UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TESIS PREVIA A LA OBTENCIÓN DEL TITULO DE INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA: REESTRUCTURACIÓN EN LA RED DE COMUNICACIONES FÍSICA Y LÓGICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO PROVINCIAL DE IMBABURA

AUTOR:

AMADA LEONOR FÉLIX BOLAÑOS

DIRECTOR:

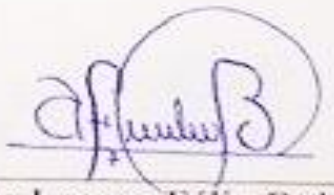
Ing. CARLOS VÁSQUEZ

Ibarra-Ecuador

01 de marzo del 2016

DECLARACIÓN

Yo, AMADA LEONOR FÉLIX BOLAÑOS, declaro que el trabajo aquí descrito es de mi autoría, no ha sido previamente presentado para ningún grado o calificación profesional y certifico la veracidad de las referencias bibliográficas que se incluyen en este documento.



Amada Leonor Félix Bolaños

040171037 1

CERTIFICACIÓN

En calidad de Director de Trabajo de Grado "Reestructuración en la red de comunicaciones física y lógica del Gobierno Autónomo Descentralizado provincial de Imbabura", presentado por la señorita Amada Leonor Félix Bolaños, para optar por el título de Ingeniero en Electrónica y Redes de Comunicación, certifico que el mencionado proyecto fue realizado bajo mi dirección.

Ing. Carlos Vásquez

DIRECTOR

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital institucional, determino la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información.

DATOS DEL CONTACTO	
CÉDULA DE IDENTIDAD:	040171037-1
APELLIDOS Y NOMBRES:	AMADA LEONOR FÉLIX BOLAÑOS
DIRECCIÓN:	GARCIA MOREONO 1009 Y PEDRO RODRIGUEZ
E-MAIL:	alfelix@utn.edu.ec
TELÉFONO MÓVIL:	0983462830

DATOS DE LA OBRA	
TÍTULO:	REESTRUCTURACIÓN EN LA RED DE COMUNICACIONES FÍSICA Y LÓGICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO PROVINCIAL DE IMBABURA
AUTOR:	AMADA LEONOR FÉLIX BOLAÑOS
FECHA:	01 de marzo del 2016
PROGRAMA:	PREGRADO
TITULO POR EL QUE OPTA:	INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN
DIRECTOR:	ING. CARLOS VÁSQUEZ

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Amada Leonor Félix Bolaños, con cédula de identidad Nro.040171037-1 en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior, Articulo 144.

3. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 01 días del mes de Marzo del 2016

EL AUTOR

Amada Leonor Félix Bolaños

CI: 040171037-1

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, Amada Leonor Félix Bolaños, con cédula de identidad Nro.040171037-1 Manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, Artículos 4,5 y 6, en calidad de autor de la obra o trabajo de grado denominado "Reestructuración en la red de comunicaciones física y lógica del Gobierno Autónomo Descentralizado provincial de Imbabura", que ha sido desarrollada para optar por el título de Ingeniero en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago la entrega del trabajo final en formato impreso y digital en la Biblioteca de la Universidad Técnica del Norte.

Nombre: Amada Leonor Félix Bolaños

Cédula: 040171037-1

Ibarra, a los 01 días del mes de Marzo del 2016

AGRADECIMIENTO

A mis padres, Augusto Félix y Angelita Bolaños, por todo el apoyo brindado en mi etapa estudiantil y ser mi ejemplo en cada una de mis metas.

A la Dirección de Tecnologías de Información del Gobierno Autónomo Descentralizado Provincial de Imbabura, en donde, gracias a su apoyo pude realizar el trabajo presente.

A mi director de Tesis, Ing. Carlos Vásquez, quien con su asesoramiento contribuyó para culminar con éxito este trabajo de titulación.

A los docentes de la carrera de Ingeniería en Electrónica y Redes, quienes a lo largo de estos años supieron transmitir sus experiencias y conocimientos.

Agradezco a Dios por haberme dado la salud y vida, así como la sabiduría, paciencia, y sobre todo la constancia de trabajo y esfuerzo que he puesto a diario para alcanzar mis objetivos

DEDICATORIA

Dedico este proyecto a mis padres que son mi ejemplo y mi principal inspiración, a ellos que trabajan día a día inalcanzablemente por nuestra familia, a ellos que desde pequeña han inculcado en mi los valores y virtudes que me han permitido concluir esta etapa de vida.

ÍNDICE GENERAL

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLAS

ÍNDICE DE ECUACIONES

REESTRUCTURACIÓN EN LA RED DE COMUNICACIONES FÍSICA Y LÓGICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO PROVINCIAL DE IMBABURA.

Autor: Leonor Félix

Tutor: Ing. Carlos Vásquez

RESUMEN

El proyecto consiste en la reestructuración de la red de comunicaciones del GAD provincial de Imbabura tanto a nivel físico como a nivel lógico, el mismo que mejore el funcionamiento de la red mediante la implementación de un nuevo modelo.

El diseño físico se basará en un modelo jerárquico contemplando los niveles organizacionales del GAD provincial de Imbabura, los requerimientos del cableado estructurado en base a la norma ANSI/TIA/EIA-568-C para la instalación de los puntos necesarios. El diseño lógico estará basado en una nueva segmentación de tráfico realizando una nueva distribución de VLANs reduciendo las colisiones existentes en la red.

El modelo jerárquico estará contemplado en base a dos capas, la capa de núcleo contraído y la capa de acceso, nos permitirá manejar parámetros de diseño por cada capa y separar las funciones que cada una realiza, así como brindar a la red escalabilidad, fácil administración y fácil mantenimiento.

REESTRUCTURACIÓN EN LA RED DE COMUNICACIONES FÍSICA Y LÓGICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO PROVINCIAL DE IMBABURA.

Author: Leonor Félix

Tutor: Ing. Carlos Vásquez

SUMMARY

The project involves the restructuring of the communications network of provincial GAD of Imbabura, physically and logical level, the same that improves network performance by implementing a new model.

The physical design is based on a hierarchical model contemplating organizational levels of GAD provincial de Imbabura, the structured cabling requirements based on the ANSI / TIA / EIA -568-C standard for the installation of the necessary points. The logical design will be based on a new segmentation of traffic making a redistribution of existing VLAN s reducing collisions on the network.

The hierarchical model will be referred based on two layers, the layer of collapsed core and the access layer, allow us to handle design parameters for each layer and separate the functions that each performs as well as providing network scalability, easy administration and easy maintenance.

PRESENTACIÓN

Las redes de comunicación hoy son una herramienta indispensable no solo en las empresas que manejan grandes volúmenes de datos, sino también para todas las personas en sus actividades diarias. Es necesario comprender que el futuro de las comunicaciones en el mundo están lideradas por las redes, desde el momento en que conectamos una PC a internet ya somos parte de la red de comunicaciones más grande que existe.

El proyecto consiste en la reestructuración de la red de comunicaciones del GAD provincial de Imbabura tanto a nivel físico como a nivel lógico, basado en el modelo de jerarquía de red, contemplando un diseño de dos capas, la capa de núcleo contraído y la capa de acceso, mediante el cual se mejore el rendimiento de la red.

Consta de seis capítulos en donde existe el planteamiento del problema, los objetivos, el alcance ya la justificación para la elaboración de este proyecto, a continuación se desarrolla un estudio del marco teórico analizando las áreas técnicas en la cuales se basa este proyecto que son: Networking para efectuar los diseños tanto físico y lógico de la red y Cableado Estructurado para garantizar la conexión entre los dispositivos activos de red, seguido se realizó un análisis de la situación actual de la red de comunicaciones tanto a nivel físico y lógico, analizando la parte pasiva y activa de la red, así como información sobre la estructura organizacional de la institución. Luego consta el nuevo diseño de red,

en donde, el diseño físico se basa en un modelo jerárquico y el diseño lógico está basado en una nueva segmentación de tráfico realizando una nueva distribución de VLANs, a continuación se detalla la instalación de los nuevos puntos de red, así como el proceso de configuración en los equipos de las diferentes capas que comprenden la red, es decir, configuraciones en el área de networking y para finalizar se expone las principales conclusiones y recomendaciones obtenidas en base al desarrollo de este proyecto.

CAPÍTULO I

1. ANTECEDENTES

En este capítulo consta el planteamiento del problema, objetivos, alcance y justificación que son las referencias para la realización de este proyecto de tesis.

1.1. PLANTEAMIENTO DEL PROBLEMA

El Gobierno Autónomo Descentralizado Provincial de Imbabura (GAD[1] provincial de Imbabura) cuenta con una red destinada a brindar diferentes servicios, lo cual permite realizar una gestión más oportuna en la institución. Acorde al paso de los años existen un sin número de equipos que se ofrecen en el mercado para satisfacer estas necesidades y mientras más ha evolucionado la tecnología más han crecido los requerimientos y exigencias de quienes administran, como de quienes reciben los servicios a través de redes, exigencias en calidad y seguridad.

Con el paso de los años el GAD provincial de Imbabura ha tenido un aumento considerable en el número de trabajadores y con ello de su infraestructura tecnológica, lo que permite que personas tanto a nivel administrativo, de servicio y visitantes tengan acceso a los diferentes servicios que presta la red de la institución. Este incremento en la capacidad de la red de comunicaciones, ha traído como consecuencia aumento de puntos de red, además la segmentación de la red no está de acuerdo a las necesidades que esta

[1] GAD=Gobierno Autónomo Descentralizado

requiere, lo que ocasiona que tenga un alto número de colisiones en diferentes puntos de la red, limitando el acceso a los recursos y servicios, una red inalámbrica poco estable y por ende inconformidad entre los usuarios. Además otro de los inconvenientes es que las configuraciones de los equipos no están realizadas de la manera más adecuada, es decir, explotando todas sus capacidades, lo que hace que la red se vuelva menos eficiente y más vulnerable a los cambios futuros.

El GAD provincial de Imbabura es una institución pública la cual contribuye a las mejoras de la provincia y tiene influencia en cada uno de los GAD Parroquiales, cuenta con una red Informática la cual brinda servicios a cientos de usuarios, sin embargo no está correctamente establecida, es por ello que con las soluciones a implementarse se logrará brindar un mejor servicio en la red de comunicaciones.

Con el transcurso de los años GAD provincial de Imbabura y a su vez la Infraestructura Tecnológica crecerán a medida de las necesidades que ésta requiera y no solo crecerá las necesidades a nivel de físico, sino también a nivel lógico, es por esto que al realizar una reestructuración de la red a nivel lógico garantizará una mayor eficiencia en la red actual y proveerá las cambios que se puedan realizar a futuro.

1.2. OBJETIVOS

Para poder realizar este proyecto de tesis es necesario tener los objetivos claros de lo que se va a realizar, para ellos se plantea los siguientes objetivos general y específicos.

1.2.1. OBJETIVO GENERAL

Potenciar el rendimiento de la red de comunicaciones del GAD provincial de Imbabura, mediante una reestructuración a nivel físico y lógico que garantice una mejora en el funcionamiento de la red.

1.2.2. OBJETIVO ESPECÍFICOS

- Detallar los fundamentos de Networking y Cableado Estructurado, para la aplicación de estos en la reestructuración de la red de comunicaciones del GAD provincial de Imbabura.
- Realizar una evaluación de la situación actual de la red de comunicaciones del GAD provincial de Imbabura tanto a nivel físico como lógico, para establecer los puntos críticos que requieran una reestructuración dentro de la red.
- Diseñar la nueva topología física para la red de comunicaciones del GAD provincial de Imbabura, contemplando los requerimientos del cableado estructurado, la distribución de cada uno de los departamentos y la estructura del centro de datos garantizando el correcto funcionamiento entre los dispositivos activos de la red.
- Diseñar la nueva topología lógica de la red de comunicaciones del GAD provincial de Imbabura que garantice mejoras en la distribución del tráfico de la red, mejoras en el funcionamiento de la red, así como disponibilidad inalámbrica.
- Implementar la reestructuración a nivel físico y lógico en la red existente en el GAD provincial de Imbabura, basado en los diseños desarrollados.

- Demostrar y evaluar el funcionamiento idóneo de la reestructuración en la red de comunicaciones, realizando pruebas de los parámetros y configuraciones realizadas.

1.3.ALCANCE

El presente proyecto de titulación consiste en la reestructuración de la red de comunicaciones del GAD provincial de Imbabura tanto a nivel físico como a nivel lógico, mediante el cual se potencialice su rendimiento de la red.

Para la consecución del proyecto propuesto, se inicia con un estudio del marco teórico analizando las áreas técnicas en la cuales se basa este proyecto que son: Networking para efectuar los diseños tanto físico y lógico de la red y Cableado Estructurado para garantizar la conexión entre los dispositivos activos de red.

Una vez realizado el estudio de las áreas técnicas, se realizará un análisis de la situación actual de la red de comunicaciones tanto a nivel físico y lógico, obteniendo información sobre la estructura organizacional del GAD provincial de Imbabura, es decir, departamentos, direcciones, subdirecciones, el número de usuarios y las aplicaciones que manejan, el modelo en el cual está estructurado la red, los equipos de redes que posee y el papel que cumple la configuración de cada uno de ellos dentro de la red, como se encuentra establecido el cableado estructurado.

Con el levantamiento de la información actual de la red de comunicaciones y conociendo a través de este las fortalezas y debilidades se procede a realizar los rediseños de las topologías a nivel físico y a nivel lógico a ser implementados en la red de comunicaciones del GAD provincial de Imbabura.

El diseño físico se basará en un modelo jerárquico contemplando los niveles organizacionales del GAD provincial de Imbabura, los requerimientos del cableado estructurado en base a la norma ANSI[2]/TIA[3]/EIA[4]-568-C para la instalación de los puntos necesarios.

El diseño lógico estará basado en una nueva segmentación de tráfico realizando una nueva distribución de VLAN[5]s reduciendo las colisiones existentes en la red.

Posteriormente se implementará el nuevo diseño tanto a nivel físico como lógico en la red existente en el GAD provincial de Imbabura, en base a los diseños planteados anteriormente.

Para finalizar se evaluará y demostrará el funcionamiento idóneo de la reestructuración en la red de comunicaciones del GAD provincial de Imbabura, realizando verificaciones de sus configuraciones.

[2] ANSI= American National Standards Institute, Instituto Americano de Estándares Nacionales
[3] TIA= Telecommunications Industry Association, Asociación de la Industria de Telecomunicaciones
[4] EIA=Electronic Industries Alliance, Alianza de Industrias Electrónicas
[5] VLAN= Virtual Local Area Network, Redes de Área Local Inalámbrica

1.4. JUSTIFICACIÓN

Con el proyecto de titulación presente se ratifica la misión de la Universidad Técnica del Norte la cual forma profesionales que generen procesos de investigación y que se vinculan con la comunidad para contribuir al desarrollo tecnológico y social de la región y del país.

El GAD provincial de Imbabura es una institución pública encargada de coordinar, planificar, ejecutar y evaluar el Plan de Desarrollo Provincial, con la finalidad de fortalecer la productividad, la vialidad, el manejo adecuado de los recursos naturales y promover la participación ciudadana, todo esto se lo realiza con el fin de mejorar la calidad de vida de los habitantes. Cuenta con un edificio principal desde el cual se comunica con sus edificios anexos brindando servicios tanto a personal administrativo y de servicio, por esto es muy fundamental que la red de comunicaciones se encuentre en un buen estado garantizando eficiencia en la entrega de servicios así como en la seguridad de la información, con una topología física y configuración lógica adecuada con cada uno de sus elementos.

El número de usuarios de red de comunicaciones de esta institución ha tenido un gran crecimiento a lo largo de los últimos años manejando actualmente gran cantidad de tráfico lo cual ocasiona congestión en la red y aumento de los dominios de broadcast, también ha crecido el número de dispositivos que utilizan la conexión inalámbrica ocasionando saturación en esta parte de la red, por ende este proyecto de titulación

permitirá mejorar las condiciones actuales segmentando la red de una manera más adecuada de acuerdo las necesidades de la red.

Al realizar este proyecto de titulación, se aplicará los conocimientos adquiridos durante toda la carrera, en si en la área de redes de comunicación, dando mayor énfasis a la investigación, todo esto contribuirá a una formación personal con criterios humanistas y técnicos adentrándonos así al perfil laboral de un Ingeniero en Electrónica y Redes de Comunicación.

CAPITULO II

2. FUNDAMENTOS TEÓRICOS

En el presente capítulo constan todos los fundamentos teóricos que nos permite tener un conocimiento general sobre los conceptos que se aplicarán para el desarrollo de este proyecto en las áreas técnicas de Networking y Cableado Estructurado necesarios para la ejecución de este proyecto, teniendo en cuenta que para una reestructuración de red es preciso un trabajo conjunto en todos los elementos de red comenzando desde el nivel físico.

2.1. LAS REDES DE COMUNICACIONES

Una red de comunicaciones es el conjunto de dos o más ordenadores enlazados entre sí mediante un canal de comunicaciones para el intercambio de información o compartir recursos utilizando protocolos de red establecidos (Stallings, 2010).

2.1.1. ANTECEDENTES

Las redes de comunicaciones remontan de muchos años atrás, pues desde los inicios de la humanidad las personas ya encontraron formas de comunicarse y en base a esta necesidad se crearon poco a poco las redes de comunicación.

Con el paso de los años y de la mano de los avances tecnológicos en diferentes áreas como electricidad, microelectrónica, tecnología óptica, estaciones de trabajo, software y otros se produjo el desarrollo de dispositivos que faciliten la creación de redes de comunicación, el primero de ellos fue “el telégrafo que a principios del siglo 19 tuvo su

auge y en base a este se crearon posteriormente la red telegráfica y la red telefónica." (Puerto, Ortega, Capmany, Cardona , & Suárez, 2008)

Inicialmente "las redes de comunicaciones fueron diseñadas para diferentes servicios, como son la red telefónica, las redes de datos y las redes de distribución como es la transmisión de imágenes de televisión" (Puerto, Ortega, Capmany, Cardona , & Suárez, 2008).

Las redes de comunicación eran redes analógicas y fue partir de los años 60 cuando surgieron los principios de transmitir información digital, con sistemas que solamente ofrecían una conexión de tipo cliente-servidor. Pero la verdadera historia de las redes de comunicación comienza con el establecimiento de las redes de conmutación de paquetes.

Según Fabregat Gesa, (2010) señala que "la primera red experimental de conmutación de paquetes se utilizó en el Reino Unido, en los National Physics Laboratories, otro similar fue en Francia la Societe Internationale de Telecommunications Aeronautics. Años después se implantaría la utilización de este tipo de redes en ARPA[6] que es la agencia de proyectos avanzados de investigación para la defensa", pero era utilizada únicamente para la defensa nacional, es decir, fines militares y políticos.

[6] ARPA=Advanced Research Projects Agency, es una agencia de Estados Unidos responsable del desarrollo de nuevas tecnologías para uso militar

A partir de 1981 cuando IBM[7] lanzo al mercado el computador personal dirigido últimos usuarios, estos vieron la necesidad de compartir información; progresivamente los usuarios fueron reuniéndose para conectarse entre sí y formar pequeños grupos para el intercambio de la información (Diaz, 2012). Poco a poco al aumentar la demanda de procesar y obtener información se han ido mejorando las técnicas de procesamiento de datos, creando así grandes avances de la tecnología informática que han hecho de las comunicaciones digitales una de las herramientas más importantes de la era actual.

2.1.2. IMPORTANCIA

Las redes de comunicación hoy son una herramienta indispensable no solo en las empresas que manejan grandes volúmenes de datos, sino también para todas las personas en sus actividades diarias. Es necesario comprender que el futuro de las comunicaciones en el mundo están lideradas por las redes, desde el momento en que conectamos una PC[8] a internet ya somos parte de la red de comunicaciones más grande que existe.

Las redes de comunicaciones no solo son importantes para compartir información sino también para compartir recursos y uno de sus objetivos es lograr que los programas, datos y equipo estén disponibles para cualquier elemento de la red que así lo requiera, sin importar la ubicación física del recurso.

La importancia de las redes se soporta en las siguientes prestaciones.

- Compartir programas, archivos y computadoras.
- Compartir recursos.
- Compartir Bases de Datos.

[7] IBM=Internatinal Business Machines, es una empresa multinacional de tecnología
[8] PC=Personal Computer, equipo de computación de uso personal

- Trabajo en grupo
- Control centralizado
- Seguridad

2.2.MODELOS DE REFERENCIA

Los modelos de referencia permiten el análisis de redes basadas en capas, nos facilitan la comprensión de los protocolos de comunicación y la arquitectura de los sistemas (Tanenbaum & Wetherall, 2012).

2.2.1. MODELO DE REFERENCIA ISO[9]/OSI[10]

Es un modelo creado por la Organización Internacional de Estandarización, el cual permite la Interconexión de Sistemas Abiertos OSI, es decir, sistemas heterogéneo (Stallings, 2010).

No es una arquitectura de red, pues no especifica servicios y protocolos que se utilizaran en cada uno de las capas, solo indica lo que cada capa realiza.

Este modelo está estructurado en 7 niveles o capas (Tanenbaum, Redes de computadoras, 2003):

- **Capa 7, Aplicación.-** Es la interfaz del usuario final con la red.
- **Capa 6, Presentación.-** establece una sintaxis y semántica de la información transmitida.
- **Capa 5, Sesión.-** Permite a usuarios en diferentes máquinas establecer una sesión.

[9] ISO=International Standards Organization, es una organización Internacional de Normalización
[10] OSI= Open Systems Interconnetion, es un sistema de interconexión abierto

- **Capa 4, Transporte.-** Establece conexiones punto a punto sin errores para el envio de mensajes, realiza el control de flujo.
- **Capa 3, Red.-** Envía los paquetes de nodo a nodo ya sea usando un circuito virtual o como datagramas, es decir, realiza enrutamiento de paquetes y control de congestión.
- **Capa 2, Enlace de datos.-** Estructura el flujo de bits bajo un formato predefinido llamado trama, transfiere tramas de forma confiables y provee control de flujo.
- **Capa 1, Física.-** Es la transmisión de bits a través del medio, maneja voltajes y pulsos eléctricos.

La comunicación entre capas es virtual, cada una transfiere los datos a su capa inferior hasta alcanzar el medio físico, los datos que se añade es información de control al mensaje que recibe de la capa superior. En la maquina destino, cada capa lleva a cabo el proceso inverso al antes mencionado. En la Imagen 1 se encuentra una representación de las capas del modelo ISO/OSI.

Imagen 1.-Capas del modelo de referencia ISO/OSI.
Referencia: Andrew Tanenbaum, Redes de computadoras 2003.

Una de las desventajas de este modelo es que existen algunos niveles vacíos y otros muy densos, además de ser muy complejo y difícil de implementar.

2.2.2. ARQUITECTURA TCP/IP[11]

Es una abreviatura de Protocolo de Control de Transmisión/ Protocolo Internet, fue creado originalmente por ARPA Agencia de Proyectos de Investigación Avanzados asociada al departamento de defensa de Estados Unidos, consiste en un conjunto de protocolos que son estándares en Internet (Stallings, 2010).

Este modelo define 4 capas (Tanenbaum, Redes de computadoras, 2003):

- **Capa 4, Aplicación.-** Consiste de programas de aplicación que usa la red como Transferencia de Archivos FTP, Correo Electrónico SMTP, Servicio de Dominio de Nombres DNS y otros.
- **Capa 3, Transporte.-** Permite la comunicación en la red mediante dos protocolos, protocolo orientado a conexión TCP que permite que los datos sean entregados sin error y protocolo no orientado a conexión UDP que es utilizado para aplicaciones en tiempo real.
- **Capa 2, Internet.-** Permite entregar paquetes a la red dejando a estos que viajen separadamente hasta su destino, define un formato de paquete y un protocolo denominado IP.
- **Capa 1, Host-Red.-** Es la encargada de interactuar con el hardware y el encaminamiento de la información a través de la red local, no se define un protocolo a usar.

[11] IP= Internet Protocol, protocolo de internet que identifica de manera lógica y jerárquica a un interfaz

En la Imagen 2 se encuentra las capas del modelo de referencia TCP/IP.

Imagen 2.- Capas del modelo de referencia TCP/IP
Referencia: Andrew Tanenbaum, Redes de computadoras 2003.

2.3. TOPOLOGÍAS DE RED

Una topología de red indica cómo se interconectan los equipos dentro de una red, pero también se puede entender interpretar como la forma en la que viaja la información a través de la red. Es así que se pueden definir dos tipos de topologías, físicas y lógicas (Comer, 1996).

2.3.1. TOPOLOGÍA FÍSICA

"Las topologías físicas dependen de cómo se conecten los equipos, es decir, su ubicación dentro de la estructura de la red". (Osorio, 2011). En las topologías físicas tenemos: topología bus, en anillo, en estrella, en árbol, malla e hibrida que es una combinación de las anteriores.

2.3.2. TOPOLOGÍA LÓGICA

"Se refiere al trayecto seguido por las señales a través de la topología física, es decir, la manera en que las estaciones se comunican", (Norber, 2013) las topologías lógicas dependen de la configuración de los equipos.

2.4.DIRECCIONAMIENTO EN REDES

Para que las redes se comuniquen, se deben poder identificar y localizar entre si y para ello el direccionamiento es una función clave de los protocolos de capa de red pues permite la transmisión de datos entre host de una red o entre diferentes.

Existen dos tipos de versiones de direccionamiento IPv4 e IPv6, IPv4 que es el direccionamiento tradicional e IPv6 que surgió debido al agotamiento de direcciones IPV4. Estas direcciones IP contiene la información necesaria para enrutar y enviar un paquete a través de la red (Comer, 1996).

2.4.1. DIRECCIONAMIENTO IPv4

Las direcciones están constituidas por 32 bits, los cuales están divididos en cuatro octetos, se suelen representar por cuatro números decimales separados por puntos, cada número equivale a cuatro bytes (Tanenbaum, Redes de computadoras, 2003).

A continuación se presenta una dirección IP en notación decimal y binaria:

123.45.67.3=01111011.00101101.01000011.00000011

El esquema de este direccionamiento consta de una porción destinada a la identificación de la red y otra porción destinada a la identificación de un host dentro de esa red.

- **Campo de red:** indica la red a la cual pertenece un dispositivo de red.

- **Campo de host:** indica el dispositivo específico de esa red.

2.4.2. CLASES DE DIRECCIÓN IPv4

Existen 5 clases de direcciones A, B, C, D, E, las mismas que se utilizan de acuerdo al tamaño de la red y de acuerdo a las aplicaciones. "A, B y C para asignar direcciones a redes y host en redes públicas y privadas, D para asignar direcciones de multicast y E para aplicaciones de experimentación e investigación" (Clariá, 2014). En la Imagen 3 se indica las clases de direcciones IPv4 con su respectiva porción de red y porción de host.

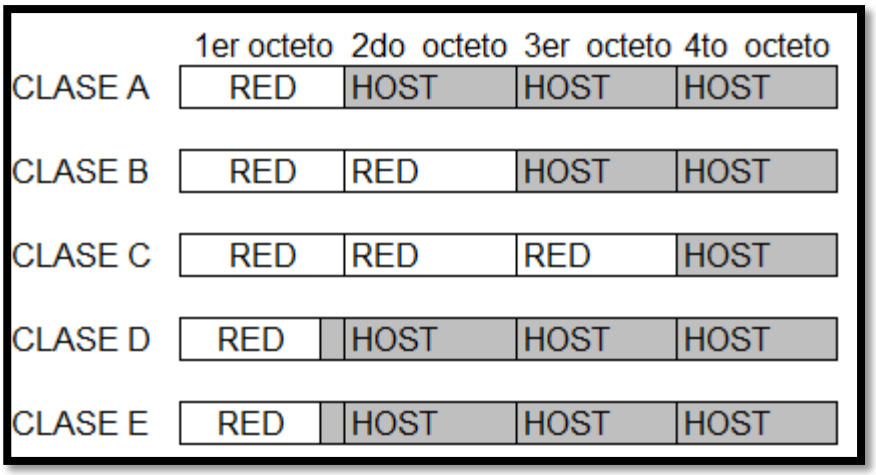


Imagen 3.- Asignación de porción de red y host en cada clase de red.
Referencia: Obtenido de http://alejollagua.blogspot.com/2012/12/direccion-ip-clase-b-c-d-y-e.html

Para identificar cada una de estas redes se lo realiza mediante su primer octeto

2.4.2.1. Clase A

Este tipo de red posee el primer bit del primer octeto siempre en cero, el rango para este tipo de direcciones es de 0.0.0.0 a 127.255.255.255.

2.4.2.2. Clase B

Este tipo de red posee el primer bit del primer octeto siempre en 1 y el segundo siempre es cero, el rango para este tipo de direcciones es de 128.0.0.0 a 191.255.255.255.

2.4.2.3. Clase C

Este tipo de red posee los 2 primeros bits del primer octeto siempre en 1 y el tercero siempre es cero, el rango para este tipo de direcciones es de 192.0.0.0 a 223.255.255.255.

2.4.2.4. Clase D

Este tipo de red posee los tres primeros bits del primer octeto siempre en 1 y el cuarto siempre es cero, el rango para este tipo de direcciones es de 224.0.0.0 a 239.255.255.255.

2.4.2.5. Clase E

Este tipo de red posee los tres primeros bits del primer octeto siempre en 1 y el cuarto siempre es cero, el rango para este tipo de direcciones es de 240.0.0.0 a 255.255.255.255.

2.4.3. NÚMEROS DE HOST Y DE RED

Según William Marin M. para determinar el número de host y de redes contenidas en cada clase se lo obtiene mediante las ecuaciones que detallamos a continuación: la Ecuación 1 es la fórmula para el cálculo del número de redes en cada clase, la Ecuación 2 es la fórmula para el cálculo del número de host en cada clase.

$$\textbf{número de redes} = 2^{n} \qquad \text{Ecuación (1)}$$

$$\textbf{número de hosts} = 2^{n} - 2 \qquad \text{Ecuación (2)}$$

Donde:

n es el número de bits asignados para la porción de hosts como para la porción de red.

En el cálculo de número de hosts se resta menos dos debido a que se debe asignar una dirección para la dirección de red y otra para la dirección de broadcast y estas no pueden ser usadas para host.

Así tenemos que por cada dirección se tiene los siguientes números de redes y de host por red como se muestra en la Tabla 1.

Tabla 1.- Número de hosts y de redes en las direcciones clases A, B y C.

Dirección	Número de redes	Número de hosts por red
Clase A	126	16777214
Clase B	16384	65534
Clase C	2097152	254

Referencia: Andrew Tanenbaum, Redes de computadoras 2003.

2.4.4. MÁSCARA DE RED

"La máscara de red es parte de una dirección IP, la cual consta de una secuencia adicional 32 bits separados en octetos" (Mayám , 2006). Nos sirve para identificar que parte de la dirección IP corresponde a la porción de red y que parte corresponde a la porción de host. Una máscara de red está constituida por unos y ceros, unos para la parte de red y ceros para la porción de host.

Si tenemos una dirección IP clase B, existirá 2 bytes de red y 2 bytes de host y obtendremos una máscara de red 255.255.0.0 como se nuestra en la Imagen 4.

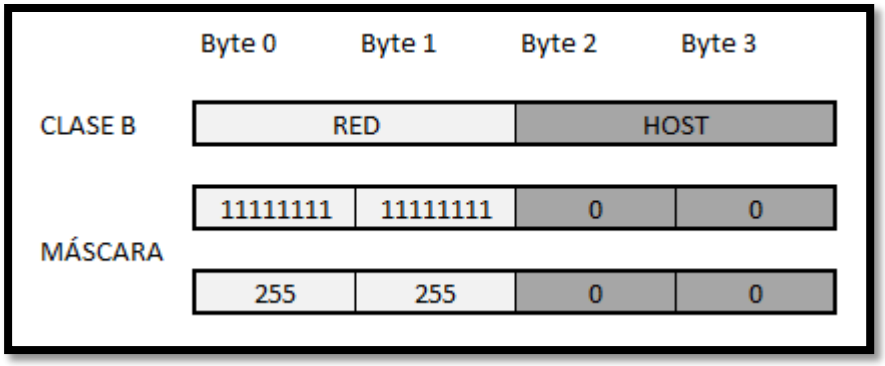


Imagen 4.- Máscara de red para una dirección clase B.
Referencia: Request for Comment 1918 (RFC 1918).

Además la máscara de red también se la identifica con un número decimal que representa la cantidad de unos existentes en la dirección, así para cada clase tenemos las siguientes máscaras de red como se indica en la Tabla 2.

Tabla 2.- Máscaras de red de las direcciones de clase A, B y C

Dirección	Máscara de red
Clase A	255.0.0.0 /8
Clase B	255.255.0.0 /16
Clase C	255.255.255.0 /24

Referencia: Request for Comment 1918 (RFC 1918),

2.4.5. DIRECCIONES IP PÚBLICAS Y PRIVADAS, RESERVADAS Y ESPECIALES

Existen algunas direcciones IPv4 las cuales se utilizan dependiendo de su aplicación, a continuación cada una de ellas (Comer, 1996).

- Las direcciones públicas son aquellas que se utilizan en la Internet y no pueden repetirse en ninguna parte del mundo.

- Las direcciones privadas jamás se las ve directamente en la Internet pública, solamente tienen significado dentro de una red además estas pueden ser utilizadas por varias ocasiones en todo el mundo.
- Las direcciones reservadas son las direcciones de red y las de broadcast, que se utilizan respectivamente para identificar una red y para enviar información a todos los host de dicha red.
- "Existen algunas direcciones reservadas para fines específicos como 127.0.0.0 para pruebas de loopback, 128.0.0.0, 191.0.0.0, 192.0.0.0 y el rango de 240.0.0.0 en adelante" (Ahutzin, 2013).

2.4.6. SUBNETING

Es el procedimiento de creación de subredes para optimizar el recurso de direcciones IPv4, esto consiste en dividir las direcciones full-clase en rangos de direcciones más pequeñas denominados subredes (Comer, 1996).

La creación de subredes hace más versátil el uso de direcciones sin clase ya que facilita y flexibiliza tanto el diseño como la administración de la red, pues estas direcciones son asignadas localmente por el administrador de red y reduce así los dominios de broadcast.

2.5. PROTOCOLOS DE ENRUTAMIENTO

Los protocolos de enrutamiento permiten que los enrutadores o routers determinen cual es la ruta que deben seguir para enviar los datos, todo esto mediante unas tablas llamadas tablas de enrutamiento. Existen protocolos de enrutamiento estático y dinámicos:

- Protocolos de enrutamiento estático: “las rutas son asignadas por el administrador de la red ingresando estas en el router” (Stallings, 2010), por lo tanto el router conoce dichas rutas y sabrá enrutar los paquetes a esas redes.
- Protocolos de enrutamiento dinámico: el administrador se encarga de configurar el protocolo de enrutamiento y los router automáticamente intercambian las tablas de enrutamiento con sus routers vecinos (Tanenbaum, Redes de computadoras, 2003).

Los protocolos de enrutamiento dinámico se clasifican en vector distancia y estado de enlace (Gonzáles Lucas).

- Vector distancia: se basa en el número de saltos, que es la cantidad de routers por los que tiene que viajar el paquete para llegar a su destino, se elige la ruta que tenga el menor número de saltos como la más óptima.
- Estado de enlace: se basa en el retardo, ancho de banda, carga y confiabilidad de los posibles enlaces para llegar a un mismo destino.

2.6.REDES DE ÁREA LOCAL

Una red de área local es una red de extensión limitada comúnmente a un edificio o a pocos kilómetros, al utilizar el término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos. La aplicación más común es para la interconexión entre ordenadores en oficinas de instituciones, empresas fábricas y otros.

2.6.1. REDES DE ÁREA LOCAL INALÁMBRICA

Las redes WLAN[12] utilizan tecnologías de radiofrecuencia para conectar los dispositivos de una red y permitir la comunicación. Es aquella que permite conectar diversos nodos estableciendo una comunicación sin utilizar una conexión física, es decir, sin la necesidad de establecer un cableado estructurado (Bueltrick & Escudero Pascual, 2007).

Este tipo de redes tiene muchas ventanas como:

- Brindar mayor comodidad,
- Ahorro de dinero en infraestructura,
- Instalación sencilla,
- Instalaciones más agradables a la vista
- Fácil incorporación de nuevos usuarios.

2.6.1.1. Estándar IEEE 802.11

El estándar IEEE 802.11 define el uso de los dos niveles más bajos de la arquitectura OSI (capa física y enlace de datos) especificando el funcionamientos dentro de una WLAN. "Este estándar se publicó en 1997 y tenía velocidades de 1 hasta 2 Mbps y trabajaba en las frecuencias de 2,4 GHZ" (Siguencia & León).

El estándar posee varias especificaciones, los mismos que se diferencian por la velocidad de transmisión, área de cobertura y la frecuencia de funcionamiento, entre las principales tenemos:

[12] WLAN= Wireless Local Area Network, redes de area local inalámbricas

2.6.1.1.1. IEEE 802.11a

Según (Bueltrick & Escudero Pascual, 2007)"IEEE aprobó en 1999 los estándares 802.11a y 802.11b, pero en el 2001 se lanzaron los productos con el estándar 802.11a. Utiliza los mismos protocolos del estándar original, opera en la banda de 5 Ghz y trabaja con una velocidad máxima de 54 Mbps". No es compatible con el estándar 802.11b y 802.11g presenta menos interferencias porque trabaja en 5 Ghz y no en 2,4 Ghz que utilizan teléfonos inalámbricos y hornos microondas, pero se requiere línea de vista por lo que se necesita instalar más puntos de acceso. Utiliza OFDM[13] (Orthogonal Frequency Division Multiplexing, Multiplicación por División de Frecuencia Ortogonal), el espectro se divide en 12 canales de 20 Mhz no sobrelapados entre sí.

2.6.1.1.2. IEEE 802.11b

Según (Siguencia & León) "Esta norma tiene una velocidad máxima de 11 Mbps y utiliza el método de acceso CSMA/CA[14] definido en el estándar original, este estándar funciona dentro del espectro radioeléctrico en la banda de 204 a 2497 Ghz, el método de modulación es DSSS[15] que se conoce como espectro de difusión de secuencia directa complementaria y utiliza modulación CCK[16] para velocidades de 5.50 a 11 Mbps".

El espectro de frecuencias se encuentra dividido en 11 canales de 22 Mhz de ancho de banda sobrelapados entre sí, pero se tiene 1 grupo de 3 canales que no se sobrelapan entre ellos, como se nuestra en la Imagen 5.

---

[13] OFDM= Orthogonal Frequency Division Multiplexing, Multiplexión por División en Frecuencias Ortogonales

[14] CSMA/CA= Carrier Sense Multiple Access/ Collision Avoidance, acceso múltiple con escucha de portadora y evasión de colisiones

[15] DSSS=Direct Sequence Spread Spectrum, espectro ensanchado por secuencia directa

[16] CCK=Complementary Code Keying, esquema de modulación utilizado con redes inalámbricas

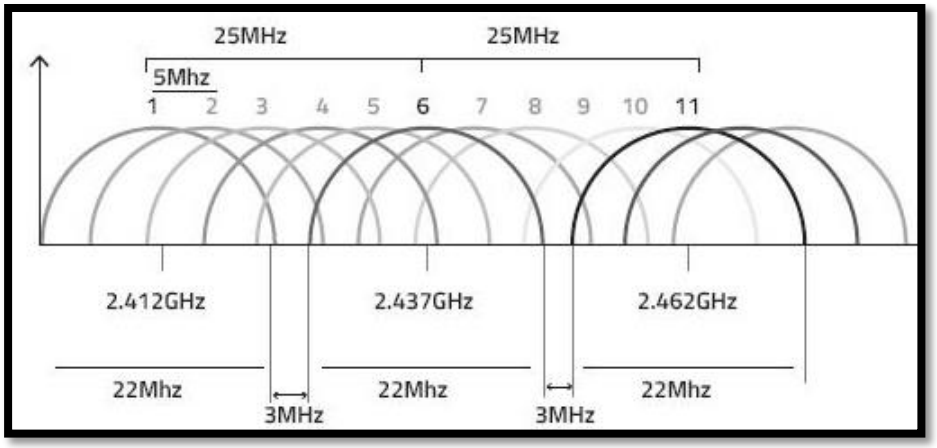


Imagen 5.- Canales del estándar 802.11b
Referencia: Pietroselome, Zennaro, Fonda, & Okay, Redes inalámbricas en los pises desarrollados, 2013.

2.6.1.1.3. IEEE 802.11g

" Opera en frecuencias de 2.4 Ghz, tiene compatibilidad con los estándares anteriores, así para velocidades de hasta 54 Mbps utiliza modulación OFDM y para velocidades hasta 11Mbps funciona igual que 802.11b" (Varela & Domínguez, 2002).

2.6.1.1.4. IEEE 802.11n

"Utiliza los mismos tipos de modulación de 8022.11a y 802.11g, opera en las frecuencia de 2.4 Ghz y 5Ghz, utiliza una técnica de multiplexación MIMO[17] para mejorar la velocidad de transmisión al utilizar varias antenas para transmisión y recepción simultáneamente, las velocidades van de 6.5 Mbps a 300 Mbps" (Pietroselome, Zennaro, Fonda, & Okay, 2013).

[17] MIMO= Multiple-input Multiple-output, múltiple entrada múltiple salida

2.7.ELEMENTOS DE LAS REDES DE COMUNICACIÓN

Las redes de comunicación se componen por varios elementos entre los cuales para el desarrollo de esta tesis los clasificaremos en: Sistema eléctrico, sistema pasivo, sistema activo, hardware y aplicaciones.

2.7.1. SISTEMA ELÉCTRICO

Este sistema permite que los equipos que existan en la red puedan entrar en funcionamiento, sin embargo pueden existir algunos disturbios eléctricos que pueden ocasionar interferencias en el funcionamiento de dichos dispositivos y en algunos casos a los seres humanos, entre los principales tenemos: impacto de rayo, transitorios, cortes de energía, sobrecargas y electricidad estática.

Por todo ello es necesario poseer en la red un sistema de protección eléctrica, el cual garantice seguridad ante esos inconvenientes, esto se lo realiza mediante la norma ANSI/TIA/EIA-607B.

2.7.1.1. ESTÁNDAR ANSI/TIA/EIA-607B.1

El propósito de esta norma es brindar los criterios de diseño e instalación del sistema de aterramiento para edificios comerciales, es decir, dicta las normas para asegurar el nivel de confiabilidad de referencia a tierra eléctrica para todos los elementos de telecomunicaciones. En abril del 2012 fue publicado el estándar ANSI/TIA/EIA-607B y actualizado en enero del 2013, incluyendo recomendaciones para aterramientos para torres y antenas.

2.7.1.1.1. Elementos

Según el estándar ANSI/TIA/EIA-607B los elementos de la norma son los siguientes:

- Barra colectora de puesta a tierra principal de telecomunicaciones (TMGB[18])
- Barra colectora de puesta a tierra de telecomunicaciones (TGB[19])
- Columna vertebral de unión telecomunicaciones (TBB[20])
- Conductor de unión para telecomunicaciones (BCT[21])
- Ecualizador de puesta a tierra (GE[22])

A continuación, en la Imagen 6 se indica una representación de los elementos según el estándar para un edificio con un solo ocupante.

[18] TMGB= Telecomunications Main Grounding Busbar, barra colectora de puesta a tierra principal de telecomunicaciones
[19] TGB= Telecommunications Grounding Busba, barra colectora de puesta a tierra de telecomunicaciones
[20] TBB= Telecommunications bonding backbone , columna vertebral de unión telecomunicaciones
[21] BCT= Bonding conductor for telecommunications, conductor de unión para telecomunicaciones
[22] GE= Grounding Equalizer, ecualizador de puesta a tierra

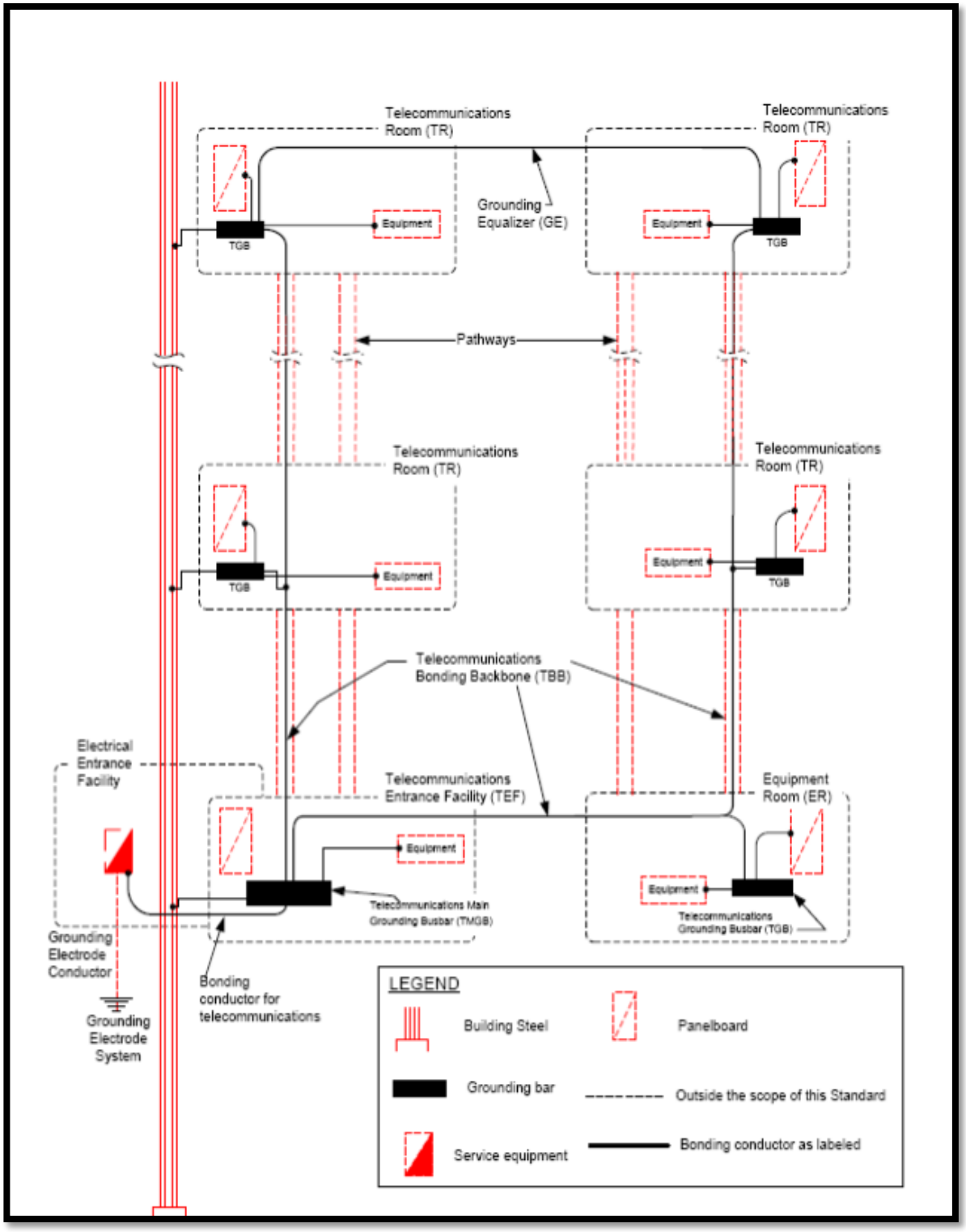


Imagen 6.- Componentes de puesta a tierra en cableado estructurado según la norma.
Referencia: Estándar ANSI/TIA/EIA-607B.1, 2013

2.7.1.1.2. Consideraciones de diseño

Según el estándar ANSI/TIA/EIA-607B las consideraciones son:

- **Barra principal de tierra para telecomunicaciones, TMGB**

Este conductor de tierra debe estar forrado, preferentemente de color verde, y debe tener una sección mínima de 6 AWG, debe estar correctamente identificado mediante etiquetas adecuadas. Es recomendable no sea ubicado dentro de canalizaciones metálicas. En caso de tener que alojarse dentro de canalizaciones metálicas, éstas deben estar eléctricamente conectadas al conductor de tierra en ambos extremos.

