiento intra e inter VLAN, de tal manera que se vincula las fortalezas de ambos tipos de enrutamiento.

2.8.6. Puerto de Enrutamiento

Se puede configurar un conmutador de capa 3 para que el puerto físico actúe como un puerto físico en el enrutador en lugar de un puerto físico en el conmutador. Ahora la lógica de enrutamiento no es la capa 2 sino la capa 3. Con esto se tendrá una puerta de enlace de enrutamiento conmutado de capa 3. Capa 3 usando SVI (interfaz virtual conmutada). Cuando un conmutador usa SVI, la interfaz física se

comporta como la interfaz real: la interfaz de Capa 2. Ahora se verá cómo configurar el conmutador para que el puerto actúe como un enrutador de capa 3. En otras palabras, el conmutador recibe una trama Ethernet, aprende la dirección MAC de origen de la trama y la transmite de acuerdo con la MAC de destino. Sin embargo, para ser enrutable, sigue la lógica de proceso de un conmutador de Capa 2, las tramas entrantes en un puerto de conmutador de tipo enrutador activarán la lógica de Capa 3, que incluye: (Cisco, 2020)

- Encabezados y colas de tramas de Ethernet
- Tome decisiones de reenvío de capa 3 comparando la dirección IP de destino con la tabla de enrutamiento de IP
- Agregar un nuevo encabezado/remolque de enlace de datos Ethernet al paquete
- Reenviar el paquete empaquetado a una nueva trama

En la figura 2.15 se puede visualizar el puerto de enrutamiento funcionando en un conmutador que se encuentra trabajando con enrutamiento inter VLAN.

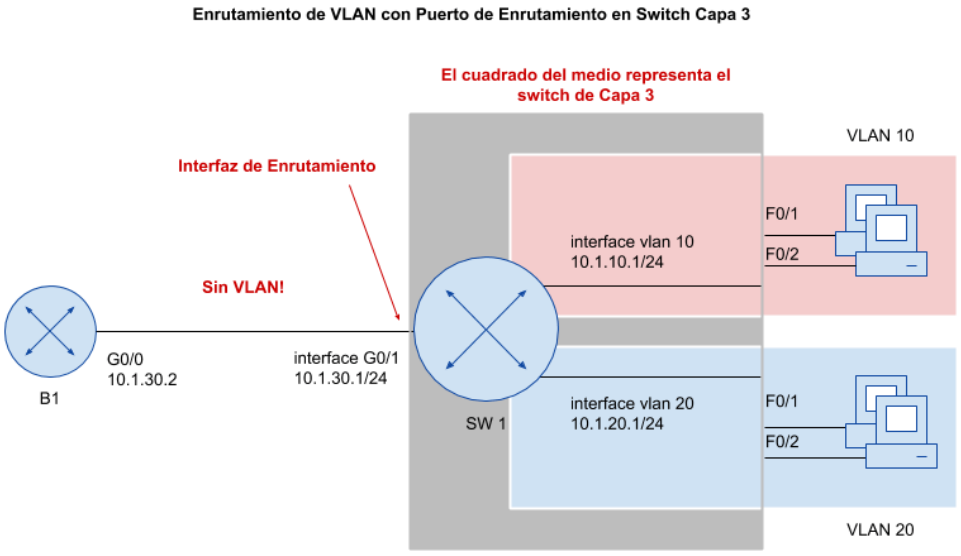


Figura 2.15: *Puerto de Enrutamiento.*
Fuente: **(Cisco, 2020)**

En la figura 2.16 se muestra un diseño de red, con 2 núcleos (Core1, Core2) y los conmutadores de red de servicios públicos (D11, D12, D21, D22) conectados a Core 1 y Core 2 realizan conmutación de Capa 3. Todos los puertos están directamente vinculados entre conmutadores de Capa 3 que pueden tener enrutamiento interfaces. Para las VLAN donde varias interfaces (acceso y troncal) se conectan a esa VLAN, el enrutamiento entre VLAN (SVI) tiene más sentido porque

SVI puede enviar y recibir tráfico hacia y desde múltiples puertos en el mismo conmutador. En este diseño, todos los puertos Core1 y Core2 deben ser puertos enrutados, mientras que los cuatro conmutadores de distribución usarán algunos puertos como enrutamiento y otros como SVI. (Cisco, 2020)

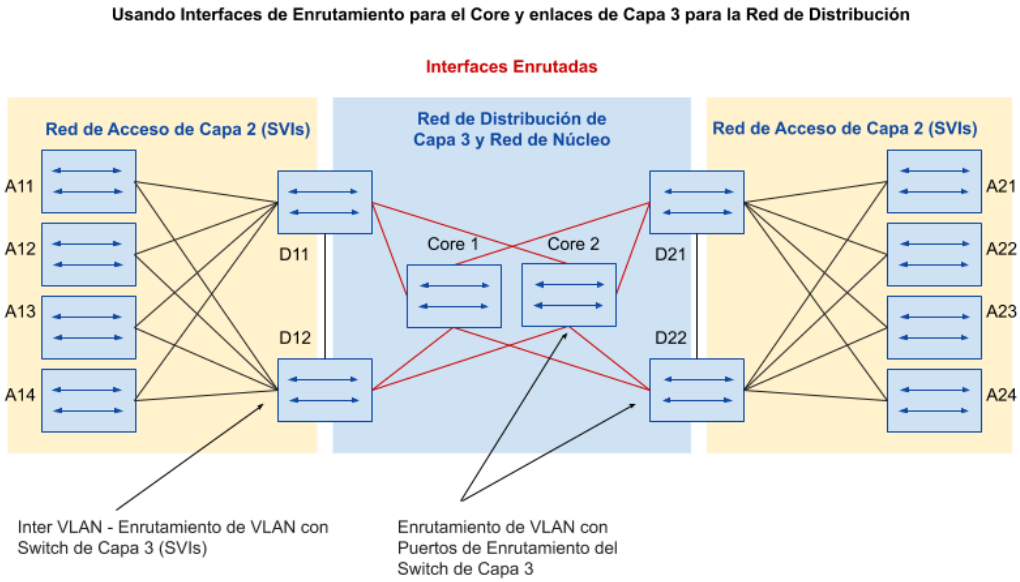


Figura 2.16: *Estados de vecinos.*
Fuente: **(Cisco, 2020)**

2.9. Modelo Jerárquico

El modelo jerárquico permite desglosar la red en grupo modulares o capas, permitiendo implementar funciones específicas, simplificando la administración de la red. La división por capas en el diseño de la red permite replicar los servicios o funciones que se implementen en ciertas zonas de esta. Si en arquitecturas planas se aplican cambios, dichos cambios afectarán a gran cantidad del sistema. Por otro lado, en el modelo jerárquico se puede restringir los cambios operativos a un subgrupo de la red, facilitando la administración. (CISCO, 2022)

El diseño modular de una red permite también una mejor comprensión de esta, ya que constará de elementos pequeños y fáciles de entender. Aislando las fallas ya que la estructura del sistema será por capas tal cual se muestra en la figura 2.17. (CISCO, 2022)

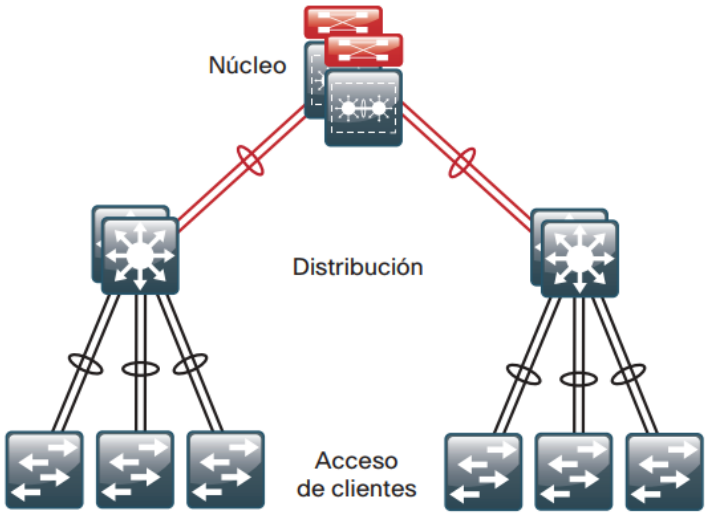


Figura 2.17: *Modelo de red jerárquico.*
Fuente: **(CISCO, 2022)**

Cada capa del diseño ofrecerá una funcionalidad distinta para la red. Según sea el escenario y necesidades el diseño puede constar de 2 o 3 capas. Por ejemplo, si la organización es pequeña y consta de tan solo un bloque solo se necesitaría la capa de distribución y capa de acceso a cliente. Por otro lado, si la empresa se extiende por más de 2 edificios se necesitaría la implementación de las tres capas, de tal manera que la red escale de dos capas sencillas a un sistema convergente con núcleo central tal cual se muestra en la figura 2.18. (CISCO, 2022)

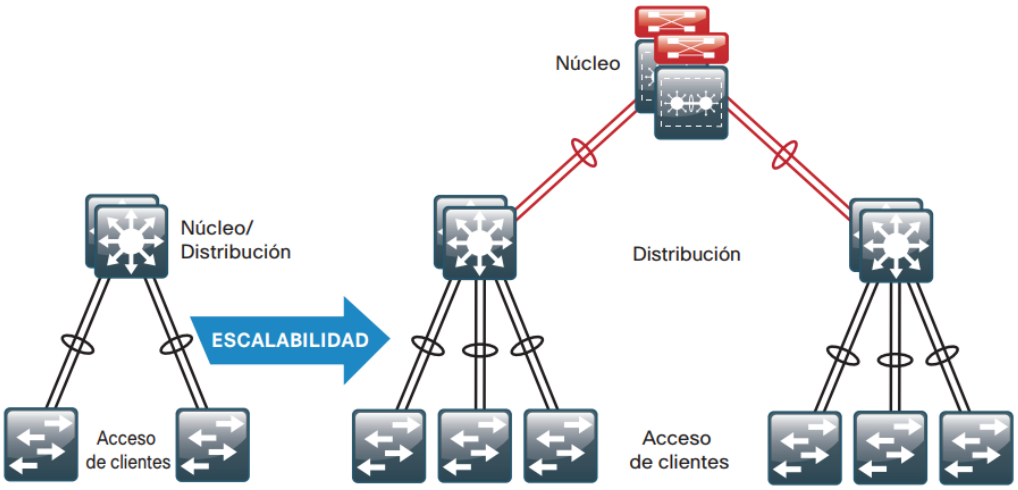


Figura 2.18: *Escalabilidad de 2 capas a 3 capas.*
Fuente: **(CISCO, 2022)**

El modelo jerárquico se divide en tres capas, las cuales se detallan a continuación:

2.9.1. Capa de acceso.

La capa de acceso es el nivel de la red por el cual los dispositivos que son usados por el usuario obtienen acceso a la red. Esta capa ofrece conectividad tanto inalámbrica como cableada. Ofrece características que aseguran la seguridad y conectividad para los dispositivos de los usuarios tal como se visualiza en la figura 2.19. (CISCO, 2022)

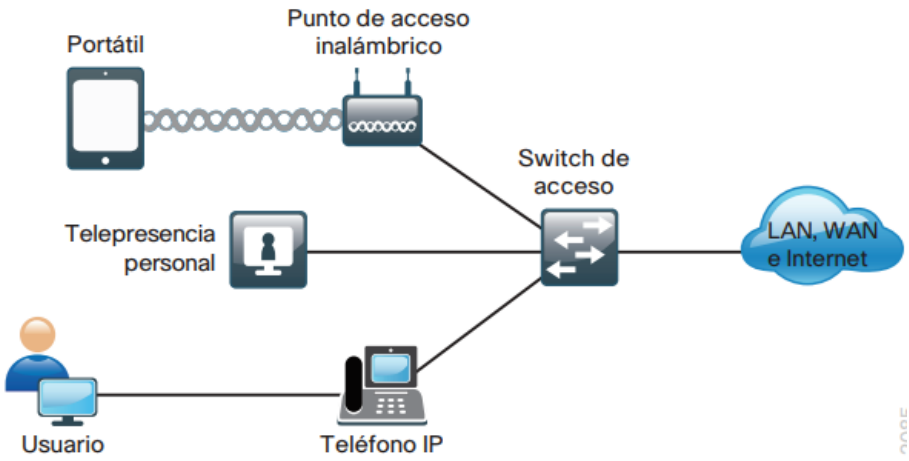


Figura 2.19: *Capa de acceso.*
Fuente: **(CISCO, 2022)**

Dentro de las características que debe cumplir esta capa están:

- Conectividad de dispositivos: Debido a que en esta capa se conectan muchos dispositivos debe ser capaz de tolerar muchas conexiones lógicas manteniendo el mejor rendimiento posible.
- Servicios de seguridad: Este punto se basa en que los usuarios solo deben tener acceso a los servicios autorizados a su perfil o área, de tal manera que otros usuarios no se apoderen de roles ajenos.
- Funcionalidades de tecnología avanzada: Debe permitir múltiple tráfico de forma simultánea, es decir debe poder transmitirse voz, video, datos de muchos dispositivos e inclusive adaptar tecnologías IoT garantizando el funcionamiento de todos estos servicios.

2.9.2. Capa de distribución.

Esta capa hace posible la conectividad entre los dispositivos de la capa de acceso y tiene dos características principales:

- Escalabilidad: La capa de distribución sirve como un punto en él se pueden agregar múltiples switches que pertenecen a la capa de acceso.

- Reducción de la complejidad y aumento en la recuperabilidad: Puede seleccionarse nodos como entidades lógicas para que funcionen como un solo dispositivo, adicional a esto al tener redundancia de componentes la recuperabilidad de sistema aumenta considerablemente.

2.9.2.1. Diseño de dos capas.

En este diseño se tiene un núcleo fusionado, esto debido a que la capa de distribución sirve como la capa de agregación de capa 3 para todos los dispositivos. A su vez los servicios y las interconexiones WAN pueden residir en un switch de la capa de distribución que agrega la conectividad a la capa de acceso LAN tal como se ilustra en la figura 2.20. (CISCO, 2022)

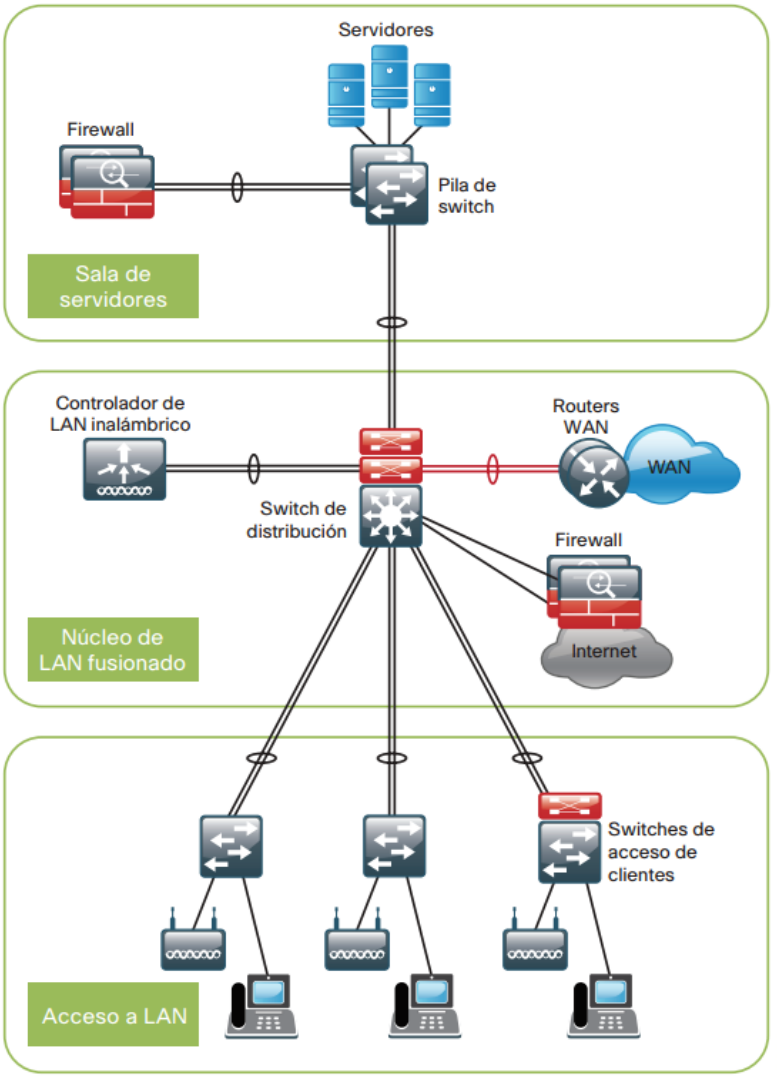


Figura 2.20: *Diseño de dos capas.*
Fuente: **(CISCO, 2022)**

2.9.2.2. Diseño de tres capas.

En redes más grandes debe existir una capa de distribución exclusiva para los servicios. Esto debido a que a medida que crezcan los servicios o se implementen dispositivos la capacidad de conectarse a un solo switch de la capa de distribución se vuelve más complicado de llevarlo a cabo de manera física y lógica. Por lo cual debe existir una capa para el núcleo de la red de la cual se deriven el resto de las capas tal cual se visualiza en la figura 2.21. (CISCO, 2022)

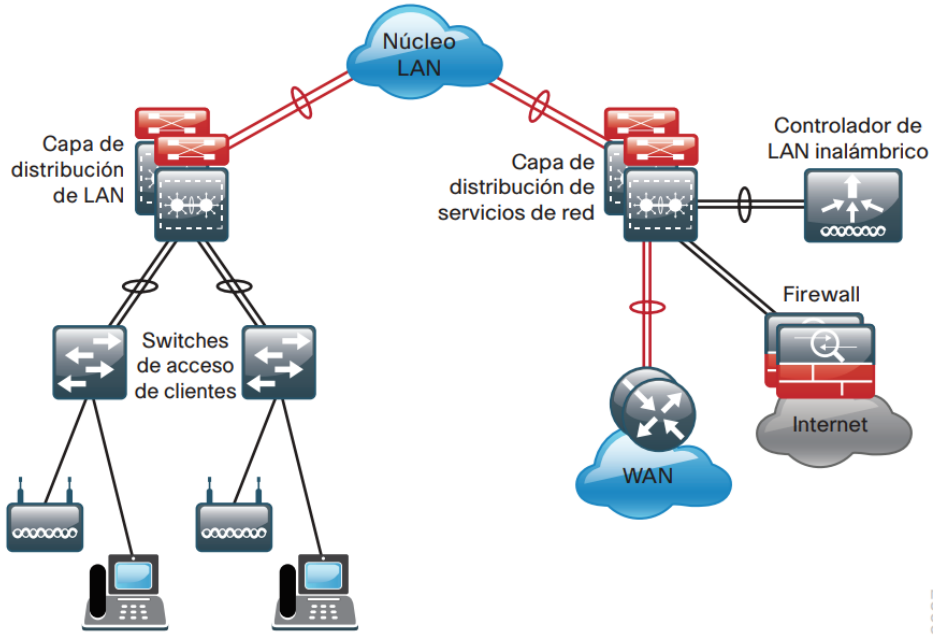


Figura 2.21: *Diseño de tres capas.*
Fuente: **(CISCO, 2022)**

2.9.3. Capa central.

En ecosistemas de red en los cuales existen múltiples Switches de capa de distribución próximos entre sí y en lo que la fibra óptica ofrece capacidad de interconexión de banda de alta velocidad la implementación se vuelve más sencilla y económica al tener un núcleo, ya que se pasaría de un modelo como se muestra en la figura 2.22 en el cual todos se conectan con todos, siendo esto más costoso y poco escalable, al segundo modelo de la figura 2.23, donde se tiene un núcleo central como pieza fundamental de la red. (CISCO, 2022)

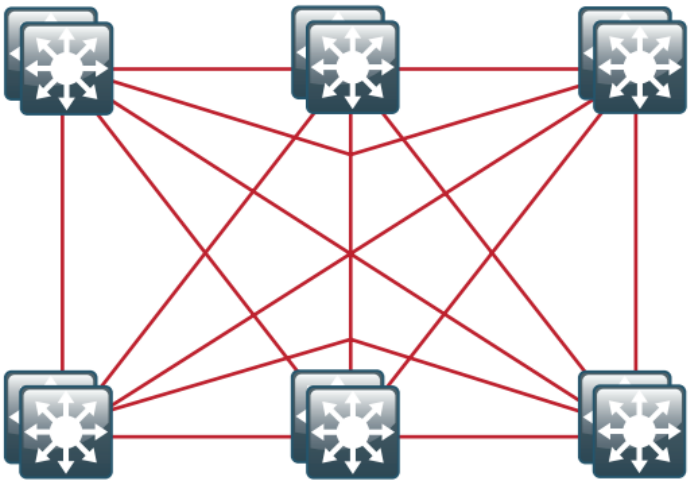


Figura 2.22: *Modelo de red malla sin núcleo.*
Fuente: **(CISCO, 2022)**

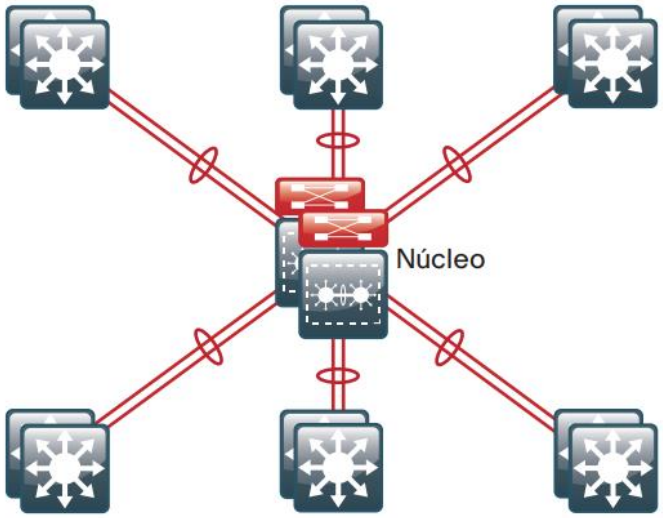


Figura 2.23: *Modelo de red con núcleo.*
Fuente: **(CISCO, 2022)**

2.10. Redes LAN inalámbricas

2.10.1. Topología de una Red LAN inalámbrica.

En la red inalámbrica, los medios se comparten entre todos los emisores y receptores de datos a través de la red, por lo que los dispositivos deben transmitir dentro de un tiempo determinado para no colisionar entre sí, esta técnica se define en el estándar 802.11. Y esto seguro te sonará en alguna parte, sí, esta técnica también se usa en una LAN Ethernet tradicional (sin switch), por ejemplo, cuando se tiene un hub semidúplex, cada dispositivo debe esperar su turno para transmitir y así evitar colisiones. IEEE 802.11 WLAN siempre es semidúplex porque las

transmisiones entre estaciones usan la misma frecuencia o canal. Solo se puede transmitir una estación a la vez; de lo contrario, se produce una colisión. Para lograr el modo dúplex completo, la transmisión de una estación debe ocurrir en una frecuencia mientras la recepción se realiza en otra, tal como funcionan los enlaces Ethernet dúplex completo. Si bien esto es ciertamente posible y práctico, el estándar 802.11 no permite la operación de dúplex completo. Algunas modificaciones al estándar permiten que múltiples dispositivos transmitan en el mismo canal al mismo tiempo, pero eso está más allá del alcance de este curso. (Cisco, 2020)

2.10.1.1. Conjunto de servicios básicos (BSS).

Existe un conjunto básico de servicios para el funcionamiento de una red inalámbrica. El estándar 802.11 lo llama Conjunto básico de servicios (BSS). El corazón del BSS es el punto de acceso inalámbrico (AP). El AP proporciona los servicios necesarios para la infraestructura de la red inalámbrica. AP y miembro BSS deben usar el mismo canal de comunicación. BSS depende del AP y, por lo tanto, está limitado al área cubierta por la señal del AP. Esto se llama el Área de Servicio Básico o BSA. Este espacio, al que se llama celda, puede adoptar diferentes formas según el tipo de antena. Los puntos de acceso utilizan un identificador BSS único (BSSID) basado en la dirección MAC del punto de acceso, tal como se muestra en la figura 2.24. (Cisco, 2020)

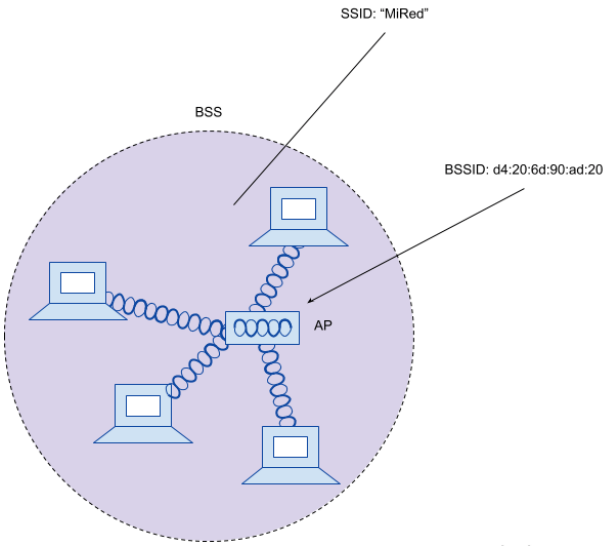


Figura 2.24: *Conjunto de servicios básicos (BSS).*
Fuente: **(Cisco, 2020)**

Además, el AP anuncia la red mediante un SSID (Identificador de grupo de servicio) que es un texto que contiene el nombre lógico de la red. La membresía del

BSS se llama asociación. Un dispositivo inalámbrico solicita asociación con el punto de acceso, el punto de acceso debe aceptar o rechazar la solicitud. Una vez vinculado, el dispositivo se convierte en cliente o estación 802.11 (STA) del BSS. Para mantener la estabilidad de la red y el control del BSS, todas las comunicaciones de los dispositivos inalámbricos deben pasar por un punto de acceso. Por lo tanto, no es posible que dos dispositivos se envíen información directamente entre sí. (Cisco, 2020)

En resumen, AP (Access Point): Proporciona los servicios necesarios para la infraestructura de la red inalámbrica. BSS (Conjunto Básico de Servicios): Dentro del BSS existe un AP (Punto de Acceso). BSA (Área de Servicio Básico): Esta es el área cubierta por el AP. BSSID: Este es el identificador del AP basado en su MAC. SSID: Cadena de texto que identifica lógicamente el punto de acceso. STA: La asociación que cualquier dispositivo establece con el punto de acceso. (Cisco, 2020)

2.10.1.2. Sistema de distribución (DS).

Cuando un dispositivo quiere comunicarse con otro dispositivo fuera de su BSS, debe usar lo que se define en el estándar 802.11 como DS (Sistema de distribución) similar al ilustrado en la figura 2.25, que es un enlace por cable ascendente. Para hacer esto, el punto de acceso maneja el mapeo de una VLAN en el SSD. (Cisco, 2020)

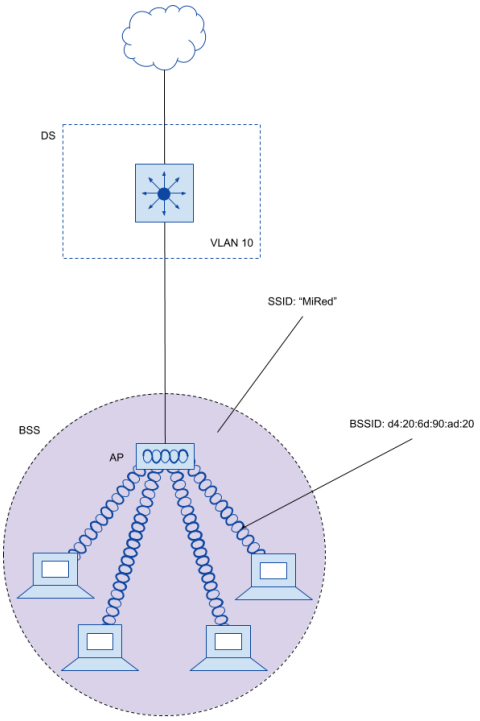


Figura 2.25: *Sistema de distribución.*
Fuente: **(Cisco, 2020)**

Este concepto se puede extender a múltiples SSID. Para hacer esto, cree un tronco VLAN con diferentes VLAN para cada SSID. Por ejemplo, en la figura 2.26, se ve que la VLAN 10 corresponde al SSID “MyNetwork”, la VLAN 20 corresponde al SSID “YourNetwork” y la VLAN 30 corresponde al SSID “Guest”. (Cisco, 2020)

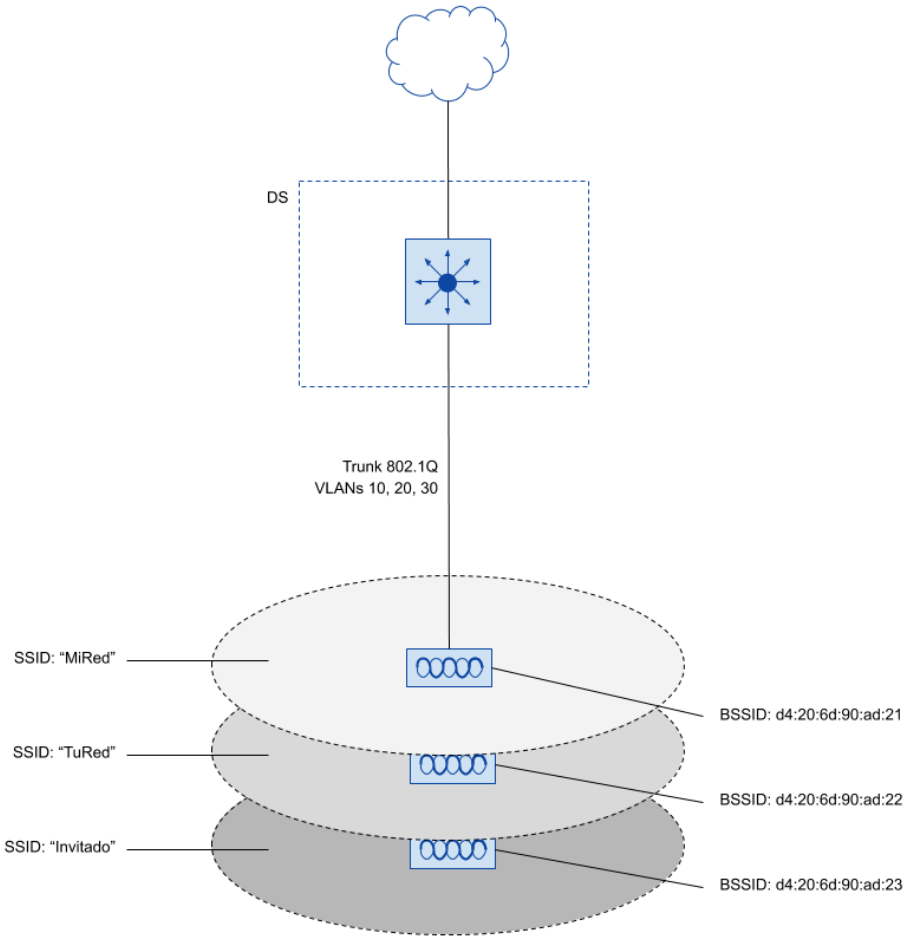


Figura 2.26: *Múltiples SSIDs.*
Fuente: **(Cisco, 2020)**

2.10.1.3. Conjunto de servicios extendidos (ESS)

Un solo punto de acceso a menudo no puede cubrir toda el área que un cliente necesita cubrir. Por ejemplo, si el cliente quiere cubrir todo el piso de un hotel, hospital o edificio grande. Para ello, se puede utilizar más de un punto de acceso, es decir, varias celdas separadas geográficamente. Cuando varios puntos de acceso están ubicados en diferentes lugares, pueden conectarse entre sí mediante un interruptor. El estándar 802.11 llama a este ESS (Extended Set of Services o en español, Extended Service Set). Idealmente, el SSID definido en un punto de acceso se utiliza para todos los puntos de acceso y evitar que los clientes tengan que reconfigurar sus dispositivos cada vez que se mueven a otra celda en la red con un SSID diferente.

Tenga en cuenta que, aunque el SSID puede ser el mismo, el BSSID siempre es diferente porque identifica físicamente el AP. (Cisco, 2020)

De esta forma el cliente puede moverse de celular en celular sin "darse cuenta" porque no tiene que reconfigurar, esto se llama roaming. Tenga en cuenta que cada AP proporciona su propio BSS en su propio canal para evitar interferencias, lo hace porque busca diferentes canales utilizados por el BSS. Finalmente, el cliente cambia de BSS a BSS, de canal a canal tal como se muestra en la figura 2.27. (Cisco, 2020)

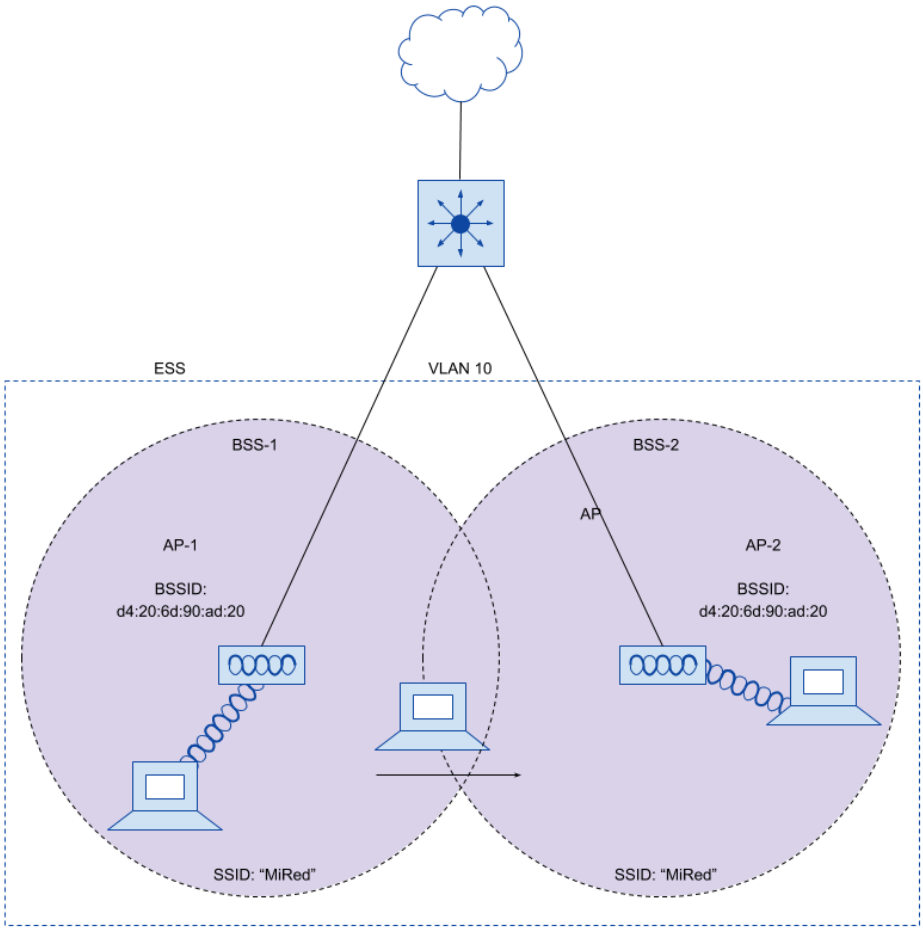


Figura 2.27: *Conjunto de servicios extendidos.*
Fuente: **(Cisco, 2020)**

2.10.1.4. Conjunto de servicios básicos independientes (IBSS)

En general, en las redes inalámbricas, los puntos de acceso se utilizan para la organización, control y escalabilidad de la red. Pero a veces eso no es posible o conveniente en una situación particular. Por ejemplo, dos personas quieren intercambiar documentos electrónicamente y no encuentran ningún BSS disponible o quieren evitarlo para no autenticarse en la red. El estándar 802.11 permite que dos

o más clientes se comuniquen directamente entre sí, esto se denomina ad-hoc o IBSS (Conjunto Básico Independiente de Servicios). (Cisco, 2020)

2.10.1.5. Repetidor.

Por lo general, cada punto de acceso tiene un conector cableado (DS) que se puede conectar a otro punto de acceso para ampliar el espectro geográfico cubierto por la celda. Pero en algunos casos esto no es posible porque, por ejemplo, el cable necesario es demasiado largo para admitir la comunicación Ethernet. En este caso se puede utilizar un punto de acceso configurado en modo repetidor. El repetidor inalámbrico toma la señal que recibe y la repite o retransmite a una nueva celda alrededor del repetidor tal como se muestra en la figura 2.28. (Cisco, 2020)