La TMGB es el punto central de tierra para los sistemas de telecomunicaciones. Se ubica en las Instalaciones de Entrada, o en la Sala de Equipo. Típicamente hay una única TMGB por edificio, y debe ser ubicada de manera de minimizar la distancia del conductor de tierra hasta el punto de aterramiento principal del edificio.

La TMGB debe ser una barra de cobre, con perforaciones roscadas según el estándar NEMA. Debe tener como mínimo 6 mm de espesor, 100 mm de ancho y largo adecuado para la cantidad de perforaciones roscadas necesarias para alojar a todos los cables que lleguen desde las otras barras de tierra de telecomunicaciones. Deben considerarse perforaciones para los cables necesarios en el momento del diseño y para futuros crecimientos

- **Barras de tierra para telecomunicaciones, TGB**

En la Sala de Equipos y en cada Sala de Telecomunicaciones debe ubicarse una TGB. Esta barra de tierra es el punto central de conexión para las tierras de los equipos de telecomunicaciones ubicadas en la Sala de Equipos o Sala de Telecomunicaciones.

De forma similar a la TMGB, la TGB debe ser una barra de cobre, con perforaciones roscadas.

Debe tener como mínimo 6 mm de espesor, 50 mm de ancho y largo adecuado para la cantidad de perforaciones roscadas necesarias para alojar a todos los cables que lleguen desde los equipos de telecomunicaciones cercanos y al cable de interconexión con el TMGB. Deben considerarse perforaciones para los cables necesarios en el momento del diseñado y para futuros crecimientos.

- **Backbone de tierras TBB**

Entre la barra principal de tierra (TMGB) y cada una de las barras de tierra para telecomunicaciones (TGB) debe tenderse un conductor de tierra, llamado TBB Telecommunications Bonding Backbone. El TBB es un conductor aislado, conectado en un extremo al TMGB y en el otro a un TGB, instalado dentro de las canalizaciones de telecomunicaciones.

El diámetro mínimo de este cable es 6 AWG y no puede tener empalmes en ningún punto de su recorrido. En el diseño de las canalizaciones se sugiere minimizar la distancia del TBB.

2.7.2. SISTEMA PASIVO

Según (Suquillo, 2011) “este sistema lo componen la infraestructura física, cableado estructurado, centro de datos”, que son los sistemas que permiten el correcto funcionamiento y transmisión de información entre los diferentes dispositivos activos de la red.

2.7.2.1. Data Center

"Un data center es un lugar diseñado y construido bajo normas internacionales de seguridad e infraestructura, tanto física como logística que sirva para situar equipos informáticos y/o información" (Palacio, 2010). El centro de datos debe cumplir con condiciones ambientales, eléctricas, escalabilidad y continuidad. Esta área tomo como base el estándar ANSI/EIA/TIA 942, la cual divide la infraestructura de un Data Center en cuatro subsistemas:

- Telecomunicaciones.
- Arquitectura.
- Sistema eléctrico.
- Sistema mecánico.

En el estándar se plantea cuatro niveles llamados Tier, en donde a mayor número de Tier mayor la disponibilidad y a su vez mayor es el costo de construcción.

Según la norma ANSI/EIA/TIA 942 los Tier se clasifican de la siguiente manera y con las siguientes caracteristicas:

Tier I.- Centro de datos Básico, con una disponibilidad del 99.671%.

- El servicio puede interrumpirse por actividades planeadas o no planeadas.
- No hay componentes redundantes en la distribución eléctrica y de refrigeración.
- Puede o no puede tener suelos elevados, generadores auxiliares o UPS.
- Tiempo medio de implementación, 3 meses.

- La infraestructura del datacenter deberá estar fuera de servicio al menos una vez al año por razones de mantenimiento y/o reparaciones (Guillarte, 2013).

Tier II.- Centro de datos Redundante, con una disponibilidad del 99.741%.

- Menos susceptible a interrupciones por actividades planeadas o no planeadas.
- Componentes redundantes (N+1)
- Tiene suelos elevados, generadores auxiliares o UPS.
- Conectados a una única línea de distribución eléctrica y de refrigeración.
- De 3 a 6 meses para implementar.
- El mantenimiento de esta línea de distribución o de otras partes de la infraestructura requiere una interrupción de las servicio.

Tier III.- Centro de datos Concurrentemente Mantenibles, con una disponibilidad del 99.982%.

- Permite planificar actividades de mantenimiento sin afectar al servicio de computación, pero eventos no planeados pueden causar paradas no planificadas.
- Componentes redundantes (N+1)
- Conectados múltiples líneas de distribución eléctrica y de refrigeración, pero únicamente con una activa.
- De 15 a 20 meses para implementar.
- Hay suficiente capacidad y distribución para poder llevar a cabo tareas de mantenimiento en una línea mientras se da servicio por otras.

Tier IV.- Centro de datos Tolerante a fallos, con una disponibilidad del 99.995%.

- Permite planificar actividades de mantenimiento sin afectar al servicio de computación críticos, y es capaz de soportar por lo menos un evento no planificado del tipo ‘peor escenario’ sin impacto crítico en la carga.
- Conectados múltiples líneas de distribución eléctrica y de refrigeración con múltiples componentes redundantes (2 (N+1) significa 2 UPS con redundancia N+1).
- De 15 a 20 meses para implementar.

2.7.2.2. Cableado Estructurado

Es el conjunto de elementos pasivos (cables, conectores, canalizaciones y dispositivos) de un edificio o varios, para interconectar equipos activos de diferentes o iguales tecnologías que nos permite la integración de diferentes sistemas o servicios que dependen del tendido de cables como datos, telefonía, control y otros.

2.7.2.2.1. Antecedentes

En la década de los 80s no existían estándares para instalar cableados para los sistemas de comunicación, cada sistema tenía sus propios requerimientos de acuerdo al servicio que brindaban. Los primeros sistemas de cableado fueron concebidos por las empresas de telefonía, seguidas por las empresas de sistemas de cómputo, la instalación del cableado de datos se realizaba después de la construcción de los edificios (Guillarte, 2013).

Conforme aumentaba el auge de los sistemas de comunicaciones, más compañías adquirían estos sistemas, y fue una gran inconformidad al tener que instalar diferentes

cableados por cada servicio, además de que con cada cambio tecnológico en sus sistemas se debía cambiar su cableado.

Así en 1985, la CCIA[23] (Computer Communications Industry Association) pidió a la EIA (Electronic Industries Alliance) realizar un estándar para los sistemas de cableados, el comité asignado fue el TR-41 quien elaboro las respectivas recomendaciones llamadas estándares, que aplican hasta la actualidad pero con ciertas actualizaciones. Uno de los estándares o norma publicados es ANSI/EIA/TIA-568 Commercial Building Telecommunications Cabling Standard que especifican una guía completa en la selección e instalación de los sistemas de cableado estructurado en edificios comerciales.

2.7.2.2.2. Importancia

La importancia de poseer un cableado estructurado se radica principalmente en los siguientes puntos:

- El tendido de cables es sencillo y fácil de administrar.
- Permite realizar el cableado sin conocer los equipos de comunicaciones que se instalaran.
- Las fallas son menores respecto a un sistema convencional y fácil de localizar.
- El costo inicial de un sistema de cableado estructurado puede ser elevado, pero permite ahorra dinero durante la vida útil del sistema (Diaz, 2012).

[23] CCIA= Computer Communications Industry Association, Asociación de la Industria en Informática Comunicaciones

2.7.2.2.3. Características

Debe cumplir con ciertas características que garanticen los requerimientos de la red.

Según Ander Delgado las características de un cableado estructurado son:

- **Capacidad.-** permite la fácil ubicación y reubicación de usuarios, además permite transmitir información de diferentes tecnologías.
- **Flexibilidad.-** permite integrar nuevos o más servicios a la red, así como modificar la distribución interna.
- **Diseño.-** permite realizar una ubicación más agradable a la vista, utilizando menos espacio que el cableado tradicional.
- **Integración.-** permite unir en una misma infraestructura los servicios de datos, telefonía, audio, video, seguridad y más.
- **Administración.-** permite un mejor manejo de los servicios conectados.
- **Modularidad.-** permite un fácil crecimiento de la red.
- **Compatibilidad.-** cumple con los estándares internacionales.

2.7.2.2.4. Organismos de Normalización

Existen algunos organismos de normalización entre los principales tenemos:

- ANSI[24].- Es una organización sin fines de lucro fundada en 1918, la cual administra y coordina el sistema de estandarización del sector privado de los Estados Unidos.

[24] ANSI= American National Standars Institute, Instituto Americano de Estándares Nacionales

- EIA[25].- Desarrolla normas y publicaciones en áreas técnicas sobre los componentes electrónicos, electrónica de consumo, información electrónica y de telecomunicaciones.
- TIA[26].- Es el estándar usado en Estados Unidos y representa el área de telecomunicaciones de la EIA.
- ISO[27].- Es la organización más grande a nivel mundial, desarrolla y publica estándares internacionales, es una red de institutos en más de 157 países.
- IEEE[28].- Se encarga de la ingeniería de procesos creando, integrando y aplicando el conocimiento.

2.7.2.2.5. Estándar ANSI/TIA/EIA-568C.2

Detalla las especificaciones y procedimientos para la validación y certificación del cableado estructurado ya instalado en una edificación. El boletín establece como marco de referencia dos tipos de configuraciones de verificación por enlace básico o canal; estos dos tipos de configuraciones se diferencian básicamente por los componentes que incluyen su configuración, en el caso del canal se abarca tanto el enlace permanente como los patch cord de conexión utilizados en el ambiente de trabajo, en cambio en el caso del enlace no se consideran los patch cord sino más bien enlaces de prueba.

Los parámetros que se analizan en la certificación del cableado estructurado, que es una verificación de las terminaciones pin a pin son los siguientes:

[25] EIA= Electronics Industry Alliance.
[26] TIA= Telecommunications Industry Association.
[27] ISO= International Standards Organization.
[28] IEEE= Intitute of Electrical and Electronics Enginners

- Continuidad con el extremo remoto.
- Pares reversos
- Pares divididos
- Pares transpuestos
- Cualquier otro defecto de conexión.

Estos parámetros se los analiza por cada uno de los conductores el mapa de cableado. La correcta conectividad está basada en los siguientes aspectos:

- **Longitud.-** La longitud física del enlace está defina por la suma de los enlaces independientes existentes entre dos puntos finales. La longitud máxima de un enlace permanente es de 90m.

- **Pérdida de inserción.-** es medida por la pérdida de señal en un enlace permanente. Ésta se origina por la pérdida de energía eléctrica en la resistencia del cable. Su valor se mide en dB, para valores más bajos de atenuación se tiene un mejor rendimiento del cable.

- **Pérdida de Retorno.-** se mide como la diferencia entre la potencia de la señal transmitida y la potencia de las reflexiones de la señal causadas debido a las variaciones en la impedancia de la señal. Los valores altos indican que los cables son más eficientes para la transmisión de señales en una red LAN ya que se pierde poca señal por causa de reflexiones.

- **Pérdida de paradiafonía NEXT[29].-** ó interferencia de extremo cercano. Causada por la interferencia de señales cercanas de un par de cables en otro par cercano. El NEXT se expresa en dB, para valores más altos de NEXT se tiene menor interferencia en la señal y un mejor rendimiento del cable utilizado.
- **Pérdida de paradiafonía por suma de potencia (PSNEXT[30]).-** es la combinación de forma estadística del crosstalk recibido de los pares desde los extremos cercanos que operan simultáneamente.

- **Pérdida de paradiafonía en el extremo lejano por igualación de nivel (ELFEXT[31]).-** indica la relación entre el FEXT[32] y la atenuación. Es una medida expresada en dB, influida por el trenzado de los cables, el apantallamiento, así también la frecuencia de trabajo y la longitud del enlace. Un nivel alto de ELFEXT indica una buena transmisión del enlace.

- **Pérdida de paradiafonía en el extremo lejano por igualación de nivel y suma de potencia (PSELFEXT[33]).-** es una medida que se deriva del cálculo de las medianas del ELFEXT de cada par de cables. Su medida se encuentra influenciada por el trenzado de los cables, su apantallamiento, además de la frecuencia de trabajo y la longitud del enlace. Un valor alto de esta medida está relacionado a una buena transmisión en el enlace.

[29] NEXT: Near-End crosstalk, Interferencia de Extremo Cercano - Paradiafonía
[30] PSNEXT: Power Sum Near-End crosstalk, Paradiafonía de suma de potencias
[31] ELFEXT: The Equal-Level Far-End Crosstalk, Telediafonía por igualación de nivel
[32] FEXT: Far-End Crosstalk, Interferencia de Extremo Lejano - Telediafonía
[33] PSELFEXT: Power Sum the Equal-Level Far-End Crosstalk, Telediafonía de suma de potencias

- **Retardo en la propagación.-** indica el tiempo en que una señal tarda en propagarse de un extremo a otro.

- **ACR[34].-** indica la relación entre la atenuación y la interferencia. Un valor alto de ACR indica que las señales recibidas son mucho más grandes que la interferencia, ó que se tiene un NEXT alto y valores de atenuación bajos.

2.7.2.2.6. Estándar ANSI/TIA/EIA-569C

Norma de recorridos y espacios de telecomunicaciones en edificios comerciales, esta norma específica el diseño de espacios y las prácticas para la construcción de un cableado estructurado, no normaliza los medios de comunicación o los equipos a utilizar. Permite al diseñador de telecomunicaciones seleccionar correctamente entre las alternativas la que más se adecue a la realidad de la infraestructura física.

A continuación se indica las vías y espacios en un edificio típico con un solo ocupante, ver Imagen 7.

[34] ACR: Attenuation/Crosstalk Ratio, Relación atenuación - diafonía

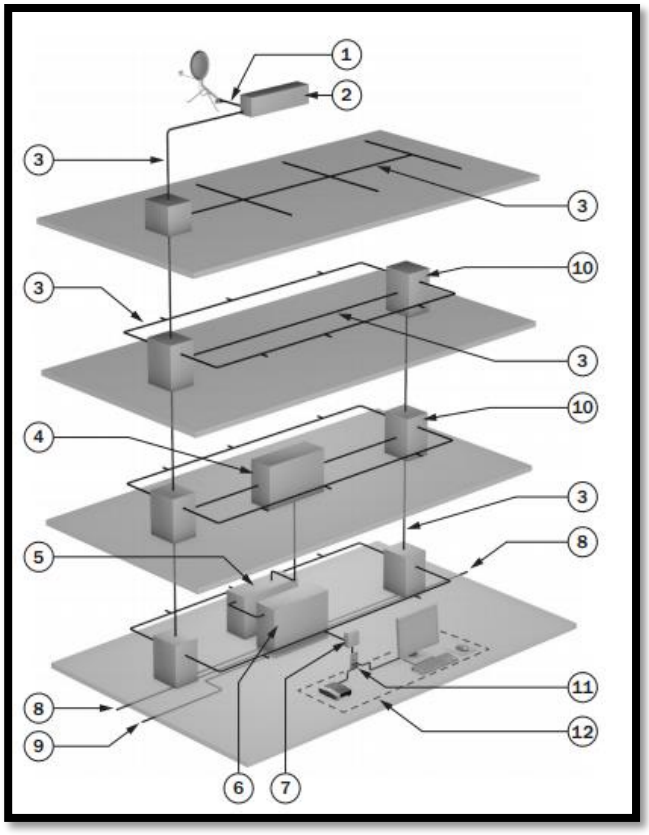


Imagen 7.- Vías y espacios en un edificio típico con un solo ocupante.
Referencia: Estándar ANSI/TIA/EIA-569C

En donde según el estándar ANSI/TIA/EIA-569C:

1. Vía de entrada de servicio inalámbrico
2. Sala de entrada
3. Vías de construcción
4. Sala de distribuidor
5. Espacio proveedor de servicios
6. Sala de entrada
7. Caja de distribución
8. Vía de entrada de servicio
9. Diversidad de las rutas de entrada

10. Sala de distribuidor
11. Toma de equipo
12. Ubicación de la toma de equipos

Según el estándar ANSI/TIA/EIA-569C:

- **Requisitos comunes para los espacios físicos de telecomunicaciones.**

Los requisitos de esta sección se aplican a los siguientes espacios de telecomunicaciones: Sala de distribuidor, sala de distribuidor común, sala de entrada, espacio proveedor de acceso, y el espacio proveedor de servicios.

- Evite seleccionar ubicaciones que están restringidas por la construcción de componentes que limitan la expansión tales como ascensores, paredes exteriores o la construcción de muros fijos.
- Altura mínima del techo será de 2,4 m y sin obstrucciones. La altura entre el suelo acabado y el punto más bajo del techo debe ser un mínimo de 3 m para dar cabida a equipos más altos y las vías aéreas.
- Iluminación de un mínimo de 500 lux en el plano horizontal y 200 lux en el plano vertical mide 1 m por encima del piso terminado.
- La puerta será de un mínimo de 0,9 m de ancho y 2 m de altura .Una puerta doble de 1,8 m de ancho por 2,3 m de altura.
- No debe haber ventanas exteriores.
- Control ambiental tales como la distribución de energía y sistemas de acondicionado y sistemas de UPS, de hasta 100 kVA.
- Protección contra incendios.

- Los espacios de telecomunicaciones no se encuentran por debajo del nivel del agua, a menos que se emplean medidas preventivas para evitar infiltración de agua.
- Deberá estar libre de las tuberías de agua o drenaje.

- **Requisitos sala de telecomunicaciones**

La sala de distribución es un punto de acceso común para los subsistemas de cableado y las vías de construcción. Puede contener equipos de telecomunicaciones, terminaciones de cables y el cableado transversal de conexión asociado. La sala de distribuidor también puede contener información de equipos de tecnología y sistemas de automatización de equipo de construcción y el cableado. La sala de distribuidor se dedica a la función de las telecomunicaciones y no debe ser compartido con instalaciones eléctricas que no sean las utilizadas para las telecomunicaciones o equipo relacionado.

- **Requisitos sala de entrada**

Es un punto de entrada para el cableado de planta externa y puede contener cables de proveedores de servicios entrantes, protectores y cables de construcción. Una sala de entrada también puede servir como una sala de distribuidor. Debe cumplir con los requisitos comunes para habitaciones además de:

- Estar ubicado en un lugar seco que no este sujeto a las inundaciones y lo más cerca posible del punto de entrada del edificio.

- Puede ser un área abierta o para los edificios que superen 2.000 m² debe proporcionarse una habitación cerrada.
- Estará situado lo más cerca posible al centro del área ocupada.
- Debe haber un mínimo de 500 lux de luz dentro del recinto.

- **Requisitos bastidores y gabinetes**

- Se dispondrá de un mínimo de 1 m de espacio libre delante de bastidores y gabinetes, pero se prefiere un 1.2 m. Se proporcionará un mínimo de 0,6 m de espacio libre detrás.
- Gabinetes serán seleccionados y configurados para proporcionar una refrigeración adecuada para el equipo que contienen. Hay muchos métodos de enfriamiento disponible.
- La altura máxima del gabinete 2,4 m. Es preferible que sean no más alto que 2.1 m para un acceso más fácil a los equipos instalados en la parte superior.
- Gabinetes deben ser de la profundidad adecuada para acomodar el equipo previsto para ser instalado, incluyendo cableado y la parte delantera y trasera, los cables de alimentación, hardware de gestión de cables y enchufes múltiples.
- Los gabinetes deben tener rieles delanteros y traseros ajustables y debería proporcionar 42 o más unidades de montaje en rack de espacio. Si los paneles de conexión están instalados en la parte delantera o trasera de los gabinetes, los rieles delanteros o traseros deben estar empotrados por lo menos 100 mm para permitir la gestión de cables.

- **Requisitos arquitectónico y ambiental**
  - Localizar la habitación distribuidor tan cerca como sea posible del centro de la zona.
  - El tamaño mínimo de un distribuidor se basará en el número puntos de distribución. La dimensión mínima es de 3 m de largo por 3 m de ancho.
  - Habrá un mínimo de una sala de distribuidor por piso.

2.7.2.2.7. Estándar ANSI/TIA/EIA-606B

Normas de administración de infraestructura de telecomunicaciones en edificios comerciales, proporciona normas para la codificación de colores, etiquetado y documentación de un sistema de cableado instalado. Aplicando esta norma nos permite realizar una mejor administración de la red, además facilita la localización de fallas.

Esta norma tiene el siguiente alcance asignar identificadores a los componentes de la infraestructura, especificando los elementos de información que conforman los registros para cada identificador.

El estándar ANSI/TIA/EIA-606B establece que:

- **Directrices de etiquetado**
  - Cada espacio de las telecomunicaciones (TS) deberá etiquetarse con el identificador TS dentro de la habitación para ser visible a alguien que trabaja en la sala.

- Cada gabinete y cremallera deberán etiquetarse con su identificador en la parte delantera y trasera a la vista.
- El texto en las etiquetas será impreso máquina.
- Los paneles de conexión deben estar etiquetados con su identificador y con el identificador del panel de conexión en el otro extremo.
- Un campus único o identificador de sitio se asignarán a cada escuela o en el sitio.
- Un identificador único edificio se asigna a cada edificio.
- Deberán etiquetarse Todos los puertos en los paneles de conexión y todas las posiciones en los bloques de terminales.
- Los cables terminados en paneles de conexión o bloques de terminación deberán ser identificados por los identificadores de los puertos / terminaciones en ambos extremos del cable.
- Cada cable interior del edificio y interbuilding se asignará un identificador único.
- Puntos de venta de equipos y sus puertos asociados deberán etiquetarse.
- El TMGB y TGB se etiquetarán con sus identificadores.
- Todos los conductores de puesta a tierra deben ser etiquetados con sus identificadores.
- Un identificador firestopping identificará cada instalación de material contra fuego.
- Un registro detallado de todos los elementos de administración se mantendrá tal como se define en la norma.

- **Etiquetas permanentes**
  - El tamaño, el color y el contraste de todas las etiquetas deben ser seleccionados para asegurarse de que los identificadores son fáciles de leer.
  - Las etiquetas deben ser visibles durante el mantenimiento normal de la infraestructura.
  - Las etiquetas deben ser resistentes a las condiciones ambientales (tales como la humedad, calor o luz ultravioleta), y deben tener una vida de diseño igual o mayor que la del componente marcado.

2.7.2.2.8. Estándar ANSI/TIA/EIA-568C. 1

El estándar ANSI/TIA/EIA-568, Cableado de telecomunicaciones para edificios comerciales con cada una de sus actualizaciones especifican los requerimientos de un sistema de cableado que sea independiente de las aplicaciones. Este estándar especifica los requerimientos del cableado dentro de un ambiente de oficina para los cables de cobre y fibra, las distancias recomendadas y parámetros de desempeño de los medios de comunicación.

El tiempo de vida de un cableado estructurado debe ser de 15 a 25 años, pero durante este periodo las tecnologías de telecomunicaciones tienen grandes cambios, es así que este estándar ha tenido varias versiones y actualizaciones, la más reciente es el estándar ANSI/TIA/EIA-568-C.1.

Este último es una revisión del ANSI/TIA/EIA-568-B que fue publicado entre 2001 y 2005, este nuevo estándar es una recopilación de los estándares originales y todas sus

modificaciones cambiando su organización y generando unos estándares más generales a todo tipo de edificios.

El estándar ANSI/TIA/EIA-568-C.1 específica la información sobre el planeamiento, instalación y verificación de cableados estructurados de edificios comerciales.

2.7.2.2.9. Elementos de un sistema de cableado estructurado

Según el estándar ANSI/TIA/EIA-568-C.1 un sistema de cableado estructurado está compuesto por los siguientes elementos:

- **Instalaciones de entrada**

También conocidas como acometidas, es el lugar por donde ingresan los servicios de telecomunicaciones al edificio o donde llegan las canalizaciones de interconexión con otros edificios de una misma empresa.

Pueden contener dispositivos de telecomunicaciones y de interfaz con las redes que prestan los servicios de telecomunicaciones. La norma recomienda que este elemento este en un cuarto aparte por razones de seguridad, pero puede estar dentro del Data Center.

- **Distribuidor o repartidor principal y secundarios**

Main / Intermediate Cross-Connect, son los distribuidores que se manejan de una forma jerárquica, el cableado hacia las áreas de trabajo parten de un punto principal que es la sala de equipos, en este punto se encuentra el distribuidor principal, además el cableado puede pasar por otro distribuidor secundario y por una sala o armario de

telecomunicaciones. El estándar dentro de su modelo jerárquico no permite más de 2 niveles de interconexión hasta la sala de telecomunicaciones.

- **Distribuidor central del cableado**

Conocido también como back-bone, cuya función es proporcionar la interconexión entre los armarios de telecomunicaciones y la sala de equipos y entre este último y las instalaciones de entrada.

Para el diseño el distribuidor central del cableado deben tener en cuenta las necesidades de la red en ese momento, así como las necesidades a futuro, reservando lugar en las canalizaciones. Este estándar admite los siguientes cables para su conexión:

- Cables UTP de 10 ohm.
- Cables de fibra óptica multimodo de 20/125 um.
- Cables de fibra óptica multimodo de 62.5/125 um.
- Cables de fibra óptica monomodo.
- Cable STP-A de 150ohm.

- **Distribuidores o repartidores horizontales**

Horizontal Cross-Connect, son aquellos distribuidores a los cuales llegan los cables de back-bone y se encuentran ubicados en la sala de telecomunicaciones, de igual manera a los repartidores horizontales llegan los cables de las áreas de trabajo. Los

paneles de interconexión pueden ser patcheras con conectores de tipo RJ-45 o regletas de diversos formatos. Si en el armario de telecomunicaciones existe equipos activos se admite conectar directamente los paneles del cableado horizontal a dichos equipos.

- **Distribución horizontal del cableado**

Conecta las áreas de trabajo con los distribuidores horizontales que están ubicados en la sala de telecomunicaciones. La distribución horizontal incluye:

- Cables de distribución horizontal.
- Conectores donde terminan los cables de distribución horizontal hacia las áreas de trabajo.
- Cables de interconexión en la sala de telecomunicaciones

- **Área de trabajo**

Es el lugar donde el personal se encuentra trabajando con computadoras, impresoras, teléfonos, cámaras de video, sistemas de alarmas, etc.

Los componentes del área de trabajo se extienden desde la terminación de la distribución horizontal del cableado hasta el equipo de usuario final. Las áreas de trabajo incluyen los conectores de telecomunicaciones o patch-cords hasta el equipamiento de usuarios finales, este tipo de equipamiento que se instale no incluye en el estándar. La distancia del cable de interconexión no debe superar los 5m.

La siguiente imagen representa los elementos de cableado estructurado de acuerdo al estándar ANSI/TIA/EIA-568C.1.

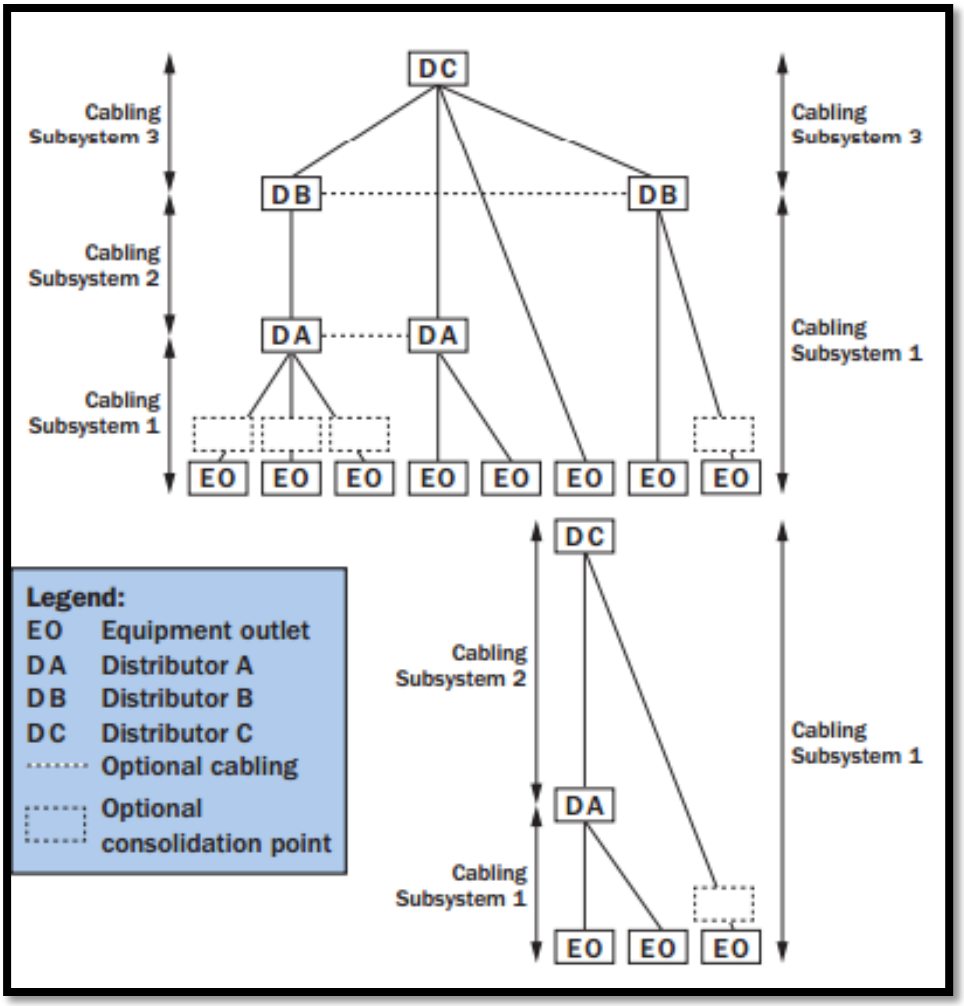


Imagen 8.-Elementos de la topología de cableado genérico
Referencia: Estándar ANSI/TIA/EIA-568C.1

La Imagen 8 es un modelo representativo de los elementos que componen un sistema de cableado genérico en una variedad de entornos. En un edificio de oficinas comercial típico donde se aplica la norma ANSI / TIA-568-C.1, Distribuidor C representa la conexión cruzada principal (MC), Distribuidor B representa la conexión cruzada intermedia (IC), Distribuidor A representa la conexión cruzada horizontal (HC) y la salida de los equipos (EO) representa la salida / conector de telecomunicaciones.

2.7.3. SISTEMA ACTIVO

Según (Suquillo, 2011) “Lo componen todos aquellos dispositivos que permiten la comunicación entre las diferentes aplicaciones y servicios de una red”. Entre ellos podemos encontrar switches, routers, firewall, IPS/IDS, infraestructura Wireless como Access Point.

2.7.3.1. Equipos de conmutación y de ruteo

Conocidos como dispositivos de red, son los dispositivos que transportan la información que deben transmitirse entre dispositivos de usuario final (Clariá, 2014). Estos dispositivos permiten el tendido de conexiones de cable, la concentración de conexiones, la conversión de los formatos de datos y la administración de la información. Algunos ejemplos de ellos son: repetidores, hubs, puentes, switches, routers.

2.7.3.1.1. Routers

Son equipos que se encargan de redirigir paquetes de información desde una interfaz hacia otra, dependiendo de la información existente en su tabla de enrutamiento.

2.7.3.1.2. Switches

Son los encargados de segmentar la red y hacer que los dominios de colisión sean más pequeños.

2.7.3.1.3. Access Point

Según (Ruiz Barcayola, 2013) “Se trata de un dispositivo utilizado en redes inalámbricas de área local, se encarga de ser una puerta de entrada a la red en un lugar específico y para una cobertura de radio determinada, para cualquier dispositivo que solicite acceder, siempre y cuando tenga los permisos necesarios”.

2.7.3.2. FIREWALL

Es un dispositivo físico o un software sobre un sistema operativo, cumple con la función de filtrar el tráfico entre redes a través de sus interfaces de red, es decir, decide si un paquete pasa, se modifica, se convierte o se descarta. En la Imagen 9 podemos ver un esquema de firewall entre una red local e internet.

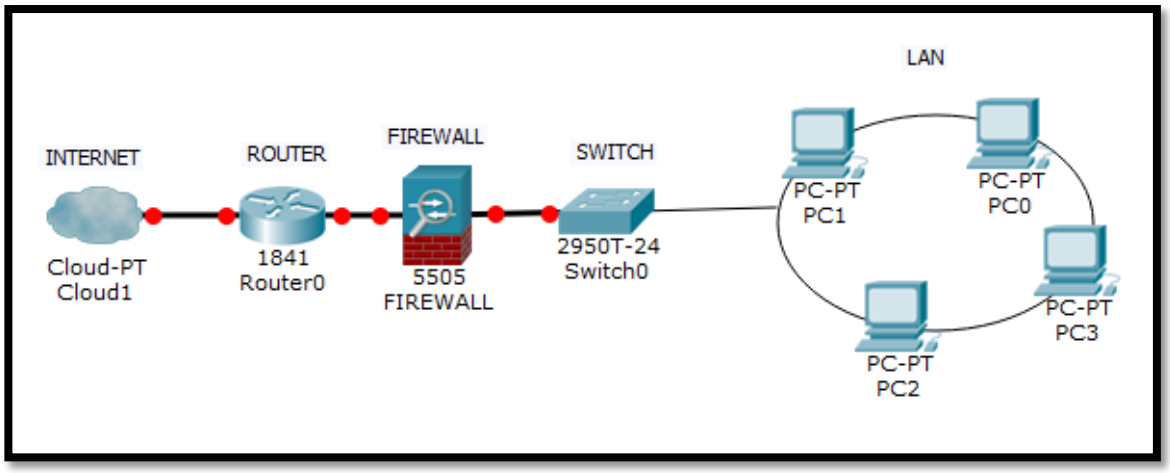


Imagen 9.- Esquema de firewall típico entre red local e internet.
Referencia: Basado en http://www.serranoprada.com/blog/manuel-practico-iptables/

Existen dos maneras de implementar un firewall (Altadill Izura, 2013) :

1. **Política por defecto aceptar.-** Todo lo que entra y sale por el firewall se acepta y solo se denegará lo que sea necesario. Facilita la gestión ya que solo debemos conocer que es lo que queremos denegar en la red.
2. **Política por defecto denegar.-** Todo esta denegado y solo se permite pasar por el firewall aquello que se necesite en la red. El firewall se convierte en muro intraspasable, pero se vuelve más difícil la gestión ya que se debe preparar mucho el firewall.

2.7.4. HARDWARE

Se trata de todos aquellos dispositivos como servidores que permiten brindar servicios en la red y equipos de trabajo que permiten a los hacer uso de esos servicios.

2.7.4.1. EQUIPOS DE TRABAJO

También conocidos como host, conectan a los usuarios con la red y permiten compartir, crear y obtener información (Egli, 2015). Estos pueden existir sin una red, pero sin ella sus capacidades se ven limitadas, pueden ser: computadoras portátiles, computadoras de escritorio, impresoras, teléfonos, entre otros.

2.7.4.2. SERVIDOR

Según (Sierra, 2013) “es un ordenador o maquina informática que está al servicio de otras máquinas suministrando todo tipo de información”, es cualquier equipo que responde a una solicitud de aplicación de cliente. Un servidor suele ser una aplicación pero ejecutados en un hardware como una computadora, es capaz de atender peticiones de un cliente y devolverle una respuesta de acuerdo al tipo de servidor que este sea.

2.7.5. APLICACIONES

Es todo aquello que se maneja en la capa aplicación, maneja protocolos de alto nivel, codificación y control de dialogo. Los protocolos más comunes son: transferencia de archivos, correo electrónico, administración de red, administración de nombres, terminal virtual.

2.8.JERARQUÍA DE RED

Para el diseño de redes LAN se puede utilizar un modelo de arquitectura de red denominado modelo jerárquico o jerarquía de red, el cual permite que la construcción de la red cumpla con las necesidades de la empresa de una manera más exitosa en comparación con otros modelos de diseño (CISCO, 2013).

Un diseño jerárquico implica dividir la red en capas independientes, así cada capa realiza funciones específicas.

2.8.1. CAPAS DE UNA RED JERÁRQUICA

Existen tres capas dentro de este modelo las cuales son: capa núcleo, distribución y acceso (Rosero, 2008).

2.8.1.1. CAPA DE ACCESO

Esta capa es la que se encuentra en contacto directo con los usuarios finales, como PC, impresoras, etc. La finalidad de esta capa es proporcionar un medio de conexión de los dispositivos hacia la red y controlar que dispositivos pueden conectarse o no.

2.8.1.2. CAPA DISTRIBUCIÓN

Esta capa agrega los datos recibidos por los dispositivos de red de la capa núcleo y los transmite hacia la capa de núcleo. En esta capa se ejecuta el enrutamiento, calidad de servicio, control de acceso, provee la recuperación de errores.

2.8.1.3. CAPA DE NÚCLEO

Esta capa es el backbone de la red y por ende debe soportar alta velocidad, se conecta directamente con la capa distribución y a través de esta capa con toda la red. En esta capa debido a su importancia se debe garantizar ciertas condiciones como:

- El núcleo debe ser disponible y redundante.
- Debe reenviar grandes cantidades de tráfico.
- La capa núcleo debe puede conectarse a los recursos de Internet.

Una red jerárquica se encuentra organizada como se muestra la Imagen 10.

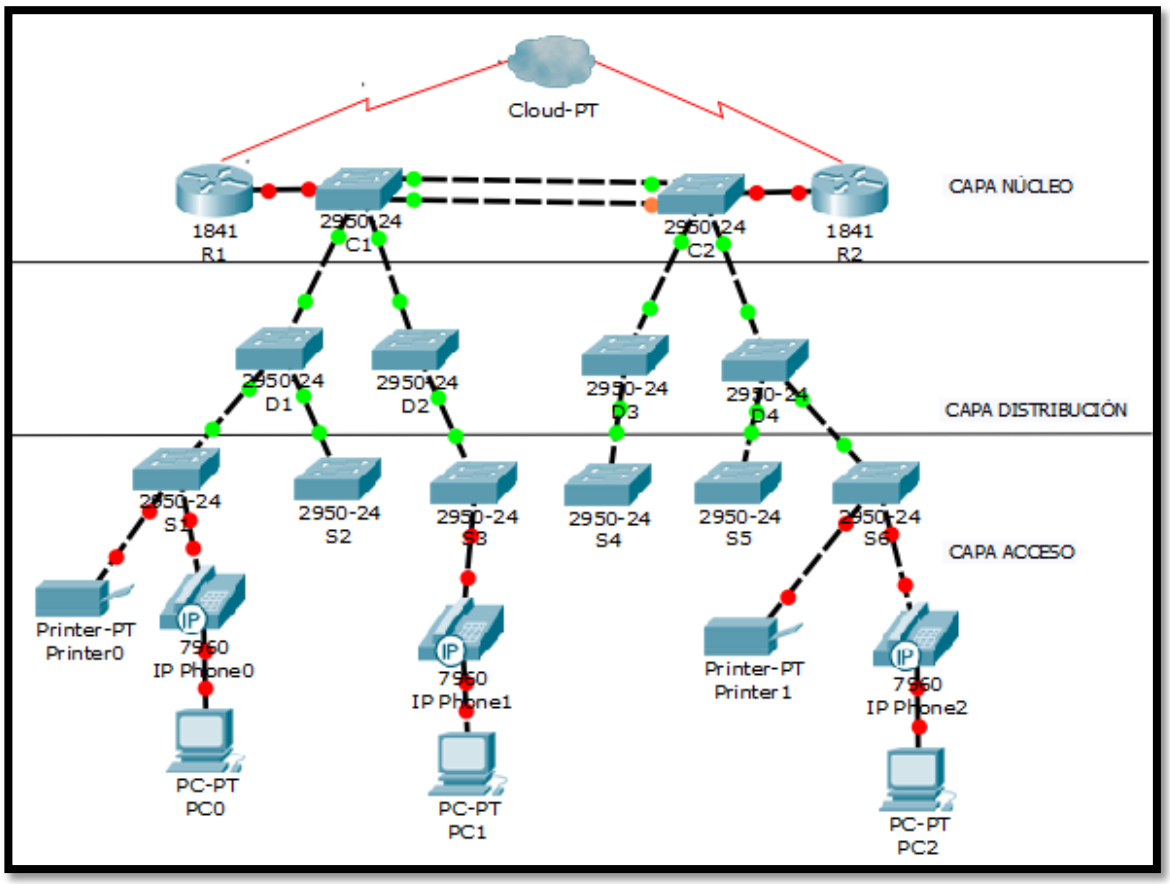


Imagen 10.- Capas de una red jerárquica.
Referencia: Basado en
http://www.systemconsultores.com/data/carpetas/2/CCNA3_Capitulo%201%20Diseno%20de%20la%20LAN.pdf

2.8.2. BENEFICIOS DE UNA RED JERÁRQUICA

Existen muchos beneficios de tener una red jerárquica como se indica a continuación (CISCO, 2013):

- **Escalabilidad.-** Permite un fácil crecimiento y expansión de la red, pues resulta fácil planificar e implementar mayor cantidad de elementos de red por cada capa.
- **Redundancia.-** Conforme una red crece, la disponibilidad de una red se hace más importante y mediante el modelo jerárquico se puede aumentar la disponibilidad fácilmente mediante la implementación de enlaces redundantes. Los enlaces redundantes se aplican desde la capa de acceso hacia la capa de distribución y de esta última hacia la capa de núcleo, así, si algún dispositivo de red (switch) falla se puede conmutar hacia otro dispositivo, no se aplica enlaces redundantes desde la capa acceso hacia el usuario final.
- **Rendimiento.-** El rendimiento en una red mejora al evitar transmitir los datos a través de switches intermedios de bajo rendimiento. Los datos se envían desde el switch de la capa acceso hacia la capa de distribución por lo general a la velocidad del cable, luego la capa distribución envía el tráfico hasta el núcleo utilizando sus capacidades de conmutar, como la capa distribución y núcleo realizan sus operaciones a altas velocidades con un diseño jerárquico apropiado se puede lograr casi la velocidad de cable entre todos los dispositivos.
- **Seguridad.-** La seguridad es más avanzada y más fácil de administrar, pues es posible configurar los switches capa por capa, en capa acceso con varias seguridades por puerto para mantener un control de los dispositivos que se conectan. En la capa distribución creando políticas de seguridad.

- **Fácil administración.-** La administración se vuelve más simple pues cada capa cumple funciones específicas y en el caso de querer realizar un cambio en un switch en una capa se puede repetirse la configuración de otro de la misma capa pues están realizando funciones similares. Además se puede realizar una resolución de problemas más rápida por cada capa.
- **Fácil mantenimiento.-** Esto debido a la escalabilidad que la red jerárquica posee, a medida que la red crece el mantenimiento se vuele mayor pero al mantener este modelo el proceso de mantenimiento es más sencillo.

2.8.3. PRINCIPIOS DE DISEÑO DE UNA RED JERÁRQUICA

El modelo jerárquico presenta algunos beneficios sin embargo estos no se adquieren simplemente al tener este modelo implementado en la red de comunicaciones, hay que realizar un diseño de acuerdo a ciertos principios (Gonzáles Piñones, 2010). Algunos principios de diseño básico son: diámetro de red, ancho de banda y redundancia, al contemplar estos principios estaremos mejorando el diseño de la red jerárquica.

2.8.3.1. DIÁMETRO DE RED

El diámetro de una red representa el número de switches que un paquete debe cruzar entre dos puntos finales. Se debe garantizar un bajo diámetro de red, ya que mientras menor sea el número de dispositivos que deba cruzar menor será la latencia.

2.8.3.2. ANCHO DE BANDA

Dependiendo del ancho de banda que una parte de la red requiera, se puede realizar agregado de ancho de banda entre capas proceso conocido como agregado de enlaces,

esto permite unir varios puertos del switch para lograr un rendimiento superior entre ellos (Norber, 2013). Existe una tecnología propia de Cisco que realiza este proceso llamado Etherchannel del cual trataremos más adelante.

2.8.3.3. REDUNDANCIA

Para garantizar una red altamente disponible, se puede proveer redundancia de varias maneras como duplicando las conexiones o duplicando los dispositivos (Tanenbaum, Redes de computadoras, 2003). La implementación de redundancia puede ser muy costosa, por eso es necesario realizar un análisis de donde se requiera realmente.

2.8.4. CONFIGURACIONES PARA UNA RED JERÁRQUICA

En un diseño de red jerárquica existen varias configuraciones. Las cuales permiten garantizar que este diseño permita obtener los beneficios que una red jerárquica ofrece.

En estas configuraciones tenemos:

2.8.4.1. REDES DE ÁREA LOCAL VIRTUALES

Conocidas como VLAN , permiten dividir a una red en varias subredes creando así una topología independiente de la física, permite agrupar a los usuarios en grupos de trabajo flexibles (Comer, 1996).

La creación de VLANs permite tener algunas ventajas como:

- Mayor flexibilidad en la administración y en los cambios de la red.
- Aumento de la seguridad, pues la información se encapsula en niveles adicionales.
- Disminución en la transmisión de tráfico en la red, ya que permite controlar el tamaño de los dominios de broadcast.

- Para asignar a un usuario a una red, no se depende del cableado físico.

Existen dos tipos de VLAN las cuales se resumen en la Tabla 3:

Tabla 3.- Tipos de VLANs.

Tipo de VLAN	Característica
Estática	Son asignadas manualmente por el administrador, se aplica cuando no existen muchos cambios en la red, configuración sencilla.
Dinámica	Se crea conforme a una base de datos centralizada que asocia direcciones MAC[35] a cada VLAN, es conveniente cuando existen muchos cambios en la red, configuración compleja.

Referencia: Basado en http://www.it.uc3m.es/jgr/publicaciones/06-jcgomez_Telecom.pdf

En la configuración de VLAN tenemos algunos parámetros importantes como son: la configuración de VTP[36], asignación de puertos, 802.1 Q, Port Security.