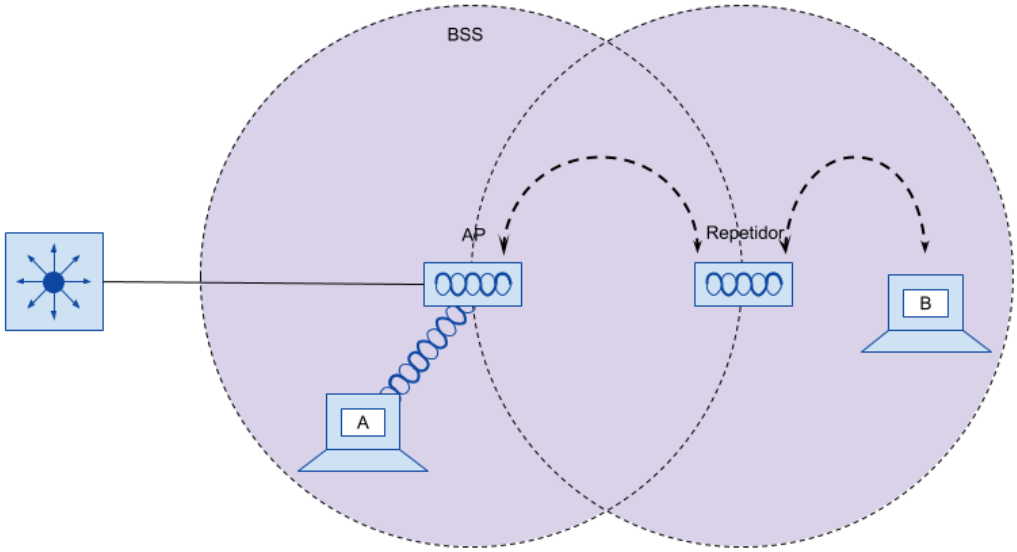


Figura 2.28: *Repetidores inalámbricos.*
Fuente: **(Cisco, 2020)**

2.10.1.6. Puente de grupo de trabajo (WGM).

WGM se conecta a un dispositivo que no tiene una conexión inalámbrica a la red inalámbrica. Por ejemplo, en la figura 2.29 se ilustra un dispositivo que no tenga una conexión inalámbrica conectado a la red, en cuyo caso se utiliza el dispositivo WGB para conectar el dispositivo a la red inalámbrica. (Cisco, 2020)

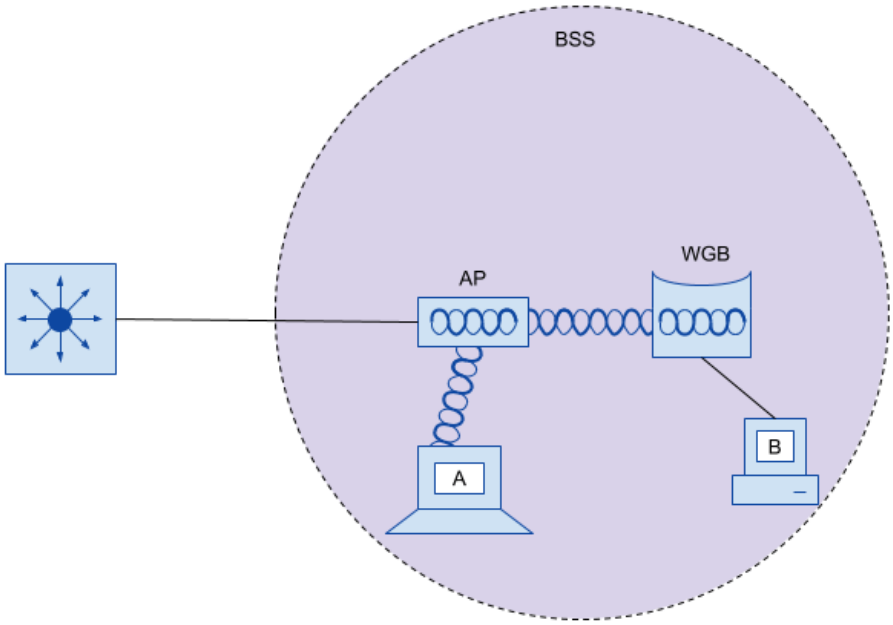


Figura 2.29: *Puente de grupo de trabajo.*
Fuente: **(Cisco, 2020)**

Puede encontrar dos tipos de Workgroup Bridges:

- Workgroup Bridges (uWGB): un solo cable desde un dispositivo que se puede conectar a una red inalámbrica.
- Workgroup Bridge (WGB): una implementación patentada de Cisco que permite que varios dispositivos cableados se unan a una red inalámbrica.

2.10.1.7. Puente al Aire Libre (BO).

Los puentes exteriores se utilizan a menudo para conectar edificios o ciudades, tal como se muestra en la figura 2.30. Se requiere un punto de acceso configurado en modo puenteado en cada extremo. Las antenas conectadas a un puente se utilizan normalmente para dirigir las señales en una dirección. Esto maximiza la distancia.

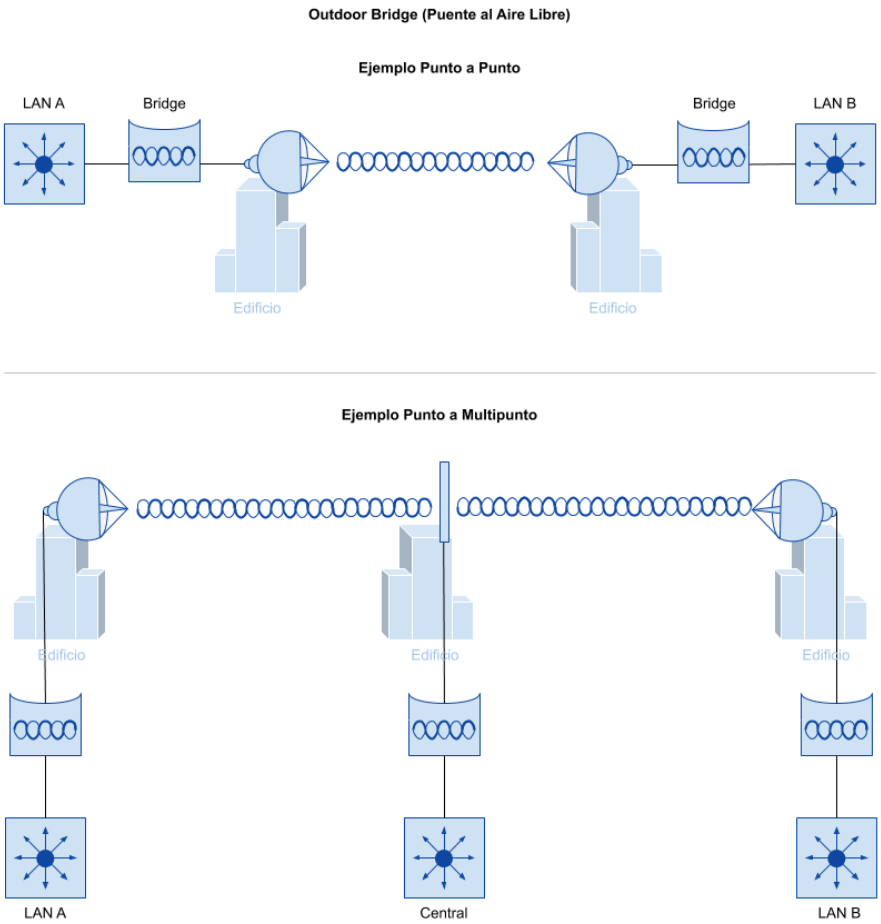


Figura 2.30: *Puente al aire libre.*
Fuente: **(Cisco, 2020)**

2.10.1.8. Red Mallada (Mesh Network).

Para proporcionar una amplia cobertura, no es práctico conectar puntos de acceso cableados entre sí. En su lugar, puede utilizar varios puntos de acceso configurados en modo de malla tal como se ilustra en la figura 2.31. (Cisco, 2020)

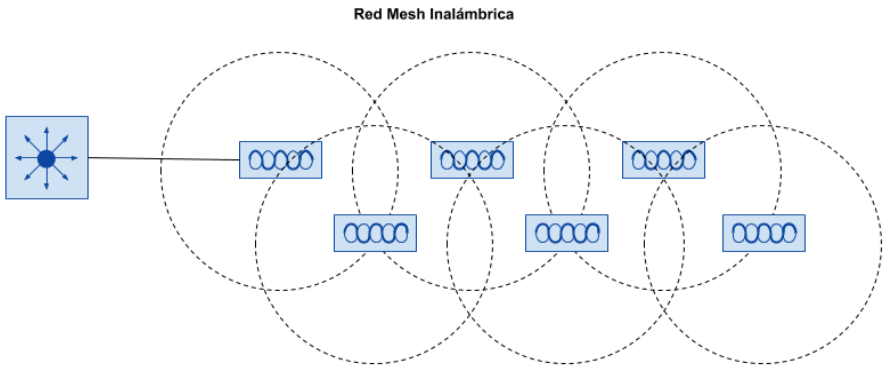


Figura 2.31: *Red mesh.*
Fuente: **(Cisco, 2020)**

2.10.2. Wireless LAN Controllers (WLC).

Los dispositivos WLC sirven para centralizar la configuración y control de los puntos de acceso inalámbricos, permitiendo que la red funciones como una red de información inteligente capaz de tolerar servicios avanzados. (CISCO, 2022)

- Dentro las características que otorgan los WLC están:
- Menores gastos operativos: Permite la implementación de configuraciones automatizadas para los puntos de accesos.
- Mejor retorno de la inversión: Permite implementar instancias virtualizadas del controlador LAN inalámbrico reduciendo el costo total gracias a que ya no se necesitaría hardware adicional para esa labor.
- Escalamiento más simple con diseño óptimo: Permite que la red escale al admitir diseños de modo local para entornos de campus.
- Conmutación activa con alta disponibilidad: Permite la conectividad sin interrupciones con los dispositivos inalámbricos que funcionan como clientes.

Los WLC son los encargados de las funciones WLAN de un sistema, funciones tales como: políticas de seguridad, prevención de intrusiones, QoS y cobertura para una movilidad total dentro del área de cobertura. Trabajan en conjunto con los puntos de acceso ligero, permitiendo el flujo desde servicios de voz hasta servicios de localización. (CISCO, 2022)

2.10.2.1. WLC Centralizado.

Una opción es colocar el WLC en el centro para maximizar la cantidad de puntos de acceso conectados al controlador. Esto a menudo se denomina implementación de WLC unifield o centralizada. La figura 2.32 muestra un ejemplo de un WLC enfocado. (Cisco, 2020)

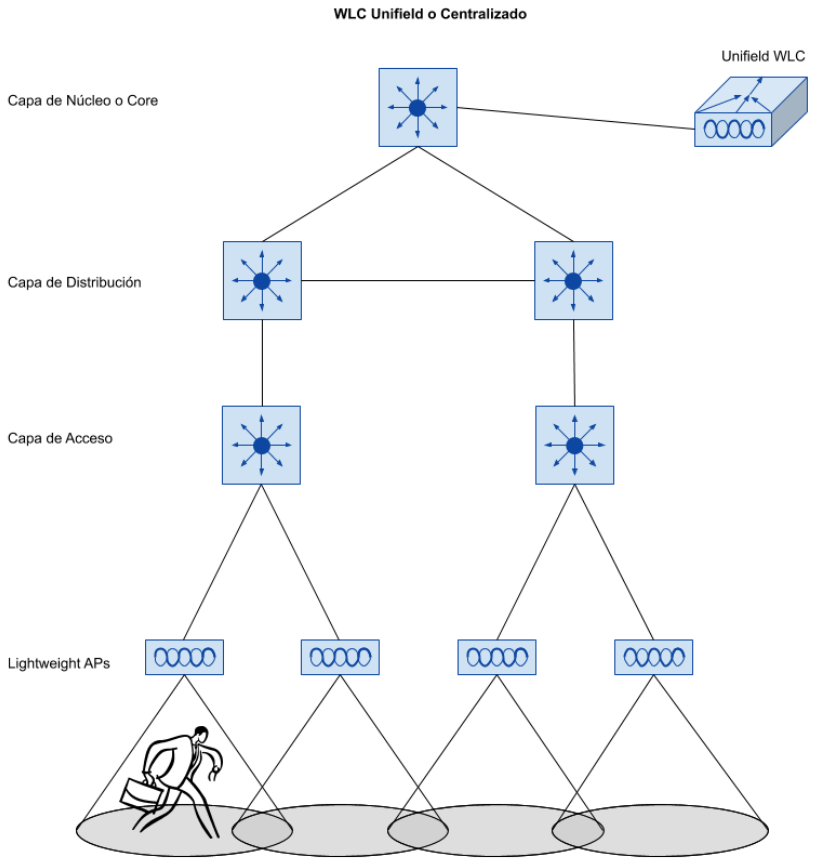


Figura 2.32: *WLC centralizado.*
Fuente: **(Cisco, 2020)**

2.10.2.2. WLC en la nube.

WLC existe como una máquina virtual en lugar de un dispositivo físico. Si ya existe una plataforma en la nube, es fácil implementar un WLC basado en la nube. Si su red inalámbrica supera esta escala, se pueden agregar WLC adicionales como máquinas virtuales tal como se ejemplifica en la figura 2.33.

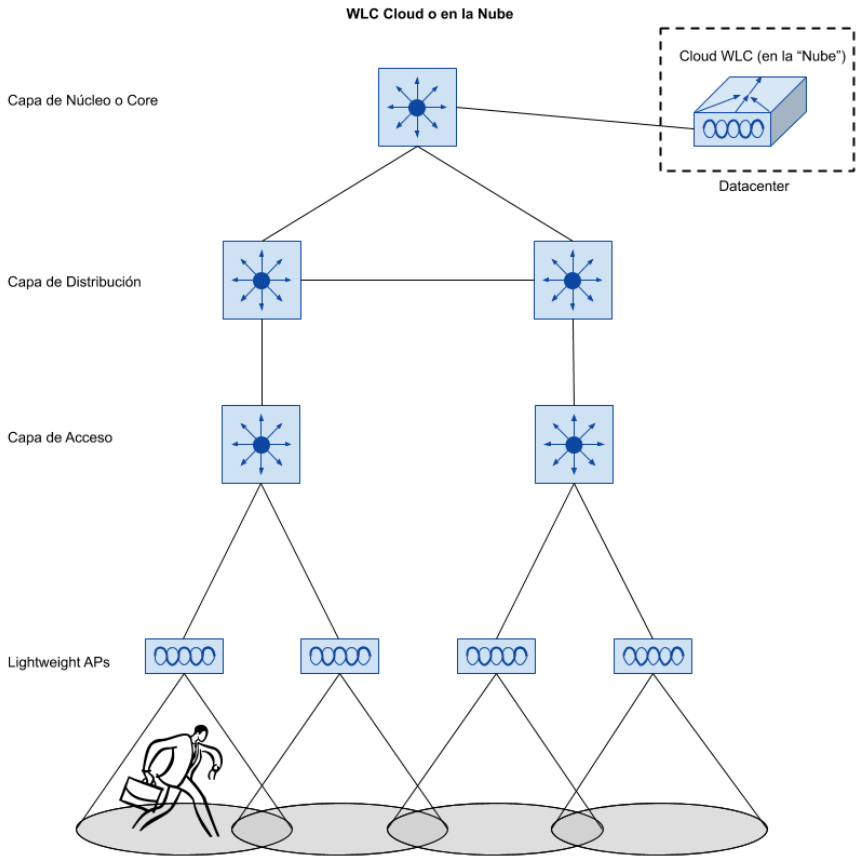


Figura 2.33: *WLC en la nube.*
Fuente: **(Cisco, 2020)**

2.10.2.3. WLC incrustado.

Para campus pequeños o sucursales distribuidas donde la cantidad de puntos de acceso es relativamente baja, el WLC se puede combinar con conmutadores, obteniendo un diseño similar al ilustrado en la figura 2.34. Se llama integrado o integrado porque está apilado en el conmutador. A medida que aumenta la cantidad de puntos de acceso, se pueden agregar WLC adicionales integrándolos en otros conmutadores de la pila.

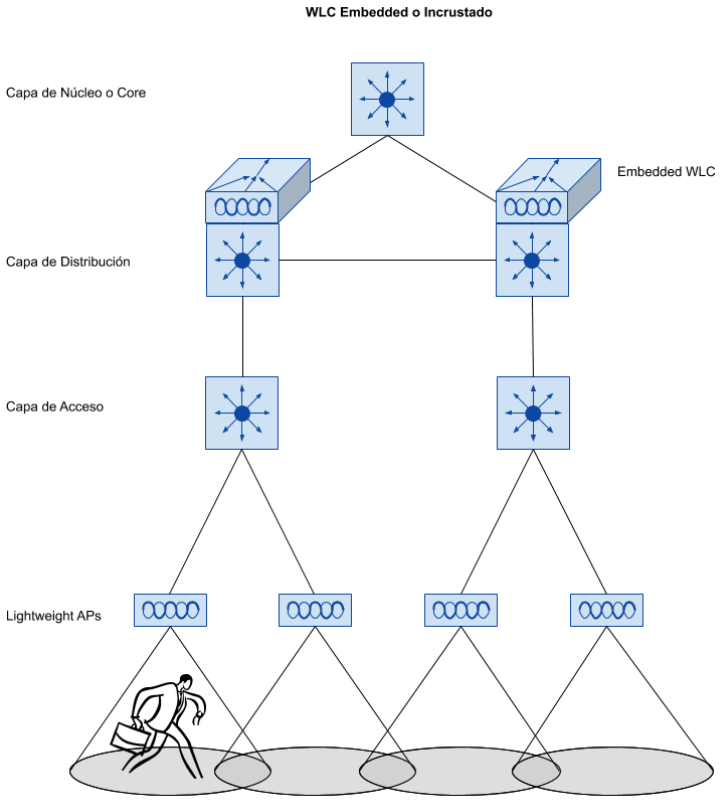


Figura 2.34: *WLC incrustado.*
Fuente: **(Cisco, 2020)**

2.10.2.4. WLC movilidad rápida.

Finalmente, en entornos de pequeña escala, como sucursales pequeñas y medianas o ubicaciones múltiples, es posible que no desee invertir en WLC dedicados. En este caso, la función WLC se puede asociar con un punto de acceso instalado en la ubicación de la sucursal. Esto se denomina implementación de WLC de Cisco Mobility Express. WLC host AP forman un túnel CAPWAP con WLC, junto con todos los demás AP en la misma ubicación, tal como se ilustra en la figura 2.35. (Cisco, 2020)

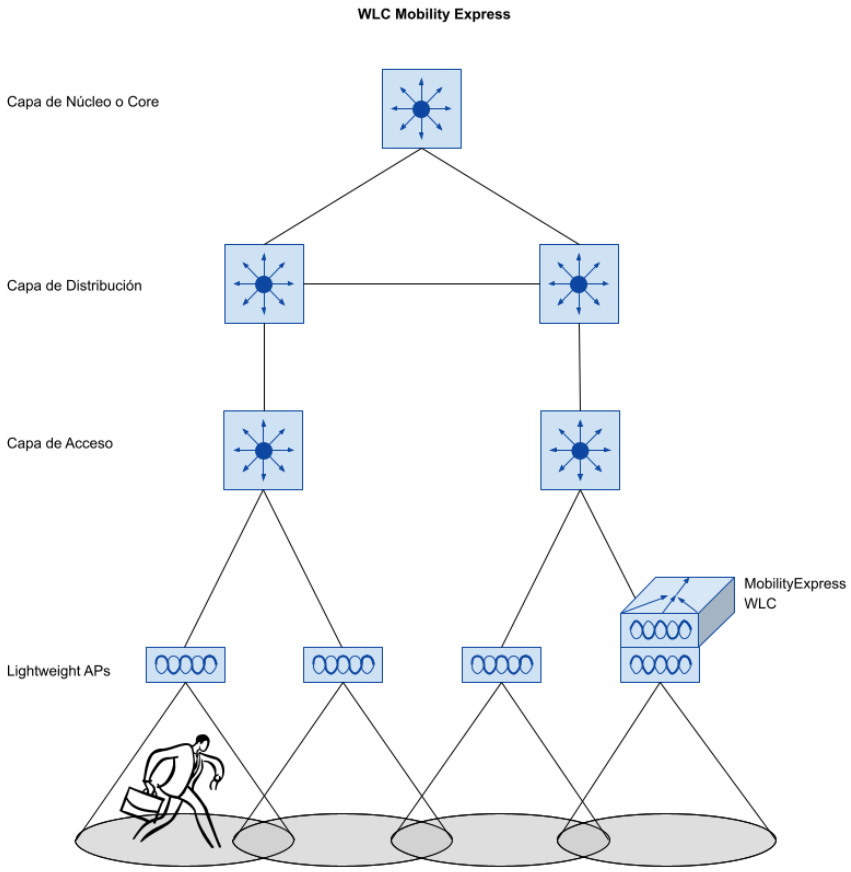


Figura 2.35: *WLC movilidad rápida.*
Fuente: **(Cisco, 2020)**

2.10.3. Puntos de Acceso Ligero.

Los puntos de acceso ligero forman parte de la arquitectura de un WLAN sin embargo no pueden operar sin un WLC, en la figura 2.36 se muestra un esquema de ejemplo. El punto de acceso ligero obtiene toda la información necesaria desde el WLC, desde su configuración hasta sincronización de firmwares. Los puntos de acceso ligero suelen implementarse en pares, para tener recuperabilidad, adicionalmente se usa un sistema de controlador primario/secundario en el cual todos los puntos de acceso prefieren unirse al controlador principal y solo se unen al secundario en caso de falla. (CISCO, 2022)

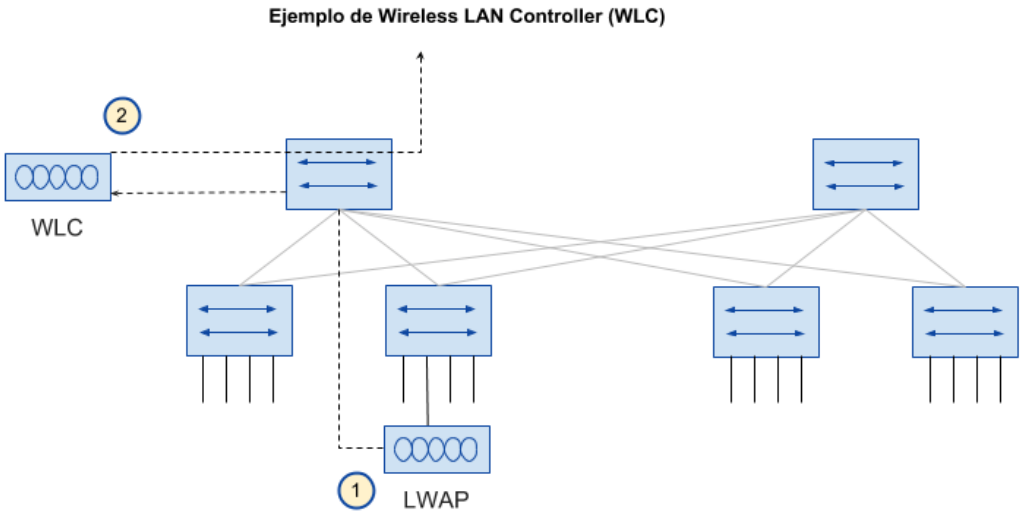


Figura 2.36: WLC esquema ejemplo
Fuente: **(Cisco, 2020)**

2.10.3.1. Modo Local.

El modo ligero predeterminado proporciona uno o más BSS que operan en un canal específico. Durante el tiempo que no está transmitiendo, el punto de acceso escanea otros canales para medir los niveles de interferencia, medir la interferencia, detectar dispositivos no deseados y compararlos con los eventos del sistema de detección de intrusos (IDS).

2.10.3.2. Modo Monitor.

El punto de acceso no transmite nada, pero su receptor se activa para actuar como un sensor dedicado. El punto de acceso busca eventos IDS, detecta puntos de acceso no autorizados y determina las ubicaciones de las estaciones a través de servicios basados en la ubicación.

2.10.3.3. Modo Flexconnect.

Un punto de acceso en un sitio remoto puede intercambiar tráfico localmente entre el SSID y la VLAN si su túnel CAPWAP al WLC está inactivo y si está configurado para hacerlo.

2.10.3.4. Modo Sniffer.

Un punto de acceso dedicado a sus radios para recibir tráfico 802.11 de otras fuentes, como rastreadores o dispositivos de captura de paquetes. El tráfico

resultante se transmitirá a una PC que ejecute un software de análisis de red como Wildpackets OmniPeek o WireShark, donde se puede analizar más a fondo.

2.10.3.5. Modo Rogue Detector.

Un punto de acceso funciona para detectar dispositivos maliciosos al correlacionar las direcciones MAC que escucha en una red cableada con las que escucha directamente. Los dispositivos maliciosos son aquellos que aparecen en ambas redes.

2.10.3.6. Modo Bridge.

Un punto de acceso se convierte en un puente dedicado (punto a punto o punto a multipunto) entre dos redes. Se pueden usar dos puntos de acceso en modo puente para conectar dos ubicaciones que están separadas por una distancia. Múltiples puntos de acceso en modo puente pueden formar redes interiores o exteriores.

2.10.3.7. Modo Flex+Bridge.

Las operaciones de FlexConnect se activan en un punto de acceso de malla.

2.10.3.8. Modo SE-Connect.

Punto de acceso radio dedicado para análisis de espectro en todos los canales inalámbricos. Puede conectar de forma remota un software de PC en ejecución, como MetaGeek Chanalyzer o Cisco Spectrum Expert, a un punto de acceso para recopilar y analizar datos de análisis de espectro para detectar fuentes de interferencia.

2.11. Servidores y servicios

Dentro de la estructura de una red deben coexistir una serie de servicios, los cuales son alojados en clústers o también llamados granjas de servidores, en caso de ser servicios ligeros un servidor podría alojar múltiples de este tipo, caso contrario el número de servidores que conforman el clúster aumentará, algunos de los servicios necesarios en la red son los siguientes:

2.11.1. Servidor DNS.

El sistema de nombres de dominio o DNS es similar al directorio telefónico, permite asociar direcciones IPs a nombres o “dominios”, de tal manera que es usuario solo escriba el nombre de interés y sea redirigido a la página o dirección IP.

2.11.2. Servidor HTTP.

El protocolo de transferencia de hipertexto permite navegar en páginas web.

2.11.3. Servidor Mail.

El servicio de mail sirve permite levantar un dominio propio para un sistema de mensajería.

2.11.4. Servidor FTP y SFTP.

“File Transfer Protocol” y “SSH File Transfer Protocol” son protocolos que permiten realizar el envío y recepción de archivos entre varios ordenadores.

2.11.5. Servidor IoT.

Un servidor IoT permite realizar telemetría y telecontrol con la ayuda de sensores y actuadores que se encuentren conectados a la red y sincronizados con el servicio o servidor IoT.

CAPÍTULO 3: DISEÑO, SIMULACIÓN Y RESULTADOS.

En este capítulo se presentará los detalles para la simulación y diseño de la red de datos, finalmente se mostrará el dimensionamiento, segmentación de la red, protocolos y tecnologías usadas.

3.1. Descripción general y territorial de la empresa Metalmax

Para el desarrollo de la red se debe conocer la ubicación geográfica de la empresa Metalmax, la cual se encuentra ubicada en la vía a Daule km 27,5 de la ciudad de Guayaquil. La figura 3.1 muestra la ubicación geográfica de la empresa, (rectángulo rojo) obtenida por Google Earth y sus coordenadas de posición (latitud y longitud) usadas son: (-1.9821881, -79.9950399). Ubicándose junto al hotel “The Secret” (rectángulo morado), a aproximadamente 400 metros de la “Facultad de Medicina Veterinaria y Zootecnia” (rectángulo verde) y a 100 metros de “La mansión Night Club” (rectángulo amarillo).

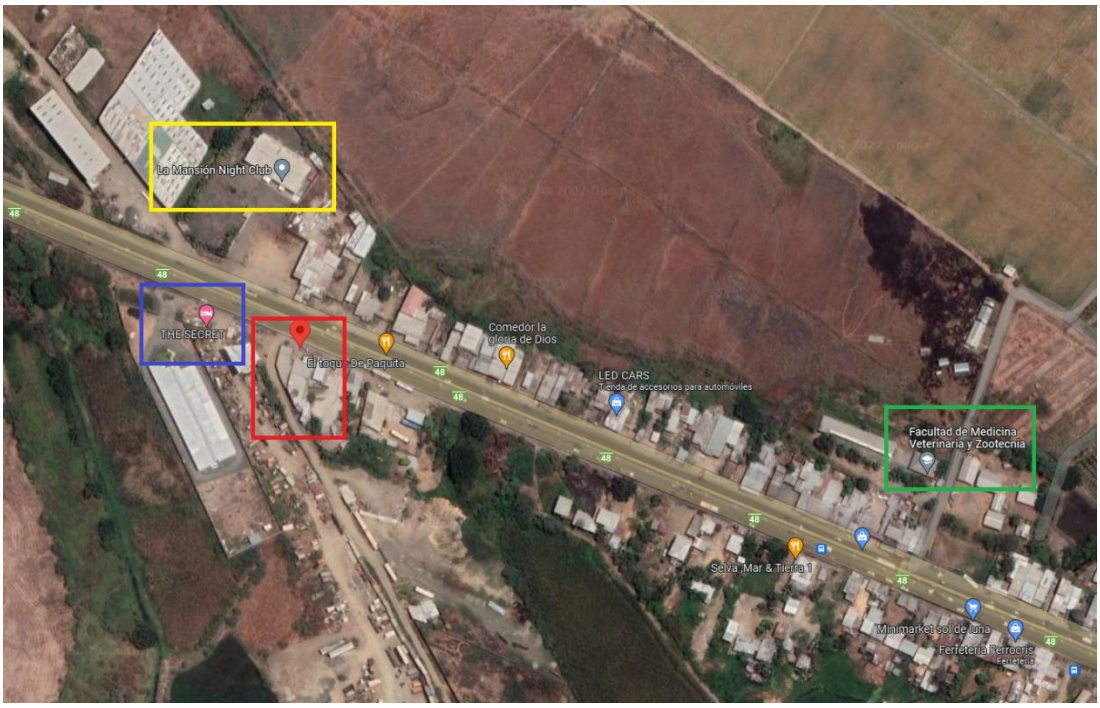


Figura 3.1: Ubicación geográfica de la empresa Metalmax
Fuente: Autor

3.2. Distribución de departamentos

La empresa consta de 5 departamentos: Financiero, Operaciones, recursos humanos, informática y administrativo, cada departamento consta de entre 5 y 10 personas, para prevenir la escasez de IPs disponibles en un futuro los departamentos

deberán tener al menos “N” cantidad de IPs disponibles. Para esto se debe saber que actualmente los departamentos constan con la siguiente cantidad de empleados:

- Informática: 2.
- Financiero: 3.
- Recursos humanos:4.
- Administrativo: 4.
- Operaciones:15.

Existe la posibilidad de que cada persona tenga hasta 4 dispositivos entre la computadora personal, computadora del trabajo, celular y otro dispositivo adicional como Tablet, motivo por el cual se necesitaría al menos la siguiente cantidad de IPs por departamento, resultante del número base de personas del departamento por un factor multiplicativo de 4.

- Informática: 8.
- Financiero: 2.
- Recursos humanos: 16.
- Administrativo: 16.
- Operaciones: 60.

3.3. Distribución de VLANs

Para cada departamento se asignará una VLAN específica de tal manera que exista un orden y adicional en caso de fallos se pueda llegar de forma rápida a la raíz del problema. Adicional a los departamentos se debe implementar una VLAN para administración de la red y también una para los visitantes o usuarios que necesitan conectarse a la red, pero no forman parte de la empresa. A continuación, detallaré la distribución de VLANs de cada departamento con su respectivo “VLAN ID”:

- VLAN para administración de red: 10.
- Informática: 2.
- Financiero: 3.
- Recursos humanos: 4.
- Administrativo: 5.
- Operaciones:6.
- Visitantes: 7.

Con la segmentación mencionada se tendrá una disponibilidad de 256 direcciones donde 254 serán hosts válidos para su uso en cada departamento. Con lo cual en caso de sumar dispositivos IPs en cualquier departamento estos tendrían asignada una IPs de forma automática gracias al servicio de DHCP de la red y la disponibilidad de direcciones. Adicionalmente la red constará de al menos 1 punto de acceso ligero por cada departamento de tal manera que se tendría una cobertura total de la WLAN, adicional a esto en cada switch departamental se puede implementar un punto de acceso en un futuro en caso de ser necesario.

3.4. Distribución de los segmentos de red

La distribución de los segmentos de red será realizada acorde a los departamentos y VLANs asignadas anteriormente en los puntos 3.2 y 3.3, a continuación, en la tabla 3.1 se muestra las divisiones de la red.

Tabla 3.1: Distribución de los segmentos de red.

Departamento	VLAN	Red	Prefijo de red CIDR
Informática	2	192.168.2.0	/24
Financiero	3	192.168.3.0	/24
Recursos humanos	4	192.168.4.0	/24
Administrativo	5	192.168.5.0	/24
Operaciones	6	192.168.6.0	/24
Visitantes	7	192.168.7.0	/24
Administración-VLAN nativa	10	10.0.0.0	/24

Fuente: Autor

3.5. Diseño de la red de datos

Para el diseño de la red se seguirá un modelo jerárquico de tres capas, en el cual se tendrá una capa de distribución y administración para servicios y por otro lado una para la distribución de los departamentos, de tal manera que a medida que crezcan los servicios o se implementen dispositivos la capacidad de conectarse no se vea comprometida. Por lo cual en el diseño propuesta se implementa una capa principal como núcleo de la red, de donde se deriva el resto de las capas como se puede observar en la figura 3.2, donde del núcleo se despliegan: capa de distribución de la red (VLANs) y la capa de distribución para los servicios.

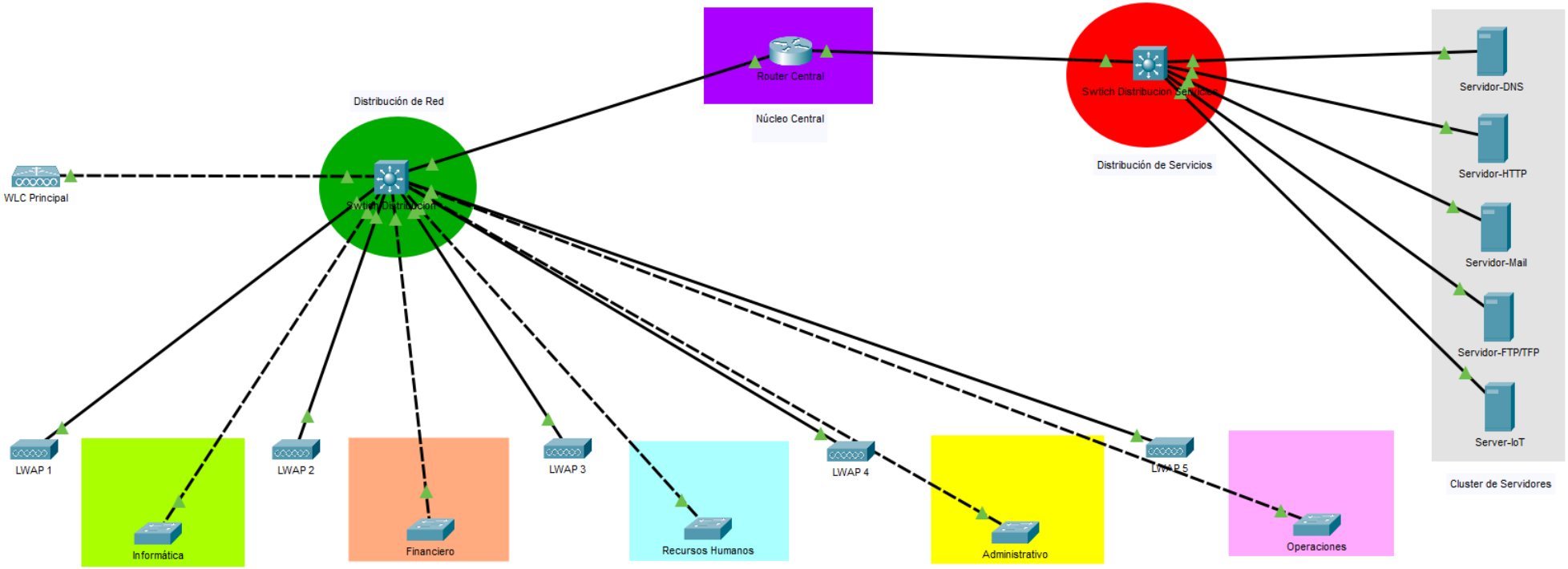


Figura 3.2: Diagrama del diseño de la red.
Fuente: Autor

En la figura 3.2 se ilustró el despliegue de las zonas de distribución de servicios (Ovalo Rojo) y zona de distribución de red (Ovalo Verde) que se derivan del núcleo central de la red (rectángulo morado). Desde el switch de distribución de servicios (Ovalo Rojo) nacerá el clúster de servidores (Rectángulo gris) donde se alojarán los servicios de DNS, HTTP, Mail, IoT, FPT, entre otro que sean necesarios en la red. Finalmente, desde el switch de distribución de red (Ovalo Verde) se derivarán los switches departamentales y los puntos de acceso ligeros que son administrados desde el WLC principal.