2.8.4.2. VLAN TRUNKING PROTOCOL

Es un protocolo que mantiene una configuración adecuada de VLAN, administrando la creación, eliminación y renombre de VLANs. Minimiza las malas e inconsistentes configuraciones, además permite realizar los cambios de una manera centralizada y no en cada uno de los equipos (Gómez Martín , García Reionoso, & Valera Pintor). Existen diferentes modos de VTP configurables los mismos que se resumen en la Tabla 4.

[35] MAC=Media Access Control, control de acceso al medio
[36] VTP= Virtual Trunking Protocol, protocolo de enlace troncal

Tabla 4.- Modos de configuración VTP.

Modo VTP	Descripción
VTP server	Puede crear, modificar y eliminar VLANs y especificar parámetros de configuración. Un servidor VTP es el encargado de anunciar las configuraciones a los otros switches que estén en el mismo dominio VTP. Guarda esta información en NVRAM.
VTP client	No puede crear, modificar ni eliminar VLANs. Transmite anuncios y sincroniza la configuración de VLAN.
VTP transparent	Los switches en modo transparente no participan en VTP. No anuncia y no sincroniza su configuración de VLAN.

Referencia: Basado en

http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/779/A5.pdf?sequence=5

2.8.4.3. 802.1 Q

Es un protocolo establecido por el IEEE, conocido como dot1Q, es un mecanismo que permite que múltiples redes compartan de forma transparente el mismo medio físico sin interferencias entre ellas, este medio físico se llama un enlace troncal el cual evita agregar enlaces por cada red (CISCO, 2013).

El estándar especifica el etiquetado de tramas para implementar VLANs insertando un campo de 4 bytes dentro de la trama Ethernet para identificar a que VLAN pertenece esa información, puede soportar hasta 4096 VLANs.

Este campo se inserta entre la dirección origen y el campo de longitud, como se muestra en la Imagen 11.

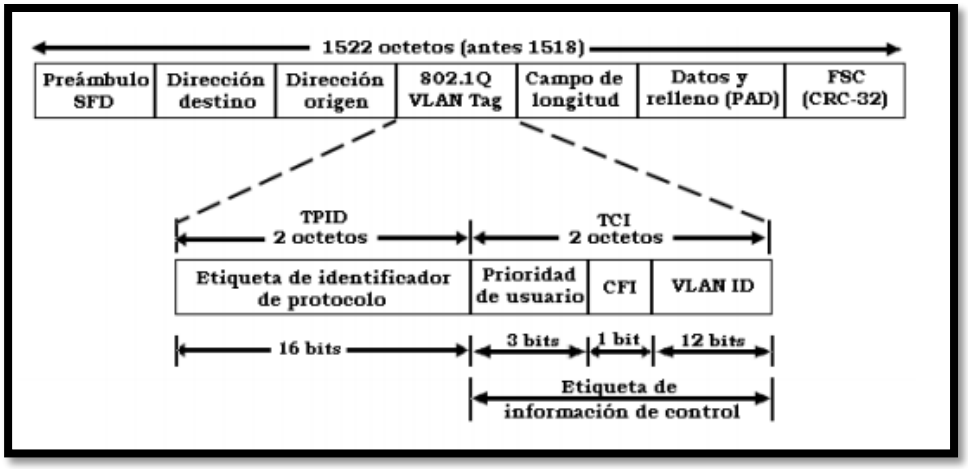


Imagen 11.-Trama Ethernet con el protocolo 802.1 Q
Referencia: Recuperado de
http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/779/A5.pdf?sequence=5

Según (Gómez Martín , García Reionoso, & Valera Pintor) "El campo agregado por 802.1Q consta de dos partes el TPID[37] campo de etiqueta de identificador de protocolo y TCI[38] etiqueta de información de control".

El campo TCI es constituido a su vez por tres sub-campos:

- **Prioridad de usuario.-** Este campo consta de 3 bits, es decir, permite ocho niveles de prioridad.
- **CFI[39].-** "Identificador de Formato Canónico, consta de un bit utilizado para indicar si el paquete encapsulado es una trama Token Ring en un formato de trama Ethernet" (Thaler, Finn, Fedyk, Parsons, & Gray, 2013).
- **VLAN ID[40].-** Indica el número de VLAN al que pertenece.

[37] TPID= Tag Protocol Identifier field, etiqueta del campo identificador de protocolo
[38] TCI= Tag Control Information, etiqueta la información de control
[39] CIF=Canonical Identifier Format, Identificador de formato canónico
[40] ID=Identification, identificación

El campo TPID consta de 2 octetos y se establece en 0 × 8100 para especificar que la etiqueta que sigue es 802.1Q

2.8.4.4. ASIGNACIÓN DE PUERTOS

Como las tramas son conmutadas a través de la red, los switches deben ser capaces de trasportarlas en base a la dirección física asignada. Las tramas son transportadas de acuerdo al tipo de conexión por la cual viajan (Fleury Vicencio, 2007).

Los puertos de cada switch deben llevar una configuración que les defina el modo trabajo que realicen, así pueden definirse como puertos en modo acceso o puertos troncales.

- **Puertos en modo acceso.-** Estos tipos de enlaces solo son parte de una VLAN, los dispositivos conectados asumen que pertenecen a un dominio broadcast, pero estos no conocen la red física. Los switches eliminan cualquier trama que no pertenezca a la VLAN antes de ser enviada a otro dispositivo por el enlace de acceso.

  Los host con este tipo de conexión no pueden comunicarse con otros host que estén fuera de su VLAN a menos que el paquete sea enrutado. Al configurar un puerto en modo acceso se crea un enlace de acceso el cual permite al dispositivo final conectarse a la VLAN correspondiente.

- **Puertos en modo troncal.-** Al configurar un puerto en modo troncal se crea un enlace troncal el cual es un enlace punto a punto entre una o más interfaces de un

switch hacia otro dispositivo como router o switch, estas troncales llevan el tráfico de múltiples VLANs, permiten la comunicación entre VLAN distintas.

2.8.4.5. PORT SECURITY

Mediante port security se puede configurar seguridad en los puertos de un switch por diferentes parámetros, como: limitar el número de direcciones que puedan ser aprendidas en esa interfaz, asignar direcciones MAC a puertos específicos, entre otros. Permite mejorar la seguridad en la capa de acceso que es la que tiene contacto directo con los dispositivos finales (Egli, 2015).

Las direcciones MAC seguras pueden ser configuradas estáticamente, sin embargo, su configuración puede ser una tarea compleja y propensa a errores, por ello la propuesta alterna es configurar port security en la interface del switch, en donde el número de direcciones MAC puede ser limitado a 1, esta primera dirección dinámicamente aprendida por el switch es la dirección segura (Rosero, 2008).

Existen tres tipos de direcciones seguras:

- **Static secure MAC addresses.-** Estas son manualmente configuradas, se almacenan en la tabla de direcciones y se agrega a la configuración del switch ejecutándose.
- **Dynamic secure MAC addresses.-** Son dinámicamente configuradas, almacenadas solamente en la tabla de direcciones y no a la configuración del switch, por ello son eliminadas cuando el switch se reinicia.
- **Sticky secure MAC addresses.-** Estas son dinámicamente configuradas, almacenándose en la tabla de direcciones y agregadas a la configuración

actualmente corriendo, es decir, cuando el switch se reinicia no necesita ser reconfigurado.

2.8.4.6. SPANNING TREE

STP[41] es un protocolo cuya función es gestionar dentro de una red la presencia de bucles en las topologías debido a la redundancia implementada en la red que frecuentemente implica topologías físicas con loops, lo que puede causar varios problemas como tormentas de broadcast, múltiples transmisiones de tramas e inestabilidad en la base de datos de control de acceso al medio. Mediante este protocolo se crea topologías lógicas evitando así los problemas antes mencionados (Ahutzin, 2013).

Este protocolo esta estandarizado en la norma IEEE 802.1d, su función es pagar puertos redundantes y formar un árbol jerárquico estableciendo un nodo raíz que contiene la ruta para alcanzar cada nodo de la red y apagando puertos redundantes, esto se logra gracias a mensajes llamados BPDU[42] que contienen el BID[43] que consiste de una prioridad de bridge que por default tiene un valor de 32768 y la dirección MAC del switch. Los BPDU son enviados cada 2 segundos (CISCO, 2013).

Los BPDUs contienen la información necesaria para que los switches puedan:

- Seleccionar el switch raíz.
- Calcular la ruta más corta hacia el switch root.
- Seleccionar los puertos para los diferentes estados de funcionamiento.

[41] STP= Spanning Tree Protocol, protocol spanning-tree
[42] BPDU= Bridge Protocol Data Unit, protocolo de unidad de enlace de datos
[43] BID= Bridge ID, identificación de bridge

Los estados que los puertos pueden tener se indican en la Tabla 5.

Tabla 5.- Estado de los puertos en STP.

Estado	Características
Bloqueado/Blocking	Solo reciben los BPDUs, las tramas de datos son descartadas y ninguna dirección puede ser aprendida, toma 20 segundos cambiar de este estado.
Escucha/Listening	Determinar si hay otras rutas hacia el root bridge, la ruta que no es la de menor costo hacia el switch root va de regreso al estado bloqueado, dura 15 segundos, los datos de usuario no son enviados y las MAC no son aprendidas.
Aprendiendo/Learning	Los datos de usuario no son reenviados, pero las direcciones MAC son aprendidas, dura 15 segundos.
Enviando/Forwarding	Los datos de usuario son enviados y las MAC continúan siendo aprendidas.
Deshabilitado/Disabled	Ocurre cuando el administrador desactiva un puerto o este falla.

Referencia: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/779/A5.pdf?sequence=5

Cuando en la red conmutada se producen cambios realiza un recalculo en el protocolo STP la cual puede tomar hasta 50 segundos, este tiempo se compone de un tiempo de convergencia máximo de 20 segundos, más el tiempo de escucha de 15 segundos y el tiempo aprendiendo de 15 segundos (CISCO, 2013).

2.8.4.7. RAPID SPANNING TREE PROTOCOL

"Este protocolo se define en el estándar IEEE 802.1w, busca mejorar los tiempos de convergencia el protocolo STP pues su tiempo de convergencia no es mayor que 15 segundos" (Egli, 2015). Introduce una aclaración de los estados y roles de puertos definiendo así:

- Un conjunto de tipos de enlace que puedan cambiar al estado forwarding rápidamente.
- Los switches generan sus propias BPDUs.
- El estado bloqueado de un puerto es renombrado como estado discarding siendo este un puerto alterno que llegara a ser el puerto designado.

2.8.4.8. PVST[44]+

PVST es un protocolo estándar de Cisco, mantiene una instancia STP por cada VLAN configurada en la red. Se basa en el estándar 802.1d y utiliza protocolo de enlace troncal ISL propietario de Cisco, impide la creación de bucles y puede balancear la carga de tráfico de la Capa 2 mediante el envío de algunas VLAN de un enlace troncal y otras de otro enlace troncal pues trata a cada VLAN como una red independiente (CISCO, 2013).

La creación de una instancia para cada VLAN aumenta los requisitos de CPU y de memoria, pero admite los puentes raíz por VLAN. Este diseño permite la optimización del árbol de expansión para el tráfico de cada VLAN, la convergencia de esta versión es similar a la convergencia de 802.1D sin embargo, la convergencia se realiza por cada VLAN existente.

"Para PVST, Cisco desarrolló varias extensiones de propiedad del IEEE 802.1D STP original, como BackboneFast, UplinkFast y PortFast" (Egli, 2015), y agrega mejoras en la protección de BPDU y de raíz.

[44] PVST=Per VLAN Spanning Tree, spanning-tree generado por VLANs

2.8.4.9. LISTAS DE CONTROL DE ACCESO

Según (Delgado Freire, 2011) "Una ACL[45] es una colección secuencial de sentencias de permiso o rechazo que se aplican a direcciones o protocolos de capa superior". Es un concepto de seguridad para implementar la separación de privilegios. Determina permisos de acceso o negación dependiendo de ciertos principios o condiciones que la red requiera. Permiten controlar el flujo del tráfico en equipos de redes como routers y switches.

Existen dos tipos de ACL:

- ACL estándar: permiten autorizar o denegar el tráfico desde direcciones IP de origen, sin importar el destino del paquete ni los puertos involucrados. Se las identifica con número de desde 1 hasta 99.
- ACL extendidas: filtran el tráfico en función de varios parámetros, como: tipo de protocolo, direcciones IP origen y destino, puertos TCP o UDP de origen o destino.

2.8.4.10. ETHERCHANNEL

Es una tecnología propiedad de Cisco, permite la agrupación lógica de varios enlaces físicos Ethernet, considerando esta agrupación como un enlace único, permite sumar la velocidad nominal de cada puerto físico Ethernet y obtener un enlace troncal de alta velocidad. El número máximo de puertos que se puede agrupar es 8 y estos deben manejar las mismas características de configuración (Delgado Freire, 2011).

Podemos configurar un Etherchannel de tres formas diferentes, Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP) o en modo ON.

[45] ACL= Access Control List, listas de control de acceso

- **Protocolo de agregación de enlaces.**

Cuando se configura PAgP el switch negocia con el otro extremo que puertos deben ponerse activos, aquellos puertos que no sean compatibles se dejan desactivados. PAgP es un protocolo propietario de Cisco, PAgP se encarga de agrupar puertos de características similares de forma automática. PAgP es capaz de agrupar puertos de la misma velocidad, modo dúplex, troncales o de asignación a una misma VLAN (Gonzáles Lucas).

PAgP se puede configurar de dos modos:

Auto: establece el puerto en una negociación pasiva, el puerto solo responderá a paquetes PAgP cuando los reciba, pero nunca iniciará la negociación.

Desirable: establece el puerto en modo de negociación activa, este puerto negociará el estado cuando reciba paquetes PAgP y también podrá iniciar una negociación contra otros puertos.

- **Protocolo de agregación de enlaces de control.**

LACP es un protocolo definido en el estándar 802.1ad y que puede ser implementado en switches cisco. LACP y PAgP funcionan de forma muy similar ya que LACP también puede agrupar puertos por su velocidad, modo dúplex, trocales, VLAN (Ruiz Barcayola, 2013).

LACP también tiene dos modos de configuración:

Activo: un puerto en este estado es capaz de iniciar negociaciones con otros puertos para establecer el grupo.

Pasivo: un puerto en este estado es un puerto que no iniciará ningún tipo de negociación pero si responderá a las negociaciones generadas por otros puertos.

Al igual que LAgP, dos puertos pasivos nunca podrán formar un grupo.

- **Configuración Modo ON.**

El modo ON es un modo de configuración en el cual se establece toda la configuración del puerto de forma manual, no existe ningún tipo de negociación entre los puertos para establecer un grupo. En este tipo de configuración es totalmente necesario que ambos lados estén en modo ON.

CAPITULO III

3. ESTUDIO DE LA SITUACIÓN ACTUAL DE LA RED DE COMUNICACIONES DEL GAD PROVINCIAL DE IMBABURA

En el presente capítulo se describe la situación actual de la red de comunicaciones del GAD Provincial de Imbabura, detallando información de la institución como es su estructura organizacional, su misión y visión, el personal que posee y también los elementos de red que la constituyen, ya sean elementos pasivos y activos, las configuraciones actuales y además se realizará un análisis del tráfico en los enlaces de la red, para conocer así los puntos críticos que requieran una reestructuración.

3.1. GOBIERNO AUTÓNOMO DESCENTRALIZADO PROVINCIAL DE IMBABURA

El gobierno provincial de Imbabura es una institución pública cuyo objetivo estratégico principal es el desarrollo económico provincial consolidando el sistema de transporte y movilidad, implementando sistemas de gestión ambiental, fortaleciendo la inclusión social y el desarrollo cultural en busca de una provincia más equitativa, solidaria e intercultural (PREFECTURA DE IMBABURA, 2015).

Imagen 12.- GAD Provincial de Imbabura
Referencia: Recuperado de http://www.gestionderiesgos.gob.ec/modelo-integral-de-gestion-de-riesgos-en-imbabura/

3.2.DESCRIPCIÓN FÍSICA DEL GOBIERNO PROVINCIAL DE IMBABURA

El GAD provincial se encuentra ubicado en la capital de la provincia, en la ciudad de Ibarra, la infraestructura física de esta institución está conformada por algunos edificios entre los cuales tenemos: el edificio principal en las calles Bolívar 744 y Oviedo, nuevo edificio en las calles García Moreno y Antonio José de Sucre, bodega en las calles José Mejía Lequerica y Pedro Rodríguez y antiguo Patronato en las calles Vicente Maldonado y Juan José Flores.

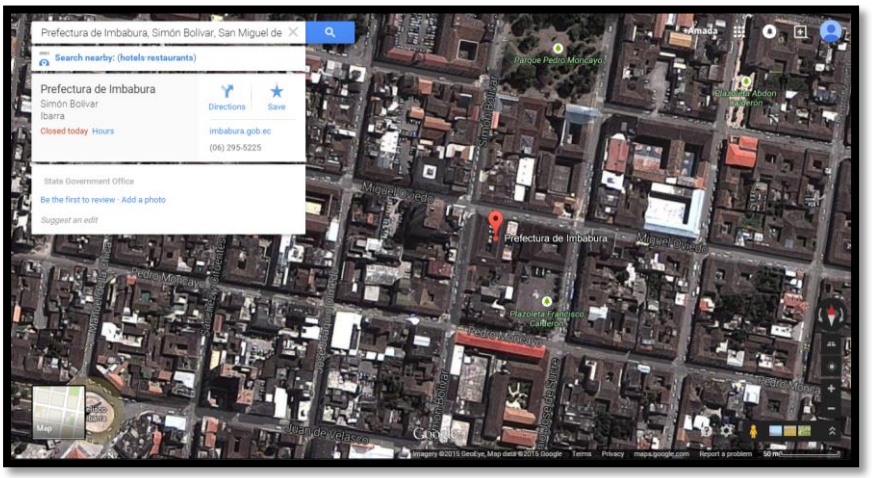


Imagen 13.- Ubicación geográfica del GAD Provincial de Imbabura.
Referencia: Recuperado de https://www.google.com.ec/maps/dir/0.3495864,-78.1183319/0.350338,-78.1159704/@0.3493704,-78.117916,395m/data=!3m1!1e3?hl=en

3.3.MISIÓN Y VISIÓN

Esta institución es de gran importancia para el desarrollo de provincia, por ello tiene muy bien definida su misión y visión, las cuales se presentan a continuación.

3.3.1. MISIÓN

La Prefectura de Imbabura es la institución encargada de coordinar, planificar, ejecutar y evaluar el Plan de Desarrollo Provincial Participativo; fortaleciendo la productividad, la vialidad, el manejo adecuado de sus recursos naturales y promoviendo la participación ciudadana; a fin de mejorar la calidad de vida de sus habitantes (GAD PROVINCIAL DE IMBABURA, 2015).

3.3.2. VISIÓN

La Prefectura de Imbabura se consolida como una institución de derecho público, autónoma, descentralizada, transparente, eficiente, equitativa, incluyente y solidaria; líder del desarrollo económico, social y ambiental provincial (GAD PROVINCIAL DE IMBABURA, 2015).

3.4.ESTRUCTURA ORGANIZACIONAL

La estructura organizacional del GAD Provincial de Imbabura, está alineada con su misión y se sustenta de acuerdo a los procesos y productos, con el propósito de asegurar su ordenamiento institucional.

Los procesos se ordenan y se clasifican en función de su grado de contribución o valor agregado al cumplimiento de la misión institucional, así tenemos su estructura organizacional constituida como se indica en la Imagen 14.

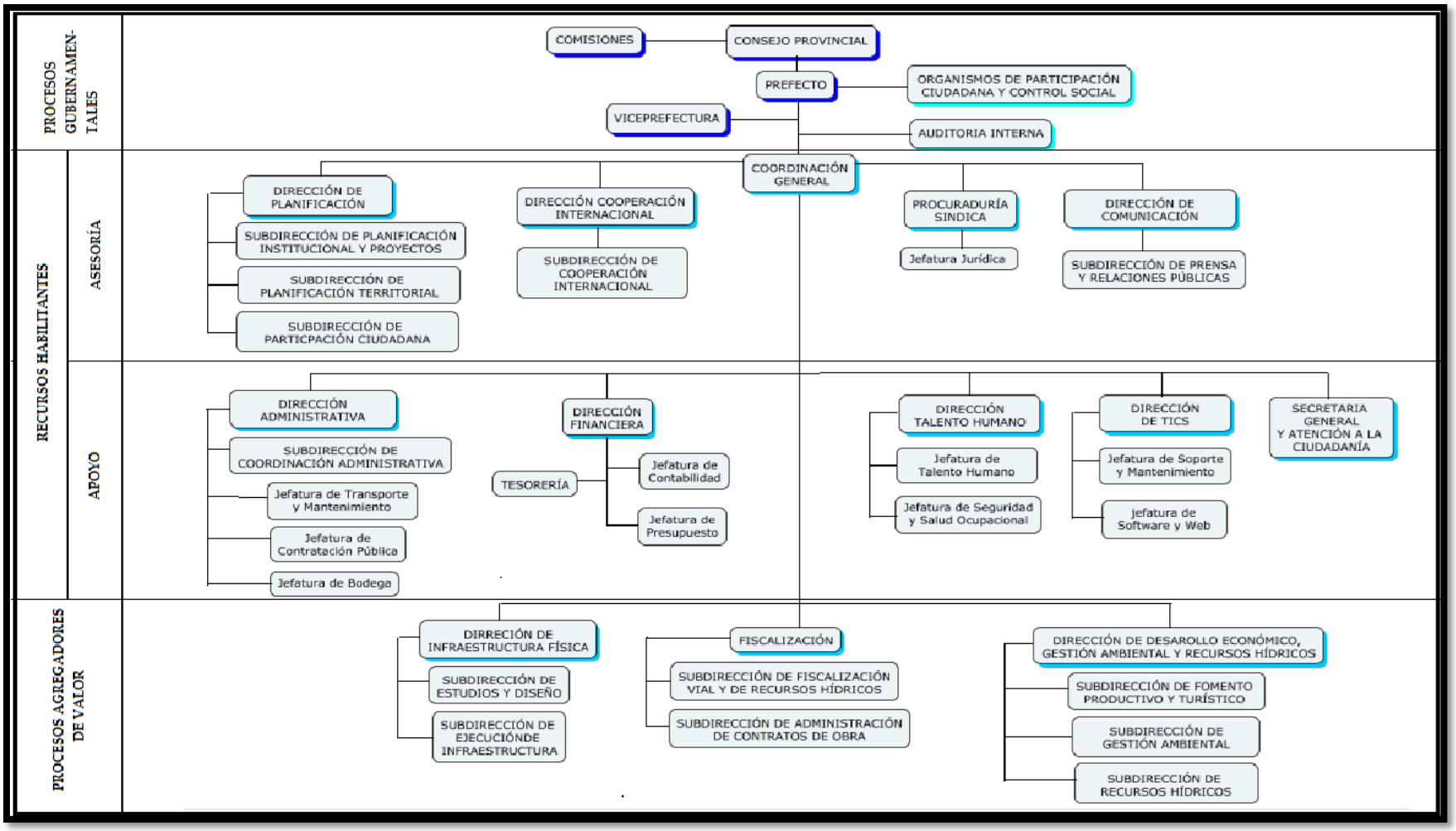


Imagen 14.- Estructura Organizacional del GAD Provincial de Imbabura.
Referencia: Estatuto Orgánico de Gestión Organizacional por procesos del GAD Provincial de Imbabura, 2014.

3.5.PERSONAL DEL GAD PROVINCIAL DE IMBABURA

En el GAD provincial de Imbabura existe 346 empleados entre trabajadores y funcionarios ya sean bajo nombramiento o contrato, la mayoría se encuentra concentrados en el edificio principal. En la Tabla 6 se muestra dicha información.

Tabla 6.- Número de trabajadores y empleados del GAD provincial de Imbabura.

Forma de contrato	**N° de empleados**
Funcionarios bajo nombramientos	133
Funcionarios bajo contrato	39
Trabajadores bajo nombramiento	145
Trabajadores bajo contrato	29
TOTAL	346

Referencia: Distributivo del personal del GAD Provincial de Imbabura, 2015.

Los empleados de esta institución se encuentran distribuidos indistintamente en cada una de las direcciones que conforman esta institución, a continuación en la Tabla 7 se presenta el número de empleados por cada dirección.

Tabla 7.- Número de trabajadores y empleados del GAD provincial de Imbabura por cada dirección.

Dirección	**N° de empleados**
Administrativa	25
Cooperación Internacional	5
Coordinación General	3
Desarrollo Económico	31
Financiero	13
Fiscalización	10
Infraestructura	152
Planificación	19
Prefectura	5
Procuraduría Sindica	8
Relaciones Públicas	10
Secretaria General	6
Talento Humano	46
Tecnologías Información	10
Viceprefectura	3
Total	346

Referencia: Distributivo del personal del GAD Provincial de Imbabura, 2015.

En el año 2012 la institución contaba con menor número de empleados y trabajadores, datos que se reflejan en la Tabla 8.

Tabla 8.- Número de trabajadores y empleados del GAD provincial de Imbabura en el año 2012.

Dirección	**N° de empleados**
Administrativa	30
Cooperación Internacional	2
Coordinación General	5
Desarrollo Económico	18
Financiero	8
Fiscalización	8
Infraestructura	115
Planificación	16
Prefectura	4
Procuraduría Sindica	5
Relaciones Públicas	8
Secretaria General	8
Talento Humano	28
Tecnologías Información	9
Viceprefectura	3
Total	266

Referencia: Dirección de Talento Humano GAD Provincial de Imbabura, 2012.

3.6. TOPOLOGIAS DE RED

Para conocer cómo se encuentra estructurada la red de comunicaciones del GAD Provincial de Imbabura se presenta a continuación los esquemas de las topologías: física y lógica.

3.6.1. TOPOLOGÍA FÍSICA

El esquema de la topología física indica la disposición o ubicación de los equipos de red existentes y como se encuentra realizadas las conexiones entre ellos, ver Imagen 15.

3.6.2. TOPOLOGÍA LÓGICA.

El esquema de la topología lógica indica el trayecto que sigue la información sobre la topología física anteriormente señalada de acuerdo a parámetros establecidos, en este caso la topología lógica se basa en la configuración de VLAN, ver Imagen 16.

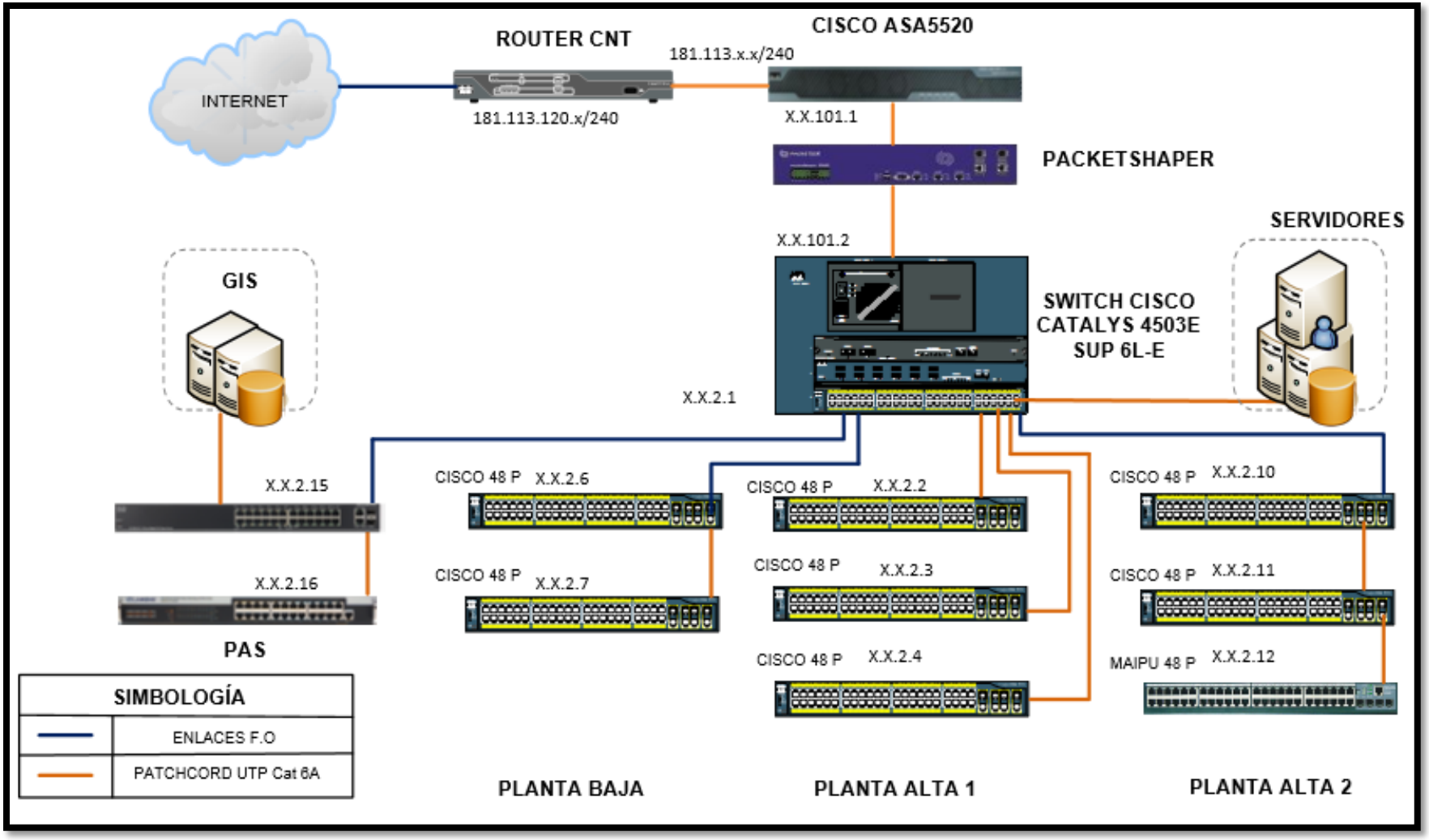


Imagen 15.- Topología física de la red de comunicación de del GAD Provincial de Imbabura.
Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura

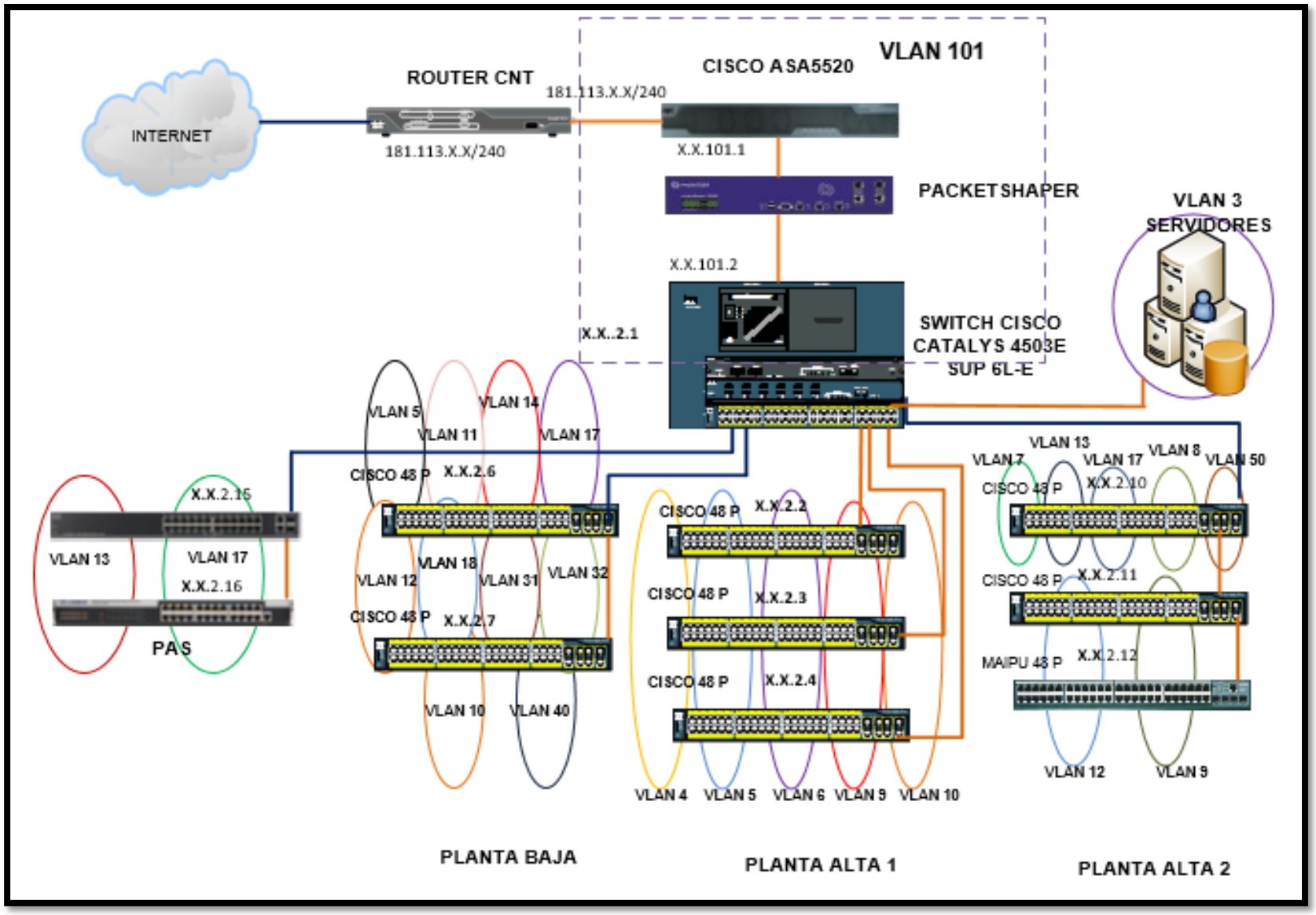


Imagen 16.- Topología lógica de la red de comunicación de del GAD Provincial de Imbabura
Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura

La distribución de VLANs de la topología lógica de red, se amplía en la Imagen 17.

Imagen 17.- Distribución actual de VLANs
Referencia: Basado en investigación teórica y práctica.

3.7.DIRECCIONAMIENTO DE LA RED

El GAD Provincial de Imbabura posee un contrato de servicio de internet de 30 Mbps con la empresa CNT, este ISP[46] provee de un pool de direcciones públicas 186.46.X.X

La red privada de la institución es una dirección de clase C y se encuentra segmentada mediante VLANs, las mismas que se indican en la Tabla 9. Por motivos de seguridad se mantiene ocultos los primeros dos octetos de su dirección.

[46] ISP= Internet Service Provider, proveedor de servicios de internet

Tabla 9.- Direccionamiento de red del GAD Provincial de Imbabura.

GRUPO	SUBGRUPO	ID VLAN	RED	GATEWAY	BROADCAST
ADMIN_EQUIPOS		2	X.X.2.0/24	X.X.2.1	X.X.2.255
SERVIDORES		3	X.X.3.0/24	X.X.3.1	X.X.3.255
GESTION_TECNOLOGICA		4	X.X.4.0/24	X.X.4.1	X.X.4.255
PREFECTURA	Prefectura Viceprefectura Secretaria general	5	X.X.5.0/24	X.X.5.1	X.X.5.255
PROCURADURIA		6	X.X.6.0/24	X.X.6.1	X.X.6.255
PLANIFICACION		7	X.X.7.0/24	X.X.7.1	X.X.7.255
GESTION_TECNICA		8	X.X.8.0/24	X.X.8.1	X.X.8.255
RELACIONES_PUBLICAS		9	X.X.9.0/24	X.X.9.1	X.X.9.255
ADMIN_GENERAL	S. Administrativa S. Financiera S. Talento Humano	10	X.X.10.0/24	X.X.10.1	X.X.10.255
INFRAESTRUCT_FISICA	S. Planificación S. Ejecución S. Estudios y Diseño	11	X.X.11.0/24	X.X.11.1	X.X.11.255
DESARROLLO_ECONOM	S. Desarrollo Económico S. Gestión Ambiental	12	X.X.12.0/24	X.X.12.1	X.X.12.255
PAS		13	X.X.13.0/24	X.X.13.1	X.X.13.255
WIFI		14	X.X.14.0/24	X.X.14.1	X.X.14.255
WIFI_EXTERNA		15	X.X.15.0/24	X.X.15.1	X.X.15.255
BODEGA		16	X.X.16.0/24	X.X.16.1	X.X.16.255
FAUSTO-GIS		17	X.X.17.0/24	X.X.17.1	X.X.17.255
FISCALIZACION		18	X.X.18.0/24	X.X.18.1	X.X.18.255
INVITADOS		30	X.X.30.0/24	X.X.30.1	X.X.30.255
RELOJES_BIOM		31	X.X.31.0/24	X.X.31.1	X.X.31.255
CAMARAS		32	X.X.32.0/24	X.X.32.1	X.X.32.255
TELEFONIA		40	X.X.40.0/24	X.X.40.1	X.X.40.255
MUTUALISTA		50	X.X.50.0/24	X.X.50.1	X.X.50.255
ENLACE_EQUIPOS		101	X.X.101.0/24	X.X.101.1	X.X.101.255

Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura.

3.8.SISTEMA ELÉCTRICO

Según Jenny Villegas (2013).

Existe una acometida eléctrica independiente, desde el cuarto de servicios eléctrico del edificio hacia el Data Center. El tendido de los conductores se realizó a través de un sistema de bandejas metálicas y tubería PVC en cuyas salidas se encuentran libre de material extraño y de humedad.

La selección de conductores está en conformidad a lo que establece el código eléctrico, con las siguientes especificaciones:

- 2 líneas para fases con cable tipo THHN nro. 4
- 1 línea para neutro con cable tipo THHN nro. 4
- 1 línea para tierra con cable tipo THHN nro. 6

Para la alimentación eléctrica del Data Center se instaló el tablero eléctrico de 220V con las siguientes especificaciones.

- 1 Breaker principal para protección de cargas
- 3 Breaker de 220V para la Alimentación, Aire acondicionado, UPS y reserva.
- 1 voltímetro digital para monitoreo eléctrico.
- Barra de cobre para distribución de fases, neutro y tierra, aisladores de barra y material consumible.

Como parte del equipamiento se realizó el montaje de un UPS[47] monofásico de

[47] UPS= Uninterruptible Power Supply

220V, el cual será encargado de entregar respaldos de energía a los equipos de redes, comunicaciones e informáticos del Data Center, contiene lo siguiente:

- 1 Breaker para el circuito de alimentación y respaldo del rack de servidores.
- 1 Breaker para el circuito de alimentación y respaldo del sistema de control de acceso y sistema de incendios.

La conexión del UPS instalado en el Data Center se muestra en la Imagen 18.

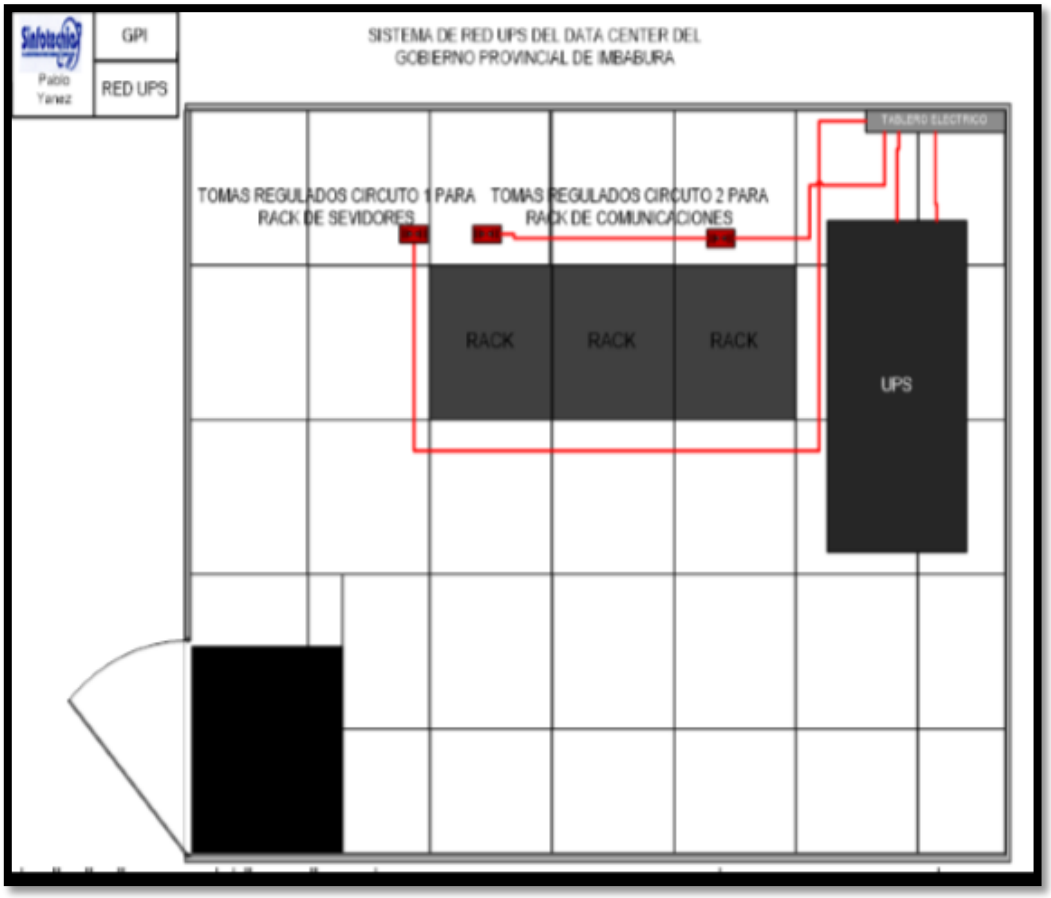


Imagen 18.-Conexión de UPS por el techo falso
Referencia: Jenny Villegas; Optimización de la administración de la red e implementación de servidores de servicios para el GAD Provincial de Imbabura, 2013.

Existen PDU[48] que es una barra de contactos, altamente confiables, con múltiples tomacorrientes, diseñada para suministrar energía regulada a los equipos de comunicaciones, están montadas en racks dentro del Data Center.

La puesta a tierra fue diseñada según las especificaciones de la norma ANSI/EIA/TIA-607 definiendo así:

- Los gabinetes y los protectores de voltaje son conectados a una barra de cobre (busbar) con "agujeros" (de 2" x 1/4")
- Estas barras se conectan al sistema de tierras (grounding backbone) mediante un cable de cobre cubierto con material aislante, mínimo número 6 AWG, de color verde y etiquetado de manera adecuada.
- Este backbone está conectado a la barra principal del sistema de telecomunicaciones (TMGB, de 4" x 1/4") en la acometida del sistema de telecomunicaciones. El TMGB se conectará al sistema de tierras de la acometida eléctrica y a la estructura de acero de cada piso.

3.9.SISTEMA PASIVO

El sistema pasivo está constituido por el data center y el cableado estructurado.

3.9.1. DATA CENTER

El data center se encuentra ubicado en el segundo piso del edificio principal del GAD Provincial de Imbabura, su área es de 15 m^2 con unas dimensiones de 3m x 5m y una altura de 4m, el nivel de Tier es de nivel 1 con las siguientes características:

- Sistema de alimentación eléctrica.

[48] PDU= Power Distribution Unit, Unidad de Distribución de Energía

- Sistema redundante de generación de energía.
- Sistema de enfriamiento.
- Sistema de UPS distribuido para protección de las cargas críticas.
- Cargas en racks con alimentación de UPS para la carga.

Tiene además los siguientes elementos: puerta de acceso tiene 1,5 m de ancho y 2 m de alto, con cerradura electromagnética y posee mirilla de vidrio antibala; cuenta con un techo falso a 1 m del techo real, con 15 módulos de 61cm x 61 cm; existen escalerillas hacia los puntos a donde salen los servicios de datos y la parte eléctrica; bandeja metálica utilizadas para llevar el cableado ubicados en la parte superior y en el techo falso; piso falso metálico con recubrimiento de vinyl, la marca es Sistemas Modulares ASM, en total 40 paneles colocados a una altura de 50 cm del piso sobre ejes pedestales; dos cámaras, una ubicada dentro del data center y otra fuera de él.

La Imagen 19 indica la utilización de escalerillas desde el piso falso al techo falso para la conducción del cableado de red hacia la plata alta 1.

Imagen 19.- Escalerilla metálica utilizadas para llevar el cableado
Referencia: Datacenter del GAD Provincial de Imbabura, 2015.

En la Imagen 20 se encuentra el sistema de UPS distribuido para protección de las cargas críticas.

Imagen 20.- Sistema de UPS distribuido para protección de las cargas críticas.
Referencia: Datacenter del GAD Provincial de Imbabura, 2015.

El datacenter cuenta con un sistema de enfriamiento para garantizar una temperatura adecuada, el mismo que se indica en la Imagen 21.

Imagen 21.- Sistema de enfriamiento
Referencia: Datacenter del GAD Provincial de Imbabura, 2015.

Para garantizar la seguridad en el datacenter se encuentran instaladas cámaras tanto dentro como fuera del sitio como se indica en la Imagen 22.

Imagen 22.-Cámaras de seguridad colocadas en el techo falso
Referencia: Datacenter del GAD Provincial de Imbabura, 2015.

El piso falso es piso falso metálico con recubrimiento de vinyl, la marca es Sistemas Modulares ASM, ver Imagen 23.

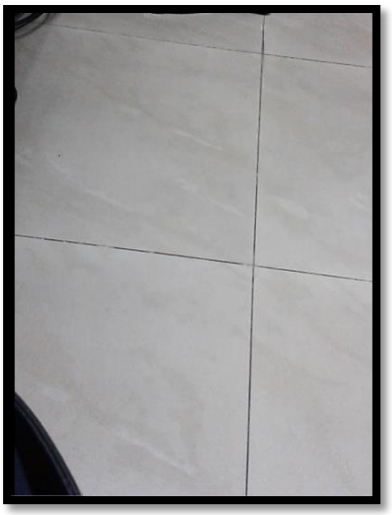


Imagen 23.-Piso falso metálico con recubrimiento de vinyl
Referencia: Datacenter del GAD Provincial de Imbabura, 2015.

3.9.2. CABLEADO ESTRUCTURADO

Desde la creación de esta institución se ha manejado una red de comunicaciones que en dichas fechas funcionaba según las necesidades básicas, por lo que no existía un cumplimiento total de las normas. Es así que en el año 2012 se registra el último cambio realizado en la red de comunicaciones por parte de una empresa de la ciudad.

Desde esa fecha hasta la actualidad el GAD Provincial de Imbabura ha tenido algunos cambios tanto de personal, de la estructura interna dentro de los edificios, adhesión de un nuevo edificio, cambios que han aumentado el número de usuarios y por ende el uso de la tecnología existente; situación que ha provocado la necesidad de reformas en la infraestructura física y lógica de la red de comunicaciones, es decir, aumento y modificaciones de los puntos de red, cambios de los enlaces con los edificios secundarios y cambios en las configuraciones de los equipos de red, los mismos que no se encuentran debidamente documentados.