Figura 3.3: Referencia de colores usados para las VLAN en el diagrama
Fuente: Autor

En la figura 3.3 se ilustran los colores referenciales usados en el diagrama de la red, de tal manera que se entienda que cada router departamental se encuentra asignado a una VLAN distinta e independiente.

3.5.1. Descripción del diseño de las capas.

Se tiene una capa de distribución LAN, la cual tiene como núcleo un conmutador de capa 3, figura 3.4, para mejorar la velocidad de respuesta y permitir switches de acceso múltiple. Este se encuentra operando como un servidor VTP, de tal manera que se encargará de manejar, distribuir y actualizar la información de las VLANs existentes al resto de conmutadores que se derivan de este, de tal manera que se tendrá una red actualizada y convergente.

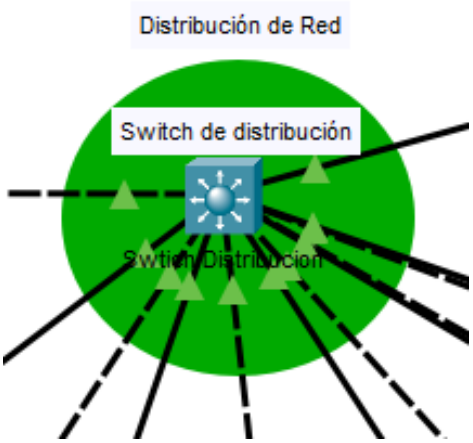


Figura 3.4: Conmutador para distribución LAN.
Fuente: Autor

A su vez se tendrá un Wireless Lan Controller (WLC), figura 3.5, que se encargue de administrar las distintas VLANs provisionadas por el switch de distribución de red y posteriormente distribuirlas a los puntos de acceso ligeros (LWAP), de tal manera que las distintas VLANs se encuentren disponibles en toda el área de la empresa y sin importar de que departamento sea la persona pueda accesar a la red desde sus dispostivos. Para asegurar esto se debe trabajar con los puntos de acceso ligeros ilustrados en la figura 3.6 que son los encargados de obtener las configuraciones y VLANs establecidas en el conmutador raíz de distribución y administradas por el WLC de la figura 3.5.

Figura 3.5: WLC para LAN.
Fuente: Autor

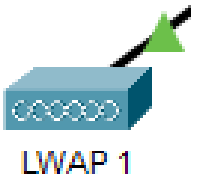


Figura 3.6: Punto de accesos ligeros.
Fuente: Autor

Por otro lado, se tendrá a un conmutador también de capa 3 encargado de la distribución de los servicios de la red, tal como se observa en la figura 3.7, donde se derivan servicios de DNS, HTTP, Mail, SFTP, FTP y otros que son necesarios en el despliegue de la red empresarial.

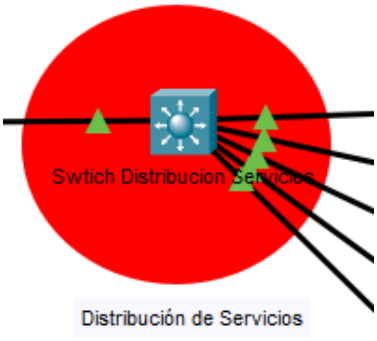


Figura 3.7: Conmutador para distribución de servicios.
Fuente: Autor

Todos los servicios mencionados anteriormente serán alojados en un clúster de servidores, figura 3.8, que si bien es cierto que están representados de forma física quizás en un futuro se podría migrar ciertos servicios a la nube optimizando la red y simplificando su manejo.

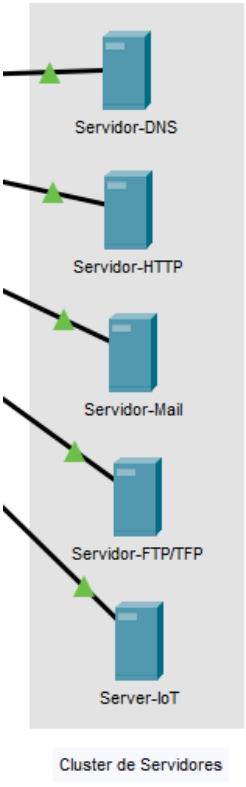


Figura 3.8: Clúster de servidores.
Fuente: Autor

Cada switch departamental fue referenciado con un color, tal como se menciona en la figura 3.3 anteriormente, de tal manera que en la figura 3.9 y 3.10 se diferencia cada conmutador departamental y aprecia a que VLAN pertenece. Estos conmutadores son de capa 2, a diferencia del conmutador raíz de esta área que es de capa 3, esto debido a que el nodo raíz tendrá más carga de procesamiento que los conmutadores departamentales, los cuales solo obtendrán la información procesada por el switch de distribución que se encuentra operando como servidor VTP.

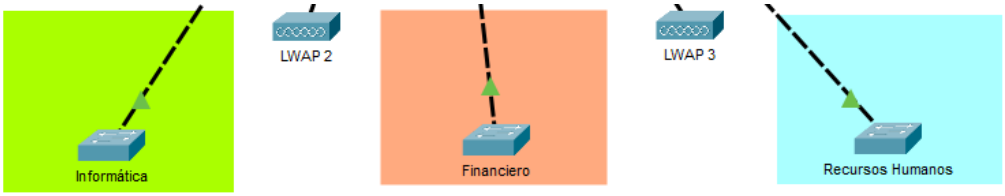


Figura 3.9: Conmutadores departamentales.
Fuente: Autor

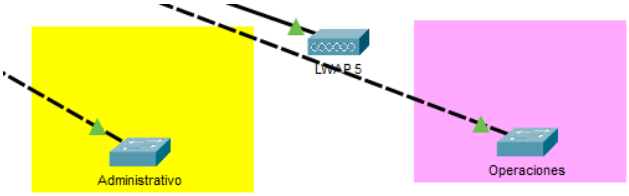


Figura 3.10: Conmutadores departamentales.
Fuente: Autor

Finalmente se tiene al núcleo principal que es un Router, figura 3.11, capaz de administrar el tráfico de la red, en este caso el de las VLANs que coexisten en la red, haciendo uso de enrutamiento intra-VLAN y encapsulamiento dot1Q. Dado que por una misma interfaz se enrutará distintas VLANs al mismo tiempo sin afectar el funcionamiento de la red.

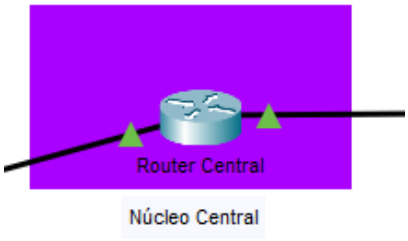


Figura 3.11: Conmutador para distribución de servicios.
Fuente: Autor

3.6. Configuraciones propuestas para los equipos principales.

Dentro del diseño de la red se deben tener en cuenta parámetros operacionales los cuales son establecidos mediante configuraciones en los nodos principales de la red para ser distribuidos a los nodos clientes de la misma. A continuación, se expondrán las posibles configuraciones para los nodos del diseño de red propuesto.

3.6.1. Configuración router principal.

El router principal será el encargado de ofertar las VLANs nacientes de las subinterfaces del dispositivo, haciendo uso del encapsulamiento dot1Q y el enrutamiento intra-VLAN de tal manera que por la misma interfaz se pueda distribuir varias VLANs al mismo tiempo, dicha configuración se ilustra a continuación en las figuras 3.12 y 3.13.

```
enable
configure terminal
hostname RouterCentral
enable secret class
no ip domain-lookup
banner motd #Prohibido el acceso no autorizado.#


username admin privilege 15 secret admin
username monitoreo privilege 5 secret monitoreo

line con 0
logging synchronous
exec-timeout 30 0
password cisco
login

line vty 0 15
logging synchronous
exec-timeout 30 0
password cisco
login

service password-encryption

interface Gig0/0/0
no shutdown

interface Gig0/0/1
no shutdown
```

Figura 3.12: Configuración del router principal - Configuración de interfaz 0. Parte 1/2
Fuente: Autor

```
interface Gig0/0/0.2
description INFORMATICA
encapsulation dot1Q 2
ip address 192.168.2.1 255.255.255.0
exit

interface Gig0/0/0.3
description FINANCIERO
encapsulation dot1Q 3
ip address 192.168.3.1 255.255.255.0
exit

interface Gig0/0/0.4
description RRHH
encapsulation dot1Q 4
ip address 192.168.4.1 255.255.255.0
exit

interface Gig0/0/0.5
description ADMINISTRATIVO
encapsulation dot1Q 5
ip address 192.168.5.1 255.255.255.0
exit

interface Gig0/0/0.6
description OPERACIONES
encapsulation dot1Q 6
ip address 192.168.6.1 255.255.255.0
exit

interface Gig0/0/0.7
description VISITANTES
encapsulation dot1Q 7
ip address 192.168.7.1 255.255.255.0
exit

interface Gig0/0/0.10
description ADMIN
encapsulation dot1Q 10
ip address 10.0.0.1 255.255.255.0
encapsulation dot1Q 10 native
exit
```

Figura 3.13: Configuración del router principal - Configuración de interfaz 0. Parte 2/2
Fuente: Autor

De cada interfaz se derivarán subinterfaces para realizar el enrutamiento intra-VLAN en las figuras 3.12 y 3.13 se ilustraba la configuración para la interfaz de la cual se deriva el conmutador que distribuye las LANs, en la figura 3.14 se muestra la configuración de la interfaz que provee de conectividad al conmutador encargado de distribuir los servicios de la red desde el clúster de servidores.

```
interface Gig0/0/1.2
description INFORMATICA
encapsulation dot1Q 2
ip address 192.168.12.1 255.255.255.0
exit

interface Gig0/0/1.3
description FINANCIERO
encapsulation dot1Q 3
ip address 192.168.13.1 255.255.255.0
exit

interface Gig0/0/1.4
description RRHH
encapsulation dot1Q 4
ip address 192.168.14.1 255.255.255.0
exit

interface Gig0/0/1.5
description ADMINISTRATIVO
encapsulation dot1Q 5
ip address 192.168.15.1 255.255.255.0
exit

interface Gig0/0/1.6
description OPERACIONES
encapsulation dot1Q 6
ip address 192.168.16.1 255.255.255.0
exit

interface Gig0/0/1.7
description VISITANTES
encapsulation dot1Q 7
ip address 192.168.17.1 255.255.255.0
exit


interface Gig0/0/1.10
description ADMIN
encapsulation dot1Q 10
ip address 10.0.1.1 255.255.255.0
encapsulation dot1Q 10 native
exit
```

Figura 3.14: Configuración del router principal - Configuración de interfaz 1.
Fuente: Autor

Dentro de las funciones del núcleo se encuentra la de asignar o proveer IPs a cada dispositivo acorde a la VLAN asignada al mismo, para lograr esto se debe levantar el servicio de DHCP del dispositivo, la configuración para llevar a cabo lo mencionado se ilustra a continuación en la figura 3.15.

```
ip dhcp pool INFORMATICA
net 192.168.2.0 255.255.255.0
dns-server 8.8.8.8
default-router 192.168.2.1
ip dhcp excluded-addres 192.168.2.1


ip dhcp pool FINANCIERO
net 192.168.3.0 255.255.255.0
dns-server 8.8.8.8
default-router 192.168.3.1
ip dhcp excluded-addres 192.168.3.1


ip dhcp pool RRHH
net 192.168.4.0 255.255.255.0
dns-server 8.8.8.8
default-router 192.168.4.1
ip dhcp excluded-addres 192.168.4.1


ip dhcp pool ADMINISTRATIVO
net 192.168.5.0 255.255.255.0
dns-server 8.8.8.8
default-router 192.168.5.1
ip dhcp excluded-addres 192.168.5.1


ip dhcp pool OPERACIONES
net 192.168.6.0 255.255.255.0
dns-server 8.8.8.8
default-router 192.168.6.1
ip dhcp excluded-addres 192.168.6.1


ip dhcp pool VISITANTES
net 192.168.7.0 255.255.255.0
dns-server 8.8.8.8
default-router 192.168.7.1
ip dhcp excluded-addres 192.168.7.1

ip dhcp pool ADMIND
net 10.0.0.0 255.255.255.0
dns-server 8.8.8.8
default-router 10.0.0.1
ip dhcp excluded-addres 10.0.0.1

ip dhcp pool ADMINS
net 10.0.1.0 255.255.255.0
dns-server 8.8.8.8
default-router 10.0.1.1
ip dhcp excluded-addres 10.0.1.1
```

Figura 3.15: Configuración del router principal - Configuración de DHCP.
Fuente: Autor

3.6.2. Configuración de conmutador para distribución LAN.

En las figuras 3.16 y 3.17 se puede observar la configuración necesaria para el conmutador que distribuye las LANs y almacena la base de datos de las VLANs. Adicional este se encuentra operando en modo servidor VTP, de tal manera que se encarga de administrar, actualizar y distribuir toda la información de las VLANs al resto de nodos que se derivan de este y se encuentren operando como cliente.

```
enable
configure terminal
hostname SWD
no ip domain lookup
enable secret cisco
banner motd #SOLO ACCESO A PERSONAL AUTORIZADO#

username admin privilege 15 secret admin
username monitoreo privilege 5 secret monitoreo

line console 0
logging synchronous
exec-timeout 30 0
login local
exit

line vty 0 15
logging synchronous
exec-timeout 30 0
login local
transport input all
exit

service password-encryption

vlan 2
name INFORMATICA
exit

vlan 3
name FINANCIERO
exit

vlan 4
name RRHH
exit

vlan 5
name ADMINISTRATIVO
exit

vlan 6
name OPERACIONES
exit

vlan 7
name VISITANTES
exit
```

Figura 3.16: Configuración del conmutador para distribución LAN. Parte 1/2.
Fuente: Autor

```
interface vlan10
ip address 10.0.0.2 255.255.255.0
vlan 10
name ADMIN
exit


interface range gig 1/0/1-24
description CONECTADO A ENLACE TRONCAL
switchport mode trunk
sw trunk allowed vlan 1,2,3,4,5,6,7,10
sw trunk native vlan 10


vtp mode server
vtp domain principal
vtp password principal
```

Figura 3.17: Configuración del conmutador para distribución LAN. Parte 1/2.
Fuente: Autor

3.6.3. Configuración de conmutador para distribución de servicios.

Las configuraciones mostradas en las figuras 3.18 y 3.19 son similares a las ilustradas en las figuras 3.16 y 3.17 ya que ambas son configuraciones necesarias para conmutadores que distribuyen ya sea LANs o servicios de una red.

```
enable
configure terminal
hostname SWD-SERVICIOS
no ip domain lookup
enable secret cisco
banner motd #SOLO ACCESO A PERSONAL AUTORIZADO#


username admin privilege 15 secret admin
username monitoreo privilege 5 secret monitoreo


line console 0
logging synchronous
exec-timeout 30 0
login local
exit

line vty 0 15
logging synchronous
exec-timeout 30 0
login local
transport input all
exit

service password-encryption
```

Figura 3.18: Configuración del conmutador para distribución de servicios. Parte 1/2.
Fuente: Autor

```
vlan 2
name INFORMATICA
exit

vlan 3
name FINANCIERO
exit

vlan 4
name RRHH
exit

vlan 5
name ADMINISTRATIVO
exit

vlan 6
name OPERACIONES
exit

vlan 7
name VISITANTES
exit

interface vlan10
ip address 10.0.1.2 255.255.255.0
vlan 10
name ADMIN
exit

interface range gig 1/0/1-24
description CONECTADO A ENLACE TRONCAL
switchport mode trunk
sw trunk allowed vlan 1,2,3,4,5,6,7,10
sw trunk native vlan 10

vtp mode server
vtp domain principal2
vtp password principal2

configure terminal
interface range gig 1/0/11-10
switchport mode access
switchport access vlan 10
```

Figura 3.19: Configuración del conmutador para distribución de servicios. Parte 2/2.
Fuente: Autor

3.6.4. Configuración de conmutadores clientes.

A diferencia de las configuraciones mostradas en los puntos 3.6.2 y 3.6.3 que pertenecen a los conmutadores que se encargan de las distribuciones principales de redes y servicios, para los clientes es más simple ya que al operar en modo acceso, modo cliente, solo copian las configuraciones establecidas en los nodos superiores que operan en modo servidor, tal como se puede visualizar en las figuras 3.20 y 3.21.

```
enable
configure terminal
hostname SWC
no ip domain lookup
enable secret cisco
banner motd #SOLO ACCESO A PERSONAL AUTORIZADO#


username admin privilege 15 secret admin
username monitoreo privilege 5 secret monitoreo


line console 0
logging synchronous
exec-timeout 30 0
login local
exit

line vty 0 15
logging synchronous
exec-timeout 30 0
login local
transport input all
exit

service password-encryption


interface range gig 0/1-2
description CONECTADO A ENLACE TRONCAL
switchport mode trunk
sw trunk allowed vlan 1,2,3,4,5,6,7,10
sw trunk native vlan 10

vtp mode client
vtp domain principal
vtp password principal
```

Figura 3.20: Configuración de los conmutadores clientes. Parte 1/2.
Fuente: Autor

```
configure terminal
interface range fa0/1-24
switchport mode access
switchport access vlan 2


configure terminal
interface range fa0/1-24
switchport mode access
switchport access vlan 3


configure terminal
interface range fa0/1-24
switchport mode access
switchport access vlan 4


configure terminal
interface range fa0/1-24
switchport mode access
switchport access vlan 5


configure terminal
interface range fa0/1-24
switchport mode access
switchport access vlan 6


configure terminal
interface range fa0/1-24
switchport mode access
switchport access vlan 7

configure terminal
interface range fa0/1-24
switchport mode access
switchport access vlan 8

configure terminal
interface range fa0/1-24
switchport mode access
switchport access vlan 10
```

Figura 3.21: Configuración de los conmutadores clientes. Parte 2/2.
Fuente: Autor

3.7. Simulación en Packet Tracer

En la figura 3.2 mostrada en el numeral 3.5 se ilustra el esquema de la red, el mismo que fue realizado en Packet Tracer, a continuación se evidenciará el funcionamiento de la simulación conectando dispositivos finales a la topología de la red. En las figuras 3.22 y 3.23 se muestra como el WLC provisiona las diferentes VLANs a los LWAPs de tal manera que las computadoras o dispositivos finales puedan tener estas a su disposición dichas redes, tal como se visualiza en la figura 3.24.

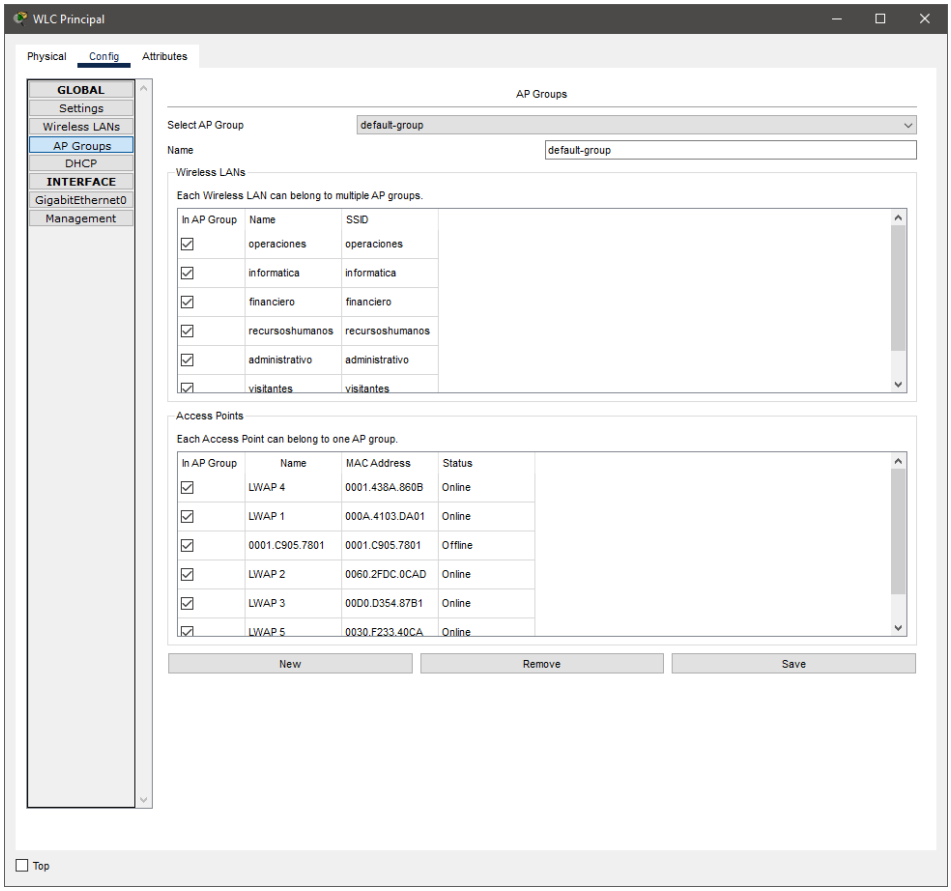


Figura 3.22: Redes disponibles en el WLC.
Fuente: Autor

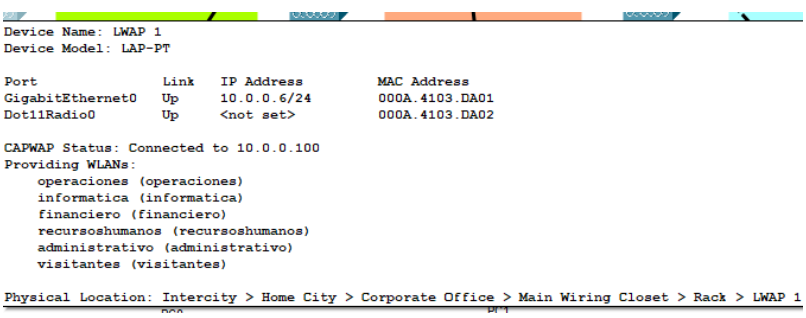


Figura 3.23: Redes aprovisionadas en los LWAPs.
Fuente: Autor

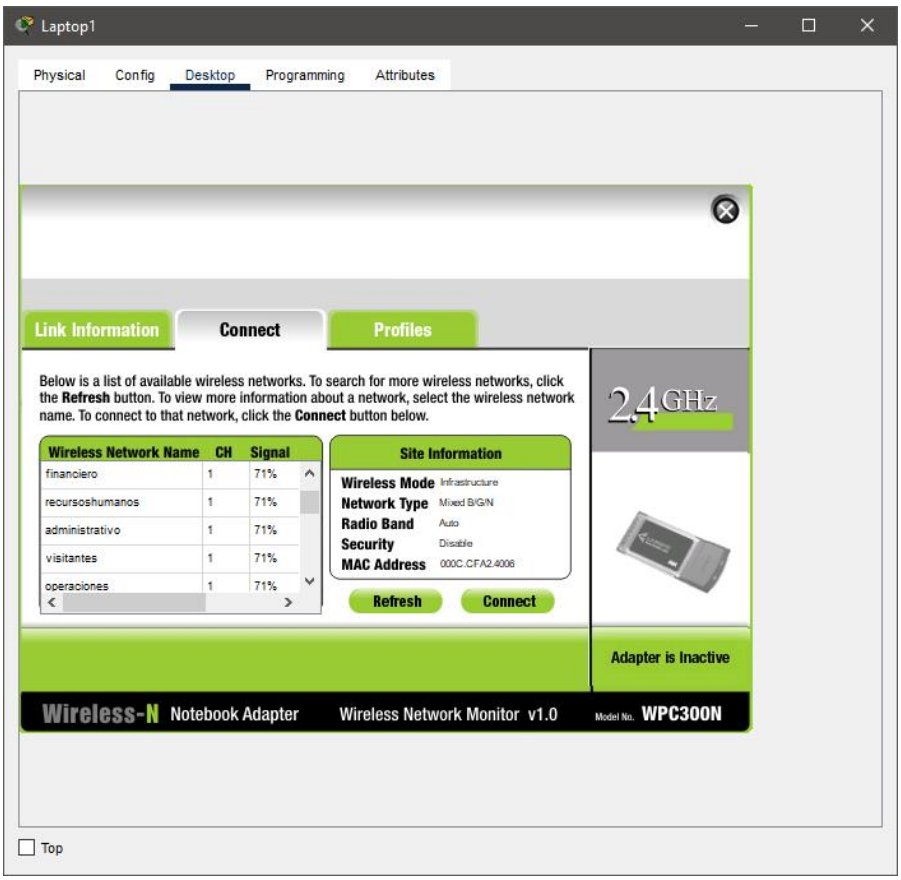


Figura 3.24: Disponibilidad de redes vista desde los dispositivos finales.
Fuente: Autor

Al hacer uso de un servidor DHCP, se tiene la ventaja que todos los dispositivos de los usuarios finales serán provisionados de IPs acorde a su departamento y niveles de acceso. Esto se evidencia en las figuras 3.25 donde al entrar en la configuración de las PCs mostradas se pasará a un panel de configuraciones donde ya está establecida un IP por el servidor DHCP tal como se muestra en la figura 3.26.

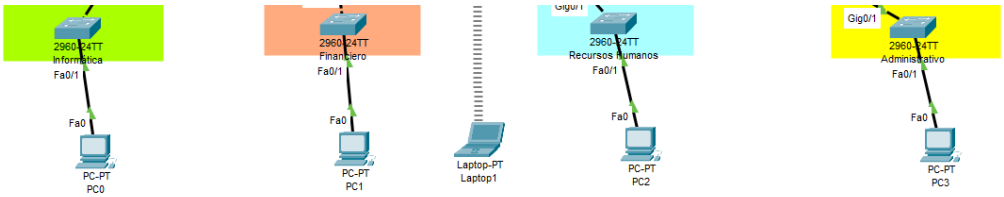


Figura 3.25: Dispositivos finales usando DHCP.
Fuente: Autor

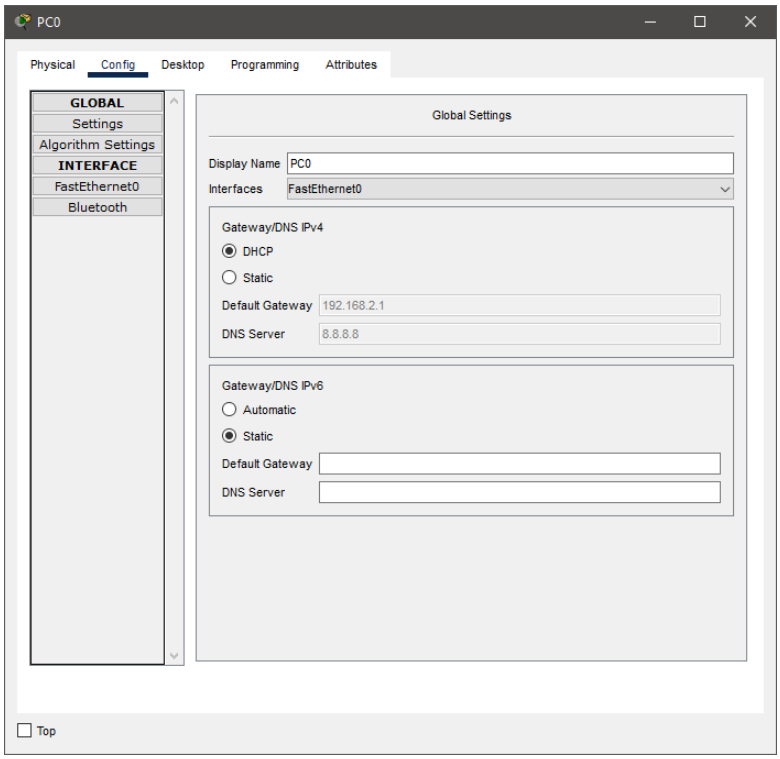


Figura 3.26: PC siendo provisionada de IP por DHCP.
Fuente: Autor

Gracias al servidor DNS se puede acceder a distintos servicios de la red tan solo usando el nombre establecido en lugar de la IP de destino, tal como se visualiza en la figura 3.27

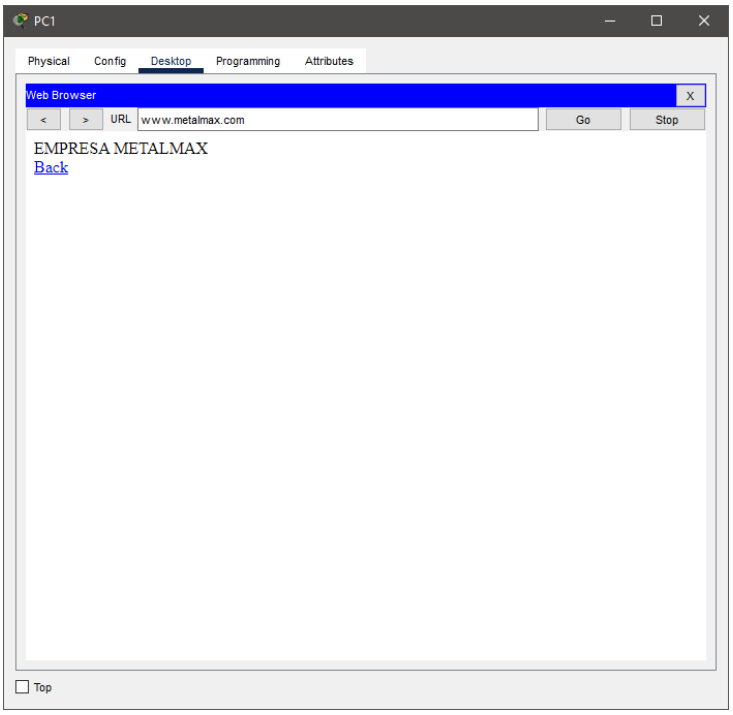


Figura 3.27: PC haciendo uso de HTTP.
Fuente: Autor

La implementación del servicio MAIL permite levantar un dominio de correos para la empresa de tal manera que los usuarios puedan comunicarse entre si usando este servicio, tal como se visualiza en las figuras 3.28 y 3.29 donde se evidencia el envío y recepción de correos.

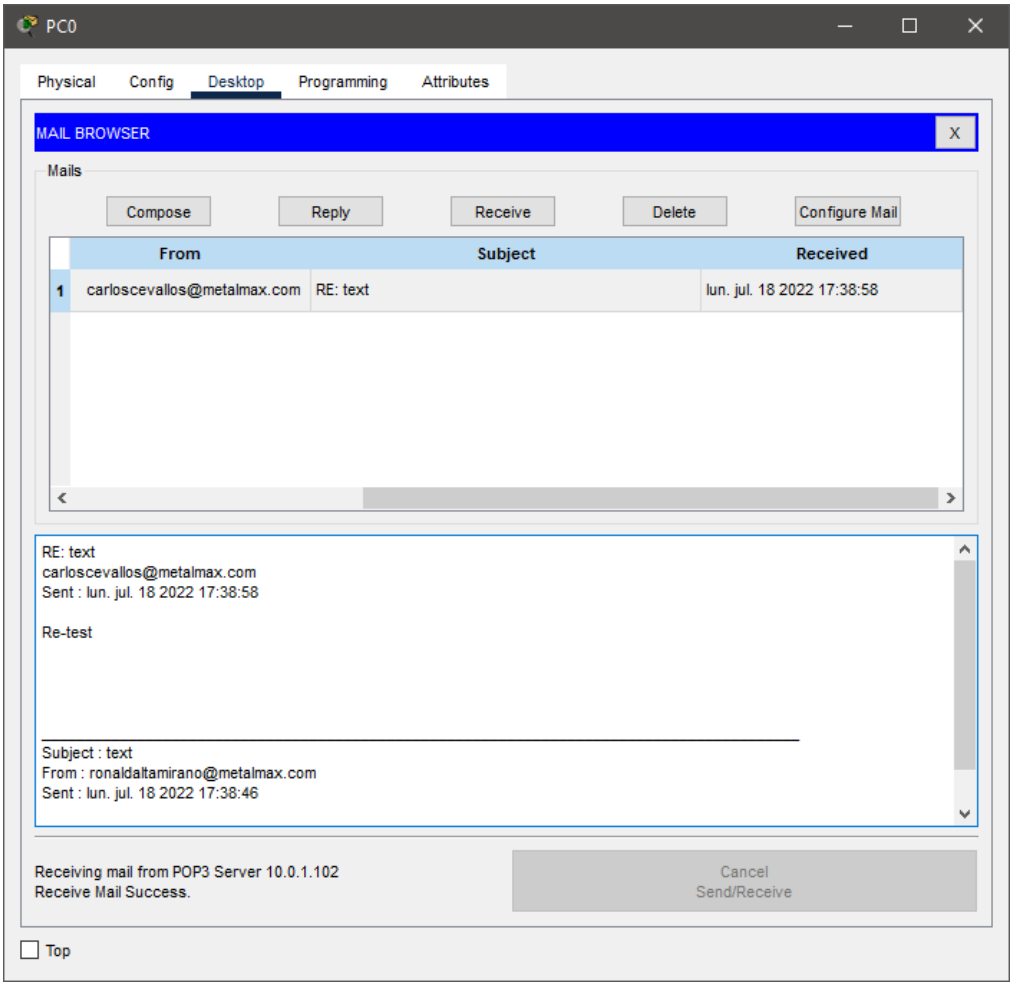


Figura 3.28: PC0 haciendo uso del servicio MAIL.
Fuente: Autor

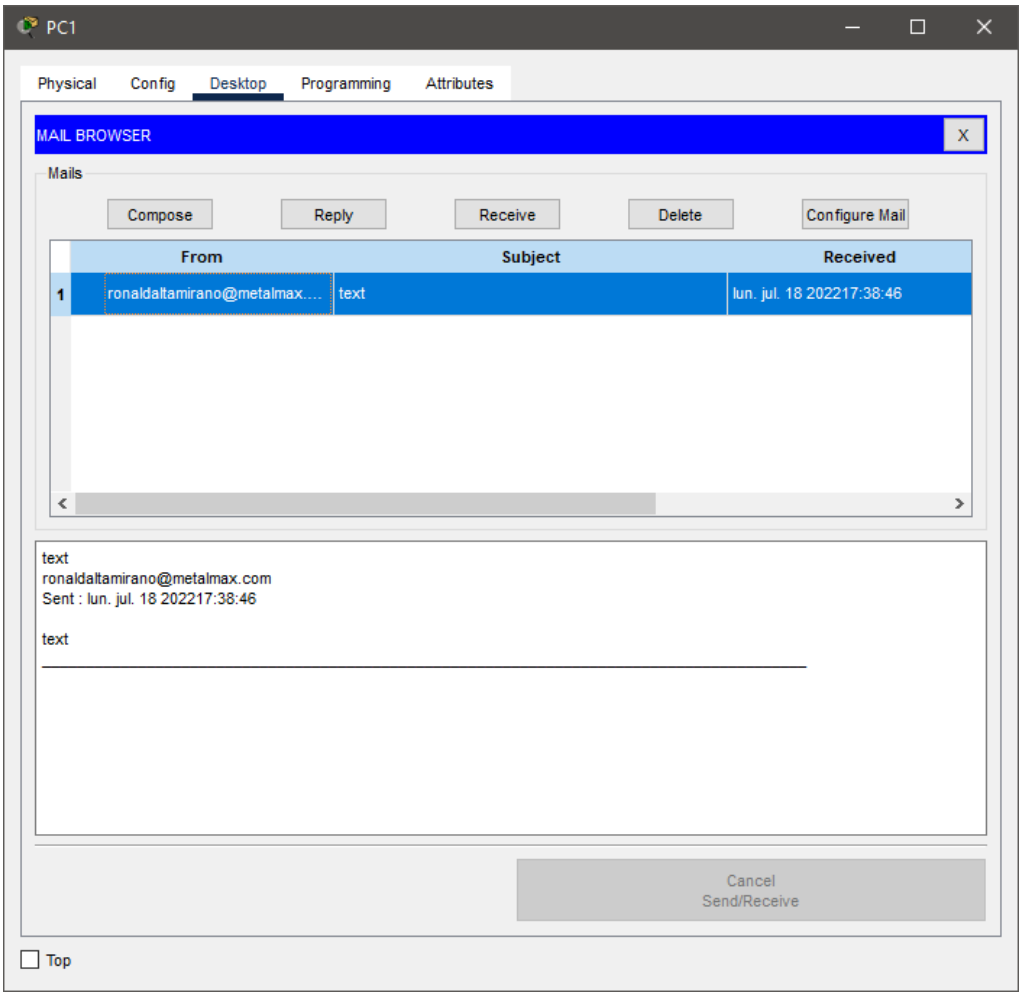


Figura 3.29: PC1 haciendo uso del servicio MAIL.
Fuente: Autor

Otro servicio muy importante en la red, es la implementación de un servidor IoT, lo cual permite implementar sensores industriales, figura 3.30, para posteriormente desde un panel de control hacer telemetría y telecontrol con estos dispositivos tal como se muestra en la figura 3.31 y 3.32.