Según el estándar ANSI/TIA/EIA-568-C.1 un sistema de cableado estructurado está compuesto por ciertos elementos, los cuales tomaremos en cuenta para realizar el levantamiento de información:

3.9.2.1. Instalaciones de entrada

La instalación de entrada se encuentra en el data center, es el lugar en el que ingresan los servicios de telecomunicaciones al edificio y/o dónde llegan las canalizaciones de interconexión con otros edificios de la institución.

La instalación de entrada contiene el dispositivo de interfaz con las redes públicas prestadoras de servicios de telecomunicaciones, ver Imagen 24.

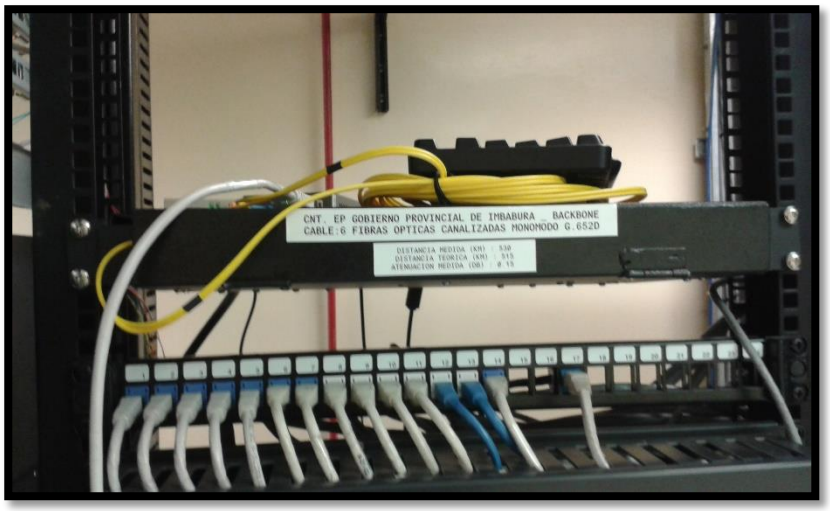


Imagen 24.- Entrada de servicios de ISP
Referencia: Datacenter del GAD Provincial de Imbabura, 2015.

3.9.2.2. Distribuidor o repartidores principales y secundarios

Esta institución cuenta con un distribuidor principal que es el data center y tres distribuidores secundarios que son los repartidores horizontales o armario de telecomunicaciones.

El data center se encuentra en la planta alta del edificio principal, junto a la Dirección de TICs, desde este punto parten la interconexión de los enlaces de fibra óptica entre pisos y también el enlace con el edificio del antiguo y nuevo Patronato del Gobierno Provincial de Imbabura.

El paso de cable se lo hizo a través de sistema de bandeja y escalerilla, la misma que se instalaron sobre el cielo falso de cada una de las oficinas.

Todo el sistema de ductería por donde se conduce el cableado se encuentra instalado sobre el cielo falso de las oficinas de cada uno de los pisos del edificio, con la finalidad de mantener la estética de las áreas donde se instalaran los puntos.

3.9.2.3. Distribuidor central del cableado

Conocido como back-bone, es un cableado de fibra óptica de un solo fabricante FURUKAWA, la fibra óptica Instalada entre pisos del edificio es de tipo OM3 para aplicaciones de trasmisión de 10 Gbps, con protección tipo armada para defensa contra roedores.

- El paso de la Fibra óptica entre Pisos del edificio, se lo realizo a través de ductos del edificio, aplicando el estándar ANSI/TIA/EIA-568-C.1 en donde se especifica el distribuidor central de cableado.
- El Paso de la fibra óptica entre el edificio del GOBIERNO PROVINCIAL DE IMBABURA y el PATRONATO se lo realizo vía área a través del sistema de Postes del Alumbrado Público.
- Todo Conectores de Fibra Óptica son Tipo SC Múltiple, con Tapa de Contacto de Circona con radio CP para perdida de Inserción y reflexiones bajas acabado anaeróbico o epóxido verificado.
- Las bandejas de Fibra Óptica son de 24 puertos, incluyen adaptadores tipo SC dúplex tienen las siguientes dimensiones 1.75 “ H x 17 “W x 8.6 “ D (4.5 x 43 x 22 cm) cumplen con las normas ETL, CSA, UL.

- Los Patch Cord de Parcheo de fibra son tipo SC Full Duplex de 3 mts 50/125 de Fabrica verificado ETL, CSA, UL. Tecnología de 50 / 125 MM 850/1300 nm OFL 500 / 500 (MHz – Km).
- La conexión de los hilos de fibra Óptica de cada uno de los enlaces se lo realizo a través de proceso de fusión. Se utilizó un equipo especializado FUSIONADORA DE FIBRA con el objeto de eliminar las pérdidas de transmisión.
- La certificación de los enlaces de Fibra Óptica fue realizado por SINFOTECNIA, en presencia del personal técnico designado por el GOBIERNO PROVINCIAL DE IMBABURA.

3.9.2.4. Distribuidores secundarios o repartidores horizontales

Conocidos como armarios de telecomunicaciones, en el edificio principal cuenta con un armario en cada piso, excepto la planta alta de donde se encuentra el data center, cada uno de los racks cuenta con patch panels con espacios para 24 salidas, topologías Universal para el manejo de los estándares EIA/TIA 568A, EIA/TIA 568B en categoría 6A y Desempeño a Gigabit Ethernet verificado.

3.9.2.4.1. Etiquetado

El cableado de racks lo realizo la empresa SYNFOTECNIA y está correctamente etiquetado de acuerdo al diseño planteado en la tesis de Jenny Villegas, el mismo que se realizó con etiquetas auto laminable. Se colocaron etiquetas en ambos extremos de los enlaces de distribución horizontal así como en la distribución central del cableado con la misma estructura realizada en las áreas de trabajo.

3.9.2.4.2. Mapeo puntos de red.

Permite identificar la ubicación los puntos del cableado con los puertos de los swiches de acceso y saber a qué VLAN pertenece dicho punto. Este mapeo completo se encuentra en el ANEXO 01, a continuación un resumen por cada planta.

- Planta Baja

En la plata baja existen dos switches, distribuidos con las siguientes VLANS en sus puertos, ver Tabla 10.

Tabla 10.- Resumen puntos de red plata baja

GPI-PLANTA BAJA		
SWITCH	RANGO DE PUERTOS	VLAN
X.X. 2.6	2-14, 27,28 32-45	INFRAESTRUCT FISICA
	15-17, 46	FISCALIZACION
	18-21	DESARROLLO ECONOM
	22,29	CAMARAS HALL
	22-25	INFORMACION
	26, 36	WIFI
	30,31	BIOMETRICOS
X.X. 2.7	2-3	DESARROLLO ECONOM
	4-5 14-16	FISCALIZACION
	6-11	ADMIN GENERAL
	12-13	CAMARAS

Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura.

- Planta alta 1

En la plata alta 1 existen tres switches. En la Tabla 11 se encuentra la distribución de los puertos de acuerdo a cada VLAN.

Tabla 11.- Resumen de puntos de red plata alta 1

GPI-PLANTA ALTA 1		
SWITCH	RANGO DE PUERTOS	VLAN
X.X. 2.2	2-11, 15-17, 18-24	PREFECTURA
	12-13, 40-41	RELACIONES PUBLICAS
	17	WIFI
	25-31	PROCURADURIA
	32-39	ADMIN GENERAL
	42-46	GESTION TECNOLOGICA
	47-48	MODO TRUNK
X.X. 2.3	2,6, 10-14	GESTION TECNOLOGICA
	3-5, 7-9, 15-26	ADMIN GENERAL
	47-48	MODO TRUNK
X.X. 2.4	2-3, 5-6, 8-11, 35	PREFECTURA
	4	WIFI
	7,21-30, 33,34, 16, 14	ADMIN GENERAL
	12, 36-27,31, 32	RELACIONES PUBLICAS
	18-20, 15	GESTION TECNOLOGICA
	17	PROCURADURIA
	13	CAMARAS
	47-48	MODO TRUNK

Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura.

- Planta alta 2

En la plata alta 2 existen tres switches. En la Tabla 12 se encuentra la distribución de los puertos de acuerdo a cada VLAN.

Tabla 12.- Resumen puntos de red plata alta 2

GPI-PLANTA ALTA 2		
SWITCH	RANGO DE PUERTOS	VLAN
X.X. 2.10	2-23	PLANIFICACION
	24	WIFI
	25-28	GESTION TECNICA
	29-34	TURISMO
	35-39	FORESTACION Y BIODEVERSIDAD
	40-42	CUENCAS HIDROGRAFICAS

	43	PAS
	47-48	MODO TRUNK
X.X. 2.11	2-16, 21-46	DESARROLLO ECONOM
	17-20	RELACIONES PUBLICAS
	47-48	MODO TRUNK
X.X. 2.12	2-6	DESARROLLO ECONOM
	7-12	RELACIONES PUBLICAS
	47-48	MODO TRUNK

Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura.

3.9.2.5. Distribución horizontal del cableado

El cableado horizontal del edificio principal es par trenzado categoría 6A de un solo fabricante HUBBEL, instalado en el 2012.

- Para la distribución existe dos armario de comunicaciones, uno en la planta baja y otro en la planta alta 2, no existe en la planta alta 1 debido a que en este piso se encuentra el data center y desde ahí se distribuye el cableado horizontal a esta planta.
- Desde las bandejas de distribución que existen en cada armario de comunicaciones hacia las salidas del cableado estructurado se utiliza tubo conduit.
- Los conectores y patch cord utilizados son categoría 6A.
- Debido al aumento de personal se ha realizado la instalación de nuevos puntos de red y se realizó la habilitación del nuevo edificio de la institución donde funciona el PAS Patronato de Amparo Social además de otras dependencias donde, el cableado horizontal es par trenzado categoría 6a. Existe un armario de comunicaciones por cada planta del edificio, existiendo así dos armarios.

- El paso de cable se lo hizo a través de sistema de bandeja y escalerilla, la misma que se instalaron sobre el cielo falso de cada una de las oficinas.
- Todo el Sistema de ductería por donde se conduce el cableado se encuentra instalado sobre el cielo falso de las oficinas de cada uno de los pisos del edificio, con la finalidad de mantener la estética de las áreas donde se instalaran los puntos.
- La distribución horizontal cuenta con un testeo de los puntos del cableado mediante la utilización del equipo FLUKE DTX 1800 SERIES, dicha certificación fue realizada por una empresa de la ciudad y los resultados se encuentran en la Dirección de Tecnologías de la Información.

3.9.2.6. Área de trabajo

En los espacios de las áreas de trabajo existe una toma por estación de trabajo como mínimo, el espacio de trabajo es por cada 10 m2, existe al menos una toma de energía cerca de cada toma de telecomunicaciones.

Los Face Plate instalados son de 1 y 2 puertos respectivamente de acuerdo la necesidad, donde se montaron los jacks para los puntos de Voz y Datos. Dichos Face Plate permiten la instalación de los jacks Rj-45 cat-6a.

Los Patch Cords instalados son ensamblados de fábrica y cumplen con los parámetros de atenuación, transmiten Voz Análoga y Voz Digital (VoIP).

3.9.2.6.1. Etiquetado

El sistema de etiquetado se lo realizó con etiquetas autolaminable colocado dentro de los faceplate de tal forma que no puedan ser manipuladas fácilmente, con el siguiente modelo para la etiqueta: PA2-D1, en donde la primera parte representa la planta del distribuidor horizontal del cableado y la segunda parte el puerto del switch, en la Tabla 13 se indica el etiquetado por cada una de las plantas.

Tabla 13.- Etiquetado por cada una de las plantas

ETIQUETADO POR CADA UNA DE LAS PLANTAS			
PLANTA	SWITCH	ID DE PLANTA	IDENTIFICADOR DE PUERTO
PLANTA BAJA	X.X.2.6	PB	D1 hasta D46
	X.X.2.7	PB	D47 hasta D64
PLANTA ALTA 1	X.X.2.2	PA1	D1 hasta D46
	X.X.2.3	PA1	D47 hasta D72
	X.X.2.4	PA1	D73 hasta D110
PLANTA ALTA 2	X.X.2.10	PA2	D1 hasta D93 D109 hasta D112
	X.X.2.11	PA2	D48 hasta D93
	X.X.2.12	PA2	D94 hasta D108 D43 hasta D47

Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura, 2015.

3.10. SISTEMA ACTIVO

Los equipos de red de comunicaciones que posee el GAD provincial de Imbabura se encuentran distribuidos en los diferentes edificios pertenecientes a esta institución.

En el edificio principal, en la planta alta se encuentra el data center que es la base de las comunicaciones para esta institución, desde allí se interconecta con los pisos y hacia los demás edificios. La conexión entre pisos del edificio principal es mediante fibra óptica,

de igual manera hacia el antiguo y nuevo edificio del Patronato de Amparo Social PAS, sin embargo el enlace hacia el antiguo PAS no se encuentra activo.

También se cuenta con enlaces de radio para poder llegar a la bodega y hacia el antiguo patronato. Los equipos utilizados para los radio enlaces son Ubiquiti AirMAX para el enlace a la bodega y Ubiquiti NanoStation5 para el enlace al antiguo PAS.

En el data center encontramos un Cisco ASA5520 que es el firewall con el que cuenta la institución, un switch Cisco Catalyst 4503E, un packetshaper Bluecoat 3500 que solo se encuentra conectado pero no está en funcionamiento y además switches con los que cuenta el edificio principal que son Cisco Catalyst 2960S de 48 puertos y 1 switch MAIPU de 48 puertos. En el nuevo edificio del PAS existen swiches de la marca Cisco SG300 y Cisco Catalyst 2960. En la bodega existe un switch cisco Catalyst 2960S y en el antiguo PAS tenemos un switch cisco SG300 y un switch Linksys.

A continuación se describen los equipos existentes por cada uno de los edificios:

3.10.1. EQUIPOS ACTIVOS EDIFICIO PRINCIPAL

En este edificio tenemos tres plantas, la planta baja, la planta alta donde se encuentra el data center y la segunda planta alta, los equipos se encuentran distribuidos de la siguiente manera:

- **Planta baja**

  En la Tabla 14, se indican los equipos activos en la planta baja del edificio principal.

Tabla 14.- Equipos de red edificio principal – planta baja

Equipos de red edificio principal – planta baja		
Nº	Equipo	Nº de puertos
2	Switch Cisco Catalyst 2960S	48

Referencia: Inventario del parque informático; Dirección de Tecnologías de la Información, 2015.

- **Planta alta 1- Data Center**

  En la Tabla 15, se indican los equipos activos en la planta alta del edificio principal.

Tabla 15.- Equipos de red edificio principal – planta alta 1 data center

Equipos de red edificio principal – planta alta 1 data center		
Nº	Equipo	Nº de puertos
3	Switch Cisco Catalys 2960S	48
1	Cisco ASA 5520	4
1	SWITCH CORE Cisco 4503E	48

Referencia: Inventario del parque informático; Dirección de Tecnologías de la Información, 2015.

- **Planta alta 2**

  En la Tabla 16, se indican los equipos activos en la planta alta 2 del edificio principal.

Tabla 16.- Equipos de red edificio principal – planta alta 2

Equipos de red edificio principal – planta alta 2		
Nº	Equipo	Nº de puertos
2	Switch Cisco Catalyst 2960S	48
1	Switch MAIPU	48

Referencia: Inventario del parque informático; Dirección de Tecnologías de la Información, 2015.

3.10.2. EQUIPOS ACTIVOS NUEVO EDIFICIO

Estos equipos fueron instalados en el año 2012, existe un distribuidor o repartidor horizontal en cada uno de los pisos los mismos que constan de los siguientes elementos.

- **Planta baja**

  En la Tabla 17, se indican los equipos activos en la planta baja del nuevo edificio.

Tabla 17.- Equipos de red nuevo edificio – planta baja

Equipos de red nuevo edificio – planta baja		
Nº	Equipo	Nº de puertos
1	Switch Cisco SG300	28

Referencia: Dirección de Tecnologías de la Información, 2015.

- **Planta alta 1**

  En la Tabla 18, se indican los equipos activos en la planta alta 1 del nuevo edificio.

Tabla 18.- Equipos de red nuevo edificio – planta baja

Equipos de red nuevo edificio – planta alta 1		
Nº	Equipo	Nº de puertos
1	Switch Cisco SG300	28
1	Switch Cisco Catalyst 2960S	24

Referencia: Dirección de Tecnologías de la Información, 2015.

- **Planta alta 2**

  En la Tabla 19, se indican los equipos activos en la planta alta 2 del nuevo edificio.

Tabla 19.- Equipos de red nuevo edificio – planta baja

Equipos de red nuevo edificio – planta alta 2		
Nº	Equipo	Nº de puertos
1	Switch Cisco SG300	28

Referencia: Dirección de Tecnologías de la Información, 2015.

- **Planta alta 3**

  En la Tabla 20, se indican los equipos activos en la planta alta 3 del nuevo edificio.

Tabla 20.- Equipos de red nuevo edificio – planta baja

Equipos de red nuevo edificio – planta alta 3		
Nº	Equipo	Nº de puertos
1	Switch Cisco SG300	28
1	Switch Cisco Catalyst 2960S	24

Referencia: Dirección de Tecnologías de la Información, 2015.

3.10.3. EQUIPOS ACTIVOS BODEGA

En la Tabla 21, se indican los equipos activos en la bodega de la institución.

Tabla 21.- Equipos de red bodega – planta baja

Equipos de red bodega – planta baja		
Nº	Equipo	Nº de puertos
1	Switch Cisco Catalyst 2960S	24

Referencia: Dirección de Tecnologías de la Información, 2015.

3.10.4. EQUIPOS ACTIVOS ANTIGUO PAS

En la Tabla 22, se indican los equipos activos en el antiguo PAS.

Tabla 22.- Equipos de red antiguo PAS – planta baja

Equipos de red antiguo PAS – planta baja		
Nº	Equipo	Nº de puertos
1	Switch Cisco SG300	24
1	Switch Linksys	24

Referencia: Dirección de Tecnologías de la Información, 2015.

3.10.5. PRINCIPALES CARACTERISTICAS DE EQUIPOS ACTIVOS.

Para realizar reestructuración en las configuraciones de los equipos activos es necesario conocer las características que estos poseen y verificar si los cambios planteados son aplicables, para ellos se realiza un detalle de los equipos activos y sus principales características.

- **Firewall Cisco ASA5520**

El Cisco ASA 5520 es un firewall que aporta una amplia gama de servicios de seguridad, con alta disponibilidad y conectividad Gigabit Ethernet para empresas medianas. En la Imagen 25, se muestra la estructura del ASA5520.

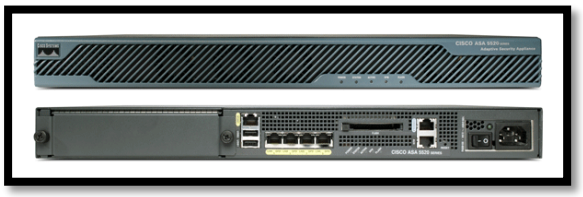


Imagen 25.-Firewall Cisco Asa5520
Referencia: Recuperado de http://www.aeonpartners.net/products/cisco/ASA-5520.html

En la Tabla 23 se detallan las principales características del ASA de la institución.

Tabla 23.-Características Asa5520

CARACTERISTICAS ASA5520	
Resumen rendimiento	
Capacidad máxima de procesamiento Mbps	450
Capacidad máxima de procesamiento de Mbps de VPN	225
Cantidad máxima de conexiones	280000
Cantidad máxima de conexiones/ segundo	9000
Paquetes por segundo	320000
Resumen técnico	
Memoria MB	512
Memoria flas del sistema MB	64
Puertos integrados	4-10-100-1000, 1-10/100
Cantidad máxima de interfaces virtuales VLAN	150
Características	
Seguridad en la capa de aplicaciones	Si
Funciones de firewall transparente de capa 2	Si
Compatibilidad con alta disponibilidad 3	A/S y A/A
Agrupación de VPN y equilibrio de carga.	Si

Referencia:https://www.cisco.com/web/ES/publicaciones/07-08-cisco-dispositivos-serie-ASA5500.pdf

- **Switch Cisco Catalyst 4503E**

Tiene una arquitectura de reenvío centralizado que permite la colaboración, virtualización y capacidad de gestión operativa a través de operaciones simplificadas y compatibilidad con versiones anteriores que abarca varias generaciones. En la Imagen 26, se muestra la estructura del switch de Core.

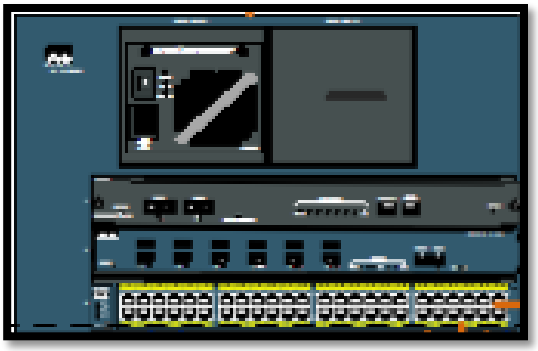


Imagen 26.- Switch Cisco Catalyst 4503E
Referencia: Recuperado de http://www.lelong.com.my/cisco-catalyst-4503-e-multi-speed-gigabit-switch-sales623-159488964-2015-03-Sale-P.htm

En la Tabla 24 se detallan las principales características del switch de Core.

Tabla 24.-Características switch Cisco Catalyst 4503E.

CARACTERISTICAS SWITCH CISCO CATALYST 4503E	
Capacidad de conmutación centralizada	280 Gbps
Rendimiento	225 Mpps para IPv4 110 Mpps para IPv6 225 Mpps para L2 Bridging
Entradas de enrutamiento IPv4	57000
Entradas de enrutamiento IPv6	30000
RAM dinámica síncrona (SDRAM)	512 MB de DRAM ampliable a 1 GB
Seguridad y QoS entradas de hardware	64.000 (32.000 por dirección)
VLANs activas	4096
Spannig-tree	Si

Referencia: http://www.lelong.com.my/cisco-catalyst-4503-e-multi-speed-gigabit-switch-sales623-159488964-2015-03-Sale-P.htm

- **Packetshaper Bluecoat 3500**

Es un dispositivo que proporciona visibilidad de aplicaciones y contenido web de las redes, permite administrar con eficacia políticas de QoS a nivel de las aplicaciones. En la Imagen 27, se muestra la estructura del Packetshaper Bluecoat.

Imagen 27.- Packetshaper Bluecoat 3500
Referencia: Recuperado de http://www.edgeblue.com/EdgeBlue-Outlet.asp

En la Tabla 25 se detallan las principales características del switch del Packetshaper Bluecoat.

Tabla 25.-Características Packetshaper BlueCoat 3500

CARACTERISTICAS PACKETSHAPER BLUECOAT 3500	
Flujos IP (TCP)	40000
Flujos IP (UDP)	20000
Clases	1024
Particiones dinámicas	1024
Particiones estáticas	512
Número máximo de reglas de juego	2562
IP Hosts	20000
Tuneles activos	30
Monitoreo solo	si
Enlace envio con shaping	2,6,10,45,100Mbps
Compresión	20Mbps

Referencia: http://www.edgeblue.com/PacketShaper-3500.asp

- **Switch Cisco Catalyst 2960S**

Son conmutadores de red independientes que proporcionan rápida conectividad Ethernet para pequeñas redes. En la Imagen 28, se muestra la estructura del Switch Cisco Catalyst 2960S.

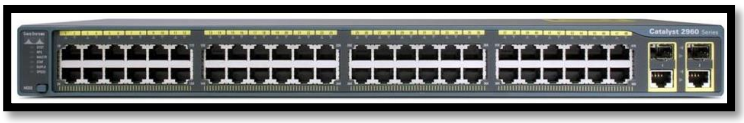


Imagen 28.- Switch Cisco Catalyst 2960S
Referencia: Recuperado de http://www.microd.eu/store/cisco-catalyst-2960-48-poe-port-network-switch-ws-c2960-48pst-s

En la Tabla 26 se detallan las principales características del switch Cisco Catalyst 2960S.

Tabla 26.- Características switch Cisco Catalyst 2960S

CARACTERISTICAS SWITCH CISCO CATALYST 2960S	
Cableado Ethernet	10 Base-T / 100Base-Tx /1000Base-T
Cantidad de puertos	52
Cantidad Lan Ethernet (RJ-45) puertos	48
Ethernet Gigabit cantidad puertos	2
Tasas de transferencia de datos	10/100/1000 Mbps
Ancho de banda	16 Gbit/s
Velocidad de transferencia de datos	1 Gbit/s
Memoria interna	64 MB
Memoria flash	32 MB
Spanning Tree Protocol	Si
Agregación de enlaces	Si
Calidad de servicio de apoyo	Si
Control de tormentas de difusión	Si
Filtrado de direcciones MAC	Si

Referencia: http://www.microd.eu/store/cisco-catalyst-2960-48-poe-port-network-switch-ws-c2960-48pst-s

- **Switch MAIPU**

Switch para el acceso a la red en empresas, ofrece el servicio de conmutación de alto rendimiento estable, fiable y seguro. Dispone de gran alcance de multidifusión y la capacidad de QoS. En la Imagen 29, se muestra la estructura del Switch Maipu.

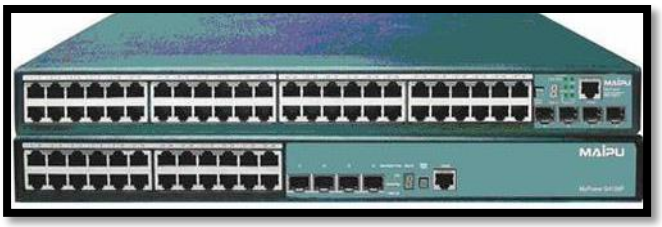


Imagen 29.- Switch MAIPU
Referencia: Recuperado de http://www.indiamart.com/spring-link/products.html

En la Tabla 26 se detallan las principales características del switch Cisco Catalyst 2960S.

Tabla 27.- Características switch MAIPU

CARACTERISTICAS SWITCH MAIPU	
Puertos de conmutación	48 ethernet 10/100 Mbit/s
Ancho de banda interno	17.6 Gbit/s
Memoria	128 MB
Memoria flash	32 MB
Puerto de consola	Si
Web de interfaz	Si
Soporte para SNMP	Si
Enrutamiento estático	Si
Soporte Ipv6	Si
VLANs	Si
Spanning Tree Protocol	Si

Referencia: http://es.specsen.com/routers-and-switches-maipu/maipu-sm4100-52tf/

- **Switch Cisco SG300**

Proporciona funciones que necesita para mejorar la disponibilidad de sus aplicaciones empresariales críticas, son fáciles de configurar y usar. Ofrece la combinación ideal de asequibilidad y funciones para empresas. En la Imagen 30, se muestra la estructura del Switch Cisco SG300.

Imagen 30.- Switch Cisco SG300
Referencia: Recuperado de http://www.ipphone-warehouse.com/Cisco-SG300-28-Switch-p/srw2024-k9-na.htm

En la Tabla 26 se detallan las principales características del switch Cisco SG300.

Tabla 28.- Caracteristicas switch Cisco SG 300

CARACTERISTICAS SWITCH CISCO SG300	
Puertos	26 x 10/100/100
Capacidad del switch	56 Gbps
Forwarding capacity	41.67 Mpps
Listas de control de acceso	Si
LAN virtuales (VLANs)	Si
Control de tormentas de difusión	Si
Implementacion automática de voz en la red	Si
Agrupación de puertos	Si

Referencia: www.cisco.com/c/dam/en/us/products/collateral/switches/small-business-smart-switches/300_Series_Switches_DS_FINAL.pdf

3.11. HARDWARE

El hardware está constituido por los distintos servidores y las estaciones o equipos de trabajo con los que cuenta la institución.

3.11.1. SERVIDORES

La institución cuenta con distintos servidores los mismos que se detallan a continuación:

1. Computadora de escritorio
2. Servidor Compaq
3. Servidor HP Prolian
4. Servidor HP Prolian
5. Un chasis HP c3000, instalado 8 cuchillas.
6. Servidor DELL EDGE
7. Servidor de Telefonía

3.11.2. ORGANIZACIÓN DE LOS SERVIDORES INSTALADOS EN EL BLADE

En el Blade existente en la institución existen 8 cuchillas instaladas, a continuación se describe los servicios en cada una de ellas.

- **Cuchilla 1**

  En la cuchilla número uno se encuentra cuatro servicios los mismos que se detallan en la Tabla 29.

Tabla 29.- Organización de servidores instados en la cuchilla 1

	Servidor	Detalle
1	Proxy	Squid
2	Hosting 1	Intranet
3	Hosting 2	www.imbabura.travel
4	Administración	XenServer

Referencia: Dirección de Tecnologías de la Información, 2015.

- **Cuchilla 2**

En la cuchilla número dos se encuentra tres servicios los mismos que se detallan en la Tabla 30.

Tabla 30.- Organización de servidores instados en la cuchilla 2

	Servidor	Detalle
1	Documentación Old	Apagado
2	Digitalización	
3	Administración	XenServer

Referencia: Dirección de Tecnologías de la Información, 2015.

- **Cuchilla 3**

En la cuchilla número tres se encuentra cinco servicios los mismos que se detallan en la Tabla 31.

Tabla 31.- Organización de servidores instados en la cuchilla 3

	Servidor	Detalle
1	Hosting 3	www.imbavial.gob.ec
2	Relojes	
3	Videos Vigilancia	Servidor cámaras
4	Geo localización	Pedido contraloría
5	Administración	XenServer

Referencia: Dirección de Tecnologías de la Información, 2015.

- **Cuchilla 4**

En la cuchilla número cuatro se encuentra cinco servicios los mismos que se detallan en la Tabla 32.

Tabla 32.- Organización de servidores instados en la cuchilla 4

	Servidor	**Detalle**
1	Proxy Wifi	
2	Wifi APs	
3	Video Streaming	
5	Administración	XenServer

Referencia: Dirección de Tecnologías de la Información, 2015.

- **Cuchilla 6**

En la cuchilla número seis se encuentra tres servicios los mismos que se detallan en la Tabla 33.

Tabla 33.- Organización de servidores instados en la cuchilla 6

	Servidor	**Detalle**
1	App Producción	
2	Hosting 4	www.imbabura.gob.ec
3	Administración	XenServer

Referencia: Dirección de Tecnologías de la Información, 2015.

- **Cuchilla 8**

En la cuchilla número ocho se encuentra siete servicios los mismos que se detallan en la Tabla 34.

Tabla 34.- Organización de servidores instados en la cuchilla 8

	Servidor	**Detalle**
1	Documentación	
2	Videos vigilancia	Seg0

3	Videos vigilancia	Seg1
4	Videos vigilancia	Seg2
5	Videos vigilancia	Seg3
6	Videos vigilancia	Seg4
7	Administración	XenServer

Referencia: Dirección de Tecnologías de la Información, 2015.

3.11.3. EQUIPOS DE TRABAJO

Para el mejor funcionamiento de la red de comunicaciones es necesario que las estaciones de trabajo se encuentren en buen estado ya que son la interfaz que se utiliza para acceder a los recursos de la red.

Los equipos de trabajo que existen en GAD Provincial de Imbabura son de diferentes marcas y modelos, pues se han ido adquiriendo de manera paulatina a lo largo de los años de vida de la institución.

Sin embargo existen equipos que debido al paso de los años y al avance de la tecnología ya no se encuentran en condiciones adecuadas y aunque la red se encuentre funcional dichos equipos no permiten realizar un uso oportuno de la red.

Existen 203 equipos de trabajo entre equipos personales y equipos de escritorio distribuidos en los diferentes edificios pertenecientes al GAD Provincial de Imbabura, a la tabla siguiente se indica el número por cada especificación.

En la Tabla 35 se indica el número de equipos de trabajo portátiles y de escritorio.

Tabla 35.- Equipos de trabajo

Equipos de trabajo	
Tipo	Nº de equipos
Escritorio	170
Portátil	33
Total	203

Referencia: Inventario del parque informático; Dirección de Tecnologías de la Información, 2015.

Estos equipos poseen diversas características una de las principales es el tipo de procesador que poseen, en la tabla siguiente se indica la descripción por cada tipo de equipo con el número por cada tipo procesador.

- **Equipos de escritorio**

En la Tabla 36 se indica el número de equipos de trabajo de escritorio con el tipo de procesador que poseen.

Tabla 36.- Equipos de escritorios y tipo de procesador

Tipo de procesador	Nº de equipos
AMD ATHION II	1
AMD EI-2500	3
INTEL CELERON	5
INTEL CORE I3	4
INTEL CORE I5	12
INTEL CORE I7	46
INTEL CORE2 DUO	66
INTEL PENTIUM 4	23
INTEL PENTIUM R	5
INTEL XEON (R)	3
QUAD-CORE INTEL XEON	1
XEON CPU E3-12220 V2	1
TOTAL	170

Referencia: Inventario del parque informático; Dirección de Tecnologías de la Información, 2015.

- **Equipos portátiles**

En la Tabla 37 se indica el número de equipos de trabajo portátiles con el tipo de procesador que poseen.

Tabla 37.- Equipos portátiles y tipo de procesador

Tipo de procesador	Nº de equipos
INTEL CORE I3	2
INTEL CORE I5	12
INTEL CORE I7	14
INTEL CORE2 DUO	5
TOTAL	33

Referencia: Inventario del parque informático; Dirección de Tecnologías de la Información, 2015.

Aquellos equipos que contaban con procesadores AMD ATHION II, AMD EI-2500, INTEL PENTIUM R, INTEL XEON (R), QUAD-CORE INTEL XEON y XEON E3-12220 V2 fueron cambiados por nuevos equipos adquiridos por la institución.

3.12. CONFIGURACIONES DE EQUIPOS

Las configuraciones que actualmente posee la red de la institución se especifica a continuación.

3.12.1. PROTOCOLO DE ENRUTAMIENTO

El protocolo de enrutamiento se encuentra configurado desde el firewall Asa, siendo esta configuración mediante rutas estáticas. Existen dos rutas estáticas, una por cada interfaz conectada en el firewall, la primera ruta en la interfaz interna “inside” y la segunda hacia la interfaz externa “outside”.

3.12.2. VLAN TRUNKING PROTOCOL

El switch de Core 4503E cumple con funcionalidades de capa 2 y capa 3, ahí se encuentra configurado el servidor de VLANs y es el equipo encargado de realizar el

enrutamiento intervlan para la conectividad total de la red. Para hacer posible el servicio de VLANs se utilizó el protocolo propietario de CISCO VLAN Trunking Protocol VTP.

En los demás switches existentes se encuentran configurados como clientes o switches en modo acceso.

3.12.3. ASIGNACION DE PUERTOS

Existen puertos en modo acceso y en modo trunk. Se encuentran configurados tanto en el switch de core como en cada uno de los swiches en modo acceso de la siguiente manera.

- De Switch Core A Servidores: Puertos en modo acceso (VLAN 3)
- De switch a switch: Puerto en modo troncal
- De switch core a ASA5520: Puerto en modo acceso (VLAN 101)
- De switch a pc y teléfono: Puerto en modo acceso
- NOTA: Los teléfonos que no son CISCO se unen a la TELEFONÍA configurados como bridge utilizando una IP perteneciente a la VLAN de datos correspondiente a la asignación mostrada en la tabla de VLAN's.
- DE SWITCH A AP-WIRELESS: Puertos en modo acceso
- De switch a relojes biométricos y cámaras: Puertos en modo acceso

Desde el switch de Core hacia cada uno de las plantas del edificio principal se encuentran los puertos designados de la siguiente manera, ver Tabla 38:

Tabla 38.- Interfaces de unión de switch Core con cada una de las plantas del edificio principal.

UNION DE EQUIPOS	INTERFACES
Switch de core- switch X.X.2.6 planta baja	GigabitEthernet3/48 - GigabitEthernet1/0/48

Switch de core- switch X.X.2.2 planta alta 1	GigabitEthernet3/47 - GigabitEthernet1/0/48
Switch de core- switch X.X.2.3 planta alta 1	GigabitEthernet3/45- GigabitEthernet1/0/48
Switch de core- switch X.X.2.4 planta alta 1	GigabitEthernet3/44- GigabitEthernet1/0/48
Switch de core- switch X.X.2.10 planta alta 2	GigabitEthernet3/42- GigabitEthernet1/0/48

Referencia: Dirección de Tecnologías de la Información, 2015.

3.12.4. GATEWAYS DE VLANS

En el switch de Core 4503E se encuentra configurado los gateways de VLANs, que consiste en asignar para cada VLAN un gateway, el cual permite que exista la comunicaciones entre VLANs diferentes.

A continuación en la Tabla 39 se indica la VLAN con su respectivo Gateway de VLAN.

Tabla 39.- VLAN con su respectivo Gateway de VLAN

GRUPO	RED
ADMIN_EQUIPOS	X.X.2.1/24
SERVIDORES	X.X.3.1/24
GESTION_TECNOLOGICA	X.X.4.1/24
PREFECTURA	X.X.5.1/24
PROCURADURIA	X.X.6.1/24
PLANIFICACION	X.X.7.1/24
GESTION_TECNICA	X.X.8.1/24
RELACIONES_PUBLICAS	X.X.9.1/24
ADMIN_GENERAL	X.X.10.1/24
INFRAESTRUCT_FISICA	X.X.11.1/24
DESARROLLO_ECONOM	X.X.12.1/24
PAS	X.X.13.1/24

WIFI	X.X.14.1/24
WIFI_EXTERNA	X.X.15.1/24
BODEGA	X.X.16.1/24
FAUSTO-GIS	X.X.17.1/24
FISCALIZACION	X.X.18.1/24
INVITADOS	X.X.30.1/24
RELOJES_BIOM	X.X.31.1/24
CAMARAS	X.X.32.1/24
TELEFONIA	X.X.40.1/24
MUTUALISTA	X.X.50.1/24
ENLACE_EQUIPOS	X.X.101.1/24

Referencia: Dirección de Tecnologías de la Información, 2015.

DEFAULT GATEWAY

En los swiches modo acceso existe la configuración default gateway, el cual indica cual es el gateway físico al que se conectan cada uno de los switches en modo acceso, en este caso el default gateway es el switch de Core en la capa de núcleo contraído.

3.12.5. NAT

El NAT se encuentra configurado en el ASA, existen configuraciones de NAT estático transformando las direcciones IP privadas de los servidores hacia las direcciones IP públicas como se indica en la Tabla 40.

Tabla 40.-NAT actual de la red del GAD provincial de Imbabura

IP PÚBLICA	SERVIDOR	IP PRIVADA
181.113.X.X	www.imbaburaturismo.gob.ec	X.X.3.31
181.113.X.X	Hosting para GIS www.gisimbabura.gob.ec	X.X.17.2
181.113.X.X	www.imbavial.gob.ec	X.X.3.22
181.113.X.X	www.imbabura.gob.ec	X.X.3.161
181.113.X.X	www.imbabura.travel	X.X.3.112
181.113.X.X	www.gpi.gob.ec	X.X.3.11
181.113.X.X	Video Streaming	X.X.3.23

Referencia: Dirección de Tecnologías de la Información, 2015.

3.12.6. PROTOCOLO SPANNING-TREE

No existe configuración del protocolo Spanning-Tree, excepto la configuración por defecto para las últimas versiones de IOS en la serie CISCO CATALYST, la cual se establece mediante la norma IEEE 802.1d.

CAPITULO IV

4. DISEÑO DE LA TOPOLOGÍA FÍSICA Y LÓGICA DE LA RED DE COMUNICACIONES PARA EL GAD PROVINCIAL DE IMBABURA

En este capítulo constan los diseños de la topología física y lógica de la red de comunicaciones, basado en los aspectos analizados en el capítulo de levantamiento de información.

4.1.DISEÑO DE LA TOPOLOGÍA FÍSICA

En el sistema pasivo que corresponde al data center y el cableado estructurado no surgen grandes cambios en su infraestructura física, debido a que cumple con las normas establecidas de acuerdo al levantamiento de información, ratificando el diseño realizado por Jenny Alexandra Villegas Limaico con su tema de tesis OPTIMIZACIÓN DE LA ADMINISTRACIÓN DE LA RED E IMPLEMENTACIÓN DE SERVIDORES DE SERVICIOS PARA EL GOBIERNO PROVINCIAL DE IMBABURA.

Los cambios en cableado estructurado se presentan en algunos de sus elementos como:

- Instalación de entrada
- Distribuidores central del cableado
- Distribuidores horizontales
- Distribución horizontal del cableado
- Área de trabajo

En la Imagen 31 se muestra la nueva topología física para la red de la institución.

4.1.1. TOPOLOGÍA FÍSICA DE RED

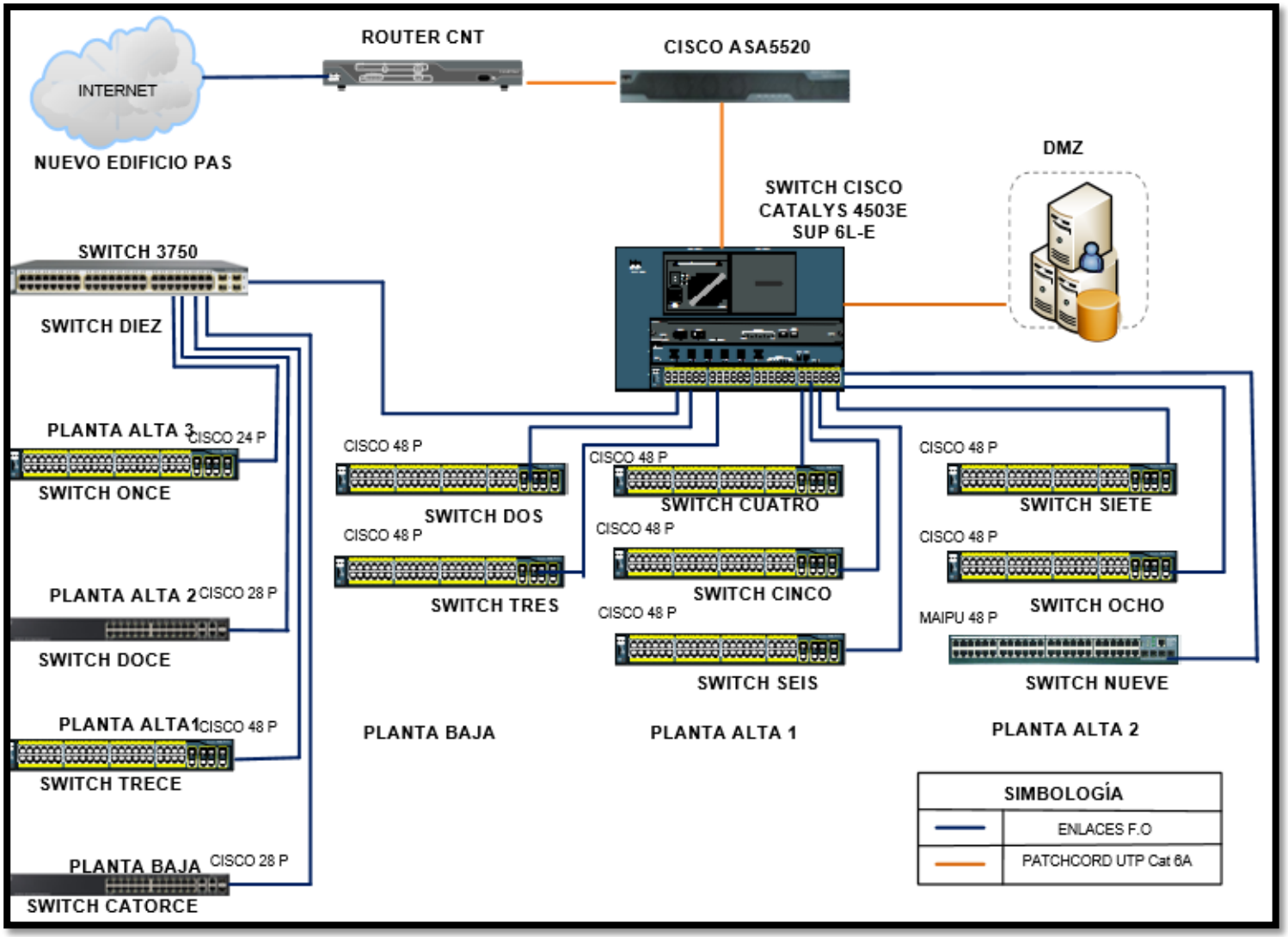


Imagen 31.- Nueva topología física de red del GAD Provincial de Imbabura.
Referencia: Basado en investigación teórica y práctica

4.1.2. INSTALACIÓN DE ENTRADA

Es el lugar por donde ingresan los servicios de telecomunicaciones al edificio o donde llegan las canalizaciones de interconexión con otros edificios de la empresa, en este caso se debe añadir la conexión del edificio principal con el edificio del PAS, la norma recomienda que este elemento este en un cuarto aparte por razones de seguridad, pero puede estar dentro del Data Center, en este caso se mantiene dentro del Data Center.

4.1.3. DISTRIBUIDOR CENTRAL DEL CABLEADO

El backbone provee la interconexión entre los repartidores horizontales y el Data Center. Para la reestructuración del distribuidor central del cableado se añade los nuevos enlaces entre el switch de core hacia cada uno de los switches de acceso de la planta baja y la planta alta 2, los enlaces pueden ser de cable UTP o fibra óptica, se instalará mediante cables de fibra óptica OM3.

4.1.4. REPARTIDORES HORIZONTALES

Los repartidores horizontales se mantienen en el mismo sitio físico actual pues cumplen con las especificaciones de la norma que indica entre ellas: que sea dedicado exclusivamente a la infraestructura de telecomunicaciones, mínimo un armario por piso, la reestructuración se realiza en la distribución y organización de los puertos de los equipos activos de acuerdo a las nuevas VLANs planteadas.

4.1.4.1. Mapeo puntos de red.

Permite identificar la ubicación de los puntos del cableado con los puertos de los swiches de acceso y saber a qué VLAN pertenece dicho punto. Este mapeo completo se encuentra en el ANEXO 03, a continuación un resumen por cada planta.

- **Planta Baja**

En la planta baja existen dos switches, distribuidos con las siguientes VLANS en sus puertos como se indica en la Tabla 41.

Tabla 41.- Resumen puntos de red plata baja

GPI-PLANTA BAJA			
SWITCH	RANGO DE PUERTOS	NOMBRE VLAN	NÚMERO VLAN
X.X.4.2	2-9, 11-14, 27,28 32-35, 37-45	INFRAESTRUCT FISICA	28
	15-17, 46	FISCALIZACION	16
	18-21	DESARROLLO ECONOM	30
	29	CAMARAS HALL	48
	24-25	PREFECTURA	10
	10, 22,23,26, 36	WIFI	52
	30,31	BIOMETRICOS	
X.X.4.3	2-3	DESARROLLO ECONOM	30
	4-5 15-16	FISCALIZACION	16
	6-11	ADMIN GENERAL	20
	12-13	CAMARAS	48
	14	TELEFONIA	40

Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura.

En la Imagen 32 se indica las VLANs que corresponde a la planta baja.