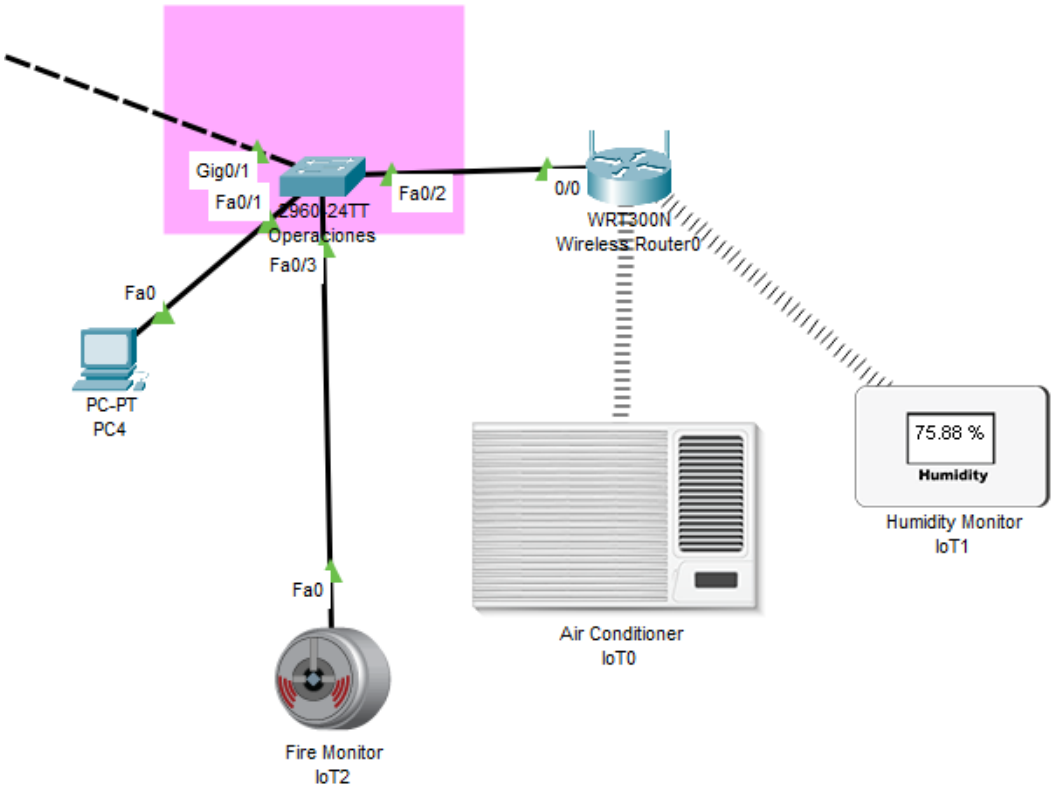


Figura 3.30: Sección con dispositivos IoT.
Fuente: Autor

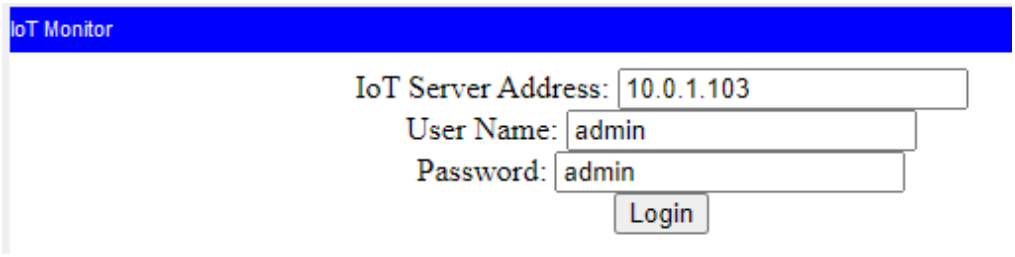


Figura 3.31: Portal del servicio IoT.
Fuente: Autor

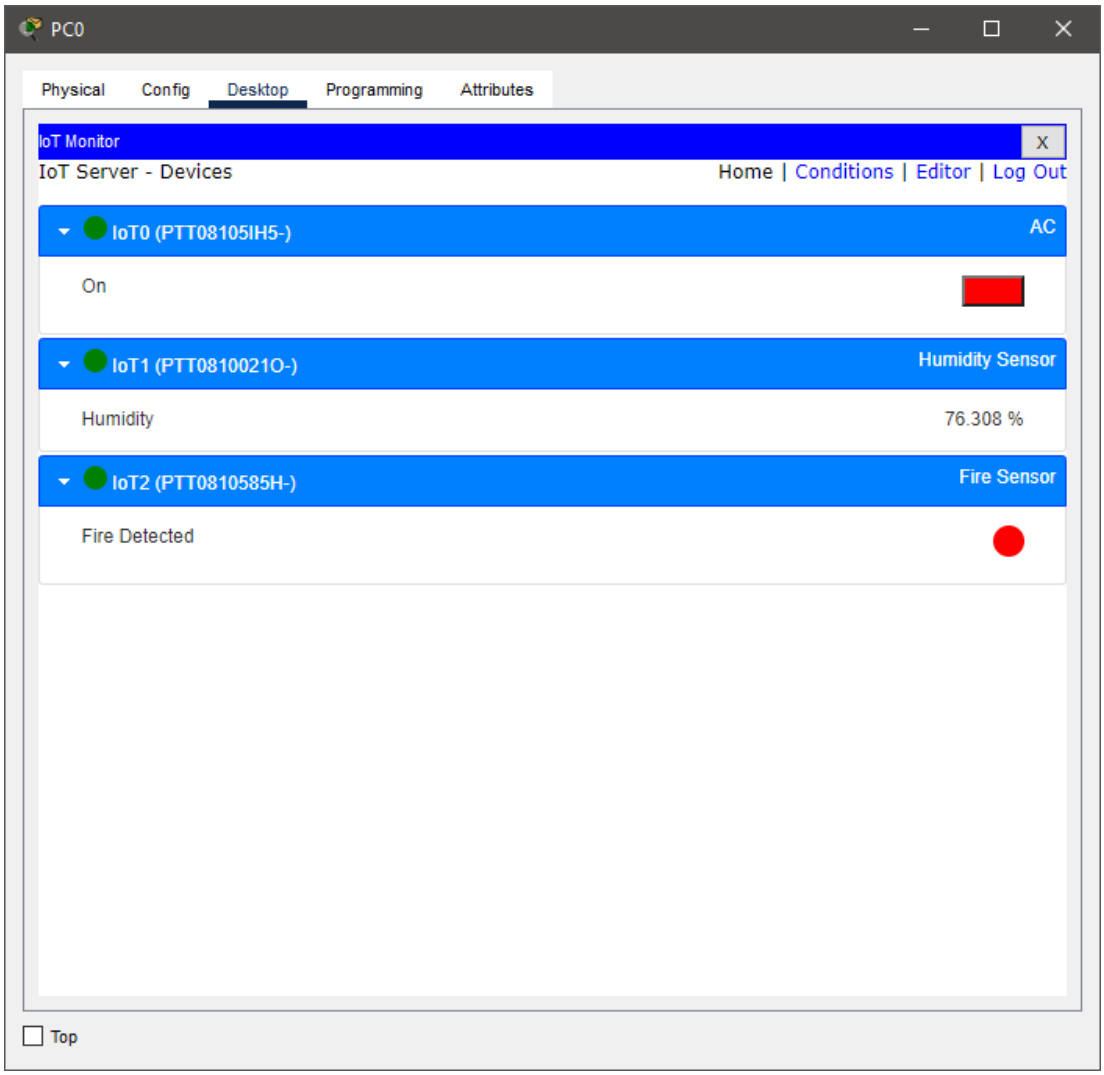


Figura 3.32: Panel de control de dispositivos IoT.
Fuente: Autor

Para una mejor visión de la explicación dada de las figuras pasadas correspondientes a la simulación a continuación en la figura 3.33 se mostrará por completo el esquema de conexión de todos los dispositivos mencionados.

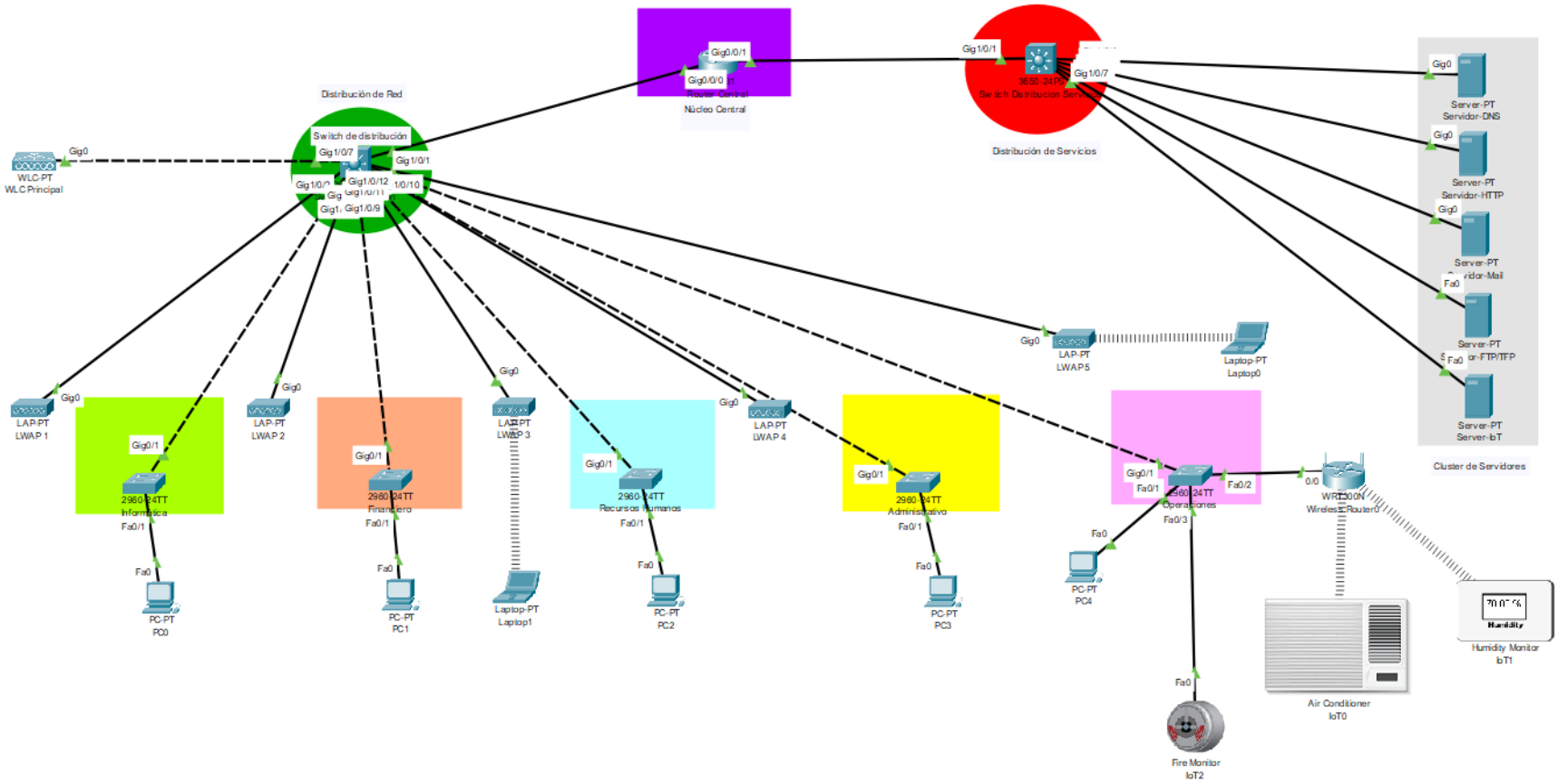


Figura 3.33: Simulación de la red con dispositivos finales y servicios.
Fuente: Autor

3.8. Características técnicas de los equipos para la propuesta de implementación de la red de datos.

En este apartado se evidenciará las características técnicas de los dispositivos necesarios para el diseño de la red.

3.8.1. Conmutadores para distribución.

Este modelo de capa 3 y 48 puertos ofrece alta fiabilidad, seguridad, rendimiento además de ser sencillo de administrar, en la figura 3.34 se mostrará un mejor detalle técnico de este dispositivo.

NOMBRE: SWITCH CISCO BUSSINESSCBS350-48T-4G-NA ADMINISTRABLE L3 DE 48 PUERTOS GIGABIT 10/100/1000 + 4 PUERTOS SFP RACKEABLE.

ESPECIFICACIONES:

- Dispone de 48 puertos Gigabit 10/100/1000Mbps + 4 slots SFP de fibra.
- Memoria SDRAM 512 MB y Flash 256 MB.
- Estándar IEEE 802.3, 802.3u, 802.3ab, 802.3ae, 802.3an, 802.3x, 802.1q/p, 802.3ad.
- Puertos MDIX automático, dúplex medio o completo.
- Capacidad de conmutación 104 Gbps.
- Capacidad de reenvío 77.38 Mpps.
- Tabla de Direcciones MAC 16k.
- Soporta hasta 4096 VLANs simultáneamente.
- Lista de Control de Acceso ACL.
- Protocolo de control de agregación de enlaces LACP.
- Protocolo Spanning Tree STP/RSTP/MSTP.
- Enrutamiento estático hasta 990 rutas.
- Compatibilidad nativa con IPv6.
- Servidor DHCP.
- Suministro de Energía Externa 100-240VAC.
- Montable en rack incluye kit.

Figura 3.34: Especificaciones técnicas del conmutador de distribución.
Fuente: Autor

3.8.2. Conmutadores para departamentos.

De forma similar al modelo de capa 3 y 48 puertos usados para distribución este también ofrece alta fiabilidad, seguridad, rendimiento además de ser sencillo de administrar con la diferencia que es de capa 2, en la figura 3.35 se mostrará un mejor detalle técnico de este dispositivo.

NOMBRE: SWITCH CISCO CBS220-48T-4G-NA ADMINISTRABLE L2 DE 48 PUERTOS GIGABIT 10/100/1000 + 4 PUERTOS SFP RACKEABLE.

ESPECIFICACIONES:

- Switch Administrable Capa 2 vía Web y CLI.
- Dispone de 48 puertos RJ-45 Gigabit 10/100/1000 Mbps + 4 Puertos Gigabit o slots para SFP.
- Estándar IEEE 802.3, 802.3u, 802.3ab, 802.3x, 802.1q/p.
- Puertos MDIX automático, dúplex medio o completo.
- Capacidad de conmutación 104 Gbps.
- Capacidad de reenvío 74,38 Mpps.
- Tabla de Direcciones MAC 8k.
- Tramas Jumbo 9k.
- Soporta hasta 256 VLANs simultáneamente.
- Lista de Control de Acceso ACL.
- Protocolo de control de agregación de enlaces LACP.
- Protocolo Spanning Tree STP/RSTP/MSTP.
- Suministro de Energía Externa 100-240VAC.
- Montable en rack incluye kit.

Figura 3.35: Especificaciones técnicas del conmutador departamental
Fuente: Autor

3.8.3. Controladoras inalámbricas.

EL WLC brindará las herramientas necesarias para la gestión centralizada de la red Wifi, las especificaciones completas se detallan en la figura 3.36.

NOMBRE: CONTROLADOR WIRELESS CISCO AIRONET AIR-CT2504-K9 DE 4 PUERTOS.

ESPECIFICACIONES:

- Switch Administrable.
- Soporta hasta 75 puntos de acceso con licencia adicional.
- Soporta hasta 1000 clientes.
- Puerto de consola conector RJ-45.
- Cuatro puertos Gigabit Ethernet de 1 Gbps RJ-45 dos con PoE+.
- Diseñado para su uso con Cisco Wireless Control System.
- Web administrador de dispositivos individuales http / https.
- Interfaz de línea de comandos Telnet, SSH, puerto serie.

Figura 3.36: Especificaciones técnicas del WLC.
Fuente: Autor

3.8.4. Puntos de acceso ligero.

Los LWAPs otorgan una red de alto rendimiento, garantizando velocidad, cobertura y conexiones estables debido a las especificaciones mostradas en la figura 3.37.

NOMBRE: ACCESS POINT WIRELESS AC1900 CISCO SMB WAP571-A-K9 PREMIUM DUAL BAND 1900MBPS GIGABIT SOPORTE POE.