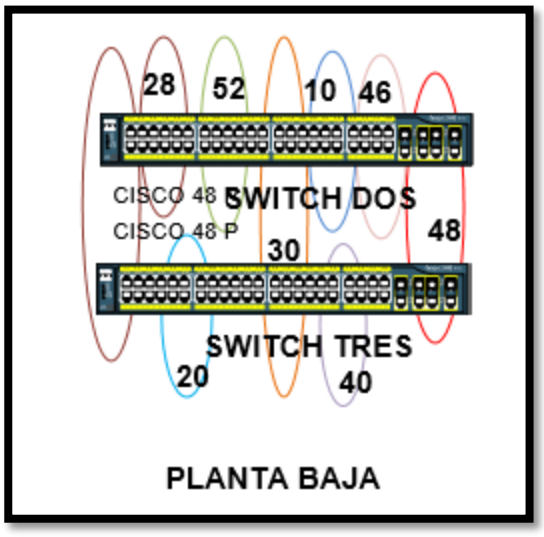


Imagen 32.- Nueva distribución de VLANs planta baja
Referencia: Basado en investigación teórica y práctica

- **Planta alta 1**

En la planta alta 1 existen tres switches, distribuidos con las siguientes VLANS en sus puertos como se indica en la Tabla 42.

Tabla 42.- Resumen de puntos de red plata alta 1

GPI-PLANTA ALTA 1			
SWITCH	RANGO DE PUERTOS	NOMBRE VLAN	NÚMERO VLAN
X.X.4.4	2-11, 14-16, 18-24	PREFECTURA	10
	12-13, 40-41	RELACIONES PUBLICAS	18
	17	WIFI	52
	25-31	PROCURADURIA	12
	32-39	COMPRAS PUBLICAS	22
	42-46	TIC	8
X.X.4.5	2,6, 10-12, 14	TICS	8
	3-5, 7-9, 13, 15-19	FINANCIERO	24
	20-26	ADMINISTRACION	20
X.X.4.6	2-3, 5-6, 8-11, 35	PREFECTURA	10
	4, 37	WIFI	52

	7, 33,34,	ADMIN GENERAL	20
	12, 36, 31, 32	RELACIONES PUBLICAS	18
	29, 30	FINANCIERO	24
	18-20, 15	TICS	8
	17	PROCURADURIA	12
	13,38	CAMARAS	48
	21-28, 16, 14	TALENTO HUMANO	26

Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura.

En la Imagen 33 se indica las VLANs que corresponde a la planta alta 1.

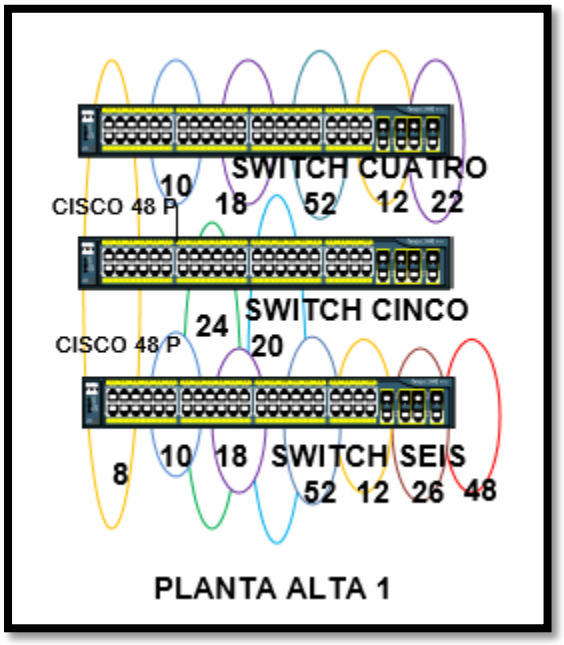


Imagen 33.-Nueva distribución de VLANs planta alta 1
Referencia: Basado en investigación teórica y práctica

- **Planta alta 2**

En la planta alta 2 existen tres switches, distribuidos con las siguientes VLANS en sus puertos como se indica en la Tabla 43.

Tabla 43.- Resumen puntos de red planta alta 2

GPI-PLANTA ALTA 2			
SWITCH	RANGO DE PUERTOS	NOOMBRE VLAN	NÚMERO VLAN
X.X.4.7	2-23, 25-43	PLANIFICACION	14
	1,24	WIFI	52
	44-46	BODEGA	44
X.X.4.8	2-16, 21-24	GESTION AMBIENTAL	34
	17-20	RELACIONES PUBLICAS	18
	25-46	RECURSOS HIDRICOS	36
X.X.4.9	2-6	DESARROLLO ECONOM	
	7-15	RELACIONES PUBLICAS	

Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura.

En la Imagen 34 se indica las VLANs que corresponde a la planta alta 2.

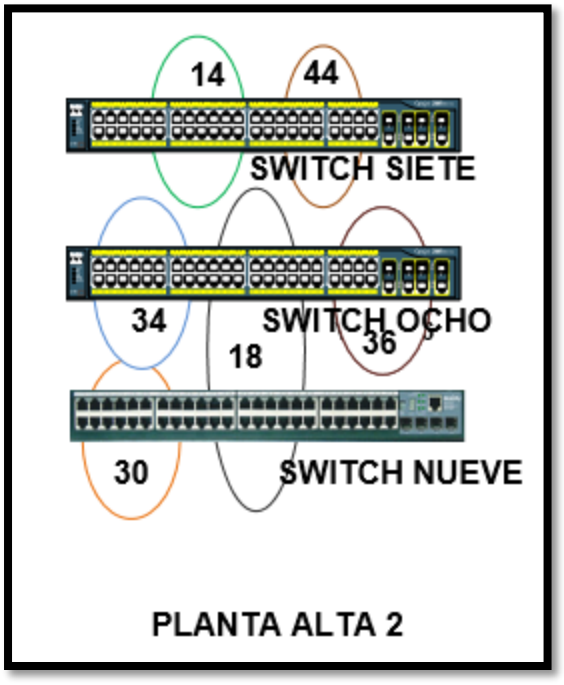


Imagen 34.-Nueva distribución de VLANs planta alta 2
Referencia: Basado en investigación teórica y práctica

- **Edificio PAS**

En el nuevo edificio PAS existen dos switches ocupados, distribuidos con las siguientes VLANS en sus puertos como se indica en la Tabla 44.

Tabla 44.- Resumen puntos de red edificio PAS

GPI-EDIFICIO PAS			
SWITCH	RANGO DE PUERTOS	NOOMBRE VLAN	NÚMERO VLAN
X.X.4.12	2-30	PAS	38
	31-48	TURISMO	32
X.X.4.13	2-48	PAS	38

Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura.

Las demás plantas del edificio del PAS no se encuentran ocupadas, además se desconoce el uso futuro de estas instalaciones, por lo tanto dichos equipos no cuentan con configuraciones de puertos para acceso de determinadas VLANs. En la Imagen 35 se indica las VLANs que corresponde a cada switch.

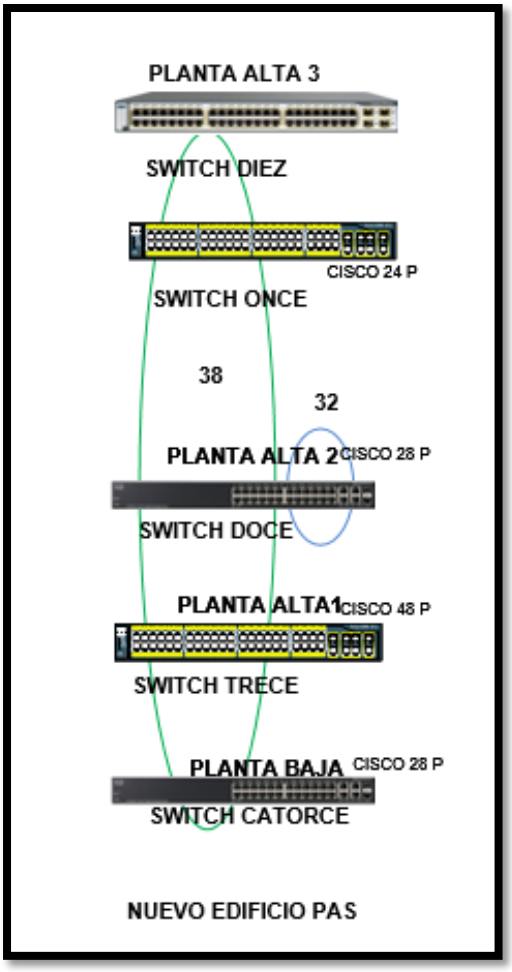


Imagen 35.-Nueva distribución de VLANs edificio PAS
Referencia: Basado en investigación teórica y práctica

4.1.5. DISTRIBUCIÓN HORIZONTAL DEL CABLEADO

La distribución horizontal interconecta el distribuidor secundario y el área de trabajo, en esta distribución no debe existir puntos de interconexión y la distancia máxima es de 90 metros independientemente de si es cobre o fibra óptica.

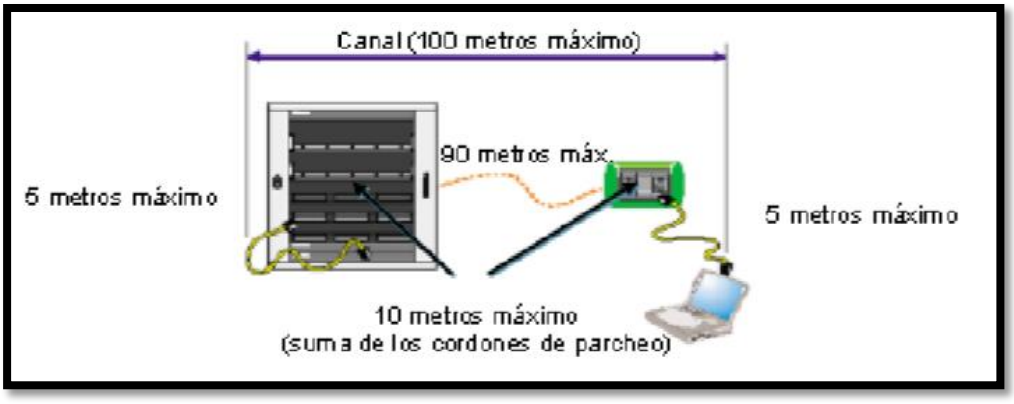


Imagen 36.- Distribución horizontal del cableado.
Fuente: Optimización de la administración de la red e implementación de servidores de servicios para el GAD provincial de Imbabura, Jenny Alexandra Villegas Limaico (2013)

La implementación de la distribución horizontal implica la instalación de cable de telecomunicaciones proveniente del distribuidor secundario hacia el área de trabajo. La instalación se realizara mediante el cielo raso o techo falso y en las partes que no existe el techo falso se utilizara canaletas como guía, se instalará de forma ordenada, evitando enredos y amontonamiento del cable.

El número de cables de distribución horizontal se basa en la colocación de nuevas estaciones de trabajo en la planta baja en el edificio principal, las cuales funcionan como foros para participación ciudadana, añadiendo mínimo dos conectores en cada área de trabajo. El cable debe ser par trenzado mínimo de categoría 5e, en este caso se utilizara categoría 6a que es con el que cuenta la empresa en la actualidad.

4.1.5.1. Etiquetado

El etiquetado de la distribución horizontal será de la misma nomenclatura actual, colocando etiquetas en ambos extremos de los enlaces. Las etiquetas serán auto

laminables con la nomenclatura PB-D1, en donde la primera parte representa la planta del distribuidor horizontal del cableado y la segunda parte el puerto del switch, esta nomenclatura es la misma de los puntos de red en las estaciones o áreas de trabajo.

4.1.6. ÁREA DE TRABAJO

Es la localización del punto de conexión entre la distribución horizontal y los dispositivos de conexión del cable en el área de trabajo, dichos puntos son la toma de Telecomunicaciones.

Es necesario una toma por estación de trabajo como mínimo o dos por área de trabajo. La destinación de espacio de trabajo es una por cada 10 m2.

Por lo menos se debe instalar una toma de energía cerca de cada toma de telecomunicaciones.

4.1.6.1. Etiquetado

El sistema de etiquetado en los nuevos puntos de red se realizará con etiquetas auto laminable colocado dentro de los faceplate de tal forma que no puedan ser manipuladas fácilmente, conservando el modelo de etiquetado actual:

PB-D1

En donde la primera parte representa la planta del distribuidor horizontal del cableado y la segunda parte el puerto del switch.

4.2.DISEÑO DE LA TOPOLOGÍA LÓGICA

La topología lógica indica cómo se comunican las estaciones de trabajo o equipos dentro de la red física, se segmentará el tráfico realizando una nueva distribución de VLANs reduciendo así los dominios de colisión existentes en la red actual.

4.2.1. DISTRIBUCIÓN LÓGICA DE LA RED

El GAD Provincial de Imbabura posee un contrato de servicio de internet de 30 Mbps con la empresa CNT, este ISP provee de un pool de direcciones públicas 181.113.X.X/27 (por confidencialidad se ha ocultado los dos últimos octetos de la dirección IP). Para la red interna se diseñara un nuevo direccionamiento con una dirección full class clase B es 170.20.0.0/16, la distribución lógica se resume en la Tabla 45.

Tabla 45.- Distribución lógica de la red.

DESCRIPCIÓN	SUBRED	MÁSCARA DE SUBRED
Red Externa	181.113.X.X	255.255.255.224
Red Interna	170.20.0.0	255.255.0.0

Referencia: Basado en investigación teórica y práctica.

4.2.2. TOPOLOGÍA LÓGICA DE RED

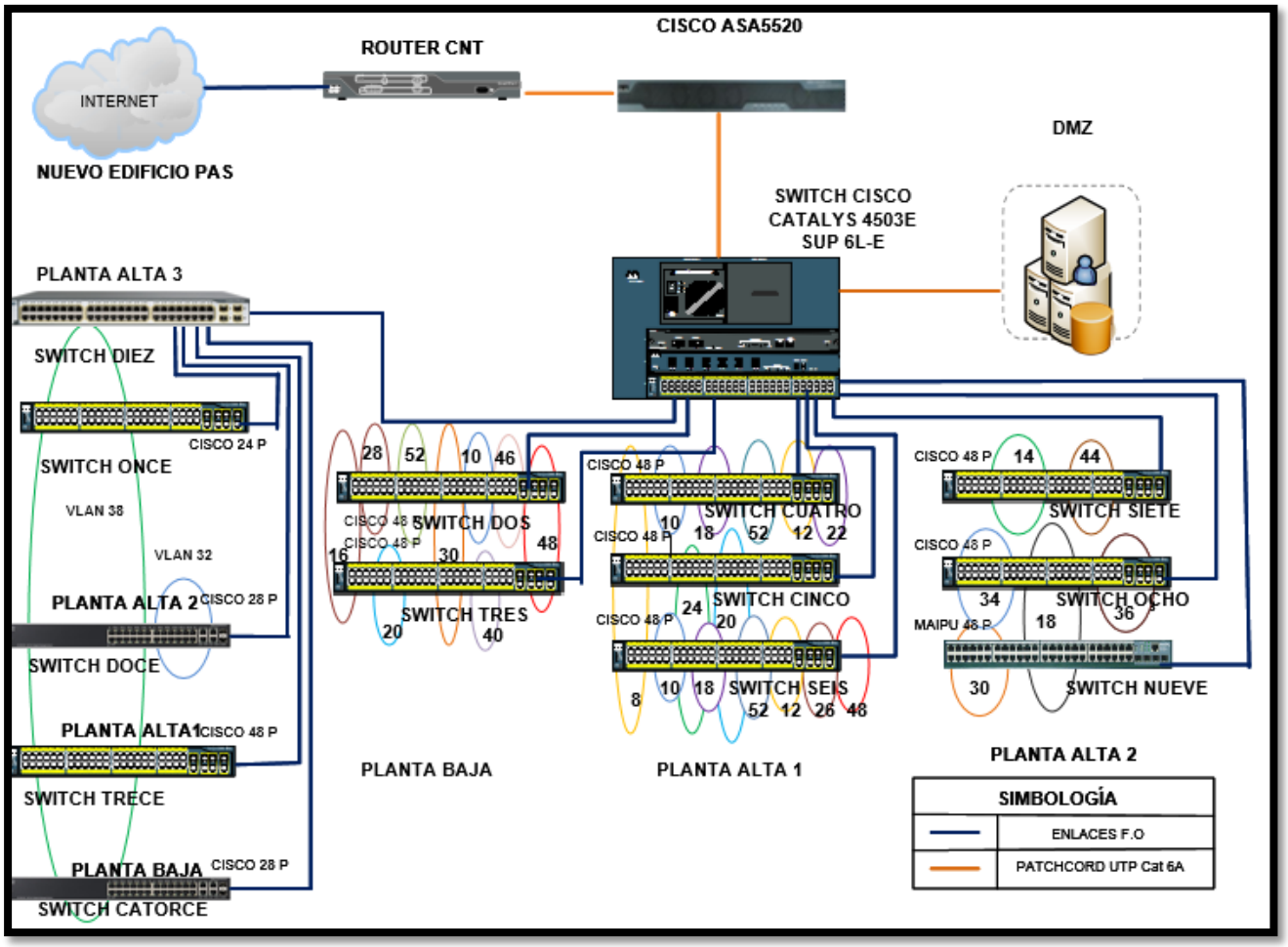


Imagen 38.- Diseño de topología lógica de red.
Referencia: Basado en investigación teórica y práctica.

4.2.3. SEGMENTACIÓN DE RED

La distribución lógica de la red ha sido diseñada de acuerdo a las necesidades y direcciones y subdirecciones existentes en la institución. En total existirán 25 VLANs distribuidas en los edificios pertenecientes al GAD provincial, como se indica en la Tabla 46.

Tabla 46.- Nuevo direccionamiento IP basado en la creación de nuevas VLANs.

GRUPO	ID VLAN	RED	GATEWAY	BROADCAST
EQUIPOS	4	170.20.4.0/24	170.20.4.1	170.20.4.255
SERVIDORES	6	170.20.6.0/24	170.20.6.1	170.20.6.255
TICS	8	170.20.8.0/24	170.20.8.1	170.20.8.255
PREFECTURA	10	170.20.10.0/24	170.20.10.1	170.20.10.255
PROCURADURIA	12	170.20.12.0/24	170.20.12.1	170.20.12.255
PLANIFICACION	14	170.20.14.0/24	170.20.14.1	170.20.14.255
FISCALIZACION	16	170.20.16.0/24	170.20.16.1	170.20.16.255
RELACIONES_PUBLICAS	18	170.20.18.0/24	170.20.18.1	170.20.18.255
ADMINISTRACIÓN	20	170.20.20.0/24	170.20.20.1	170.20.20.255
COMPRAS_PUBLICAS	22	170.20.22.0/24	170.20.22.1	170.20.22.255
FINANCIERO	24	170.20.24.0/24	170.20.24.1	170.20.24.255
TALENTO_HUMANO	26	170.20.26.0/24	170.20.26.1	170.20.26.255
INFRAESTRUCT_FISICA	28	170.20.28.0/24	170.20.28.1	170.20.28.255
DESARROLLO_ECONOM	30	170.20.30.0/24	170.20.30.1	170.20.30.255
TURISMO	32	170.20.32.0/24	170.20.32.1	170.20.32.255
GESTION_AMBIENTAL	34	170.20.34.0/24	170.20.34.1	170.20.34.255
RECURSOS_HIDRICOS	36	170.20.36.0/24	170.20.36.1	170.20.36.255
PAS	38	170.20.38.0/24	170.20.38.1	170.20.38.255
TELEFONIA	40	170.20.40.0/24	170.20.40.1	170.20.40.255

BODEGA	44	170.20.44.0/24	170.20.44.1	170.20.44.255
BIOMETRICOS	46	170.20.46.0/24	170.20.46.1	170.20.46.255
CAMARAS	48	170.20.48.0/24	170.20.48.1	170.20.48.255
MUTUALISTA	50	170.20.50.0/24	170.20.50.1	170.20.50.255
WIFI	52	170.20.52.0/22	170.20.52.1	170.20.55.255
ENLACE_EQUIPOS	100	170.20.100.0/24	170.20.100.1	170.20.100.255

Referencia: Basado en investigación teórica y práctica.

4.2.4. MODELO DE RED

El rediseño para la red del GAD provincial debe estar alineado a garantizar el cumplimiento del objetivo de este proyecto, es decir, potenciar el rendimiento de la red. Para lograr ello se considera la implementación de un modelo de red jerárquico, el cual ofrece algunos beneficios como: escalabilidad, seguridad, fácil administración, fácil mantenimiento.

El modelo jerárquico está basado en diseño por capas, las cuales son: núcleo, distribución y acceso, sin embargo la red que posee el GAD provincial es de tamaño mediana, por lo tanto la capa núcleo en donde se encuentra el switch de Core 4503E funciona a la vez como capa distribución, esta capa se denomina núcleo contraído , excepto para el nuevo edificio PAS que cuenta con un switch Cisco 3750 que pertenece a la capa de distribución para los switches de acceso de cada una de las plantas de este edificio.

El modelo de red quedaría contemplando dos capas con los siguientes switches por plantas y representados de la siguiente manera, ver Tabla 47.

Tabla 47.- Nombres switches de acceso y core.

NOMBRES PARA CADA SWITCH		
SWITCH	PLANTA	NOMBRE
Switch Catalys 4503E	ALTA1	CORE
Cisco Catalyst 2960S	BAJA	DOS
Cisco Catalyst 2960S	BAJA	TRES
Cisco Catalyst 2960S	ALTA 1	CUATRO
Cisco Catalyst 2960S	ALTA 1	CINCO
Cisco Catalyst 2960S	ALTA 1	SEIS
Cisco Catalyst 2960S	ALTA 2	SIETE
Cisco Catalyst 2960S	ALTA 2	OCHO
Switch MAIPU	ALTA 2	NUEVE
Cisco 3750	ALTA 3-PAS	DIEZ
Cisco Catalyst 2960S	ALTA 3-PAS	ONCE
Cisco SG300	ALTA 2-PAS	DOCE
Cisco Catalyst 2960S	ALTA 1-PAS	TRECE
Cisco SG300	BAJA-PAS	CATORCE

Referencia: Basado en investigación teórica y práctica

El modelo de red quedaría con un diseño en dos capas que son: la capa de núcleo contraído y la capa de acceso, como se indica en la Imagen 37.

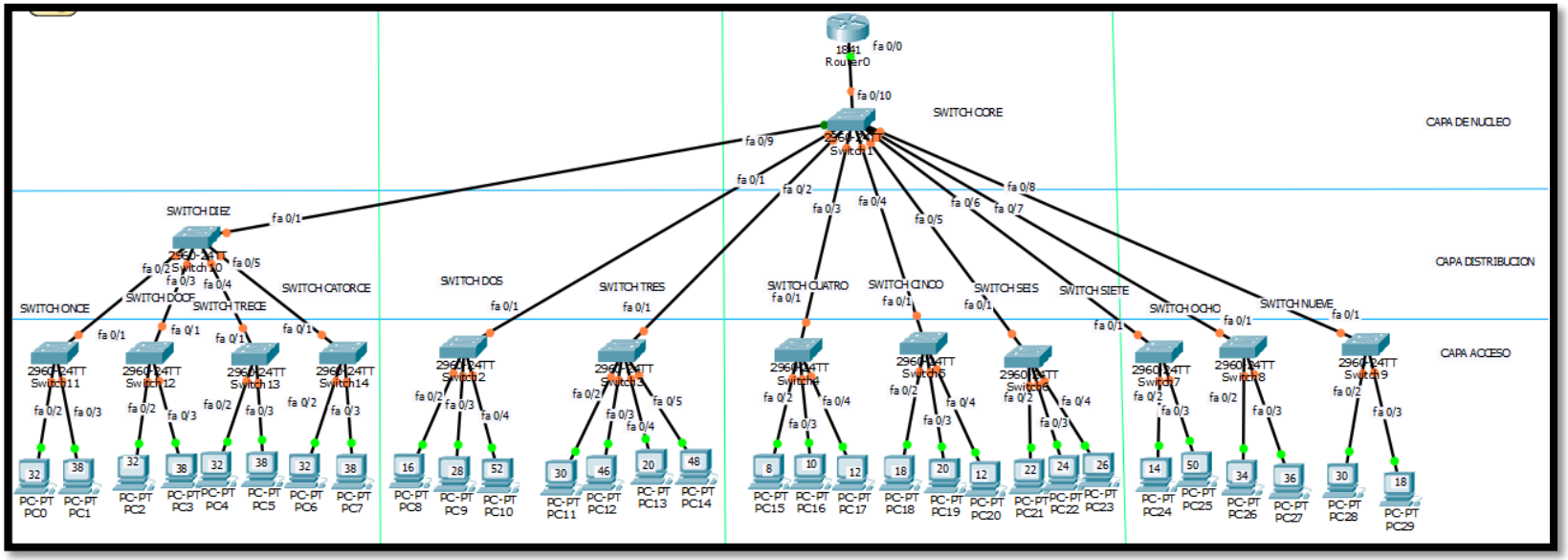


Imagen 37.-Modelo jerárquico para la red del GAD Provincial de Imbabura.
Referencia: Basado en investigación teórica y práctica

Los enlaces entre los switches de cada capa serán mediante fibra óptica como se indicó en el diseño de distribución central de cableado, se conectará mediante los puertos en modo trunk designados de la siguiente manera, ver Tabla 48:

Tabla 48.-Interfaces de unión entre el switch la capa de núcleo contraído y a capa de acceso.

UNION DE EQUIPOS	INTERFACES
Switch de core- switch dos	GigabitEthernet3/40 hacia la interfaz GigabitEthernet1/0/48
Switch de core- switch tres	GigabitEthernet3/41 hacia la interfaz GigabitEthernet1/0/48
Switch de core- switch cuatro	GigabitEthernet3/42 hacia la interfaz GigabitEthernet1/0/48
Switch de core- switch cinco	GigabitEthernet3/43 hacia la interfaz GigabitEthernet1/0/48
Switch de core- switch seis	GigabitEthernet3/44 hacia la interfaz GigabitEthernet1/0/48
Switch de core- switch siete	GigabitEthernet3/45 hacia la interfaz GigabitEthernet1/0/48
Switch de core- switch ocho	GigabitEthernet3/46 hacia la interfaz GigabitEthernet1/0/48
Switch de core- switch nueve	GigabitEthernet3/47 hacia la interfaz GigabitEthernet1/0/48
Switch de core- switch diez	GigabitEthernet3/48 hacia la interfaz GigabitEthernet1/0/48
Switch diez - switch once	GigabitEthernet3/10 hacia la interfaz GigabitEthernet1/0/24
Switch diez - switch doce	GigabitEthernet3/11 hacia la interfaz GigabitEthernet1/0/24
Switch diez - switch trece	GigabitEthernet3/12 hacia la interfaz GigabitEthernet1/0/24
Switch diez - switch catorce	GigabitEthernet3/13 hacia la interfaz GigabitEthernet1/0/24

Referencia: Basado en investigación teórica y práctica.

4.2.4.1. CAPA ACCESO

Esta capa será la que se encuentre en contacto tanto con el switch de core en la capa de núcleo como también en contacto con los usuarios finales. La finalidad de esta capa es proporcionar un medio de conexión de los dispositivos hacia la red y controlar que dispositivos pueden conectarse o no.

En esta capa es importante que se maneje equipos con características idóneas para garantizar un buen rendimiento de la red. Los equipos que sirven como switches de distribución y acceso son:

- Cisco Catalyst 2960S
- Cisco SG300
- Switch MAIPU

Los mismos que permiten configuración de VLANs, VTP cliente, asignación de puertos sea en modo acceso y modo trunk, PVST+ y port security.

4.2.4.1.1. VLAN Trunking Protocol -VTP client

Para la configuración de VLANs en los switches de la capa acceso se realiza mediante el protocolo VTP, se configura cada equipo en modo VTP client, en estos switches se propaga las VLANs creadas por el VTP server y no se puede modificar ninguna de ellas.

Los switches en modo cliente se detallan a continuación en la Tabla 49.

Tabla 49.-Listado de switches clientes VTP

LISTADO DE SWITCH CLIENTES VTP		
SWITCH	PLANTA	NOMBRE
Cisco Catalyst 2960S	BAJA	DOS
Cisco Catalyst 2960S	BAJA	TRES

Cisco Catalyst 2960S	ALTA 1	CUATRO
Cisco Catalyst 2960S	ALTA 1	CINCO
Cisco Catalyst 2960S	ALTA 1	SEIS
Cisco Catalyst 2960S	ALTA 2	SIETE
Cisco Catalyst 2960S	ALTA 2	OCHO
Switch MAIPU	ALTA 2	NUEVE
Cisco 3750	ALTA 3-PAS	DIEZ
Cisco Catalyst 2960S	ALTA 3-PAS	ONCE
Cisco SG300	ALTA 2-PAS	DOCE
Cisco Catalyst 2960S	ALTA 1-PAS	TRECE
Cisco SG300	BAJA-PAS	CATORCE

Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura.

La configuración de VTP en el modo cliente se lo realiza mediante el comando VTP client y se define un dominio de VTP y una contraseña. El dominio y contraseña nos permite establecer el grupo de trabajo en el cual deben establecerse los switches clientes. El establecimiento de VTP client se lo realiza como el siguiente ejemplo, ver Imagen 38.

```
Switch#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

Switch(vlan)#vtp client
Setting device to VTP CLIENT mode.
Switch(vlan)#vtp domain gpi_2016
Changing VTP domain name from NULL to gpi_2016
Switch(vlan)#vtp password vlans2016
Setting device VLAN database password to vlans2016
Switch(vlan)#exit
APPLY completed.
Exiting....
Switch#
```

Imagen 38.-Ejemplo de configuración de VTP cliente
Referencia: Basado en investigación teórica y práctica

4.2.4.1.2. Asignación de puertos

Para la propagación de las VLANs se debe establecer en los switches de acceso los puertos de los enlaces entre la capa de núcleo contraído y switches de acceso en modo

trunk, estos enlace en modo trunk se manejan mediante la VLAN nativa que es la administración de equipos VLAN 4 y no con la VLAN default que es la VLAN 1. Se plantea el diseño de la VLAN 4 como la VLAN de administración de equipos y no la VLAN 1, para mejorar la seguridad de acceso a los equipos ya que la VLAN 1 es la VLAN de deafult y la más conocida.

Además en la capa acceso de debe configurar los demás puertos en modo acceso para aquellos en los cuales se conecta un usuario para una VLAN especifica.

En el mapeo de puertos se puede verificar los puertos de cada switch de acceso y su VLAN correspondiente, a continuación se indica los puertos y su modo de configuración por cada switch.

- PLANTA BAJA

En la Tabla 50 se asigna los puertos en modo acceso y troncal por cada switch para la planta baja.

Tabla 50.- Asignación de puertos planta baja

ASIGNACIÓN DE PUERTOS PLANTA BAJA		
SWITCH	PUERTOS	MODO
DOS	1-46	acceso
	47-48	troncal
TRES	1-16	acceso
	47-48	troncal

Referencia: Basado en investigación teórica y práctica.

- PLANTA ALTA 1

En la Tabla 51 se asigna los puertos en modo acceso y troncal por cada switch para la planta alta 1.

Tabla 51.- Asignación de puertos planta alta 1

ASIGNACIÓN DE PUERTOS PLANTA BAJA		
SWITCH	PUERTOS	MODO
CUATRO	1-46	acceso
	47-48	troncal
CINCO	1-26	acceso
	47-48	troncal
SEIS	1-38	acceso
	47-48	troncal

Referencia: Basado en investigación teórica y práctica.

- PLANTA ALTA 2

En la Tabla 52 se asigna los puertos en modo acceso y troncal por cada switch para la planta alta 2.

Tabla 52.- Asignación de puertos planta alta 2

ASIGNACIÓN DE PUERTOS PLANTA BAJA		
SWITCH	PUERTOS	MODO
SIETE	1-46	acceso
	47-48	troncal
OCHO	1-46	acceso
	47-48	troncal
NUEVE	1-15	acceso
	47-48	troncal

Referencia: Basado en investigación teórica y práctica.

- EDIFICIO PAS

En la Tabla 53 se asigna los puertos en modo acceso y troncal por cada switch para la planta baja.

Tabla 53.- Asignación de puertos edificio PAS

ASIGNACIÓN DE PUERTOS PLANTA BAJA		
SWITCH	PUERTOS	MODO
DIEZ	-	acceso
	10-20	troncal
ONCE	-	acceso
	23-24	troncal
DOCE	1-46	acceso
	23-24	troncal

TRECE	1-46	acceso
	23-24	troncal
CATORCE	-	acceso
	23-24	troncal

Referencia: Basado en investigación teórica y práctica.

Para configurar los puertos en modo acceso o modo troncal se lo realiza como se datalla a continuación.

En la Imagen 39 tenemos un ejemplo de configuración de puerto en modo troncal

```
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 4
Switch(config-if)#no shutdown
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

Imagen 39.- Ejemplo de configuración de puerto en modo troncal
Referencia: Basado en investigación teórica y práctica

En la Imagen 40 tenemos un ejemplo de configuración de puerto en modo acceso

```
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastethernet 0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 28
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
Switch#
```

Imagen 40.- Ejemplo de configuración de puerto en modo acceso
Referencia: Basado en investigación teórica y práctica

Cuando se desea configurar varios puertos en un mismo modo y para agilitar el proceso y no realizar interfaz por interfaz existe la configuración por rangos que se realiza de la siguiente manera, ver Imagen 41.

```
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fastethernet 0/1-9
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk native vlan 4
Switch(config-if-range)#no shutdown
Switch(config-if-range)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

Imagen 41.-Ejemplo de configuración de rango de puertos.
Referencia: Basado en investigación teórica y práctica

4.2.4.1.3. PVST+

Mediante este protocolo se maneja un árbol de expansión independiente por VLAN designando un switch determinado como el switch raíz para cada VLAN existente, de esta manera se garantiza una mejor distribución del tráfico de la red, impide la creación de bucles y balancea la carga de tráfico de la Capa 2.

En este caso, no contamos con enlaces redundantes, por lo tanto el switch de Core será designado como el switch primario para todas las VLANs de la red y si en el futuro se cuenta con redundancia se deberá configurar cual será el switch secundario para cada VLAN.

En los switches de acceso se activa el protocolo PVST+ para que puedan reconocer al switch de Core como su raíz principal, como se nuestra en la Imagen 42.

```
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#spanning-tree mode pvst
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
Switch#
```

Imagen 42.-Ejemplo de activación de PVST+
Referencia: Basado en investigación teórica y práctica

4.2.4.1.4. Port Security

Para mejorar el acceso a la red se configura seguridad en los puertos de los switches, lo cual permite mejorar la seguridad en la capa de acceso.

Las direcciones MAC seguras pueden ser configuradas estáticamente, sin embargo, su configuración puede ser una tarea compleja y propensa a errores, por ello la propuesta alterna es configurar port security en la interface del switch, en donde se puede limitar el número de direcciones MAC que pueden ser aprendidas en una interfaz. El número de direcciones MAC por puerto será limitado a 1, es decir, la primera dirección dinámicamente aprendida por el switch llega a ser la dirección segura.

La dirección segura se planteara mediante Sticky secure MAC addresses, en donde las direcciones MAC son dinámicamente configuradas, las mismas que se almacenan en la tabla de direcciones y en la configuración corriendo, por lo tanto cuando el switch se reinicie, las interfaces no necesitan reconfigurarlas dinámicamente.

La direcciones MAC aprendidas pueden ser limitas a un cierto número, en este caso será limitado a 1, esta primera dirección dinámicamente aprendida por el switch es la dirección segura.

En el caso de existir un tipo de violación a esta restricción, es decir, se intente agregar otro dispositivo a una interfaz, la acción a ser tomada es shutdown, la cual coloca a la inreface en error-disabled y el puerto es apagado.

Cuando un puerto seguro están en el estado de error-disabled, se puede sacarlo de este estado con el comando de configuración global errdisable recovery cause psecureviolation o manualmente re-habilitarlo ingresando los comandos shutdown y no shutdown en configuración de interface.

A continuación en la Imagen 43 se indica un ejemplo de la configuración de seguridad por puertos en el rango de interfaces 4 a 6 de un switch.

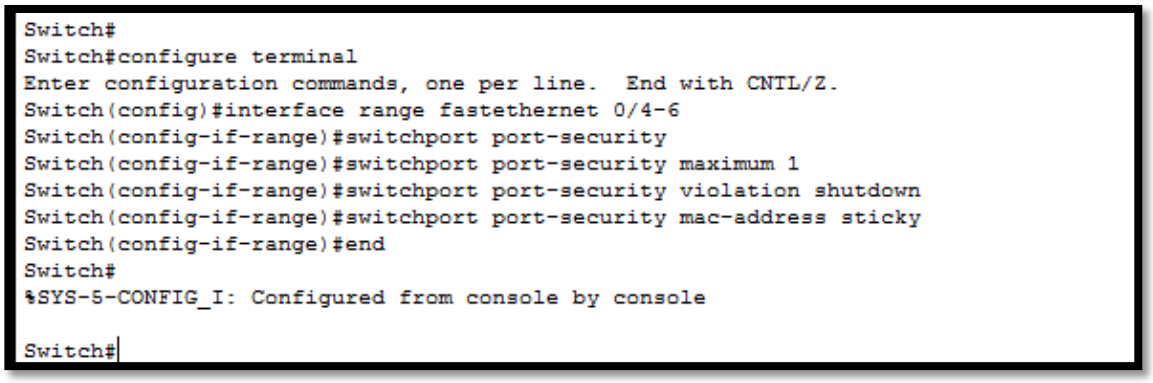


Imagen 43.-Ejemplo de configuración de seguridad de puertos.
Referencia: Basado en investigación teórica y práctica

4.2.4.2. CAPA NÚCLEO CONTRAIDO

Esta capa es el backbone de la red y por ende debe soportar alta velocidad, se conecta directamente con la capa de acceso y a través de esta capa con todos los usuarios la red. En esta capa debido a su importancia se debe garantizar ciertas condiciones como: debe reenviar grandes cantidades de tráfico, la capa núcleo debe puede conectarse a los recursos de internet. En este nivel se conservará el Switch Catalys 4503E cuyas características son

idóneas para esta función, debido a que posee 280 Gbps de capacidad de conmutación con 225 millones de paquetes por segundo (Mpps) de rendimiento.

El switch Cisco 4503E posee características de capa 2 y capa 3, en este se establecerá el manejo de VLANs contemplando ahí la configuración de VTP, es decir, VTP Server, puertos en modo trunk, así como también la configuración de access-list.

Debido a que el switch de core maneja todo el tráfico generado para la red se manejara un diseño con una nueva segmentación de la red a nivel lógico mediante la configuración de VLANs.

Para la reestructuración de la red no se considera el equipo packetshaper Bluecoat 3500 debido a que el ancho de banda que maneja es menor al servicio brindado por el ISP por lo tanto este equipo está convirtiéndose en un cuello de botella y eleva el diámetro de la red al agregar un salto más por donde deba viajar los datos.

4.2.4.2.1. VLAN Trunking Protocol - VTP server

Para la creación de VLANs se utiliza el protocolo VTP, en el switch de Core se configura VTP en modo server (VTP server) y se crea cada uno de las VLANs con sus nombres respectivos, desde este equipo servidor que mantiene una configuración adecuada de VLANS, administrando la creación, eliminación y renombre de VLANs.

Las VLANs no se desarrollaran solo por las diferentes direcciones de la institución, debido a que existen direcciones de la institución que poseen subdirecciones y por ende mayor número de usuarios que otras.

Las VLANs que se implementarán están de acuerdo a direcciones, subdirecciones, número de usuarios en cada VLAN, y tipo de información que manejan para que en lo posterior se puede realizar calidad de servicio (QoS[49]) quedando las VLANs de la siguiente manera, ver Tabla 54.

Tabla 54.- Nuevo diseño de VLANs

NÚMERO DE VLAN	NOMBRE DE VLAN
4	Equipos
6	Servidores
8	TICSs
10	Prefectura
12	Procuraduría
14	Planificación
16	Fiscalización
18	Relaciones publicas
20	Administración
22	Compras publicas
24	Financiero
26	Talento humano
28	Infraestructura física
30	Desarrollo económico
32	Turismo
34	Gestión ambiental
36	Recursos hídricos
38	PAS
40	Telefonía
44	Bodega
46	Biométricos
48	Cámaras
50	Mutualista
52	Red inalámbrica
100	Enlace equipos

Referencia: Basado en investigación teórica y práctica.

[49] QoS=Quality of Service, calidad de servicio

Para la creación de VTP debe existir un dominio y una contraseña, esto permite que para la creación de nuevas VLAN se deba conocer estos parámetros. A continuación en la Imagen 44 se indica un ejemplo del modo de configuración de VTP server.

```
Switch#
Switch#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

Switch(vlan)#vtp server
Setting device to VTP SERVER mode.
Switch(vlan)#vtp domain gpi_2016
Domain name already set to gpi_2016.
Switch(vlan)#vtp password vlans2016
Password already set to vlans2016
Switch(vlan)#exit
APPLY completed.
Exiting....
Switch#
Switch#
```

Imagen 44.-Ejemplo de configuración de VTP server
Referencia: Basado en investigación teórica y práctica

Todos los equipos que manejan la configuración de VTP deben estar en el mismo dominio, caso contrario no pueden recibir la información propagada por el VTP Server.

4.2.4.2.2. Asignación de puertos

En el switch de Core se configura los puertos modo troncal (trunk) para unir la capa núcleo con la capa acceso y de esta manera las VLANs creadas en el VTP server puedan ser propagadas a los switches de acceso que se encuentran configurados en modo VTP cliente, además se configura en modo trunk para que pueda existir convergencia entre las distintas VLANs, es decir, los enlaces en modo trunk llevan la información de distintas VLANs. El modo trunk se configura con la VLAN nativa VLAN 4 y no con la VLAN nativa por defecto que es la VLAN 1, además se configura en modo acceso aquellos

puertos hacia los servidores VLAN 6. En la Tabla 55 se indica la asignación de los puertos para modo acceso y modo troncal.

Tabla 55.-Asignación de puertos switch de Core

ASIGNACIÓN DE PUERTOS SWITCH DE CORE		
SWITCH	PUERTOS	MODO
CORE	3/1-3/26	acceso
	3/40-3/48	troncal

Referencia: Basado en investigación teórica y práctica.

4.2.4.2.3. Protocolo 802.1Q

Al ser el switch de core un equipo de capa 3, permite establecer la comunicación intervlans mediante el protocolo IEEE 802.1Q el cual realiza un etiquetado de tramas, introduciendo un encabezado de etiqueta de 12 bits dentro del encabezado Ethernet que especifica el ID de VLAN.

Para ello en la capa de núcleo contraído se configura los gateways de VLANs los cuales son el Gateway lógico para cada VLAN, en la Tabla 56 se indica la VLAN y su Gateway de VLAN.

Tabla 56.-Gateway de VLANs

NÚMERO DE VLAN	**NOMBRE DE VLAN**	**GATEWAY DE VLAN**
4	Equipos	170.20.4.1
6	Servidores	170.20.6.1
8	TICSs	170.20.8.1
10	Prefectura	170.20.10.1
12	Procuraduría	170.20.12.1
14	Planificación	170.20.14.1
16	Fiscalización	170.20.16.1
18	Relaciones publicas	170.20.18.1

20	Administración	170.20.20.1
22	Compras publicas	170.20.22.1
24	Financiero	170.20.24.1
26	Talento humano	170.20.26.1
28	Infraestructura física	170.20.28.1
30	Desarrollo económico	170.20.30.1
32	Turismo	170.20.32.1
34	Gestión ambiental	170.20.34.1
36	Recursos hídricos	170.20.36.1
38	PAS	170.20.38.1
40	Telefonía	170.20.40.1
44	Bodega	170.20.44.1
46	Biométricos	170.20.46.1
48	Cámaras	170.20.48.1
50	Mutualista	170.20.50.1
52	Red inalámbrica	170.20.52.1
100	Enlace equipos	170.20.100.1

Referencia: Basado en investigación teórica y práctica.

La configuración de Gateway de VLAN se lo realiza como se muestra en la Imagen 45 y para cada una de las VLANs.

```
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int vlan 9
Switch(config-if)#ip address 172.16.9.1 255.255.255.0
Switch(config-if)#description PREFECTURA
Switch(config-if)#no shutdown
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#END
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

Imagen 45.-Ejemplo de configuración de Gateway de vlan.
Referencia: Basado en investigación teórica y práctica

4.2.4.2.4. PVST+

Como se explicó en el diseño de PVST+ en la capa de acceso debido a que no existen enlaces redundantes el switch de Core será el designado como switch primario para cada una de las VLANs existentes.

La configuración del switch de core como el switch primario se realiza asignándole todas las VLANs existentes de la siguiente manera, ver Imagen 46.

```
Switch#
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#spanning-tree vlan
38,32,16,28,52,20,30,46,48,8,10,12,18,20,12,22,24,26,14,50,34,36,30,18 root
primary
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

Imagen 46.-Ejemplo de configuración del switch raíz primario
Referencia: Basado en investigación teórica y práctica

4.2.4.2.5. Access List

En el switch de Core se configurará una access-list para que solamente quienes pertenecen a la VLAN de tecnologías de información TICs 170.20.8.0/24 tengan acceso a la VLAN de administración de equipos 170.20.4.0/24, con la finalidad de limitar el tráfico de la red y brindar un nivel de seguridad básico.

Las demás configuraciones de access-list se encuentran realizadas mediante el equipo Asa 5520 que es el encargado de limitar y permitir el tráfico ya sea por VLANs, servicios o host. También se realiza limitación de tráfico mediante el servidor proxy de la institución.

CAPITULO V

5. IMPLEMENTACIÓN DE LOS NUEVOS DISEÑOS FÍSICO Y LÓGICO DE LA RED DE COMUNICACIONES PARA EL GAD PROVINCIAL DE IMBABURA

En este capítulo se detalla la instalación de los nuevos puntos de red y sus cambios en las diferentes partes que comprende el cableado estructurado, así como el proceso de configuración en los equipos de las diferentes capas que comprenden la red, es decir, configuraciones en el área de networking.

5.1. CABLEADO ESTRUCTURADO

Las área de cableado estructurado que tienen reestructuración son las siguientes.

5.1.1. INSTALACIÓN DE ENTRADA

Se debe añadir la conexión del edificio principal con el edificio del PAS, la norma recomienda que este elemento este en un cuarto aparte por razones de seguridad, pero puede estar dentro del Data Center, en este caso se mantiene la misma ubicación dentro del Data Center como se muestar en la Imagen 47.

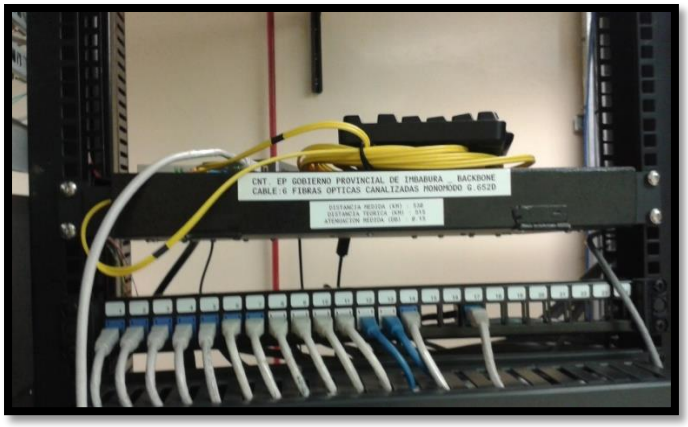


Imagen 47.- Conexión hacia el nuevo edificio PAS.
Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura, 2015.

5.1.2. REPARTIDORES HORIZONTALES

Los repartidores horizontales se mantienen en el mismo sitio físico actual pues cumplen con las especificaciones que la norma que indica entre ellas: que sea dedicado exclusivamente a la infraestructura de telecomunicaciones, mínimo un armario por piso, la reestructuración se realiza en la distribución y organización de los puertos de los equipos activos de acuerdo a las nuevas VLANs planteadas y a las nuevos puntos de red en la planta baja.

5.1.3. DISTRIBUCIÓN HORIZONTAL

La distribución horizontal interconecta el distribuidor secundario y el área de trabajo, en esta distribución no deben existir puntos de interconexión y la distancia máxima es de 90 metros independientemente de si es cobre o fibra óptica, se realiza mediante el techo falso y en las partes que no existe este mediante canaletas.

En la Imagen 48 se indica el techo falso de la planta baja de la institución por donde se pasó el cable de la distribución horizontal.

Imagen 48.-Distribución horizontal en techo falso
Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura, 2015.

En las áreas que no era posible el paso del cable por el techo falso se lo realizo mediante la utilización de canaletas como se muestra en la Imagen 49.

Imagen 49.- Distribución horizontal en techo falso
Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura, 2015.

5.1.3.1. Etiquetado

El etiquetado de la distribución horizontal será de la misma nomenclatura actual, colocando etiquetas en ambos extremos de los enlaces. Las etiquetas serán auto laminables.

Las etiquetadas de la distribución horizontal es la misma de las estaciones de trabajo y corresponden desde PB-D65 hasta PB-D74.

5.1.4. AREA DE TRABAJO

Es el punto de conexión entre la distribución horizontal y los dispositivos de conexión del cable en el área de trabajo, dichos puntos son la toma de Telecomunicaciones.

Es necesario una toma por estación de trabajo como mínimo o dos por área de trabajo. La destinación de espacio de trabajo es una por cada 10 m2.

Por lo menos se debe instalar una toma de energía cerca de cada toma de telecomunicaciones. La instalación se lo realizó como se indica en la Imagen 50.

Imagen 50.-Instalación puntos de red
Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura, 2015.

5.1.4.1. Etiquetado

El sistema de etiquetado en los nuevos punto de red se realizará con etiquetas auto laminable colocados dentro de los faceplate de tal forma que no puedan ser manipuladas fácilmente, conservando el modelo de etiquetado actual: PA1-D1, en donde la primera parte representa la planta del distribuidor horizontal del cableado y la segunda parte el puerto del switch. En la Tabla 57 se indica la estructura del etiquetado de los nuevos puntos de red, de acuerdo a la planta que se encuentren.

Tabla 57.- Etiquetas nuevos puntos de red

ETIQUETAD	VLAN	PUERTO	DESCRIPCION
PB-D65	20	PUERTO 17	ADMIN GENERAL
PB-D66	20	PUERTO 18	ADMIN GENERAL
PB-D67	20	PUERTO 19	ADMIN GENERAL
PB-D68	20	PUERTO 20	ADMIN GENERAL
PB-D69	20	PUERTO 21	ADMIN GENERAL
PB-D70	20	PUERTO 22	ADMIN GENERAL
PB-D71	20	PUERTO 23	ADMIN GENERAL
PB-D72	20	PUERTO 24	ADMIN GENERAL
PB-D73	20	PUERTO 25	ADMIN GENERAL
PB-D74	20	PUERTO 26	ADMIN GENERAL

Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura, 2015.

5.2.CONFIGURACIÓN DE LOS EQUIPOS ACTIVOS DE RED

Para la implementación de la reestructuración de red se debe seguir un procedimiento que garantice un cambio sistemático y no altere la funcionalidad de la red. Primero se debe garantizar un respaldo de la información sacando las configuraciones de los equipos activos de red, seguido se debe respaldar la configuración de las interfaces, esto permitirá

que en el caso de presentar algún problema en la implementación se pueda restaurar las configuraciones anteriores sin ningún inconveniente.

Debido a que con esta reestructuración se presenta un nuevo direccionamiento de red, se debe cambiar el direccionamiento IP a los servidores, es decir, Chasis Blade, Firewall y cada uno de los switches: Core y acceso. Los cambios de direcciones en los switches se deben realizar primero en los switches de acceso y luego en el switch de Core, pues si se realiza primero en el switch de Core se perderá la conectividad con los switches de acceso y ya no se puede realizar las configuraciones de forma remota, lo que obliga a trasladarse al lugar y configurar mediante consola.

En la Tabla 58 se indican los equipos con las respectivas configuraciones a implementar:

Tabla 58.-Equipos y configuraciones a implementar.

CAPA	EQUIPO	CONFIGURACIONES
NÚCLEO CONTRAIDO	SWITCH CORE	-VLAN Trunking Protocol, VTP SERVER -Asignación de puertos -PVST+ -Etherchannel -Access List
ACCESO	SWITCHES ACCESO	-VLAN Trunking Protocol ,VTP CLIENT -Asignación de puertos -PVST+ -Etherchannel -Port Security.

Referencia: Basado en investigación teórica y práctica.

5.2.1. ASIGNACIÓN DE PUERTOS EN MODO TRONCAL

Se realiza la conexión entre todos los equipos activos de la red mediante los enlaces en modo troncal, en el diseño se indicó los puertos designados para modo troncal y se configura de la siguiente manera.

- **Puertos en modo trunk switches de acceso**

Los puertos en modo trunk son dos por cada switch de acceso, para unir cada uno de ellos hacia la capa superior de núcleo contraido, se ocupa un solo puerto porque es un solo enlace, pero se configura dos por si en el puerto principal ocurra un error, así solamente se cambia el enlace al siguiente puerto. En la Imagen 51 se indica la configuración de un puerto en modo troncal.

```
SW_DOS#
SW_DOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_DOS(config)#interface fastethernet 0/1
SW_DOS(config-if)#switchport mode trunk
SW_DOS(config-if)#switchport trunk native vlan 4
SW_DOS(config-if)#no shutdown
SW_DOS(config-if)#
```

Imagen 51.- Configuración de puertos en modo trunk en switch acceso
Referencia: Basado en investigación teórica y práctica.

Para verificar la configuración del puerto lo realizamos con el comando **show running-config** como se indica en la Imagen 52 o con el comando **show interface trunk** como se indica en la Imagen 53.

```
!
interface FastEthernet0/1
 switchport trunk native vlan 4
 switchport mode trunk
!
```

Imagen 52.- Verificación de puerto en modo trunk en running-config
Referencia: Basado en investigación teórica y práctica.

```
SW_DOS#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      4
Fa0/2       on           802.1q         trunking      4
Fa0/3       on           802.1q         trunking      4
```

Imagen 53.- Verificación de puerto en modo trunk en interfaces trunk
Referencia: Basado en investigación teórica y práctica.

- **Puertos en modo trunk switch de Core**

Los puertos en modo trunk son 9, uno para cada switch de acceso y su configuración se la realiza como se indica en la Imagen 54.

```
CORE#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CORE(config)#interface range fastethernet 0/1-8
CORE(config-if-range)#switchport mode trunk
CORE(config-if-range)#switchport trunk native vlan 4
CORE(config-if-range)#no shutdown
CORE(config-if-range)#
```

Imagen 54.-Asignación de puertos en modo trunk switch de Core
Referencia: Basado en investigación teórica y práctica.

5.2.2. VLAN TRUNKING PROTOCOL

El protocolo VTP es configurado tanto la capa de nucleo contraído como en la capa de acceso.

5.2.2.1. Capa núcleo contraído

El VTP server será el switch de core y debe tener el mismo dominio que los VTP client para que las VLANs puedan ser propagadas.

- **VTP Server**

VTP server solamente se configura en el switch de core, como se indica en la Imagen 55.

```
CORE#enable
CORE#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CORE(config)#ip routing
CORE(config)#vtp mode server
Device mode already VTP SERVER.
CORE(config)#vtp domain gpi_2016
Changing VTP domain name from NULL to gpi_2016
CORE(config)#vtp password vlans2016
Password already set to vlans2016
CORE(config)#
```

Imagen 55.- Configuración de VTP Server en switch core
Referencia: Basado en investigación teórica y práctica.

- **Creación de VLANs.**

En el switch de core se configura la creación de las VLANs que manejará la red, en la Imagen 56 se indica la configuración para la VLAN de administración de equipos.

```
CORE#
CORE#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

CORE(vlan)#vlan 4 name EQUIPOS
VLAN 4 modified:
    Name: EQUIPOS
CORE(vlan)#
```

Imagen 56.- Creación de VLANs switch de core.
Referencia: Basado en investigación teórica y práctica.

- **Gateways de VLANs**

Al manejar una red con diferentes VLANs se realiza la configuración de gateway de VLAN el cual permite la comunicación entre VLANs. Para cada VLAN se debe configurar su Gateway, como se indica en la Imagen 57. Para su verificación lo realizamos mediante el comando **show running-config.**

```
CORE#
CORE#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CORE(config)#int vlan 10
CORE(config-if)#ip address 170.20.10.1 255.255.255.0
CORE(config-if)#description PREFECTURA
CORE(config-if)#no shutdown
CORE(config-if)#end
```

Imagen 57.-Configuración de Gateway de VLAN para la VLAN PREFECTURA.
Referencia: Basado en investigación teórica y práctica.

5.2.2.2. Capa acceso

En los switches de acceso la configuración es en modo cliente dentro del dominio de VTP, hay que tener muy en cuenta que se debe manejar el mismo dominio para que las VLANs puedan ser propagadas. Esta configuración es válida para todos los switches de la capa acceso.

- **VTP Cliente**

Todos los switches de la capa acceso deben ser configurados como clientes como se indica en la Imagen 58.

```
SW_DOS#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

SW_DOS(vlan)#vtp client
Device mode already VTP CLIENT.
SW_DOS(vlan)#vtp domain gpi_2016
Domain name already set to gpi_2016.
SW_DOS(vlan)#vtp password vlans2016
Password already set to vlans2016
SW_DOS(vlan)#
```

Imagen 58.- Configuración de VTP Client en switch acceso
Referencia: Basado en investigación teórica y práctica.

Para verificar la configuración de VTP lo realizamos mediante el comando **show vtp status,** en donde comprobamos el modo cliente, el dominio de VTP y el número de configuración de revisión que debe ser igual al número de revisión del Core al igual que el dominio VTP, en la Imagen 59 podemos visualizar dicha verificación.

```
SW_DOS#
SW_DOS#show vtp status
VTP Version                     : 2
Configuration Revision          : 75
Maximum VLANs supported locally : 255
Number of existing VLANs        : 30
VTP Operating Mode              : Client
VTP Domain Name                 : gpi_2016
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x62 0xED 0xEB 0x30 0x42 0x3A 0xE7 0x0B
Configuration last modified by 0.0.0.0 at 3-1-93 00:13:11
SW_DOS#
```

Imagen 59.- Verificación de VTP Client en switch acceso
Referencia: Basado en investigación teórica y práctica.

Una vez que se haya realizado la configuración de todas las interfaces en modo trunk y la creación de las VLANs en el VTP server, se puede ya verificar la propagación de las VLANs en el switch de acceso con el comando **show vlan,** ver Imagen 60.

```
SW_DOS#
SW_DOS#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
4    EQUIPOS                          active
6    SERVIDORES                       active
8    TICS                             active
10   PREFECTURA                       active
12   PROCURADURIA                     active
14   PLANIFICACION                    active
16   FISCALIZACION                    active    Fa0/4
18   RELACIONES_PUBLICAS              active
20   ADMINISTRACIN                    active
22   COMPRAS_PUBLICAS                 active
24   FINANCIERO                       active
26   TALENTO_HUMANO                   active
28   INFRAESTRUCTURA_FISICA           active
30   DESARROLLO_ECONOMICO             active
32   TURISMO                          active
34   GESTION_AMBIENTAL                active
36   RECURSOS_HIDRICOS                active
38   PAS                              active
40   TELEFONIA                        active
44   BODEGA                           active
46   BIOMETRICOS                      active
48   CAMARAS                          active
50   MUTUALISTA                       active
52   WIFI                             active
100  ENLACES_EQUIPOS                  active
```

Imagen 60.-Verificación de VLANs propagadas en switch de acceso.
Referencia: Basado en investigación teórica y práctica.

5.2.3. EQUIPOS CAPA ACCESO

En esta capa tenemos los switches de acceso en donde las configuraciones principales son: configuraciones básicas, configuración de switches cliente de VLANs o VTP Client, configuración de las interfaces o asignación de puertos en modo trunk y en modo acceso, PVST+, Port Security, todas ellas se detallan a continuación:

5.2.3.1. Configuración básica

La configuración básica es válida para todos los switches de acceso, donde configuramos:

- Nombre
- Banner
- Contraseñas
    - Consola
    - Enable
    - Enable secret
    - Habilitación telnet
    - Ssh
    - Contraseña encriptada
- Copiar configuración a NVRAM
- Desactivar la búsqueda DNS

Las configuraciones básicas se encuentran en el ANEXO 04.

5.2.3.2. Interfaz de administración

Las interfaces de administración de los equipos se encuentran dentro de la VLAN EQUIPOS que es la VLAN 4 de administración, las direcciones para cada equipo se detallan a continuación en la Tabla 59 en concordancia a los nombres asignados en el diseño de PVST+ y las direcciones IP señaladas en la topología lógica de la red.

Tabla 59.-Interfaces de administración switches de acceso.

INTERFACES DE ADMINISTRACIÓN	
SWITCH DOS	170.20.4.2
SWITCH TRES	170.20.4.3
SWITCH CUATRO	170.20.4.4
SWITCH CINCO	170.20.4.5
SWITCH SEIS	170.20.4.6
SWITCH SIETE	170.20.4.7
SWITCH OCHO	170.20.4.8
SWITCH NUEVE	170.20.4.9
SWITCH DIEZ	170.20.4.10
SWITCH ONCE	170.20.4.11
SWITCH DOCE	170.20.4.12
SWITCH TRECE	170.20.4.13
SWITCH CATORCE	170.20.4.14

Referencia: Basado en investigación teórica y práctica.

La configuración de la interfaz de administración se indica en la Imagen 61 y es válida para todo los switches de acceso:

```
SW_DOS#
SW_DOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_DOS(config)#int vlan 4
SW_DOS(config-if)#ip address 170.20.4.2 255.255.255.0
SW_DOS(config-if)#no shutdown
SW_DOS(config-if)#
```

Imagen 61.- Configuración de interfaz de administración en switch acceso
Referencia: Basado en investigación teórica y práctica.

Para verificar la configuración de la interfaz de administración se lo realiza con el comando show **running-config** como se indica en la Imagen 62.

```
!
interface Vlan4
 ip address 170.20.4.2 255.255.255.0
!
!
!
!
```

Imagen 62.- Verificación de configuración de interfaz de administración.
Referencia: Basado en investigación teórica y práctica.

5.2.3.3. Asignación de puertos

En esta capa se configuran puertos tanto en modo trunk como en modo acceso, en modo trunk de switch a switch como se indicó en la asignación de puertos en modo troncal y en modo access de switch a PC, estas configuraciones son validas para todos los switches de acceso.

- **Puertos en modo acceso.**

Los puertos en modo acceso se configuran para cada una de las VLANs que maneje el switch, en la Imagen 63 se muestra la configuración de un puerto en modo acceso a la VLAN 16.

```
SW_DOS#
SW_DOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_DOS(config)#interface fastethernet 0/4
SW_DOS(config-if)#switchport mode access
SW_DOS(config-if)#switchport access vlan 16
SW_DOS(config-if)#no shutdown
SW_DOS(config-if)#
```

Imagen 63.- Configuración de puertos en modo access en switch acceso
Referencia: Basado en investigación teórica y práctica.

Para la verificar la configuración de los puertos en modo acceso se realiza mediante el comando **show ruuning-config** como se muestra en la Imagen 64.

```
!
interface FastEthernet0/4
 switchport access vlan 16
 switchport mode access
 switchport voice vlan 40
 mls qos trust cos
!
```

Imagen 64.- Verificación de puerto en modo access.
Referencia: Basado en investigación teórica y práctica.

- **Configuración rango de puertos**

Para configurar varios puertos a la vez ya sea en modo trunk o en modo acceso se lo realiza utilizando el comando **interface range**, de la siguiente manera, ver Imagen 65.

```
SW_DOS#
SW_DOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_DOS(config)#interface range fastethernet 0/1-3
SW_DOS(config-if-range)#switchport mode trunk
SW_DOS(config-if-range)#switchport trunk native vlan 4
SW_DOS(config-if-range)#no shutdown
SW_DOS(config-if-range)#
```

Imagen 65.-Configuración de un rango de puertos
Referencia: Basado en investigación teórica y práctica.

- **Configuración de puertos para la VLAN de voz**

La configuración en el puerto del switch para que soporte VLAN de datos y al mismo tiempo la VLAN de voz se realiza utilizando la voice VLAN de Cisco que se indica en la Imagen 66.

```
SW_DOS#
SW_DOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_DOS(config)#interface fastethernet 0/4
SW_DOS(config-if)#switchport voice vlan 40
SW_DOS(config-if)#mls qos trust cos
SW_DOS(config-if)#no shutdown
SW_DOS(config-if)#
```

Imagen 66.- Configuración de puertos para la VLAN de voz en switch acceso
Referencia: Basado en investigación teórica y práctica.

5.2.3.4. Default Gateway

El default Gateway para los switches de acceso es el switch de Core, por ello configuramos su dirección IP como como el default Gateway, es decir, la dirección 170.20.4.1 como se muestra en la Imagen 67.

```
SW_DOS#
SW_DOS#
SW_DOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_DOS(config)#ip default-gateway 170.20.4.1
SW_DOS(config)#do write
Building configuration...
[OK]
SW_DOS(config)#
```

Imagen 67.- Configuración de default Gateway en switch acceso
Referencia: Basado en investigación teórica y práctica.

5.2.3.5. PVST+

Como se indicó en el capítulo de diseño para la configuración de PVST+ el switch principal será el de Core para cada una de las VLANs. En los switches de acceso se configura el modo pvst para que la red funcione con ese protocolo, la configuración se indica en la Imagen 68.

```
SW_CUATRO#
SW_CUATRO#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_CUATRO(config)#spanning-tree mode pvst
SW_CUATRO(config)#
SW_CUATRO(config)#
```

Imagen 68.-Configuración para establecer PVST+ rápido como el modo STP – switch CUATRO
Referencia: Basado en investigación teórica y práctica.

Para verificar la configuración lo realizamos mediante el comando **show running-config** donde se obtiene la siguiente información, ver Imagen 69.

```
!
!
spanning-tree mode pvst
!
```

Imagen 69.-Verificación del PVST+
Referencia: Basado en investigación teórica y práctica.

5.2.3.6. Port Security

El número de direcciones MAC por puerto será limitado a 1, es decir, la primera dirección dinámicamente aprendida por el switch llega a ser la dirección segura para ellos se utiliza mediante Sticky secure MAC addresses, la configuración se la realiza como se indica en la Imagen 70

```
SW_DOS#
SW_DOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_DOS(config)#interface range fastethernet 0/4-6
SW_DOS(config-if-range)#switchport port-security
SW_DOS(config-if-range)#switchport port-security maximum 1
SW_DOS(config-if-range)#switchport port-security violation shutdown
SW_DOS(config-if-range)#switchport port-security mac-address sticky
SW_DOS(config-if-range)#end
SW_DOS#
```

Imagen 70.-Configuración de port-security mediante sticky secure
Referencia: Basado en investigación teórica y práctica.

Para verificar su configuración se realiza mediante el comando **show running-config** como se indica en la Imagen 71 o con el comando **show port-security**

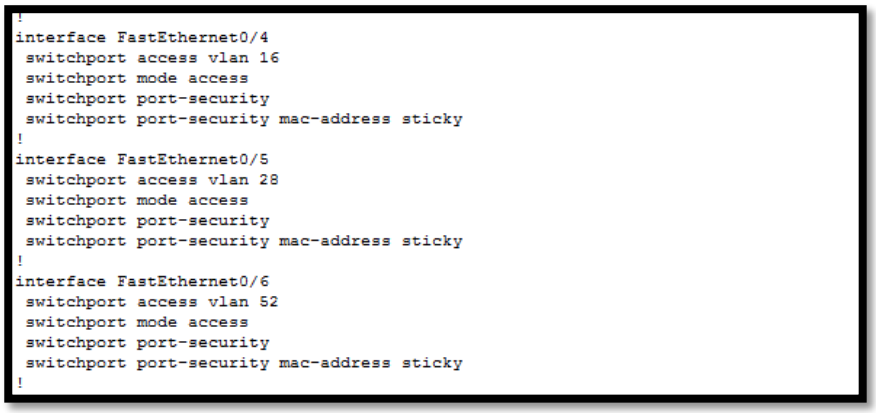


Imagen 71.-Verificación de sticky secure antes de reconocer las MAC
Referencia: Basado en investigación teórica y práctica.

En la Imagen 72 se muestra la verificación mediante el comando show running-config luego de que la interfaz haya aprendido la dirección MAC segura.

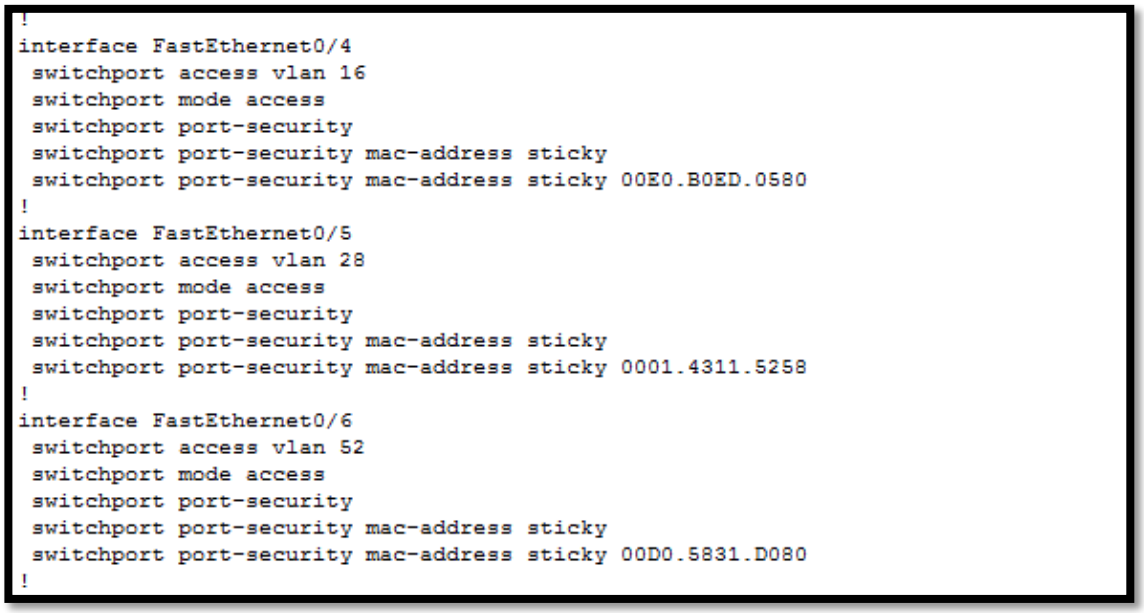


Imagen 72.- Verificación de sticky secure después de reconocer las MAC
Referencia: Basado en investigación teórica y práctica.

También podemos verificar mirando la configuración por cada interfaz como se indica en la Imagen 73.

```
SW_DOS#show port-security interface fastEthernet 0/4
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

SW_DOS#
```

Imagen 73.- Verificación de sticky secure mediante la interfaz
Referencia: Basado en investigación teórica y práctica.

También podemos verificar las direcciones MAC aprendidas mediante el comando show mac-address-table, ver Imagen 74.

```
SW_DOS#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0007.ec24.cc01    DYNAMIC     Fa0/1
   1    0090.0c78.0e01    DYNAMIC     Fa0/2
   4    0007.ec24.cc01    DYNAMIC     Fa0/1
   6    0007.ec24.cc01    DYNAMIC     Fa0/1
   8    0007.ec24.cc01    DYNAMIC     Fa0/1
  10    0007.ec24.cc01    DYNAMIC     Fa0/1
  12    0007.ec24.cc01    DYNAMIC     Fa0/1
  14    0007.ec24.cc01    DYNAMIC     Fa0/1
  16    0001.9713.d301    DYNAMIC     Fa0/1
  16    0007.ec24.cc01    DYNAMIC     Fa0/1
  16    00e0.b0ed.0580    STATIC      Fa0/4
  18    0007.ec24.cc01    DYNAMIC     Fa0/1
  20    0007.ec24.cc01    DYNAMIC     Fa0/1
  22    0007.ec24.cc01    DYNAMIC     Fa0/1
  24    0007.ec24.cc01    DYNAMIC     Fa0/1
  26    0007.ec24.cc01    DYNAMIC     Fa0/1
  28    0001.4311.5258    STATIC      Fa0/5
  28    0001.9713.d301    DYNAMIC     Fa0/1
  28    0007.ec24.cc01    DYNAMIC     Fa0/1
  30    0007.ec24.cc01    DYNAMIC     Fa0/1
  32    0007.ec24.cc01    DYNAMIC     Fa0/1
  34    0007.ec24.cc01    DYNAMIC     Fa0/1
```

Imagen 74.- Verificación de direcciones MAC aprendidas.
Referencia: Basado en investigación teórica y práctica.

En el caso de existir un tipo de violación a esta restricción, es decir, se intente agregar otro dispositivo a una interfaz, la acción a ser tomada es shutdown, la cual coloca a la interface en error-disabled y el puerto es apagado. Cuando un puerto seguro están en el estado de error-disabled, se puede sacarlo de este estado con el comando de configuración global errdisable recovery cause psecureviolation o manualmente re-habilitarlo ingresando los comandos shutdown y no shutdown en configuración de interface.

En la Imagen 75 se encuentra la verificación de port-security en un puerto, en donde comprobamos la violación que ha surgido en un puerto en la última línea Security Violation Count.

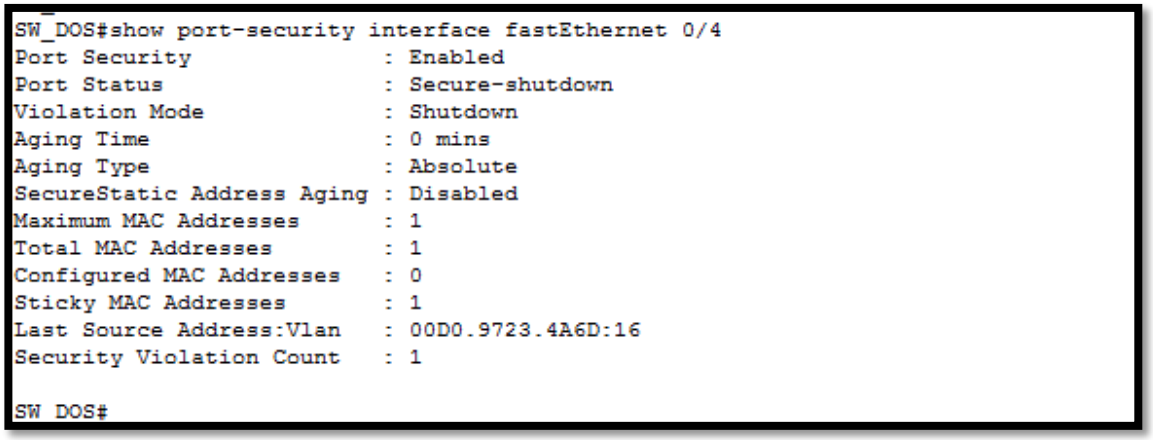


Imagen 75.- Violación de puerto
Referencia: Basado en investigación teórica y práctica.

En la Imagen 76 se indica la forma de rehabiliatr un puerto que ha surgido una violacion y ha sido bloqueado.

```
SW_DOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_DOS(config)#interface fastethernet 0/4
SW_DOS(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
SW_DOS(config-if)#no shutdown

SW_DOS(config-if)#end
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to
up

SW_DOS#
```

Imagen 76.-Rehabilitación de interfaz
Referencia: Basado en investigación teórica y práctica.

5.2.4. EQUIPO CAPA NÚCLEO CONTRAIDO

En esta capa tenemos el switch de Core en donde la configuración principal es la creación de VLANs mediante VTP, configurando este equipo como el switch servidor de VLANs o VTP Server como se indicó en la configuración VTP , configuración de las interfaces o asignación de puertos en modo trunk y acceso, configuraciones básicas, todas ellas se detallan a continuación:

5.2.4.1. Configuración básica

La configuración básica es válida para todos los switches de acceso, donde configuramos:

- Nombre
- Banner
- Contraseñas

- Consola
- Enable
- Enable secret
- Habilitación telnet
- Ssh
- Contraseña encriptada

- Copiar configuración a NVRAM
- Desactivar la búsqueda DNS

Las configuraciones básicas se encuentran en el ANEXO 04.

5.2.4.2. Configuración de DHCP[50] para la VLAN inalámbrica

Dentro de las VLANs creadas existe una VLAN para la red inalámbrica en la cual la asignación de direcciones IP se las realiza mediante DHCP como se indica en la Imagen 77.

```
CORE#
CORE#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CORE(config)#ip dhcp pool wifi
CORE(dhcp-config)#network 170.20.52.0 255.255.252.0
CORE(dhcp-config)#default-router 170.20.52.1
CORE(dhcp-config)#dns-server 200.107.10.52
CORE(dhcp-config)#exit
CORE(config)#ip dhcp excluded-address 170.20.52.1 170.20.52.20
CORE(config)#end
CORE#
```

Imagen 77.- Configuración de DHCP para la VLAN inalámbrica
Referencia: Basado en investigación teórica y práctica.

[50] DHCP= Dynamic Host Configuration Protocol, Protocolo de configuración dinámica de Host

5.2.4.3. Interfaz de administración

La interfaz de administración se encuentra dentro de la VLAN de equipos que es la VLAN 4, la dirección asignada para este equipo es la 170.20.4.1, la configuración se indica en la Imagen 78.

```
CORE#
CORE#
CORE#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CORE(config)#int vlan 4
CORE(config-if)#ip address 170.20.4.1 255.255.255.0
CORE(config-if)#no shutdown
CORE(config-if)#exit
CORE(config)#
```

Imagen 78.- Configuración interfaz de administración switch de core
Referencia: Basado en investigación teórica y práctica.

5.2.4.4. Asignación de puertos

En esta capa se configura puertos en modo trunk para unir el switch de Core con los switches de acceso como se realizó en la configuración de asignación de puertos en modo troncal y además se configura los puertos en modo acceso para la VLAN de servidores.

5.2.4.5. PVST+

En el diseño de la capa acceso se indicó detalladamente cual es el esquema para PVST+ tanto para la capa acceso como núcleo, señalando cuales serían los switches primarios y secundarios para las VLANs de cada uno de los pisos.

El switch de Core será el designado como switch primario para cada una de las VLANs creadas.

Primero utilizamos el comando **spanning-tree mode** para establecer que los switches utilicen PVST+ rápido como el modo STP, ver Imagen 79.

```
CORE#
CORE#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CORE(config)#spanning-tree mode pvst
CORE(config)#exit
CORE#
%SYS-5-CONFIG_I: Configured from console by console

CORE#
```

Imagen 79.- Configuración para establecer PVST+ rápido como el modo STP – switch de Core
Referencia: Basado en investigación teórica y práctica.

Luego configuramos al switch de Core como primario para las VLANs establecidas como se indica en la Imagen 80.

```
CORE#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CORE(config)#spanning-tree vlan
4,6,8,10,12,14,16,18,20,22,24,26,28,30,32,34,36,38,40,44,46,48,50,52,100 root
primary
CORE(config)#exit
CORE#
%SYS-5-CONFIG_I: Configured from console by console
```

Imagen 80.- Configuración de switch de Core como primario para las VLANs establecidas.
Referencia: Basado en investigación teórica y práctica.

Para verificar la configuración lo realizamos mediante el comando **show running-config** o mediante **show spanning-tree**.

5.2.4.6. Access List

En el switch de Core se configurará una access-list para que solamente quienes pertenecen a la VLAN de TICs VLAN 8 tengan acceso a la VLAN 4 de administración

de equipos, con la finalidad de limitar el tráfico de la red y brindar un nivel de seguridad básico, ver Imagen 81.

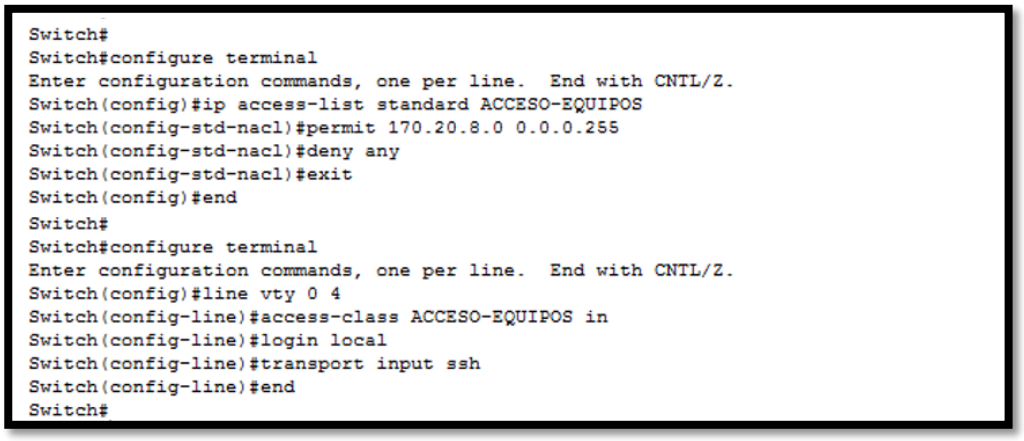


Imagen 81.-Configuración de lista de acceso
Referencia: Basado en investigación teórica y práctica.

CAPITULO VI

6. CONCLUSIONES Y RECOMENDACIONES

En este capítulo se expone las principales conclusiones y recomendaciones obtenidas en base al desarrollo de este proyecto.

6.1.CONCLUSIONES

- Mediante el presente proyecto se potencializó el funcionamiento de la red de comunicaciones del GAD provincial de Imbabura debido al manejo de un modelo con estructura jerárquica que brinda beneficios entre ellos: escalabilidad que permite una fácil expansión de la red en cada una de sus capas, seguridad en la capa acceso y fácil administración al separar la red por capas, evitando transmitir datos a través de switches intermedios de bajo rendimiento.
- De acuerdo a la evaluación de la situación actual de la red de comunicaciones del GAD provincial de Imbabura a nivel físico se definió que cumple con las normas de cableado estructurado especificadas en el estándar ANSI/TIA/EIA-568-C, sin embargo se determinó la necesidad de instalación de nuevos puntos de red. La restructuración en la topología física de red se desarrolló contemplando el modelo de red jerárquico en base a capas, de esta manera se realizó la conexión de cada uno de los equipos de la capa acceso hacia la capa de núcleo contraído.
- De acuerdo a la evaluación de la situación actual de la red de comunicaciones del GAD provincial de Imbabura a nivel lógico, se establecieron los puntos críticos que requerían una reestructuración dentro de la red de comunicaciones, por

ejemplo: a nivel lógico la red actual no contaba con enlaces redundantes, manejo de spanning-tree, agregación de enlaces, seguridad a nivel de acceso y las VLANS actuales no estaban de acuerdo a las necesidades de la red.

- Debido al tamaño de la red del GAD Provincial de Imbabura nos permite elegir una reestructuración jerárquica que consta de 2 capas: núcleo contraído y acceso, que no disminuye los principios de diseño de red jerárquica y ahorra recursos económicos con los que la institución no cuenta actualmente.
- El diseño en la topología lógica de la red se basa en la segmentación del tráfico, realizando una nueva distribución de VLANs de acuerdo a las diferentes direcciones y subdirecciones de la institución, así como el tipo de información que se maneje, reduciendo así los dominios de colisión existentes en la red.
- No existe enlaces redundantes planteados en el diseño de red sin embargo se estableció la implementación del protocolo spanning-tree para mejorar la escalabilidad de la red para enlaces futuros y evitar los inconvenientes que implica poseer enlaces redundantes. Se desarrolló mediante su versión PVST+ el cual mantiene una instancia de spanning-tree por cada VLAN, estableciendo al switch de core como el switch raíz de todas las VLANs existentes.
- Con la aplicación de la access-list para permitir acceso a la VLAN de administración solo a aquellos equipos que se encuentren en la VLAN de tecnologías de información, se logró la restricción del tráfico cursado entre VLANs y brindar seguridad al momento de acceder a la administración de los equipos activos.

- Para mejorar el acceso a la red de comunicaciones y de acuerdo al levantamiento de información se cambió aquellos equipos finales (computadoras) que poseían características de baja gama y no permitan un acceso oportuno a la red.

- La seguridad a nivel de puertos de switches se configuró mediante sticky secure MAC addresses limitando el número de direcciones MAC que pueden ser aprendidas en una interfaz, lo cual permite mejorar la seguridad en la capa de acceso evitando la conexión de máquinas no autorizadas.
- La reestructuración de la red se realizó tanto a nivel físico como lógico basada en los diseños planteados, realizando las nuevas configuraciones en cada uno de los equipos así como instalación de los nuevos puntos de red requeridos.

6.2.RECOMENDACIONES

- Para mejorar la estructura física y lógica de la red de comunicaciones, posteriormente se puede implementar el modelo de red jerárquico contemplando el manejo de sus 3 capas: núcleo, distribución y acceso.

- Una red redundante se aplica no solo a los enlaces sino también a equipos, por ello a futuro y de acuerdo al presupuesto anual de la institución se puede implementar redundancia en equipos, añadiendo un nuevo equipo en la capa de núcleo contraído el cual sirva como backup para cada uno de los switches de la capa acceso.

- Con la finalidad de realizar una mejor gestión y administración de la red es necesario el uso de un software para monitoreo de la red que permita al

administrador reaccionar de manera más eficiente ante fallos y le permita analizar el estado de la red y la toma de decisiones.

- La seguridad a nivel del perímetro de una red ayuda al administrador a proteger la información que circula por su red, sin embargo existen muchas formas en las cuales se puede aplicar como es a través de firewall, pero se puede realizar mejoras mediante la implementación de diferentes funcionalidades como IDS e IPS.
- La aplicación de seguridad a nivel de puertos de switches de acceso se configuró para limitar el número de direcciones MAC aprendidas a uno, pero para mejorar la seguridad se puede realizar una configuración estática mediante static secure MAC address que aunque es más compleja asegura que solo las máquinas autorizadas e inventariadas dentro de la red de la institución tengan acceso hacia la red.
- Se recomienda realizar una documentación oportuna todos los cambios que se realicen en la red, ya sea a nivel de usuarios, enlaces, direccionamiento, VLANs, de tal manera que se pueda mantener la información actualizada y se pueda bazar en ella para la toma de decisiones.

- Respecto a los incidentes producidos en la red, se debe realizar un informe de dichos inconvenientes y de sus soluciones, de esta manera se podrá tener en forma documentada cuales son los problemas más recurrentes en los que se deberá poner mayor atención.

- Para mejorar la disponibilidad a la red, se debe instalar rutas diferentes en los enlaces de conexión, ya que si llega a producirse una falla en el enlace, el canal alterno no sufra daño alguno y se asegure la continuidad del servicio.

- Como ayuda en la administración y gestión de la red, se recomienda realizar backup periódicos de las configuraciones de los quipos activos para que en caso de surgir algún daño en las configuraciones estas pueda establecer el servicio mediante las configuraciones de backup. Los backups de configuraciones se deben guardar no solamente de la última versión, sino se debe poseer de versiones anteriores para que en el caso de daños se pueda recuperar información mucho más antigua si es necesario.

- Los puertos de los equipos activos que no sean utilizados deben ser deshabilitados para controlar la seguridad de la red a nivel de acceso y evitar el tráfico se propague por dichos puertos.

- Es necesario que la institución, en decir, el área de redes y comunicaciones cuente con un equipo testeador de cableado de tal manera que cuando existan problemas frecuentes en ciertas área, se pueda realizar una verificación del estado del enlace en ese punto y realizar cambios del mismo de ser necesario.

- La institución cuenta actualmente con un manual de uso de la red de comunicaciones, es importante que este manual sea socializado con los empleados para que conozcan y se pueda aplicar las recomendaciones que en dicho manual se indica y de esta manera la red sea utilizada solamente para las labores de la institución.

- Para el equipo packetshaper con el que cuenta la institución y que en la actualidad no se encuentra funcional, se debe adquirir la actualización o mejora del software de administración de tal forma que pueda funcionar de acuerdo al ancho de banda que maneja la red.

- Con el nuevo direccionamiento y la nueva segmentación de la red, se puede plantear proyectos de calidad de servicio, de acuerdo a los requerimientos que la red tenga y de esta manera controlar el flujo de tráfico que cursa por la red.

- El IOS manejado por el Asa de la institución funciona correctamente en la actualidad, sin embargo existen versiones más actualizadas y para seguir a la vanguardia de los avances de la tecnología y de acuerdo a las necesidades, sería conveniente que en un futuro dicho IOS sea actualizado.

- A pesar de que algunos equipos de trabajo ya han sido cambiadas debido a que poseen muchos años de vida, existe equipos de trabajo que aún deben ser cambiados y deben ser tomados en cuanta dentro de los siguientes presupuestos.

- Para mejorar configuración de Port Security en la acción a tomar cuando surja una violación, se puede configurar en vez de shutdown la opción trap que como dice su nombre genera un trap de Simple Network Management Protocol.

GLOSARIO DE ABREVIATURAS Y TÉRMINOS

ACL: Access Control List, listas de control de acceso

ACR: Attenuation/Crosstalk Ratio, Relación atenuación – diafonía

ANSI: American National Standards Institute, Instituto Americano de Estándares Nacionales

ARPA: Advanced Research Projects Agency, es una agencia de Estados Unidos responsable del desarrollo de nuevas tecnologías para uso militar

ASDM: Adaptive Security Device Manager, dispositivo de manejo de seguridad

CCK: Complementary Code Keying, esquema de modulación utilizado con redes inalámbricas

BCT: Bonding conductor for telecommunications, conductor de unión para telecomunicaciones

BID: Bridge ID, identificación de bridge

BPDU: Bridge Protocol Data Unit, protocolo de unidad de enlace de datos

CIF: Canonical Identifier Format, identificador de formato canónico

CSMA/CA: Carrier Sense Multiple Access/ Collision Avoidance, acceso múltiple con escucha de portadora y evasión de colisiones

DHCP: Dynamic Host Configuration Protocol, protocolo de configuración dinámica de host

DSSS: Direct Sequence Spread Spectrum, espectro ensanchado por secuencia directa

EIA: Electronic Industries Alliance, Alianza de Industrias Electrónicas

ELFEXT: The Equal-Level Far-End Crosstalk, telediafonía por igualación de nivel

FEXT: Far-End Crosstalk, interferencia de extremo lejano – telediafonía

GAD: Gobierno Autónomo Descentralizado

GE: Grounding Equalizer, ecualizador de puesta a tierra

IBM: Internatinal Business Machines, es una empresa multinacional de tecnología

ID: Identification, identificación

IEEE: Intitute of Electrical and Electronics Enginners, Instituto de ingenieros eléctricos y electrónicos.

IP: Internet Protocol, protocolo de internet que identifica de manera lógica y jerárquica a un interfaz

ISO: International Standards Organization, es una organización Internacional de Normalización

ISP: Internet Service Provider, proveedor de servicios de internet

MAC: Media Access Control, control de acceso al medio

MIMO: Multiple-input Multiple-output, múltiple entrada múltiple salida

NEXT: Near-End crosstalk, interferencia de extremo cercano - paradiafonía

OFDM: Orthogonal Frequency Division Multiplexing, Multiplexión por División en Frecuencias Ortogonales

OSI: Open Systems Interconnetion, es un sistema de interconexión abierto

PC: Personal Computer, equipo de computación de uso personal

PDU: Power Distribution Unit, Unidad de Distribución de Energía

PSNEXT: Power Sum Near-End crosstalk, paradiafonía de suma de potencias

PSELFEXT: Power Sum the Equal-Level Far-End Crosstalk, telediafonía de suma de potencias

PVST: Per VLAN Spanning Tree, spanning-tree generado por VLANs

QoS: Quality of Service, calidad de servicio

STP: Spanning Tree Protocol, protocol spanning-tree

TBB: Telecommunications bonding backbone , columna vertebral de unión telecomunicaciones

TCI: Tag Control Information, etiqueta de información de control

TGB: Telecommunications Grounding Busba, barra colectora de puesta a tierra de telecomunicaciones

TIA: Telecommunications Industry Association, Asociación de la Industria de Telecomunicaciones

TMGB: Telecomunications Main Grounding Busbar, barra colectora de puesta a tierra principal de telecomunicaciones

TPID: Tag Protocol Identifier field, etiqueta del campo identificador de protocolo

UPS: Uninterruptible Power Supply, fuente de poder ininterrumpible

VLAN: Virtual Local Area Network, Redes de Área Local Virtuales

VTP: Virtual Trunking Protocol, protocolo de enlace truncal

WLAN: Wireless Local Area Network, redes de área local inalámbricas

BIBLIOGRAFIA

LIBROS

Bueltrick, S., & Escudero Pascual, A. (2007). *Infraestructura básica de redes inalambricas.* TRICALCAR.

Comer, D. (1996). *REDES GLOBALES DE INFORMACION CON INTERNET Y TCP/IP.* México.

Gómez Martín , J., García Reionoso, J., & Valera Pintor, F. (s.f.). *Redes y Servicios Internet de Nueva Generación* . Obtenido de Redes y Servicios Internet de Nueva Generación : http://www.it.uc3m.es/jgr/publicaciones/06-jcgomez_Telecom.pdf

Stallings, W. (2010). *Comunicaciones y Redes de Computadores.* Prentice Hall.

Tanenbaum, A. (2003). *Redes de computadoras.* México: PEARSON EDUCACIÓN.

Tanenbaum, A., & Wetherall, D. (2012). *REDES DE COMPUTADORAS.* México : PEARSON EDUCATION.

Varela, C., & Domínguez, L. (2002). *Redes Inalámbricas.*

TESIS

Alulema Chiluiza, D. V. (2008). *ESTUDIO Y DISEÑO DE UN SISTEMA DE SEGURIDAD PERIMETRAL PARA LA RED QUITO MOTORS, UTILIZANDO TECNOLOGIA UTM (UNIFIED THREAT MANAGEMENT).* Quito.