ESPECIFICACIONES:

- Dispone de 2 puertos PoE RJ-45 Gigabit Ethernet 10/100/1000 Mbps.
- Soporta Power Over Ethernet 802.3at.
- Alimentación via Fuente de Poder o Inyector PoE.
- Dispone de 6 antenas omni internas 4 dBi de 5 GHz y 2.4 GHz.
- Compatible con estándar WiFi IEEE 802.11a/b/g/n/ac.
- Tecnología Wi-Fi Dual Band 2.4GHz + 5GHz MIMO 3×3 simultánea.
- Velocidad inalámbrica AC de hasta 1900 Mbps.
- Clave de seguridad WPA-PSK, WPA/WPA2 Enterprise TKIP/AES, 802.1X.
- Soporta más de 32 SSID.
- Modo de trabajo Access Point, WDS Bridge, FindIT.
- Soporta cluster de hasta 50 AP hasta 200 usuarios.
- Protocolos DHCP, WMM, SNMP, WDS, VLAN.
- Filtrado por MAC ACL.
- Administración por Web Browser.

Figura 3.37: Especificaciones técnicas del LWAP
Fuente: Autor

3.8.5. Puntos de acceso.

Este modelo de AP permite la multiplexación espacial, algoritmos de programación y beamforming para mejorar el rendimiento y distribución de ancho de banda junto a otras ventajas detalladas en la figura 3.38.

NOMBRE: ROUTER WIRELESS AC3200 LINKSYS WRT3200ACM MU-MIMO TRI BAND GIGABIT USB 3.0/E-SATA CUATRO ANTENAS.

ESPECIFICACIONES:

- Dispone de 4 puertos LAN y 1 puerto WAN RJ-45 Gigabit 10/100/1000 Mbps.
- Dispone de 4 antenas externas desmontables en 2.4GHz y 5Ghz.
- Dispone de 1 puerto USB 3.0 y 1 puerto combo eSATA/USB 2.0.
- Compatible con standard WiFi IEEE 802.11a/b/g/n/ac.
- Velocidad inalambrica AC3200 de hasta 600+2600 Mbps.
- Clave de seguridad WEP, WPA, WPA2, WPA-PSK, WPA2-PSK.
- Modo de trabajo Router, Repetidor WDS con DD-WRT.
- Protocolos PPPoE, PPTP, L2TP, DHCP, WMM.
- Control de Ancho de Banda.
- Control paterno para que sus hijos tengan una experiencia segura en Internet.
- Administración por Web Browser o App.

Figura 3.38: Especificaciones técnicas del AP.
Fuente: Autor

3.8.6. Router central.

Como núcleo de red se tiene un router con servicios integrados, con alta resiliencia, confiabilidad y seguridad, las especificaciones técnicas se detallan en la figura 3.39.

NOMBRE: CISCO ISR4331/K9 V04 4300 SERIES INTEGRATED SERVICES ROUTER.

ESPECIFICACIONES:

- Network interface module slots (NIM): 2.
- Maximum switched Ethernet LAN ports with PoE: 24.
- EtherSwitch Service Module type (width): 1 single.
- PoE support (wattage) without PoE boost: 250 W.
- Intrusion prevention: Yes.
- Cisco Cloud Web Security: Yes.
- Form factor: 1 Rack Unit.
- SSL VPN: No.
- Module online insertion and removal (OIR): Yes.
- Power supply type: Internal; AC, PoE.
- Maximum switched Ethernet ports: 24.
- Hardware VPN acceleration (DES, 3DES, AES): No.
- Redundant power supply: No.
- Management port: 1 GE (Integated Out of Band).
- PoE support (wattage) with PoE boost: 530 W.
- Integrated Services Card (ISC) slots: 1 (PVDM 4).
- Server virtualization platform (UCS E-Series): 2-core single-wide; 4-core single-wide.
- Enhanced Services Module (SM-X): 1 single-wide.
- Identity-based networking: No.
- Zone-based fiewall and NAT services.
- VRF-Aware Firewall and Network Address Translation (NAT).
- USB Ports (type A): 1.
- Integrated WAN ports: 1 GE / SFP, 1 GE, 1 SFP.
- Default/max DRAM: 4 GB / 16 GB.
- Default/max Flash: 4 GB / 16 GB.
- Performance: 100 Mbps Upgradeable to 300 Mbps.

Figura 3.39: Especificaciones técnicas del router central.
Fuente: Autor

3.8.7. Servidores.

Los servidores deben constar de una alta capacidad y resiliencia a nivel de hardware para soportar los diversos servicios incluyendo virtualización y colaboración. Las especificaciones se detallan a continuación en la figura 3.40.

NOMBRE: SERVIDOR CISCO UCS-SPRC240M4-V2, 2XINTEL XEON E5-2650V3 2.3GHZ 10 CORE, RAM 16GB (2X8GB DDR4 PC4-17000 2133MHZ ECC) 1,5TB (MAX), DISCOS DURO SATA 2TB (2X1TB PARA RAID).

ESPECIFICACIONES:

- Incluye 2 Procesadores Intel Xeon E5-2650 V3 de 2.3GHz de 10 núcleos cada uno.
- Caché inteligente 20MB en cada procesador.
- Chipset Intel serie C610.
- Memoria RAM 16GB (2x8GB) DDR4 PC4-17000 de 2133MHz ECC.
- Capacidad Disco Duro 2TB (2x1TB para RAID).
- Dispone de 24 ranuras para módulos DIMM registrados (RDIMM) ofreciendo una capacidad total de hasta 1.5TB.
- Cuenta con 24 slots para discos duros SAS 2.5" Hot Swap de acceso frontal intercambiables en caliente SFF, (proporcionando opciones de
- redundancia y facilidad de mantenimiento).
- Intercambiables en caliente SAS, SATA o unidades SSD.
- Controladora para 24 discos SAS de 12 Gbps ofrece arreglos RAID 0, 1, 5, 6, 10, 50 y 60.
- Tarjeta RAID modular PCI-e Gen 3.0 está conectado a una ranura PCIe dedicada, dejando a las dos ranuras PCIe que quedan disponibles para
- otras tarjetas de expansión.
- Ofrece soporte de 3 ranuras PCI-e 3.0 y compatibilidad con PCI-e 2.0 (Mayor rendimiento y flexibilidad de E/S).
- Soporta una ranura mLOM que puede instalar NIC sin consumir una ranura PCI-e.
- Dispone de ventiladores duales redundantes.
- Fuentes de alimentación redundantes intercambiables en caliente de 1200W cada una para la confiabilidad de clase empresarial y el tiempo de actividad.
- El servidor admite dos tarjetas SD internas redundantes Cisco FlexFlash, que pueden usarse para instalar un sistema operativo de arranque o hipervisor integrado.
- Chasis de servidor de 2UR.
- NIC integrada de dos puertos Gigabit Ethernet i350 de Intel.
- USB 3.0 interno admite 1 unidad flash.
- Controlador de administración de placa base integrada (BMC).
- Un puerto Gigabit Ethernet fuera de banda de la interfaz de gestión.
- CLI y herramienta de gestión para WebGUI, gestión automatizada de apagar las luces.
- Conector del panel frontal Un conector de consola KVM (suministro 2 USB, 1 VGA, y el conector serie 1).
- Conectores traseros adicionales incluyen un puerto de vídeo VGA, 2 puertos USB 3.0, un puerto serie RJ45, 1 puerto de administración Gigabit.
- Ethernet y dos puertos Ethernet de 1 Gigabit.
- Juego de rieles de Cisco con el brazo reversible para montaje en rack.
- Sistemas operativos soportados: Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012, Microsoft Windows Server 2008 R2, Red Hat Enterprise Linux, Servidor de Novell SUSE Linux Enterprise, Oracle Linux (Kernel irrompible Empresa (UEK)), Solaris de Oracle, Servidor Ubuntu, CentOS.
- Virtualización como: VMware vSphere ESXi, Oracle Virtual Machine servidor (UEK), Citrix XenServer.

Figura 3.40: Especificaciones técnicas del servidor.
Fuente: Autor

3.9. Costos aproximados

Los costos por dispositivos y el costo global son detallados en la tabla 3.2, en la cual se detalla la cantidad, precio unitario y total. Estos costos fueron extraídos desde el portal de venta de TECNIT, distribuidor de tecnología local.

Tabla 3.2: Costos aproximados de dispositivos.

N°	Descripción	Precio Unitario	Cantidad	Precio Total
1	SWITCH CISCO BUSSINESSCBS350-48T-4G-NA ADMINISTRABLE L3 DE 48 PUERTOS GIGABIT 10/100/1000 + 4 PUERTOS SFP RACKEABLE	$ 18.999,99	2	$ 37.999,98
2	SWITCH CISCO CBS220-48T-4G-NA ADMINISTRABLE L2 DE 48 PUERTOS GIGABIT 10/100/1000 + 4 PUERTOS SFP RACKEABLE	$ 12.999,99	5	$ 64.999,95
3	CONTROLADOR WIRELESS CISCO AIRONET AIR-CT2504-K9 DE 4 PUERTOS	$ 389,99	5	$ 1.949,95
4	ACCESS POINT WIRELESS AC1900 CISCO SMB WAP571-A-K9 PREMIUM DUAL BAND 1900MBPS GIGABIT SOPORTE POE	$ 379,99	15	$ 5.699,85
5	ROUTER WIRELESS AC3200 LINKSYS WRT3200ACM MU-MIMO TRI BAND GIGABIT USB 3.0/e-SATA CUATRO ANTENAS	$ 439,99	10	$ 4.399,90
6	Cisco ISR4331/K9 V04 4300 Series Router de servicios integrados	$ 1.750,00	1	$ 1.750,00

7	SERVIDOR CISCO UCS-SPRC240M4-V2, 2xINTEL XEON E5-2650V3 2.3GHz 10 CORE, RAM 16GB (2x8GB DDR4 PC4-17000 2133MHz ECC) 1,5TB (max), DISCOS DURO SATA 2TB (2x1TB PARA RAID)	$	4.999,99	2	$ 9.999,98
TOTAL					$ 126.799,61

Fuente: Autor

CONCLUSIONES

- Por medio de la descripción teórica y técnica de los fundamentos de redes alámbricas e inalámbricas, se pudo comprender la clasificación, tecnologías disponibles, topologías y diferentes modelos de diseño de redes que pueden ser desarrollados para su posterior implementación en la industria.

- Con el uso de herramientas de mapeo satelital y análisis técnico de la empresa “Metalmax” se pudieron establecer los requerimientos técnicos de los equipos necesarios para el diseño de la red propuesta.

- A través del estudio realizado en la empresa y usando el software “Packet Tracer” se planteó un diseño de red que sigue el modelo jerárquico, el cual cumple con las especificaciones técnicas para una futura implementación, siendo un modelo híbrido conformado por conexiones alámbricas e inalámbricas para brindar cobertura y conectividad a los distintos usuarios y dispositivos de la empresa, los cuales pueden ser fijos o móviles.

- La implementación del diseño de red propuesto posee un beneficio alto respecto al costo, siendo un monto aproximado de $126.799,61, asegurando que los equipos cumplan todas las especificaciones técnicas referentes a: compatibilidad tecnológica, facilidad de implementación, conectividad, resiliencia y escalabilidad para que en un futuro la red siga creciendo sin limitación alguna.

RECOMENDACIONES

- Realizar un estudio de propagación de señales inalámbricas en la empresa, de tal manera que se pueda configurar los dispositivos inalámbricos en las bandas y canales con menor saturación y ruido existente mejorando así el desempeño de la red.

- Establecer el personal con los conocimientos necesarios para la administración y soporte de la red, siendo guía para el resto de trabajadores y llevando a cabo un correcto uso de los equipos de red de manera que se obtenga el mejor rendimiento.

- Incentivar a la empresa a la implementación de dispositivos inteligentes de tal manera que estos se acoplen a la red y puedan ser administrados de forma más sencilla y eficiente sacando el máximo provecho de los recursos disponibles en la red propuesta.

Bibliografía

Almentero Arrieta, F., & Mieles Montes, C. V. (2008). Diseño de redes convergentes. http://biblioteca.utb.edu.co/notas/tesis/0045010.pdf. https://repositorio.utb.edu.co/handle/20.500.12585/1717

Cuellar Valderrama, J. J., & Luna Torres, A. (2008). Servicios en las redes convergentes. http://biblioteca.utb.edu.co/notas/tesis/0043237.pdf. https://repositorio.utb.edu.co/handle/20.500.12585/2830

Fajardo, Á. M. M. (2004). Redes convergentes. Ciencia e Ingeniería Neogranadina, 14, 64-74. https://doi.org/10.18359/rcin.1269

Benyamina, D., Hafid, A., & Gendreau, M. (2012). Wireless Mesh Networks Design—A Survey. IEEE Communications Surveys & Tutorials, 14(2), 299–310. https://doi.org/10.1109/SURV.2011.042711.00007

Guha, S., Meyerson, A., & Munagala, K. (2000). Hierarchical placement and network design problems. Proceedings 41st Annual Symposium on Foundations of Computer Science, 603–612. https://doi.org/10.1109/SFCS.2000.892328

Hu, W.-H., Wang, C., & Bagherzadeh, N. (2012). Design and Analysis of a Mesh-based Wireless Network-on-Chip. 2012 20th Euromicro International Conference on Parallel, Distributed and Network-based Processing, 483–490. https://doi.org/10.1109/PDP.2012.19

Kijmanawat, K., & Ieda, H. (2004). Multilevel Hierarchical Network Design. 土木学会論文集, 2004(751), 139–150. https://doi.org/10.2208/jscej.2004.139

Shakkottai, S., Rappaport, T. S., & Karlsson, P. C. (2003). Cross-layer design for wireless networks. IEEE Communications Magazine, 41(10), 74–80. https://doi.org/10.1109/MCOM.2003.1235598

Sheu, J.-B., & Lin, A. Y.-S. (2012). Hierarchical facility network planning model for global logistics network configurations. Applied Mathematical Modelling, 36(7), 3053–3066. https://doi.org/10.1016/j.apm.2011.09.095

Son, I. K., & Mao, S. (2010). Design and Optimization of a Tiered Wireless Access Network. 2010 Proceedings IEEE INFOCOM, 1–9. https://doi.org/10.1109/INFCOM.2010.5462107

Wang, C., Huang, N., Zhang, S., Zhang, Y., & Wu, W. (2017). A hierarchical network model for network topology design using genetic algorithm. MATEC Web of Conferences, 119, 01008. https://doi.org/10.1051/matecconf/201711901008

Zhang, J., & Liu, X. (2018). Evaluation of network service model based on network convergence. EURASIP Journal on Wireless Communications and Networking, 2018(1), 40. https://doi.org/10.1186/s13638-018-1053-1

CCNA. (2022). *Study-CCNA*. Retrieved 07 2022, from https://study-ccna.com/vtp-modes/

Cervantes, I. I. (2015). *REDES III*. (I. I. Cervantes, Editor, & I. I. Cervantes, Producer) Retrieved 06 2022, from https://sites.google.com/site/redes3isi/home

CISCO. (2014). *Resumen de diseño de redes.* (CISCO, Ed.) Retrieved 06 2022, 19, from https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus-wireless_wp_cte_es-xl_42333.pdf

Cisco (Ed.). (2020). *CCNA Desde Cero*. (Cisco, Producer, & Cisco) Retrieved 06 2022, from CCNA Desde Cero: https://ccnadesdecero.com/curso/

CISCO. (2022). *CISCO SOLUTIONS.* (CISCO, Ed.) Retrieved 06 2022, from CISCO SOLUTIONS: https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus-wireless_wp_cte_es-xl_42333.pdf

Collado, E. (2018). *Redes, hosting, software libre*. Retrieved 07 2022, from Podcast de Redes: https://www.eduardocollado.com/2018/04/02/pocast-142-vtp-vlan-trunking-protocol/

Network Lessons. (2022). *Network Lessons*. Retrieved 07 2022, from https://networklessons.com/switching/introduction-to-vtp-vlan-trunking-protocol

TECNIT. (n.d.). *TECNIT*. Retrieved from https://tecnit.com.ec/

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Altamirano Maxi, Ronald Xavier** con C.C: # 092385830-2 autor del Trabajo de Titulación: **Estudio y diseño de una red corporativa de datos para la empresa Metalmax ubicada en la vía a Daule km 27,5 de la ciudad de Guayaquil** previo a la obtención del título de **INGENIERO EN TELECOMUNICACIONES** en la Universidad Católica de Santiago de Guayaquil

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 15 de septiembre del 2022

f. _____

Nombre: Altamirano Maxi, Ronald Xavier

C.C: 092385830-2

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	Estudio y diseño de una red corporativa de datos para la empresa Metalmax ubicada en la vía a Daule km 27,5 de la ciudad de Guayaquil		
AUTOR(ES)	Altamirano Maxi, Ronald Xavier		
REVISOR(ES)/TUTOR(ES)	Ing. Romero Rosero, Carlos Bolívar		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Educación Técnica para el Desarrollo		
CARRERA:	Ingeniería en Telecomunicaciones		
TITULO OBTENIDO:	Ingeniería en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	15 de septiembre del 2022	**No. DE PÁGINAS:**	85
ÁREAS TEMÁTICAS:	Redes de datos y Redes convergentes		
PALABRAS CLAVES/ KEYWORDS:	REDES, INALÁMBRICO, ALÁMBRICO, MODELO JERÁRQUICO, REDES CONVERGENTES, PACKET TRACER		

RESUMEN/ABSTRACT (150-250 palabras):

El presente trabajo de titulación aborda el "Estudio y diseño de una red corporativa de datos para la empresa Metalmax ubicada en la vía a Daule km 27,5 de la ciudad de Guayaquil". El documento brinda información sobre la importancia del diseño de redes acorde a las necesidades, tanto como redes alámbricas como inalámbricas, pero siguiendo un modelo que abarque todas las necesidades. En el Capítulo 1 se presenta la descripción general del trabajo de titulación. El Capítulo 2 describe a las redes, sus fundamentos, modelos existentes, tecnologías disponibles y las aplicaciones en los diversos casos de la industria. El capítulo 3 presenta el diseño de la red propuesto, mediante la descripción del (1) sector o empresa a intervenir, (2) análisis técnico de los requerimientos empresariales, (3) características de los equipos necesarios para la implementación, (4) diseño de la red en el software "Packet Tracer" y (5) presupuesto de la implementación.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-980293712	E-mail: ronald.altamirano@cu.ucsg.edu.ec
CONTACTO CON LA INSTITUCIÓN: COORDINADOR DEL PROCESO DE UTE	**Nombre:** Velez Tacuri, Efrain Oliverio	
	Teléfono: +593994084215	
	E-mail: efrain.velez@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	