Jácome Zambrano , G. P., & Quiroga Chauca, L. A. (2013). *DISEÑO DE UNA RED MULTISERVICIOS PARA EL CENTRO DE REHABILITACION MEDICO No.3 Y LA DIRECCION PROVINCIAL MIES-INFA EN PORTOVIEJO.* Quito.

Jaramillo Pinos, E. (2013). *REDISEÑO DE RED MULTISERVICIOS PARA EL COLEGIO FERNANDO DAQUILEMA DE LA CIUDAD DE RIOBAMBA.* Quito.

Mosquera Tello, C. E. (2013). *IMPLEMENTACIÓN, FASE CABLEADO ESTRUCTURADO DEL LABORATORIO # 4 EN CATEGORÍA 6A COMO APORTE A LA FORMACIÓN PROFESIONAL DE LOS ESTUDIANTES DE LAS CISC Y CIN, APLICANDO ESTÁNDARES INTERNACIONALES DE*

CABLEADO GENÉRICO, RUTAS Y ESPACIOS DE TELECOMUNICACIO. Guayaquil.

Ramón Ibujes, N. (2013). *"REINGENIERÍA DE LA RED DE DATOS DE UN ENTE DEL MINISTERIO DE DEFENSA NACIONAL (MIDENA)".* Ibarra.

Torres Bolaños, R. J. (2014). *SEGURIDAD PERIMETRAL EN LA RED DE DISTRIBUCION DE LA.* Ibarra.

Villegas, J. (2013). *OPTIMIZACIÓN DE LA ADMISTRACIÓN DE LA RED E IMPLEMENTACIÓN DE SERVIDORES DE SERVICIOS PARA EL GOBIERNO PROVINCIAL DE IMBABURA.* Ibarra.

PAGINAS WEB

Ahutzin, G. (2013). *Catarina UDLAP.* Obtenido de Catarina UDLAP: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/ahuatzin_s_gl/capitulo2.pdf

Altadill Izura, P. X. (2013). *Redes de computadores.* Obtenido de Redes de computadores: http://redesdecomputadores.umh.es/iptables.htm

CISCO, N. (2013). *CISCO NETWORKING ACADEMY*. Obtenido de CISCO NETWORKING ACADEMY: http://www.cisco.com/c/es_es/index.html

Clariá, N. J. (5 de Julio de 2014). *BrazilFW-Firewall and Router.* Obtenido de BrazilFW-Firewall and Router: http://wiki.brazilfw.com.br/es:ipv4

Delgado Freire, A. (29 de Agosto de 2011). *Scribd.* Obtenido de Scribd: http://es.scribd.com/doc/63485942/Listas-de-Acceso-ACL-Teoria-y-Practica#scribd

Diaz, L. (4 de febrero de 2012). Obtenido de slideshare: http://www.slideshare.net/luishdiaz/132b-modelos-de-referencia

Egli, P. (2015). *indigoo.com.* Obtenido de indigoo.com: http://www.indigoo.com/dox/itdp/17_LAN-Layer2/STP-RSTP.pdf

Fleury Vicencio, D. (Junio de 2007). Obtenido de http://cdigital.uv.mx/bitstream/123456789/31219/1/cesareofleurivicencio.pdf

GAD PROVINCIAL DE IMBABURA. (2015). Obtenido de GAD PROVINCIAL DE IMBABURA: http://www.imbabura.gob.ec/institucion/mision-vision.html

Gonzáles Lucas, L. (s.f.). *IES Los Viveros.* Obtenido de IES Los Viveros: http://www.ieslosviveros.es/alumnos/asig8/carpeta812/PROTOCOLOS_DE_ENRUTAMIENTO.pdf

Gonzáles Piñones, F. (1 de Mayo de 2010). *REDES FRAN-CISCO.* Obtenido de REDES FRAN-CISCO: http://redesfran-cisco.blogspot.com/2010/05/principios-de-diseno-de-redes.html

Guillarte, M. (14 de Marzo de 2013). *mcpro.* Obtenido de mcpro: http://www.muycomputerpro.com/2013/03/14/que-es-un-tier

Mayám , D. (2006). *UNLaM COMUNICACION DE DATOS.* Obtenido de UNLaM COMUNICACION DE DATOS: http://unalm-construcion2010.wikispaces.com/file/view/p)+Redes+y+subredes.pdf

Norber, B. (11 de Abril de 2013). *slideshare*. Obtenido de slideshare: http://es.slideshare.net/norberbarraza/topolia-y-tipologia

Oficial, P. (s.f.). *UNIVERSIDAD TÉCNICA DEL NORTE*. Obtenido de http://www.utn.edu.ec/web/portal/index.php?option=com_content&view=article&id=118&Itemid=179

Oficial, P. (s.f.). *UNIVERSIDAD TÉCNICA DEL NORTE*. Obtenido de http://www.utn.edu.ec/fica/carreras/electronica/?page_id=9

Osorio, G. (13 de Mayo de 2011). *Tecno Info blog.* Obtenido de Tecno Info blog: http://gustavoaol.fullblog.com.ar/topologias-fisicas-y-logicas-de-red.html

Palacio, G. (2010). *Data Centers hoy.* España: MARCOMBO S.A.

Pietroselome, E., Zennaro, M., Fonda, C., & Okay, S. (2013). *Redes inalámbricas en los paises desarrollados.*

PREFECTURA DE IMBABURA. (2015). Obtenido de http://www.imbabura.gob.ec/institucion/mision-vision.html

Primo Guijarro, A. (14 de 01 de 2012). Obtenido de https://alvaroprimoguijarro.files.wordpress.com/2012/01/ud03_sad_alvaroprimoguijarro.pdf

Puerto, G., Ortega, B., Capmany, J., Cardona , K., & Suárez, C. (9 de Mayo de 2008). Obtenido de http://www.scielo.org.co/pdf/rfiua/n45/n45a13

Rosero, L. (28 de Noviembre de 2008). *IP reference.* Obtenido de IP reference: https://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/

Ruiz Barcayola, L. (6 de Julio de 2013). *Slideshare.* Obtenido de Slideshare: http://www.slideshare.net/LarryRuiz/access-pointpuntos-de-acceso

Sierra, M. (2013). *apr.* Obtenido de apr: http://aprenderaprogramar.com/index.php?option=com_content&view=article&id=542:que-es-un-servidor-y-cuales-son-los-principales-tipos-de-servidores-proxydns-webftppop3-y-smtp-dhcp&catid=57:herramientas-informaticas&Itemid=179

Siguencia, H., & León, E. (s.f.). Normas IEEE 802.11. Cuenca, Azuay, Ecuador.

Suquillo, R. (Noviembre de 2011). Arquitectura de Redes. *Arquitectura de Redes*.

Thaler, P., Finn, N., Fedyk, D., Parsons, G., & Gray, E. (10 de Marzo de 2013). *IEEE 802.1 Q.* Obtenido de IEEE 802.1 Q: https://www.ietf.org/meeting/86/tutorials/86-IEEE-8021-Thaler.pdf

NORMAS Y ESTANDARES

ANSI/TIA/EIA-568C. (s.f.). *ANIXTER-STANDARDS REFERENCE GUIDE.* Obtenido de ANIXTER-STANDARDS REFERENCE GUIDE.

ANSI/TIA/EIA-569C. (s.f.). *ANIXTER-STANDARDS REFERENCE GUIDE.* Obtenido de ANIXTER-STANDARDS REFERENCE GUIDE.

ANSI/TIA/EIA-606B. (s.f.). *ANIXTER-STANDARDS REFERENCE GUIDE.* Obtenido de ANIXTER-STANDARDS REFERENCE GUIDE.

ANSI/TIA/EIA-607B, E. (s.f.). *ANIXTER-STANDARDS REFERENCE GUIDE.* Obtenido de ANIXTER-STANDARDS REFERENCE GUIDE.

ANEXO 01 MAPEO PUNTOS DE RED

Permite identificar la ubicación los puntos del cableado con los puertos de los swiches de acceso y saber a qué VLAN pertenece dicho punto.

- Planta Baja

Tabla 60.- Puntos de red plata baja

GPI-PLANTA BAJA			
PUNTOS	**VLAN**	**PUERTOS**	**NOMBRE**
PB-D1	11	**172.16.2.6** (PUERTO 1)	INFRAESTRUCT FISICA
PB-D2	11	PUERTO 2	INFRAESTRUCT FISICA
PB-D3	17	PUERTO 3	FAUSTO GIS
PB-D4	11	PUERTO 4	INFRAESTRUCT FISICA
PB-D5	11	PUERTO 5	INFRAESTRUCT FISICA
PB-D6	11	PUERTO 6	INFRAESTRUCT FISICA
PB-D7	11	PUERTO 7	INFRAESTRUCT FISICA
PB-D8	11	PUERTO 8	INFRAESTRUCT FISICA
PB-D9	11	PUERTO 9	INFRAESTRUCT FISICA
PB-D10	14	PUERTO 10	WIFI
PB-D11	11	PUERTO 11	INFRAESTRUCT FISICA
PB-D12	11	PUERTO 12	INFRAESTRUCT FISICA
PB-D13	11	PUERTO 13	INFRAESTRUCT FISICA
PB-D14	11	PUERTO 14	INFRAESTRUCT FISICA
PB-D15	18	PUERTO 15	FISCALIZACION
PB-D16	18	PUERTO 16	FISCALIZACION
PB-D17	18	PUERTO 17	FISCALIZACION
PB-D18	12	PUERTO 18	DESARROLLO ECONOM
PB-D19	12	PUERTO 19	DESARROLLO ECONOM
PB-D20	12	PUERTO 20	DESARROLLO ECONOM

PB-D21	12	PUERTO 21	DESARROLLO ECONOM
PB-D22	32	PUERTO 22	CAMARAS HALL
PB-D23	32	PUERTO 23	INFORMACION
PB-D24	5	PUERTO 24	INFORMACION
PB-D25	5	PUERTO 25	INFORMACION
PB-D26	14	PUERTO 26	AP
PB-D27	11	PUERTO 27	SALA DE REUNIONES
PB-D28	11	PUERTO 28	SALA DE REUNIONES
PB-D29	32	PUERTO 29	CAMARA BIOMETRICOS
PB-D30	31	PUERTO 30	RELOJES BIOMETRICOS
PB-D31	31	PUERTO 31	RELOJES BIOMETRICOS
PB-D32	11	PUERTO 32	INFRAESTRUCT FISICA
PB-D33	11	PUERTO 33	INFRAESTRUCT FISICA
PB-D34	17	PUERTO 34	FAUSTO GIS
PB-D35	11	PUERTO 35	INFRAESTRUCT FISICA
PB-D36	14	PUERTO 36	WIFI INFRAESTRUCTURA
PB-D37	11	PUERTO 37	INFRAESTRUCT FISICA
PB-D38	11	PUERTO 38	INFRAESTRUCT FISICA
PB-D39	11	PUERTO 39	INFRAESTRUCT FISICA
PB-D40	11	PUERTO 40	INFRAESTRUCT FISICA
PB-D41	11	PUERTO 41	INFRAESTRUCT FISICA
PB-D42	18	PUERTO 42	INFRAESTRUCT FISICA
PB-D43	11	PUERTO 43	INFRAESTRUCT FISICA
PB-D44	11	PUERTO 44	INFRAESTRUCT FISICA
PB-D45	11	PUERTO 45	INFRAESTRUCT FISICA
PB-D46	18	PUERTO 46	FISCALIZACION
PB-D47	**ENLACE PB-PA1**	**ENLACE PB-PA1**	OBS: PUERTO 47 Y 48 TRUNK
PB-D48	**ENLACE PB-PA1**	**ENLACE PB-PA1**	
PB-D49	12	**172.16.2.7** (PUERTO 1)	DESARROLLO ECONOM

PB-D50	12	PUERTO 2	DESARROLLO ECONOM
PB-D51	12	PUERTO 3	DESARROLLO ECONOM
PB-D52	18	PUERTO 4	FISCALIZACION
PB-D53	18	PUERTO 5	FISCALIZACION
PB-D54	10	PUERTO 6	ADMIN GENERAL
PB-D55	10	PUERTO 7	TRABAJO SOCIAL
PB-D56	10	PUERTO 8	ARCHIVO
PB-D57	10	PUERTO 9	ARCHIVO
PB-D58	10	PUERTO 10	ARCHIVO
PB-D59	10	PUERTO 11	ODONTOLOGO
PB-D60	32	PUERTO 12	CAMARA HALL PASILLO
PB-D61	31	PUERTO 13	CAMARA FRENTE GARITA
PB-D62	40	PUERTO 14	GUARDIA
PB-D63	18	PUERTO 15	FISCALIZACION
PB-D64	18	PUERTO 16	FISCALIZACION

Referencia*:* Dirección de Tecnologías de la Información del GAD Provincial de Imbabura.

- Planta alta 1

Tabla 61.- Puntos de red plata alta 1

GPI-PLANTA ALTA1			
PUNTOS	**VLAN**	**PUERTOS**	**NOMBRE**
PA1-D1	5	**172.16.2.2** (PUERTO 1)	PREFECTURA
PA1-D2	5	PUERTO 2	PREFECTURA
PA1-D3	5	PUERTO 3	PREFECTURA
PA1-D4	5	PUERTO 4	PREFECTURA
PA1-D5	5	PUERTO 5	PREFECTURA
PA1-D6	5	PUERTO 6	PREFECTURA
PA1-D7	5	PUERTO 7	PREFECTURA
PA1-D8	5	PUERTO 8	PREFECTURA
PA1-D9	5	PUERTO 9	PREFECTURA
PA1-D10	5	PUERTO 10	PREFECTURA
PA1-D11	5	PUERTO 11	PREFECTURA
PA1-D12	9	PUERTO 12	RELACIONES PUBLICAS
PA1-D13	9	PUERTO 13	RELACIONES PUBLICAS
PA1-D14	5	PUERTO 14	PREFECTURA

PA1-D15	5	PUERTO 15	PREFECTURA
PA1-D16	5	PUERTO 16	PREFECTURA
PA1-D17	5	PUERTO 17	AP
PA1-D18	5	PUERTO 18	PREFECTURA
PA1-D19	5	PUERTO 19	PREFECTURA
PA1-D20	5	PUERTO 20	PREFECTURA
PA1-D21	5	PUERTO 21	PREFECTURA
PA1-D22	5	PUERTO 22	PREFECTURA
PA1-D23	5	PUERTO 23	PREFECTURA
PA1-D24	5	PUERTO 24	PREFECTURA
PA1-D25	6	PUERTO 25	PROCURADURIA
PA1-D26	6	PUERTO 26	PROCURADURIA
PA1-D27	6	PUERTO 27	PROCURADURIA
PA1-D28	6	PUERTO 28	PROCURADURIA
PA1-D29	6	PUERTO 29	PROCURADURIA
PA1-D30	6	PUERTO 30	PROCURADURIA
PA1-D31	6	PUERTO 31	PROCURADURIA
PA1-D32	10	PUERTO 32	ADMIN GENERAL
PA1-D33	10	PUERTO 33	ADMIN GENERAL
PA1-D34	10	PUERTO 34	ADMIN GENERAL
PA1-D35	10	PUERTO 35	ADMIN GENERAL
PA1-D36	10	PUERTO 36	ADMIN GENERAL
PA1-D37	10	PUERTO 37	ADMIN GENERAL
PA1-D38	10	PUERTO 38	ADMIN GENERAL
PA1-D39	10	PUERTO 39	ADMIN GENERAL
PA1-D40	9	PUERTO 40	RELACIONES PUBLICAS
PA1-D41	9	PUERTO 41	RELACIONES PUBLICAS
PA1-D42	4	PUERTO 42	GESTION TECNOLOGICA
PA1-D43	4	PUERTO 43	GESTION TECNOLOGICA
PA1-D44	4	PUERTO 44	GESTION TECNOLOGICA
PA1-D45	4	PUERTO 45	GESTION TECNOLOGICA
PA1-D46	4	PUERTO 46	GESTION TECNOLOGICA
		PUERTO 47	OBS: PUERTO 47-48 TRUNK
		PUERTO 48	
PA1-D47	4	**172.16.2.3** (PUERTO 1)	GESTION TECNOLOGICA
PA1-D48	4	PUERTO 2	GESTION TECNOLOGICA

PA1-D49	10	PUERTO 3	ADMIN GENERAL
PA1-D50	10	PUERTO 4	ADMIN GENERAL
PA1-D51	10	PUERTO 5	ADMIN GENERAL
PA1-D52	4	PUERTO 6	GESTION TECNOLOGICA
PA1-D53	10	PUERTO 7	ADMIN GENERAL
PA1-D54	10	PUERTO 8	ADMIN GENERAL
PA1-D55	10	PUERTO 9	ADMIN GENERAL
PA1-D56	4	PUERTO 10	GESTION TECNOLOGICA
PA1-D57	4	PUERTO 11	GESTION TECNOLOGICA
PA1-D58	4	PUERTO 12	GESTION TECNOLOGICA
PA1-D59	10	PUERTO 13	ADMIN GENERAL
PA1-D60	4	PUERTO 14	GESTION TECNOLOGICA
PA1-D61	10	PUERTO 15	ADMIN GENERAL
PA1-D62	10	PUERTO 16	ADMIN GENERAL
PA1-D63	10	PUERTO 17	ADMIN GENERAL
PA1-D64	10	PUERTO 18	ADMIN GENERAL
PA1-D65	10	PUERTO 19	ADMIN GENERAL
PA1-D66	10	PUERTO 20	ADMIN GENERAL
PA1-D67	10	PUERTO 21	ADMIN GENERAL
PA1-D68	10	PUERTO 22	ADMIN GENERAL
PA1-D69	10	PUERTO 23	ADMIN GENERAL
PA1-D70	10	PUERTO 24	ADMIN GENERAL
PA1-D71	10	PUERTO 25	ADMIN GENERAL
PA1-D72	10	PUERTO 26	ADMIN GENERAL
			OBS: PUERTO 47-48 TRUNK
PA1-D73	5	**172.16.2.4** (PUERTO 1)	PREFECTURA
PA1-D74	5	PUERTO 2	PREFECTURA
PA1-D75	5	PUERTO 3	PREFECTURA
PA1-D76	6	PUERTO 4	AP PROCURADURIA
PA1-D77	5	PUERTO 5	PREFECTURA
PA1-D78	5	PUERTO 6	PREFECTURA
PA1-D79	10	PUERTO 7	ADMIN GENERAL
PA1-D80	5	PUERTO 8	PREFECTURA
PA1-D81	5	PUERTO 9	PREFECTURA
PA1-D82	5	PUERTO 10	PREFECTURA
PA1-D83	5	PUERTO 11	PREFECTURA

PA1-D84	9	PUERTO 12	RELACIONES PUBLICAS
PA1-D85	4	PUERTO 37	PROYECTOR GES TECNOLOG
PA1-D86	9	PUERTO 36	RELACIONES PUBLICAS
PA1-D87	5	PUERTO 35	PREFECTURA
PA1-D88	10	PUERTO 34	ADMIN GENERAL
PA1-D89	10	PUERTO 33	ADMIN GENERAL
PA1-D90	9	PUERTO 32	RELACIONES PUBLICAS
PA1-D91	9	PUERTO 31	RELACIONES PUBLICAS
PA1-D92	10	PUERTO 30	ADMIN GENERAL
PA1-D93	10	PUERTO 29	ADMIN GENERAL
PA1-D94	10	PUERTO 28	ADMIN GENERAL
PA1-D95	10	PUERTO 27	ADMIN GENERAL
PA1-D96	10	PUERTO 26	ADMIN GENERAL
PA1-D97	10	PUERTO 25	ADMIN GENERAL
PA1-D98	10	PUERTO 24	ADMIN GENERAL
PA1-D99	10	PUERTO 23	ADMIN GENERAL
PA1-D100	10	PUERTO 22	ADMIN GENERAL
PA1-D101	10	PUERTO 21	ADMIN GENERAL
PA1-D102	4	PUERTO 20	GESTION TECNOLOGICA
PA1-D103	4	PUERTO 19	GESTION TECNOLOGICA
PA1-D104	4	PUERTO 18	GESTION TECNOLOGICA
PA1-D105	6	PUERTO 17	PROCURADURIA
PA1-D106	10	PUERTO 16	ADMIN GENERAL
PA1-D107	4	PUERTO 15	GESTION TECNOLOGICA
PA1-D108	10	PUERTO 14	ADMIN GENERAL
PA1-D109	4	PUERTO 13	CAMARA GES TECNOLOG
PA1-D110	4	PUERTO 38	CAMARA GES TECNOLOG
		PUERTO 47	OBS: PUERTO 47-48 TRUNK
		PUERTO 48	

Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura.

- Planta alta 2

Tabla 62.- Puntos de red plata alta 1

GPI-PLANTA BAJA			
PUNTOS	**VLAN**	**PUERTOS**	**NOMBRE**
PA2-D1	7	**172.16.2.10** (PUERTO 1)	PLANIFICACION (AP)
PA2-D2	7	PUERTO 2	PLANIFICACION
PA2-D3	7	PUERTO 3	PLANIFICACION
PA2-D4	7	PUERTO 4	PLANIFICACION
PA2-D5	7	PUERTO 5	PLANIFICACION
PA2-D6	7	PUERTO 6	PLANIFICACION
PA2-D7	7	PUERTO 7	PLANIFICACION
PA2-D8	7	PUERTO 8	PLANIFICACION
PA2-D9	7	PUERTO 9	PLANIFICACION
PA2-D10	7	PUERTO 10	PLANIFICACION
PA2-D11	7	PUERTO 11	PLANIFICACION
PA2-D12	7	PUERTO 12	PLANIFICACION
PA2-D13	7	PUERTO 13	PLANIFICACION
PA2-D14	7	PUERTO 14	PLANIFICACION
PA2-D15	7	PUERTO 15	PLANIFICACION
PA2-D16	17	PUERTO 16	FAUSTO GIS
PA2-D17	7	PUERTO 17	PLANIFICACION
PA2-D18	7	PUERTO 18	PLANIFICACION
PA2-D19	17	PUERTO 19	FAUSTO GIS
PA2-D20	17	PUERTO 20	FAUSTO GIS
PA2-D21	7	PUERTO 21	PLANIFICACION
PA2-D22	7	PUERTO 22	PLANIFICACION
PA2-D23	7	PUERTO 23	PLANIFICACION
PA2-D24	7	PUERTO 24	PLANIFICACION (AP)
PA2-D25	17	PUERTO 25	FAUSTO GIS
PA2-D26	8	PUERTO 26	GESTION TECNICA
PA2-D27	8	PUERTO 27	GESTION TECNICA
PA2-D28	8	PUERTO 28	GESTION TECNICA
PA2-D29		PUERTO 29	SALA DE REUNIONES
PA2-D30		PUERTO 30	SALA DE REUNIONES
PA2-D31		PUERTO 31	TURISMO
PA2-D32		PUERTO 32	TURISMO
PA2-D33		PUERTO 33	TURISMO
PA2-D34		PUERTO 34	TURISMO
PA2-D35		PUERTO 35	FORESTACION Y BIODEVERSIDAD

PA2-D36		PUERTO 36	FORESTACION Y BIODEVERSIDAD
PA2-D37		PUERTO 37	FORESTACION Y BIODEVERSIDAD
PA2-D38		PUERTO 38	FORESTACION Y BIODEVERSIDAD
PA2-D39		PUERTO 39	FORESTACION Y BIODEVERSIDAD
PA2-D40		PUERTO 40	CUENCAS HIDROGRAFICAS
PA2-D41		PUERTO 41	CUENCAS HIDROGRAFICAS
PA2-D42		PUERTO 42	CUENCAS HIDROGRAFICAS
PA2-D109	13	PUERTO 43	RADIO PAS
PA2-D110	50	PUERTO 44	RADIO BODEGA
PA2-D111	50	PUERTO 45	RADIO UBIQUITI
PA2-D113	50	PUERTO 46	RADIO UBIQUITI
PA2-D112	TRUNK	PUERTO 47	RADIO MUTUALISTA
		PUERTO 48	OBS: PUERTO 48 Y 52 TRUNK
PA2-D48		**172.16.2.11** (PUERTO 1)	
PA2-D49	12	PUERTO 2	DESARROLLO ECONOM
PA2-D50	12	PUERTO 3	DESARROLLO ECONOM
PA2-D51	12	PUERTO 4	DESARROLLO ECONOM
PA2-D52	12	PUERTO 5	DESARROLLO ECONOM
PA2-D53	12	PUERTO 6	DESARROLLO ECONOM
PA2-D54	12	PUERTO 7	DESARROLLO ECONOM
PA2-D55	12	PUERTO 8	DESARROLLO ECONOM
PA2-D56	12	PUERTO 9	DESARROLLO ECONOM
PA2-D57	12	PUERTO 10	DESARROLLO ECONOM
PA2-D58	12	PUERTO 11	DESARROLLO ECONOM
PA2-D59		PUERTO 12	EDUC. Y GESTION AMBIENTAL
PA2-D60	12	PUERTO 13	DESARROLLO ECONOM
PA2-D61	12	PUERTO 14	DESARROLLO ECONOM
PA2-D62	12	PUERTO 15	DESARROLLO ECONOM
PA2-D63	12	PUERTO 16	DESARROLLO ECONOM
PA2-D64	9	PUERTO 17	RELACIONES PUBLICAS
PA2-D65	9	PUERTO 18	RELACIONES PUBLICAS
PA2-D66	9	PUERTO 19	RELACIONES PUBLICAS
PA2-D67	9	PUERTO 20	RELACIONES PUBLICAS
PA2-D68	12	PUERTO 21	DESARROLLO ECONOM
PA2-D69	12	PUERTO 22	DESARROLLO ECONOM
PA2-D70	12	PUERTO 23	DESARROLLO ECONOM
PA2-D71	12	PUERTO 24	DESARROLLO ECONOM
PA2-D72	12	PUERTO 25	DESARROLLO ECONOM
PA2-D73	12	PUERTO 26	DESARROLLO ECONOM

PA2-D74	12	PUERTO 27	DESARROLLO ECONOM
PA2-D75	12	PUERTO 28	DESARROLLO ECONOM
PA2-D76	12	PUERTO 29	DESARROLLO ECONOM
PA2-D77	12	PUERTO 30	DESARROLLO ECONOM
PA2-D78	12	PUERTO 31	DESARROLLO ECONOM
PA2-D79	12	PUERTO 32	DESARROLLO ECONOM
PA2-D80	12	PUERTO 33	DESARROLLO ECONOM
PA2-D81	12	PUERTO 34	DESARROLLO ECONOM
PA2-D82	12	PUERTO 35	DESARROLLO ECONOM
PA2-D83	12	PUERTO 36	DESARROLLO ECONOM
PA2-D84	12	PUERTO 37	DESARROLLO ECONOM
PA2-D85	12	PUERTO 38	DESARROLLO ECONOM
PA2-D86	12	PUERTO 39	DESARROLLO ECONOM
PA2-D87	12	PUERTO 40	DESARROLLO ECONOM
PA2-D88	12	PUERTO 41	DESARROLLO ECONOM
PA2-D89	12	PUERTO 42	DESARROLLO ECONOM
PA2-D90		PUERTO 43	EDUC. Y GESTION AMBIENTAL
PA2-D91	12	PUERTO 44	DESARROLLO ECONOM
PA2-D92	12	PUERTO 45	DESARROLLO ECONOM
PA2-D93	12	PUERTO 46	DESARROLLO ECONOM
		PUERTO 47	OBS: PUERTO 47-48 TRUNK
		PUERTO 48	
PA2-D94	12	**172.16.2.12** (PUERTO 1)	DESARROLLO ECONOM
PA2-D95	12	PUERTO 2	DESARROLLO ECONOM
PA2-D96	12	PUERTO 3	DESARROLLO ECONOM
PA2-D97	12	PUERTO 4	DESARROLLO ECONOM
PA2-D98	12	PUERTO 5	DESARROLLO ECONOM
PA2-D99	12	PUERTO 6	DESARROLLO ECONOM
PA2-D100	9	PUERTO 7	RELACIONES PUBLICAS
PA2-D101	9	PUERTO 8	RELACIONES PUBLICAS
PA2-D102	9	PUERTO 9	RELACIONES PUBLICAS
PA2-D103	9	PUERTO 10	RELACIONES PUBLICAS
PA2-D104	9	PUERTO 11	RELACIONES PUBLICAS
PA2-D105	9	PUERTO 12	RELACIONES PUBLICAS
PA2-D106		PUERTO 13	CONTRALORIA
PA2-D107		PUERTO 14	CONTRALORIA
PA2-D108	9	PUERTO 15	RELACIONES PUBLICAS
PA2-D43		PUERTO 42	
PA2-D44		PUERTO 43	
PA2-D45		PUERTO 44	
PA2-D46		PUERTO 45	

PA2-D47	PUERTO 46	
	PUERTO 47	
	PUERTO 48	OBS: PUERTO 4748 TRUNK

Referencia: Dirección de Tecnologías de la Información del GAD Provincial de Imbabura.

ANEXO 02 SERVIDORES DE LA INSTITUCIÓN

La red de comunicaciones del GAD provincial de Imbabura cuenta con algunos servidores, a continuación se documenta la descripción de ellos.

1. Computadora de escritorio
    - Procesador Inteli7
    - Memoria ram8G
    - Disco duro: 1TB
2. Servidor Compaq
    - Modelo Proliand
    - Procesador: Intel Xeon 2.4GHz
    - Memoria ram:512 MB
    - Disco duro: 80G
3. Servidor HP Prolian
    - Modelo:DL360 G6
    - Procesador: Intel Xeon
    - Memoria ram:6GB
    - Disco duro: 600G
    - Espacio utilizable endisco:300
4. Servidor HP Prolian
    - Modelo:DL360 G6
    - Procesador: IntelXeon
    - Memoria ram:6GB
    - Disco duro: 1.2T

5. Un chasis HP c3000, instalado 8 cuchillas.

Cuchillas tipo B

- Modelo: Proliant BL460c G7
- Procesador: Six-Core Intel Xeon,2667 Mhz
- Memoria ram:16 GB
- Disco duro: 1000G
- Espacio utilizable endisco:500G

Cuchillas tipo C

- Modelo: Proliant BL460c G7
- Procesador: 2xSix-Core Intel Xeon,2667 Mhz
- Memoria ram:16 GB
- Disco duro: 600G

Cuchillas tipo D

- Modelo:Proliant BL460c G8
- Procesador: 2xSix-Core Intel Xeon,2500 Mhz
- Memoria ram:32 GB
- Disco duro: 600G
- Espacio utilizable endisco:300G

Cuchillas tipoE

- Modelo: Proliant BL460c G8
- Procesador: 1xSix-Core Intel Xeon,2500 Mhz
- Memoria ram:32 GB
- Disco duro: 600G

- Espacio utilizable endisco:300G

6. Servidor DELL EDGE
7. Servidor de Telefonía

   Modelo: Clon

   Procesador: Intel Pentium(R) 3GHz

   Memoria ram:2 GB

   Disco duro: 300G

   Espacio utilizable: 150G

SERVICIOS OPERATIVOS:

1. Proxyficacióndelinternet para la red cableadae inalámbrica
2. Correo electrónico
   - imbabura.gob.ec
   - imbavial.gob.ec
3. Hosting
   - www.imbabura.gob.ec
   - www.imbaburaturismo.gob.ec
   - www.imbabura.travel
   - www.imbavial.gob.ec
   - pas.imbabura.gob.ec
4. Aplicacionesen producción
5. Pruebas (aplicacionesybase de datos)

6. Archivo documental (Alfresco)

7. Sistema de documentación

8. Intranet(aplicaciones ybasesde datos)

9. Sistema financiero

10. Sistemas de vídeo vigilancia

11. Sistemas de GeolocalizaciónyRegistro histórico de Geolocalización

12. Sistema de almacenamiento paraVideo(Sistemas de Streaming

ANEXO 03 MAPEO PUNTOS DE RED DE ACUERDO A LAS NUEVAS VLANS

A continuación se presenta la distribución de los puertos de cada switch en los repartidores horizontales de acuerdo a la nueva distribución de VLANs:

- Planta Baja

Los puertos en el switch dos se encuentran distribuidos entre las VLANs 16, 28 y 52, los puertos en el switch tres se encuentran distribuidos entre las VLANs 20, 30, 46 y 48.

Tabla 63.- Nueva distribución de puntos de red plata baja

GPI-PLANTA BAJA			
PUNTOS	**VLAN**	**PUERTOS**	**NOMBRE**
PB-D1	28	**170.20.4.2** (PUERTO 1)	INFRAESTRUCT FISICA
PB-D2	28	PUERTO 2	INFRAESTRUCT FISICA
PB-D3	28	PUERTO 3	INFRAESTRUCT FISICA
PB-D4	28	PUERTO 4	INFRAESTRUCT FISICA
PB-D5	28	PUERTO 5	INFRAESTRUCT FISICA
PB-D6	28	PUERTO 6	INFRAESTRUCT FISICA
PB-D7	28	PUERTO 7	INFRAESTRUCT FISICA
PB-D8	28	PUERTO 8	INFRAESTRUCT FISICA
PB-D9	28	PUERTO 9	INFRAESTRUCT FISICA
PB-D10	52	PUERTO 10	WIFI
PB-D11	28	PUERTO 11	INFRAESTRUCT FISICA
PB-D12	28	PUERTO 12	INFRAESTRUCT FISICA
PB-D13	28	PUERTO 13	INFRAESTRUCT FISICA

PB-D14	28	PUERTO 14	INFRAESTRUCT FISICA
PB-D15	16	PUERTO 15	FISCALIZACION
PB-D16	16	PUERTO 16	FISCALIZACION
PB-D17	16	PUERTO 17	FISCALIZACION
PB-D18	30	PUERTO 18	DESARROLLO ECONOM
PB-D19	30	PUERTO 19	DESARROLLO ECONOM
PB-D20	30	PUERTO 20	DESARROLLO ECONOM
PB-D21	30	PUERTO 21	DESARROLLO ECONOM
PB-D22	52	PUERTO 22	WIFI
PB-D23	52	PUERTO 23	WIFI
PB-D24	10	PUERTO 24	PREFECTURA
PB-D25	10	PUERTO 25	PREFECTURA
PB-D26	52	PUERTO 26	WIFI
PB-D27	28	PUERTO 27	INFRAESTRUCT FISICA
PB-D28	28	PUERTO 28	INFRAESTRUCT FISICA
PB-D29	48	PUERTO 29	CAMARAS
PB-D30	46	PUERTO 30	RELOJES
PB-D31	46	PUERTO 31	RELOJES
PB-D32	28	PUERTO 32	INFRAESTRUCT FISICA
PB-D33	28	PUERTO 33	INFRAESTRUCT FISICA
PB-D34	28	PUERTO 34	INFRAESTRUCT FISICA
PB-D35	28	PUERTO 35	INFRAESTRUCT FISICA
PB-D36	52	PUERTO 36	WIFI
PB-D37	28	PUERTO 37	INFRAESTRUCT FISICA
PB-D38	28	PUERTO 38	INFRAESTRUCT FISICA
PB-D39	28	PUERTO 39	INFRAESTRUCT FISICA
PB-D40	28	PUERTO 40	INFRAESTRUCT FISICA
PB-D41	28	PUERTO 41	INFRAESTRUCT FISICA
PB-D42	16	PUERTO 42	INFRAESTRUCT FISICA
PB-D43	28	PUERTO 43	INFRAESTRUCT FISICA
PB-D44	28	PUERTO 44	INFRAESTRUCT FISICA

PB-D45	28	PUERTO 45	INFRAESTRUCT FISICA
PB-D46	16	PUERTO 46	FISCALIZACION
PB-D47	**ENLACE PB-PA1**	**ENLACE PB-PA1**	OBS: PUERTO 47 Y 48 TRUNK
PB-D48	**ENLACE PB-PA1**	**ENLACE PB-PA1**	
PB-D49	30	**170.20.4.3** (PUERTO 1)	DESARROLLO ECONOM
PB-D50	30	PUERTO 2	DESARROLLO ECONOM
PB-D51	30	PUERTO 3	DESARROLLO ECONOM
PB-D52	16	PUERTO 4	FISCALIZACION
PB-D53	16	PUERTO 5	FISCALIZACION
PB-D54	20	PUERTO 6	ADMIN GENERAL
PB-D55	20	PUERTO 7	ADMIN GENERAL
PB-D56	20	PUERTO 8	ADMIN GENERAL
PB-D57	20	PUERTO 9	ADMIN GENERAL
PB-D58	20	PUERTO 10	ADMIN GENERAL
PB-D59	20	PUERTO 11	ADMIN GENERAL
PB-D60	48	PUERTO 12	CAMARA HALL PASILLO
PB-D61	48	PUERTO 13	CAMARA FRENTE GARITA
PB-D62	40	PUERTO 14	TELEFONIA GUARDIA
PB-D63	16	PUERTO 15	FISCALIZACION
PB-D64	16	PUERTO 16	FISCALIZACION
PB-D65	20	PUERTO 17	ADMIN GENERAL
PB-D66	20	PUERTO 18	ADMIN GENERAL
PB-D67	20	PUERTO 19	ADMIN GENERAL
PB-D68	20	PUERTO 20	ADMIN GENERAL
PB-D69	20	PUERTO 21	ADMIN GENERAL
PB-D70	20	PUERTO 22	ADMIN GENERAL
PB-D71	20	PUERTO 23	ADMIN GENERAL
PB-D72	20	PUERTO 24	ADMIN GENERAL
PB-D73	20	PUERTO 25	ADMIN GENERAL
PB-D74	20	PUERTO 26	ADMIN GENERAL
PB-D95	**ENLACE PB-PA1**	**ENLACE PB-PA1**	OBS: PUERTO 47 Y 48 TRUNK
PB-D96	**ENLACE PB-PA1**	**ENLACE PB-PA1**	

Referencia: Basado en investigación teórica y práctica

- Planta alta 1

Los puertos en el switch cuatro se encuentran distribuidos entre las VLANs 8, 10 y 12, los puertos en el switch cinco se encuentran distribuidos entre las VLANs 18, 20 y 12, los puertos en el switch seis se encuentran distribuidos entre las VLANs 22, 24 y 26.

Tabla 64.- Nueva distribución de puntos de red plata alta 1

GPI-PLANTA ALTA1			
PUNTOS	**VLAN**	**PUERTOS**	**NOMBRE**
PA1-D1	10	**170.20.4.4** (PUERTO 1)	PREFECTURA
PA1-D2	10	PUERTO 2	PREFECTURA
PA1-D3	10	PUERTO 3	PREFECTURA
PA1-D4	10	PUERTO 4	PREFECTURA
PA1-D5	10	PUERTO 5	PREFECTURA
PA1-D6	10	PUERTO 6	PREFECTURA
PA1-D7	10	PUERTO 7	PREFECTURA
PA1-D8	10	PUERTO 8	PREFECTURA
PA1-D9	10	PUERTO 9	PREFECTURA
PA1-D10	10	PUERTO 10	PREFECTURA
PA1-D11	10	PUERTO 11	PREFECTURA
PA1-D12	18	PUERTO 12	RELACIONES PUBLICAS
PA1-D13	18	PUERTO 13	RELACIONES PUBLICAS
PA1-D14	10	PUERTO 14	PREFECTURA
PA1-D15	10	PUERTO 15	PREFECTURA
PA1-D16	10	PUERTO 16	PREFECTURA
PA1-D17	52	PUERTO 17	WIFI
PA1-D18	10	PUERTO 18	PREFECTURA
PA1-D19	10	PUERTO 19	PREFECTURA
PA1-D20	10	PUERTO 20	PREFECTURA
PA1-D21	10	PUERTO 21	PREFECTURA
PA1-D22	10	PUERTO 22	PREFECTURA
PA1-D23	10	PUERTO 23	PREFECTURA
PA1-D24	10	PUERTO 24	PREFECTURA
PA1-D25	12	PUERTO 25	PROCURADURIA
PA1-D26	12	PUERTO 26	PROCURADURIA
PA1-D27	12	PUERTO 27	PROCURADURIA
PA1-D28	12	PUERTO 28	PROCURADURIA

PA1-D29	12	PUERTO 29	PROCURADURIA
PA1-D30	12	PUERTO 30	PROCURADURIA
PA1-D31	12	PUERTO 31	PROCURADURIA
PA1-D32	22	PUERTO 32	COMPRAS PUBLICAS
PA1-D33	22	PUERTO 33	COMPRAS PUBLICAS
PA1-D34	22	PUERTO 34	COMPRAS PUBLICAS
PA1-D35	22	PUERTO 35	COMPRAS PUBLICAS
PA1-D36	22	PUERTO 36	COMPRAS PUBLICAS
PA1-D37	22	PUERTO 37	COMPRAS PUBLICAS
PA1-D38	22	PUERTO 38	COMPRAS PUBLICAS
PA1-D39	22	PUERTO 39	COMPRAS PUBLICAS
PA1-D40	18	PUERTO 40	RELACIONES PUBLICAS
PA1-D41	18	PUERTO 41	RELACIONES PUBLICAS
PA1-D42	8	PUERTO 42	TICS
PA1-D43	8	PUERTO 43	TICS
PA1-D44	8	PUERTO 44	TICS
PA1-D45	8	PUERTO 45	TICS
PA1-D46	8	PUERTO 46	TICS
		PUERTO 47	OBS: PUERTO 47-48 TRUNK
		PUERTO 48	
PA1-D47	8	**170.20.4.5** (PUERTO 1)	GESTION TECNOLOGICA
PA1-D48	8	PUERTO 2	GESTION TECNOLOGICA
PA1-D49	24	PUERTO 3	FINANCIERO
PA1-D50	24	PUERTO 4	FINANCIERO
PA1-D51	24	PUERTO 5	FINANCIERO
PA1-D52	8	PUERTO 6	TICS
PA1-D53	24	PUERTO 7	FINANCIERO
PA1-D54	24	PUERTO 8	FINANCIERO
PA1-D55	24	PUERTO 9	FINANCIERO
PA1-D56	8	PUERTO 10	TICS
PA1-D57	8	PUERTO 11	TICS
PA1-D58	8	PUERTO 12	TICS
PA1-D59	24	PUERTO 13	FINANCIERO
PA1-D60	8	PUERTO 14	TICS
PA1-D61	24	PUERTO 15	FINANCIERO
PA1-D62	24	PUERTO 16	FINANCIERO
PA1-D63	24	PUERTO 17	FINANCIERO
PA1-D64	24	PUERTO 18	FINANCIERO
PA1-D65	24	PUERTO 19	FINANCIERO

PA1-D66	20	PUERTO 20	ADMINISTRACION
PA1-D67	20	PUERTO 21	ADMINISTRACION
PA1-D68	20	PUERTO 22	ADMINISTRACION
PA1-D69	20	PUERTO 23	ADMINISTRACION
PA1-D70	20	PUERTO 24	ADMINISTRACION
PA1-D71	20	PUERTO 25	ADMINISTRACION
PA1-D72	20	PUERTO 26	ADMINISTRACION
			OBS: PUERTO 47-48 TRUNK
PA1-D73	10	**170.20.4.6** (PUERTO 1)	PREFECTURA
PA1-D74	10	PUERTO 2	PREFECTURA
PA1-D75	10	PUERTO 3	PREFECTURA
PA1-D76	52	PUERTO 4	WIFI
PA1-D77	10	PUERTO 5	PREFECTURA
PA1-D78	10	PUERTO 6	PREFECTURA
PA1-D79	20	PUERTO 7	ADMIN GENERAL
PA1-D80	10	PUERTO 8	PREFECTURA
PA1-D81	10	PUERTO 9	PREFECTURA
PA1-D82	10	PUERTO 10	PREFECTURA
PA1-D83	10	PUERTO 11	PREFECTURA
PA1-D84	18	PUERTO 12	RELACIONES PUBLICAS
PA1-D85	8	PUERTO 37	TICS
PA1-D86	18	PUERTO 36	RELACIONES PUBLICAS
PA1-D87	10	PUERTO 35	PREFECTURA
PA1-D88	24	PUERTO 34	ADMIN GENERAL
PA1-D89	24	PUERTO 33	ADMIN GENERAL
PA1-D90	18	PUERTO 32	RELACIONES PUBLICAS
PA1-D91	18	PUERTO 31	RELACIONES PUBLICAS
PA1-D92	24	PUERTO 30	FINANCIERO
PA1-D93	24	PUERTO 29	FINANCIERO
PA1-D94	26	PUERTO 28	TALENTO HUMANO
PA1-D95	26	PUERTO 27	TALENTO HUMANO
PA1-D96	26	PUERTO 26	TALENTO HUMANO
PA1-D97	26	PUERTO 25	TALENTO HUMANO
PA1-D98	26	PUERTO 24	TALENTO HUMANO
PA1-D99	26	PUERTO 23	TALENTO HUMANO
PA1-D100	26	PUERTO 22	TALENTO HUMANO
PA1-D101	26	PUERTO 21	TALENTO HUMANO

PA1-D102	8	PUERTO 20	TICS
PA1-D103	8	PUERTO 19	TICS
PA1-D104	8	PUERTO 18	TICS
PA1-D105	12	PUERTO 17	PROCURADURIA
PA1-D106	26	PUERTO 16	TALENTO HUMANO
PA1-D107	8	PUERTO 15	TICS
PA1-D108	26	PUERTO 14	TALENTO HUMANO
PA1-D109	48	PUERTO 13	CAMARAS
PA1-D110	48	PUERTO 38	CAMARAS
		PUERTO 47	OBS: PUERTO 47-48 TRUNK
		PUERTO 48	

Referencia: Basado en investigación teórica y práctica

- Planta alta 2

Los puertos en el switch siete se encuentran distribuidos entre las VLANs 15 y 50, los puertos en el switch ocho se encuentran distribuidos entre las VLANs 34 y 36, los puertos en el switch nueve se encuentran distribuidos entre las VLANs 30 y 18.

Tabla 65.- Nueva distribución de puntos de red plata alta 2

GPI-PLANTA BAJA			
PUNTOS	**VLAN**	**PUERTOS**	**NOMBRE**
PA2-D1	52	**170.20.4.7** (PUERTO 1)	WIFI
PA2-D2	14	PUERTO 2	PLANIFICACION
PA2-D3	14	PUERTO 3	PLANIFICACION
PA2-D4	14	PUERTO 4	PLANIFICACION
PA2-D5	14	PUERTO 5	PLANIFICACION
PA2-D6	14	PUERTO 6	PLANIFICACION
PA2-D7	14	PUERTO 7	PLANIFICACION
PA2-D8	14	PUERTO 8	PLANIFICACION
PA2-D9	14	PUERTO 9	PLANIFICACION
PA2-D10	14	PUERTO 10	PLANIFICACION
PA2-D11	14	PUERTO 11	PLANIFICACION
PA2-D12	14	PUERTO 12	PLANIFICACION
PA2-D13	14	PUERTO 13	PLANIFICACION
PA2-D14	14	PUERTO 14	PLANIFICACION
PA2-D15	14	PUERTO 15	PLANIFICACION

PA2-D16	14	PUERTO 16	PLANIFICACION
PA2-D17	14	PUERTO 17	PLANIFICACION
PA2-D18	14	PUERTO 18	PLANIFICACION
PA2-D19	14	PUERTO 19	PLANIFICACION
PA2-D20	14	PUERTO 20	PLANIFICACION
PA2-D21	14	PUERTO 21	PLANIFICACION
PA2-D22	14	PUERTO 22	PLANIFICACION
PA2-D23	14	PUERTO 23	PLANIFICACION
PA2-D24	52	PUERTO 24	WIFI
PA2-D25	14	PUERTO 25	PLANIFICACION
PA2-D26	14	PUERTO 26	PLANIFICACION
PA2-D27	14	PUERTO 27	PLANIFICACION
PA2-D28	14	PUERTO 28	PLANIFICACION
PA2-D29	14	PUERTO 29	PLANIFICACION
PA2-D30	14	PUERTO 30	PLANIFICACION
PA2-D31	14	PUERTO 31	PLANIFICACION
PA2-D32	14	PUERTO 32	PLANIFICACION
PA2-D33	14	PUERTO 33	PLANIFICACION
PA2-D34	14	PUERTO 34	PLANIFICACION
PA2-D35	14	PUERTO 35	PLANIFICACION
PA2-D36	14	PUERTO 36	PLANIFICACION
PA2-D37	14	PUERTO 37	PLANIFICACION
PA2-D38	14	PUERTO 38	PLANIFICACION
PA2-D39	14	PUERTO 39	PLANIFICACION
PA2-D40	14	PUERTO 40	PLANIFICACION
PA2-D41	14	PUERTO 41	PLANIFICACION
PA2-D42	14	PUERTO 42	PLANIFICACION
PA2-D109	14	PUERTO 43	PLANIFICACION
PA2-D110	44	PUERTO 44	BODEGA
PA2-D111	44	PUERTO 45	BODEGA
PA2-D113	44	PUERTO 46	BODEGA
PA2-D112	TRUNK	PUERTO 47	RADIO MUTUALISTA
		PUERTO 48	OBS: PUERTO 48 Y 52 TRUNK
PA2-D48		**170.20.4.8** (PUERTO 1)	
PA2-D49	34	PUERTO 2	GESTION AMBIENTAL
PA2-D50	34	PUERTO 3	GESTION AMBIENTAL
PA2-D51	34	PUERTO 4	GESTION AMBIENTAL
PA2-D52	34	PUERTO 5	GESTION AMBIENTAL
PA2-D53	34	PUERTO 6	GESTION AMBIENTAL
PA2-D54	34	PUERTO 7	GESTION AMBIENTAL
PA2-D55	34	PUERTO 8	GESTION AMBIENTAL

PA2-D56	34	PUERTO 9	GESTION AMBIENTAL
PA2-D57	34	PUERTO 10	GESTION AMBIENTAL
PA2-D58	34	PUERTO 11	GESTION AMBIENTAL
PA2-D59	34	PUERTO 12	GESTION AMBIENTAL
PA2-D60	34	PUERTO 13	GESTION AMBIENTAL
PA2-D61	34	PUERTO 14	GESTION AMBIENTAL
PA2-D62	34	PUERTO 15	GESTION AMBIENTAL
PA2-D63	34	PUERTO 16	GESTION AMBIENTAL
PA2-D64	18	PUERTO 17	RELACIONES PUBLICAS
PA2-D65	18	PUERTO 18	RELACIONES PUBLICAS
PA2-D66	18	PUERTO 19	RELACIONES PUBLICAS
PA2-D67	18	PUERTO 20	RELACIONES PUBLICAS
PA2-D68	34	PUERTO 21	GESTION AMBIENTAL
PA2-D69	34	PUERTO 22	GESTION AMBIENTAL
PA2-D70	34	PUERTO 23	GESTION AMBIENTAL
PA2-D71	34	PUERTO 24	GESTION AMBIENTAL
PA2-D72	36	PUERTO 25	RECURSOS HIDRICOS
PA2-D73	36	PUERTO 26	RECURSOS HIDRICOS
PA2-D74	36	PUERTO 27	RECURSOS HIDRICOS
PA2-D75	36	PUERTO 28	RECURSOS HIDRICOS
PA2-D76	36	PUERTO 29	RECURSOS HIDRICOS
PA2-D77	36	PUERTO 30	RECURSOS HIDRICOS
PA2-D78	36	PUERTO 31	RECURSOS HIDRICOS
PA2-D79	36	PUERTO 32	RECURSOS HIDRICOS
PA2-D80	36	PUERTO 33	RECURSOS HIDRICOS
PA2-D81	36	PUERTO 34	RECURSOS HIDRICOS
PA2-D82	36	PUERTO 35	RECURSOS HIDRICOS
PA2-D83	36	PUERTO 36	RECURSOS HIDRICOS
PA2-D84	36	PUERTO 37	RECURSOS HIDRICOS
PA2-D85	36	PUERTO 38	RECURSOS HIDRICOS
PA2-D86	36	PUERTO 39	RECURSOS HIDRICOS
PA2-D87	36	PUERTO 40	RECURSOS HIDRICOS
PA2-D88	36	PUERTO 41	RECURSOS HIDRICOS
PA2-D89	36	PUERTO 42	RECURSOS HIDRICOS
PA2-D90	36	PUERTO 43	RECURSOS HIDRICOS
PA2-D91	36	PUERTO 44	RECURSOS HIDRICOS
PA2-D92	36	PUERTO 45	RECURSOS HIDRICOS
PA2-D93	36	PUERTO 46	RECURSOS HIDRICOS
		PUERTO 47	OBS: PUERTO 47-48 TRUNK
		PUERTO 48	
PA2-D94	30	**172.16.4.9** (PUERTO 1)	DESARROLLO ECONOM

PA2-D95	30	PUERTO 2	DESARROLLO ECONOM
PA2-D96	30	PUERTO 3	DESARROLLO ECONOM
PA2-D97	30	PUERTO 4	DESARROLLO ECONOM
PA2-D98	30	PUERTO 5	DESARROLLO ECONOM
PA2-D99	30	PUERTO 6	DESARROLLO ECONOM
PA2-D100	18	PUERTO 7	RELACIONES PUBLICAS
PA2-D101	18	PUERTO 8	RELACIONES PUBLICAS
PA2-D102	18	PUERTO 9	RELACIONES PUBLICAS
PA2-D103	18	PUERTO 10	RELACIONES PUBLICAS
PA2-D104	18	PUERTO 11	RELACIONES PUBLICAS
PA2-D105	18	PUERTO 12	RELACIONES PUBLICAS
PA2-D106	18	PUERTO 13	RELACIONES PUBLICAS
PA2-D107	18	PUERTO 14	RELACIONES PUBLICAS
PA2-D108	18	PUERTO 15	RELACIONES PUBLICAS
PA2-D43		PUERTO 42	
PA2-D44		PUERTO 43	
PA2-D45		PUERTO 44	
PA2-D46		PUERTO 45	
PA2-D47		PUERTO 46	
		PUERTO 47	
		PUERTO 48	OBS: PUERTO 4748 TRUNK

Referencia: Basado en investigación teórica y práctica.

- Planta alta 1 PAS

Los puertos en el switch trece se encuentran distribuidos en la VLANs 38.

Tabla 66.- Nueva distribución de puntos de red plata alta 1 PAS

GPI-PLANTA BAJA			
PUNTOS	**VLAN**	**PUERTOS**	**NOMBRE**
PA1-D1	38	**170.20.4.13** (PUERTO 1)	PAS
PA1-D2	38	PUERTO 2	PAS
PA1-D3	38	PUERTO 3	PAS
PA1-D4	38	PUERTO 4	PAS
PA1-D5	38	PUERTO 5	PAS
PA1-D6	38	PUERTO 6	PAS
PA1-D7	38	PUERTO 7	PAS

PA1-D8	38	PUERTO 8	PAS
PA1-D9	38	PUERTO 9	PAS
PA1-D10	38	PUERTO 10	PAS
PA1-D11	38	PUERTO 11	PAS
PA1-D12	38	PUERTO 12	PAS
PA1-D13	38	PUERTO 13	PAS
PA1-D14	38	PUERTO 14	PAS
PA1-D15	38	PUERTO 15	PAS
PA1-D16	38	PUERTO 16	PAS
PA1-D17	38	PUERTO 17	PAS
PA1-D18	38	PUERTO 18	PAS
PA1-D19	38	PUERTO 19	PAS
PA1-D20	38	PUERTO 20	PAS
PA1-D21	38	PUERTO 21	PAS
PA1-D22	38	PUERTO 22	PAS
PA1-D23	38	PUERTO 23	PAS
PA1-D24	38	PUERTO 24	PAS
PA1-D25	38	PUERTO 25	PAS
PA1-D26	38	PUERTO 26	PAS
PA1-D27	38	PUERTO 27	PAS
PA1-D28	38	PUERTO 28	PAS
PA1-D29	38	PUERTO 29	PAS
PA1-D30	38	PUERTO 30	PAS
PA1-D31	38	PUERTO 31	PAS
PA1-D32	38	PUERTO 32	PAS
PA1-D33	38	PUERTO 33	PAS
PA1-D34	38	PUERTO 34	PAS
PA1-D35	38	PUERTO 35	PAS
PA1-D36	38	PUERTO 36	PAS
PA1-D37	38	PUERTO 37	PAS
PA1-D38	38	PUERTO 38	PAS
PA1-D39	38	PUERTO 39	PAS
PA1-D40	38	PUERTO 40	PAS
PA1-D41	38	PUERTO 41	PAS
PA1-D42	38	PUERTO 42	PAS
PA1-D109	38	PUERTO 43	PAS
PA1-D110	38	PUERTO 44	PAS
PA1-D111	38	PUERTO 45	PAS
PA1-D113	38	PUERTO 46	PAS
PA1-D112	38	PUERTO 47	PAS
		PUERTO 48	OBS: PUERTO 48 Y 52 TRUNK

Referencia: Basado en investigación teórica y práctica.

- Planta alta 2 PAS

Los puertos en el switch once se encuentran distribuidos en la VLANs 38 y 32

Tabla 67.- Nueva distribución de puntos de red plata alta 2 PAS

GPI-PLANTA BAJA			
PUNTOS	**VLAN**	**PUERTOS**	**NOMBRE**
PA2-D1	38	**170.20.4.12** (PUERTO 1)	PAS
PA2-D2	38	PUERTO 2	PAS
PA2-D3	38	PUERTO 3	PAS
PA2-D4	38	PUERTO 4	PAS
PA2-D5	38	PUERTO 5	PAS
PA2-D6	38	PUERTO 6	PAS
PA2-D7	38	PUERTO 7	PAS
PA2-D8	38	PUERTO 8	PAS
PA2-D9	38	PUERTO 9	PAS
PA2-D10	38	PUERTO 10	PAS
PA2-D11	38	PUERTO 11	PAS
PA2-D12	38	PUERTO 12	PAS
PA2-D13	38	PUERTO 13	PAS
PA2-D14	38	PUERTO 14	PAS
PA2-D15	38	PUERTO 15	PAS
PA2-D16	38	PUERTO 16	PAS
PA2-D17	38	PUERTO 17	PAS
PA2-D18	38	PUERTO 18	PAS
PA2-D19	38	PUERTO 19	PAS
PA2-D20	38	PUERTO 20	PAS
PA2-D21	38	PUERTO 21	PAS
PA2-D22	38	PUERTO 22	PAS
PA2-D23	38	PUERTO 23	PAS
PA2-D24	38	PUERTO 24	PAS
PA2-D25	38	PUERTO 25	PAS
PA2-D26	38	PUERTO 26	PAS
PA2-D27	38	PUERTO 27	PAS
PA2-D28	38	PUERTO 28	PAS
PA2-D29	38	PUERTO 29	PAS
PA2-D30	32	PUERTO 30	PAS

PA2-D31	32	PUERTO 31	TURISMO
PA2-D32	32	PUERTO 32	TURISMO
PA2-D33	32	PUERTO 33	TURISMO
PA2-D34	32	PUERTO 34	TURISMO
PA2-D35	32	PUERTO 35	TURISMO
PA2-D36	32	PUERTO 36	TURISMO
PA2-D37	32	PUERTO 37	TURISMO
PA2-D38	32	PUERTO 38	TURISMO
PA2-D39	32	PUERTO 39	TURISMO
PA2-D40	32	PUERTO 40	TURISMO
PA2-D41	32	PUERTO 41	TURISMO
PA2-D42	32	PUERTO 42	TURISMO
PA2-D109	32	PUERTO 43	TURISMO
PA2-D110	32	PUERTO 44	TURISMO
PA2-D111	32	PUERTO 45	TURISMO
PA2-D113	32	PUERTO 46	TURISMO
PA2-D112	TRUNK	PUERTO 47	
		PUERTO 48	OBS: PUERTO 48 Y 52 TRUNK

Referencia: Basado en investigación teórica y práctica.

Las demás plantas del edificio del PAS no se encuentran ocupadas, además se desconoce el uso futuro de estas instalaciones, por lo tanto dichos equipos no cuentan con configuraciones de puertos para acceso de determinadas VLANs.

ANEXO 04 CONFIGURACIÓN BASICA PARA SWITCHES DE CAPA ACCESO Y NÚCLEO CONTRAIDO

Las configuraciones básicas son válidas tanto para los switches de acceso como para el switch de Core, excepto el default Gateway el cual se configura en todos los switches de acceso pero no en el switch de core en la capa de núcleo contraído.

- **Nombre**

El nombre es una identificación para el switch, se utilizará los nombres designados en el diseño de VTP teniendo así switches con nombres de número del dos al catorce.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW_DOS
SW_DOS(config)#
SW_DOS(config)#
```

Imagen 82.-Configuración de nombre de switch acceso
Referencia: Basado en investigación teórica y práctica.

Enseguida de su configuración podemos mirar el cambio automático del nombre del switch, pero también podemos confirmar observando la configuración actual utilizando el comando show **running-config** donde se despliega la siguiente información:

```
!
hostname SW_DOS
!
```

Imagen 83.-Verificación del nombre en el switch de acceso DOS
Referencia: Basado en investigación teórica y práctica.

- **Banner**

El banner es un mensaje de bienvenida al momento de ingresar al equipo, nos permite presentar información referente al equipo.

```
SW_DOS#
SW_DOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_DOS(config)#banner motd c
Enter TEXT message.  End with the character 'c'.

*****************************ACCESO RESTRINGIDO*****************************
*************************GAD PROVINCIAL DE IMBABURA*************************
****************SWITCH DOS - PLANTA BAJA EDIFICIO CENTRAL******************

c

SW_DOS(config)#
```

Imagen 84.- Configuración de banner en switch acceso
Referencia: Basado en investigación teórica y práctica.

Podemos confirmar observando la configuración actual utilizando el comando show **running-config** donde se despliega la siguiente información:

```
!
banner motd ^C

*****************************ACCESO RESTRINGIDO*****************************
*************************GAD PROVINCIAL DE IMBABURA*************************
****************SWITCH DOS - PLANTA BAJA EDIFICIO CENTRAL******************

^C
!
```

Imagen 85.- Verificación de banner en switch acceso
Referencia: Basado en investigación teórica y práctica.

- **Contraseñas**

Existen algunas contraseñas que se pueden configurar como son: consola, telnet, ssh, contraseña encriptada.

Consola:

```
SW_DOS#
SW_DOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_DOS(config)#line console 0
SW_DOS(config-line)#password gpi@2016
SW_DOS(config-line)#login
SW_DOS(config-line)#exit
SW_DOS(config)#
SW_DOS(config)#exit
SW_DOS#
%SYS-5-CONFIG_I: Configured from console by console

SW_DOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_DOS(config)#enable password gpi@2016
SW_DOS(config)#enable secret gpi2016
SW_DOS(config)#
```

Imagen 86.- Configuración de contraseña de consola en switch acceso
Referencia: Basado en investigación teórica y práctica.

Habilitando telnet :

```
SW_DOS#
SW_DOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_DOS(config)#line vty 0 4
SW_DOS(config-line)#password gpi2016
SW_DOS(config-line)#login
SW_DOS(config-line)#
```

Imagen 87.- Configuración de contraseña de telnet en switch acceso
Referencia: Basado en investigación teórica y práctica.

Ssh:

```
SW_DOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_DOS(config)#username gpi71 password gpi71
SW_DOS(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
SW_DOS(config)#line vty 0 4
SW_DOS(config-line)#login local
SW_DOS(config-line)#transport input ssh
SW_DOS(config-line)#end
SW_DOS#
```

Imagen 88.- Configuración de contraseña de ssh en switch acceso
Referencia: Basado en investigación teórica y práctica.

Contraseña encriptada:

```
SW_DOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW_DOS(config)#service password-encryption
SW_DOS(config)#
SW_DOS(config)#
```

Imagen 89.- Configuración de contraseña encriptada en switch acceso
Referencia: Basado en investigación teórica y práctica.

Verificamos que la contraseña se encuentre encriptada utilizando el comando show **running-config** donde se despliega la siguiente información:

```
!
line con 0
 password 7 08265C47294B554644
 login
!
line vty 0 4
 password 7 08265C475B495441
 login local
 transport input ssh
line vty 5 15
 login
!
```

Imagen 90.- Verificación de contraseña encriptada en switch acceso
Referencia: Basado en investigación teórica y práctica.

- **Copiar configuración a NVRAM**

Las configuraciones actuales (running-config) se encuentran en la RAM y al utilizar este comando guardamos esta configuración a la NVRAM (startup-config), de tal forma que al iniciar nuevamente el equipo dichas configuraciones se haya guardado.

```
SW_DOS#
SW_DOS#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW_DOS#
SW_DOS#
```

Imagen 91.-Guardar configuración
Referencia: Basado en investigación teórica y práctica.

- **Desactivar la búsqueda DNS**

Si se escribe algo que no sea un comando de Cisco IOS o se comete un error, el switch asume que ha escrito un nombre de dominio y trata de resolver, el equipo se vuelve insensible durante unos cuantos segundos tratando de resolver el nombre, esto bloquea el teclado y no se puede configura en el equipo.

Imagen 92.- Desactivar la búsqueda DNS
Referencia: Basado en investigación teórica y práctica.

ANEXO 05 CAMBIO DE DIRECCIONAMIENTO FIREWALL ASA 5520

FIREWALL CISCO ASA 5520

Debido al cambio de direccionamiento de la red interna es necesario cambiar las configuraciones al firewall Asa 5520.

Para la configuración del firewall se lo realiza mediante el Adaptive Security Device Manager (ASDM[51]) que es el software administrador de dispositivos de Seguridad el cual permite realizar una configuración en modo gráfico, aunque también se puede realizar la configuración en modo consola. En este equipo se deben configurar las interfaces del firewall, routing, NAT y las reglas de acceso que permitirán o denegarán el acceso a los diferentes servicios.

- **Configuración de interfaces**

Las interfaces configuramos ingresando en la sección de configuración, seguido de interfaces, para configurar las interfaces ingresamos mediante **Edit** y agregamos las interfaces. Las interfaces a manejar serán 3, las mismas que tendrán un nivel de seguridad específico, se define una interfaz hacia la red externa OUTSIDE, otra para la red interna INSIDE y una para el manejo del equipo MANAGEMENT.

[51] ASDM=Adaptive Security Device Manager, dispositivo de manejo de seguridad

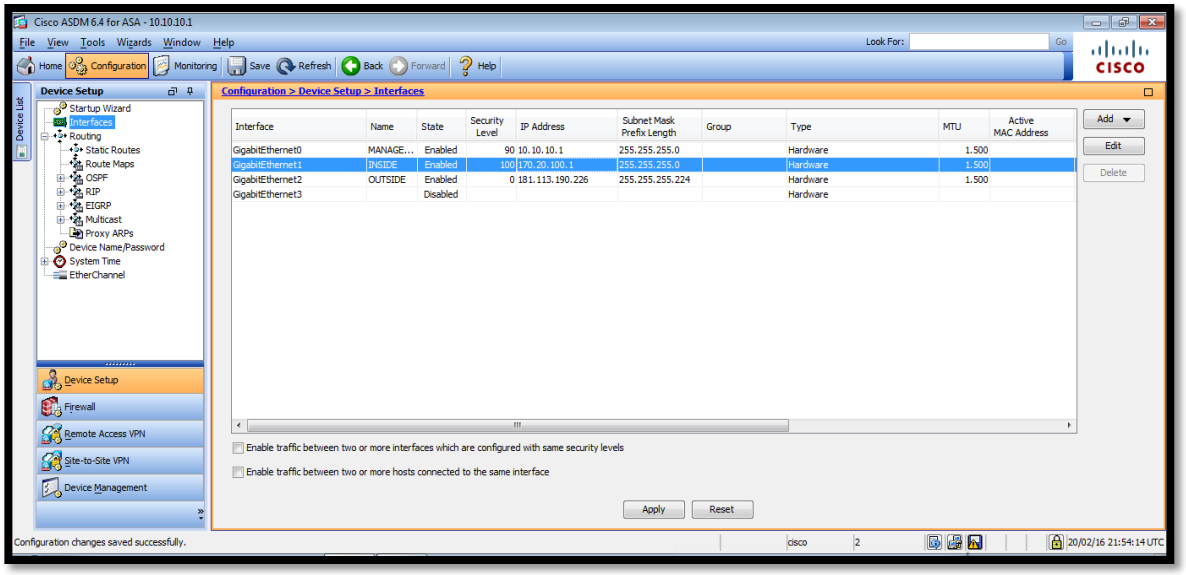


Imagen 93.-Configuración de interfaces.
Referencia: Basado en investigación teórica y práctica.

- **Routing**

El proceso de routing se lo realiza mediante la creación de rutas estáticas, permitiendo el tráfico desde la red interna INSIDE y todo el tráfico de la red OUTSIDE.

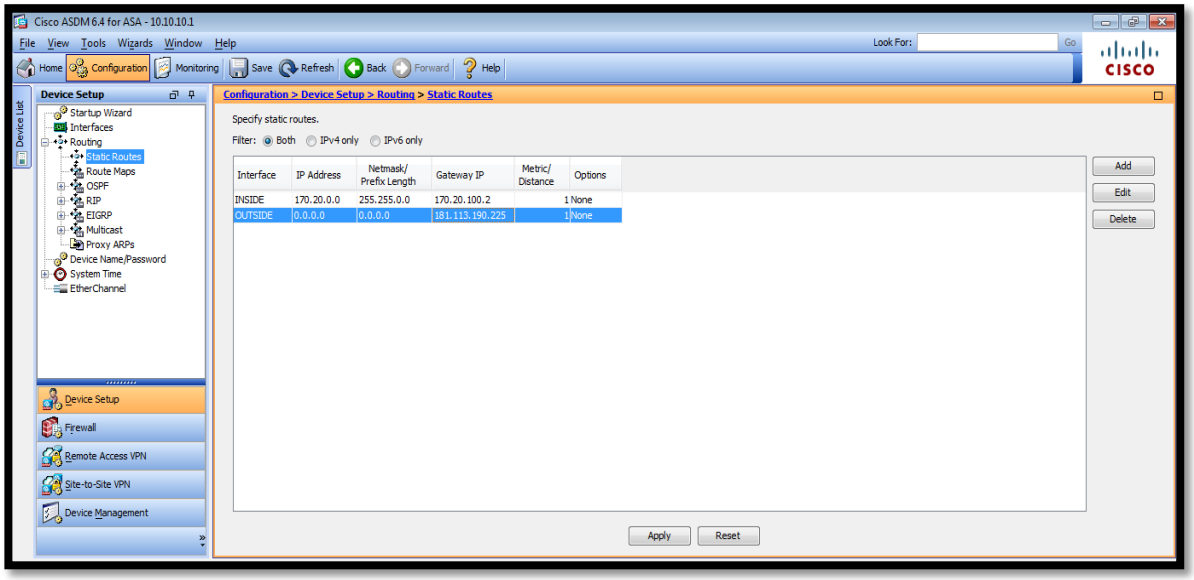


Imagen 94.- Configuración de rutas estáticas, ASA 5520
Referencia: Basado en investigación teórica y práctica.

- **NAT**

La configuración de NAT se realiza de acuerdo a los servidores que son de acceso de acceso interno y acceso externo, los que tienen acceso externo serán Nateados hacia las IP publicas correspondiente, como se indica en la siguiente imagen.

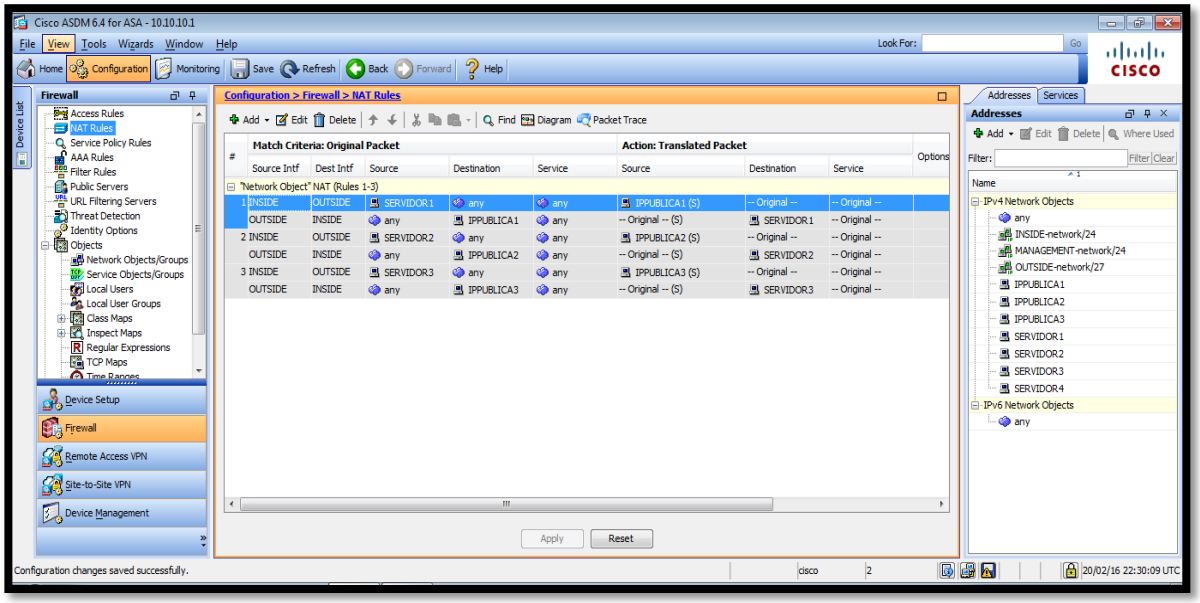


Imagen 95.- Configuración de NAT static.
Referencia: Basado en investigación teórica y práctica.

- **Access rules**

Las reglas de acceso implantadas se basan en los permisos y negaciones a los usuarios a diferentes servicios y por puertos específicos.

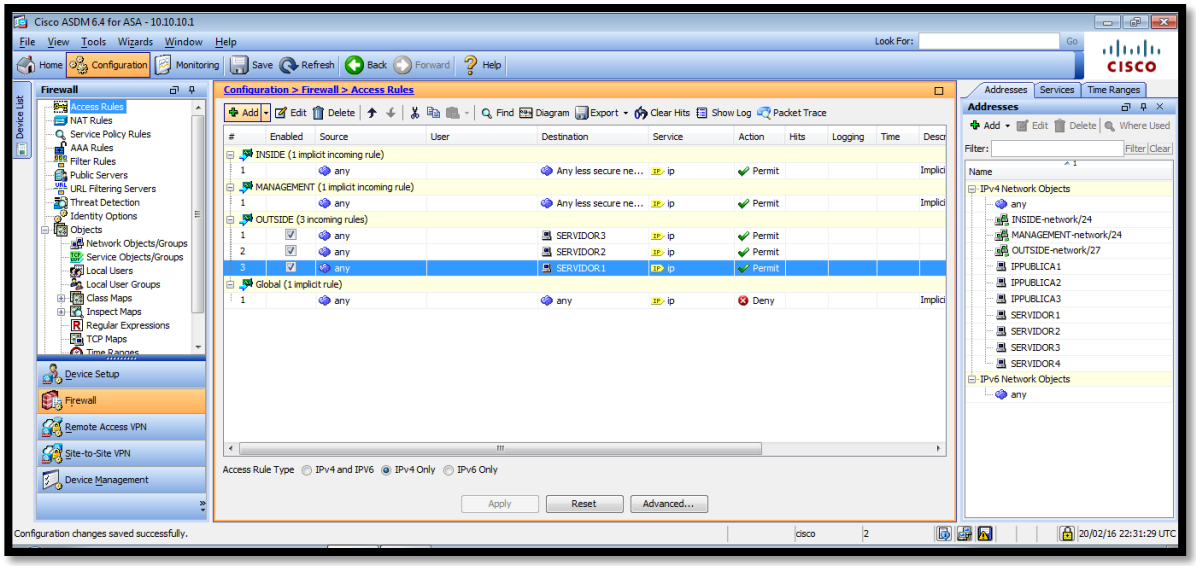


Imagen 96.-Configuración de reglas de acceso.
Referencia: Basado en investigación teórica y práctica.

ANEXO 06 CAMBIO DE DIRECCIONAMIENTO CHASIS BLADE

El chasis blade de la institución de es de marca HP de la serie c3000, en este equipo se cambia las direcciones IP configuradas debido al cambio de direccionamiento de la red interna.

Para ingresar a la configuración del equipo se lo realiza mediante HTTPS con la dirección IP actual y luego cambiamos las configuración del equipo, de cado uno de los Bay o cuchillas, la interconexión entre cuchillas.

- **Dirección de Chasis Blade**

Para cambiar la dirección del chasis blade nos dirigimos a Enclousure Information - Enclousure Settings – EnclousureTCP/IP Settings

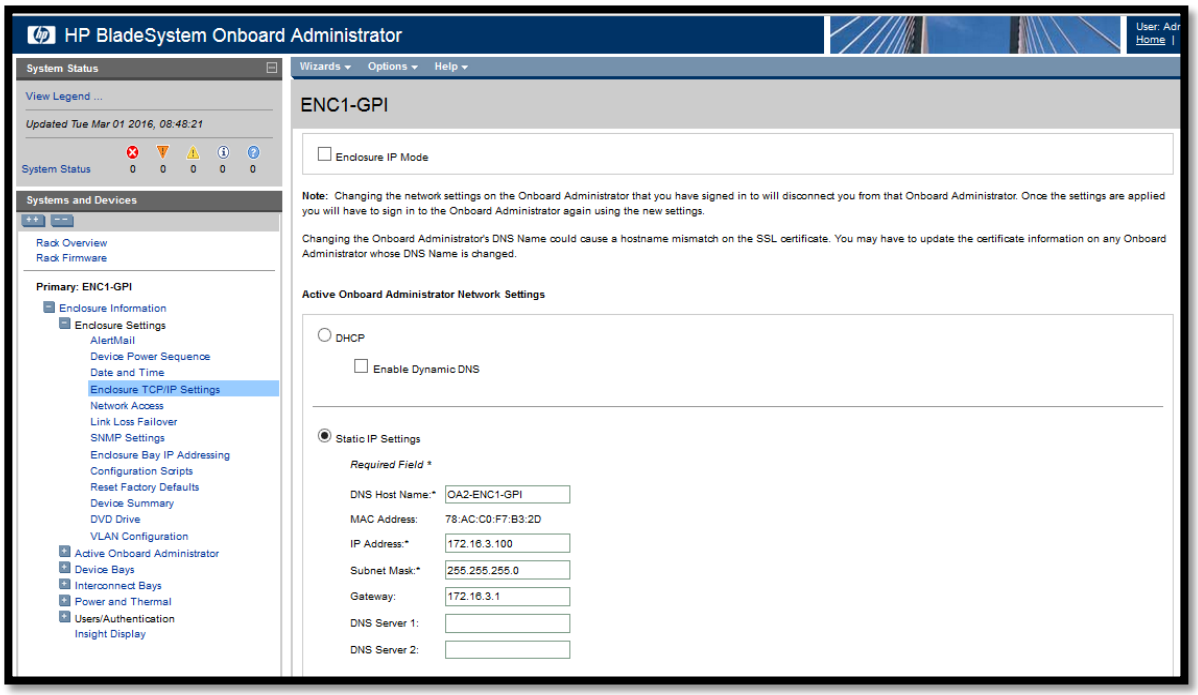


Imagen 97.- Cambio de dirección IP chasis blade HP c3000
Referencia: Basado en investigación teórica y práctica.

- Cambio de IP en las cuchillas

Para realizar el cambio de IP en las 8 cuchillas existentes nos dirigimos hacia Enclousure Information - Enclousure Settings - Enclousure Bay IP Addressing

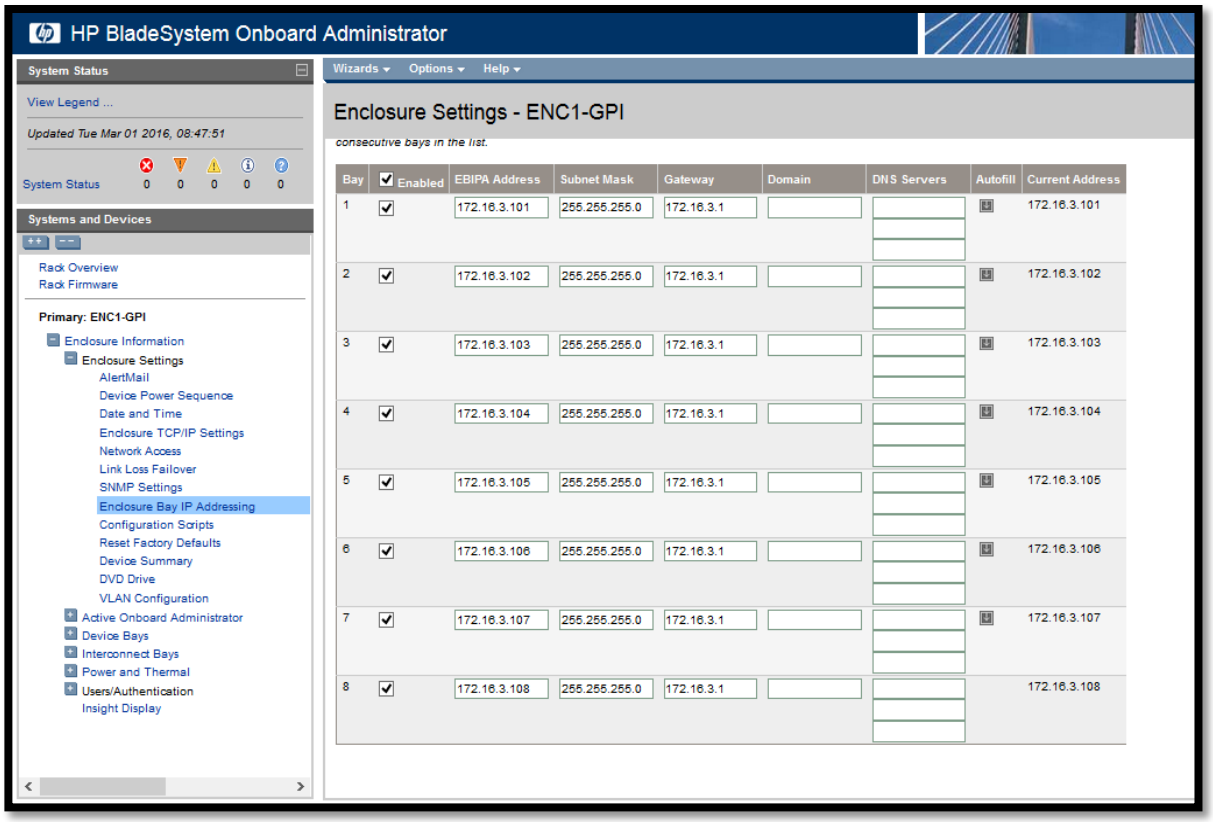


Imagen 98.- Cambio de direcciones IP cuchillas de chasis blade HP c3000
Referencia: Basado en investigación teórica y práctica.

- **Interconnect Bays**

Para cambiar las IP de interconexión de cuchillas se lo realiza en Enclousure Information - Enclousure Settings - Enclousure Bay IP Addressing – Interconect Bays

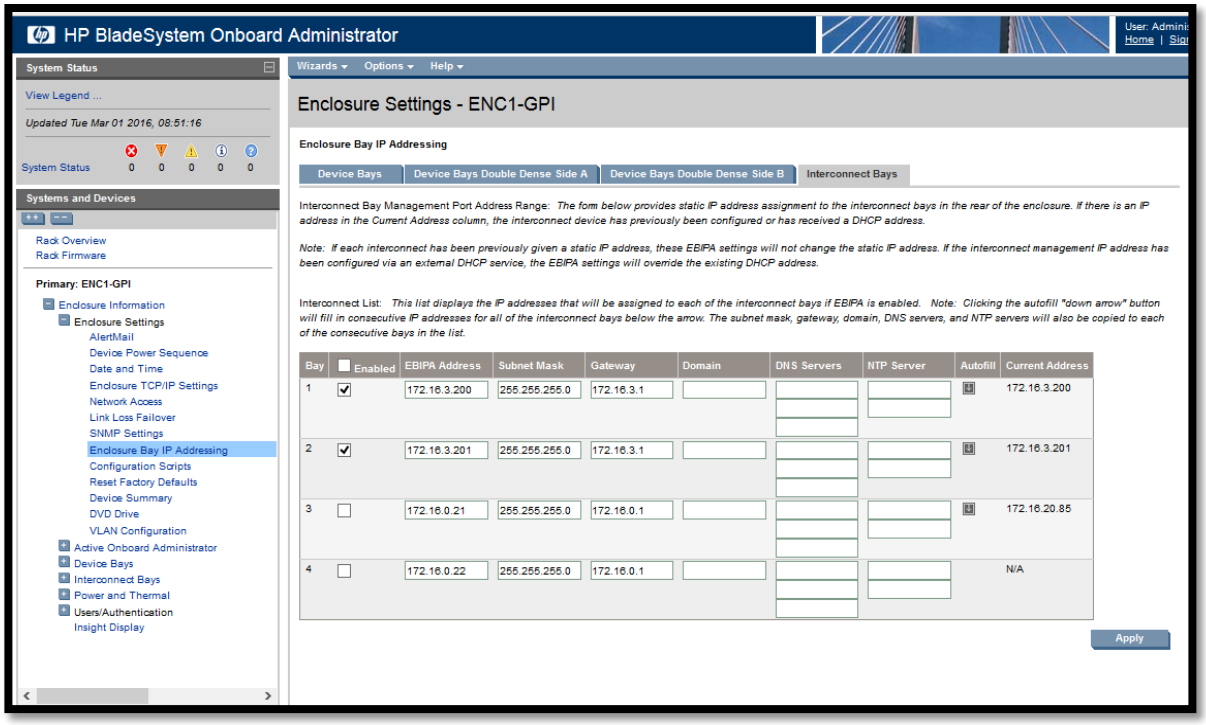


Imagen 99.- Cambio de direcciones IP interconexión cuchillas de chasis blade HP c3000
Referencia: Basado en investigación teórica y práctica.

ANEXO 07 GUIA DE SIMULACIÓN DEL DISEÑO DE RED.

Para demostrar el correcto funcionamiento del nuevo diseño de red, se ha realizado la simulación de la red en el programa Cisco Packet Tracer.

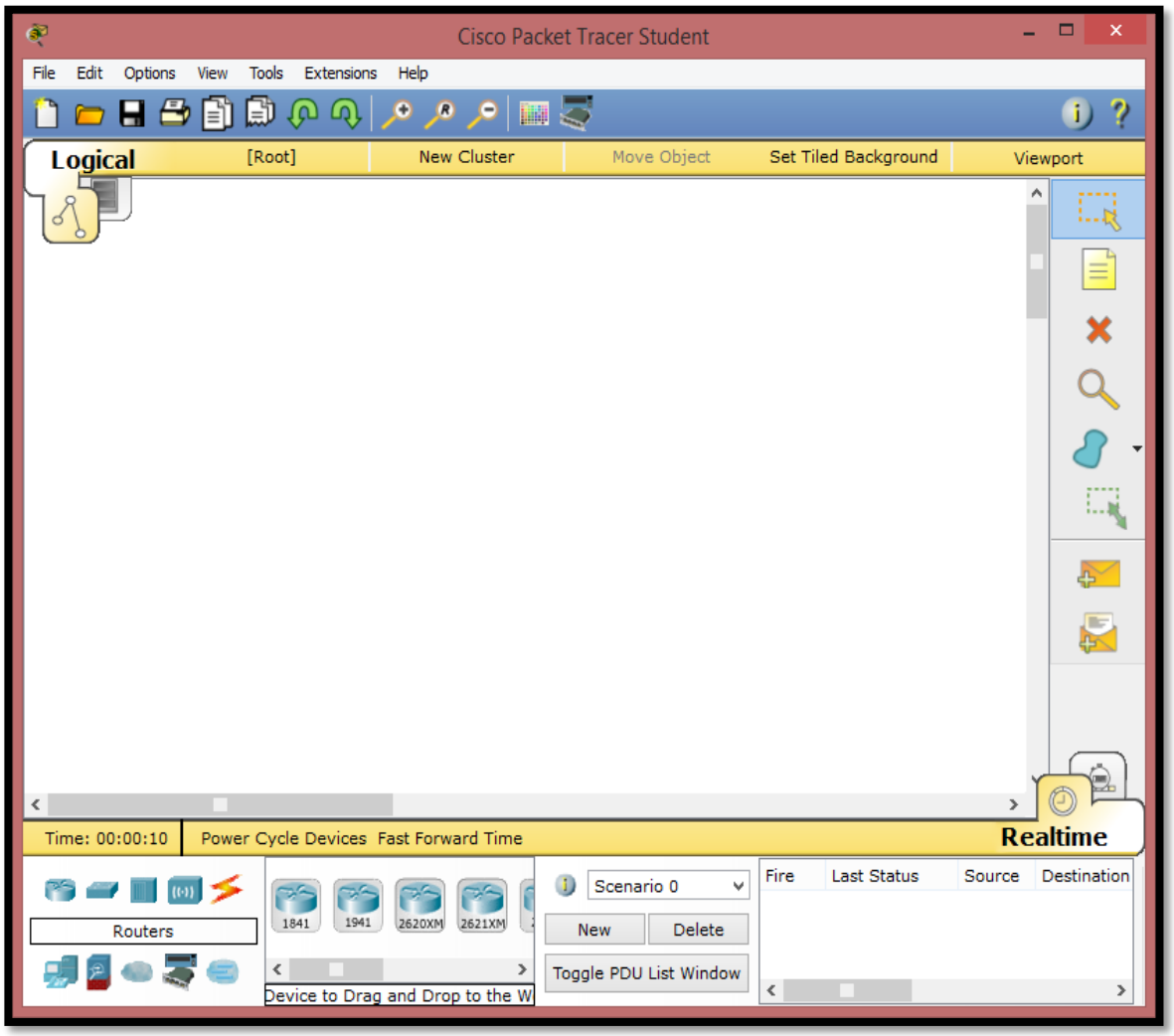


Imagen 100.- Programa Cisco Packet Tracer
Referencia: Basado en investigación teórica y práctica.

Cisco Packet Tracer, es una herramienta de simulación de redes para el aprendizaje de configuracion de equipos. Puede simular equipos de red como switches, routers, clouds, módems, equipos finales y otros.

La topología de red quedaría contemplada de la siguiente manera.

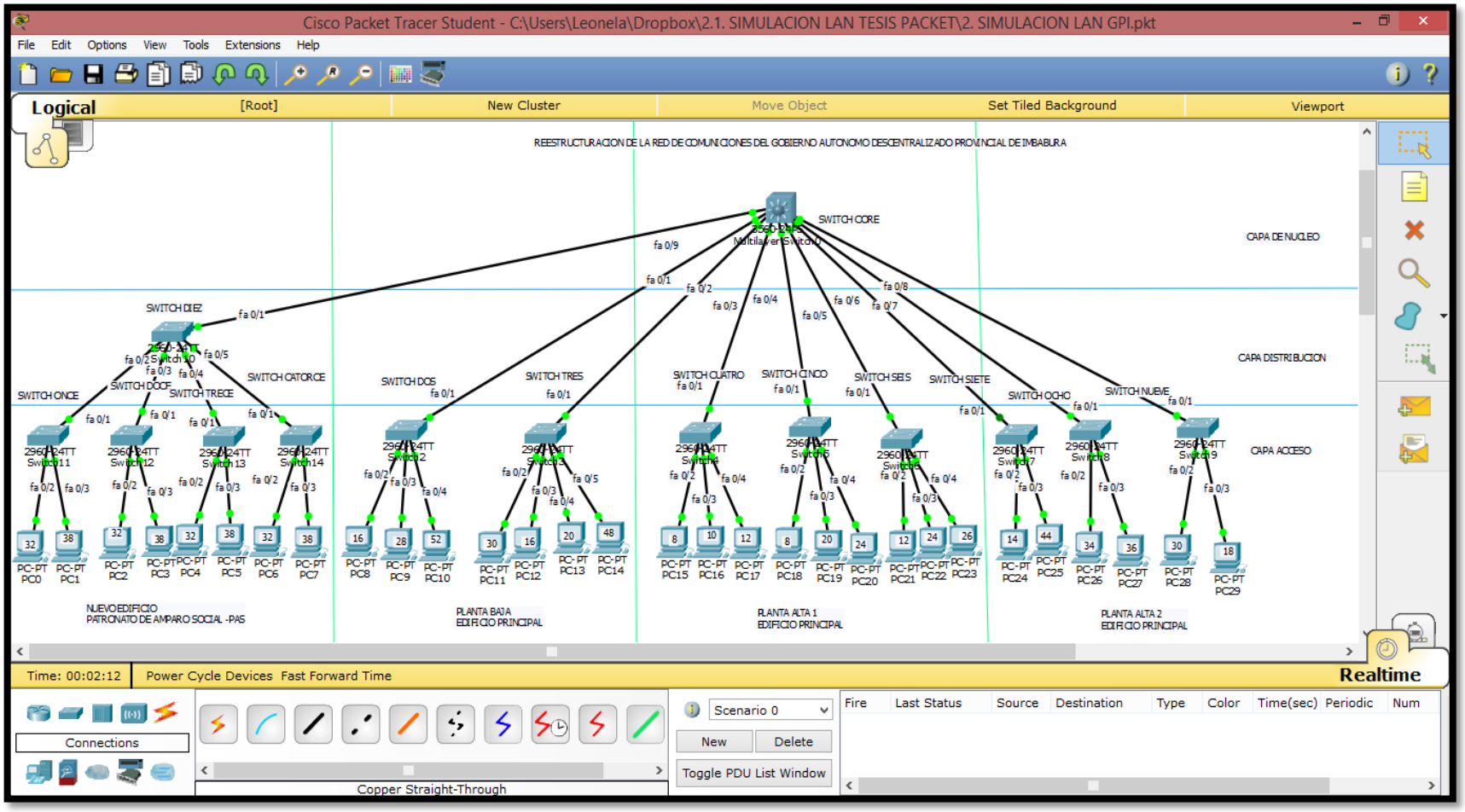


Imagen 101.-Topología en Packet Tracer de la red de comunicaciones del GAD Provincial de Imbabura.
Referencia: Basado en investigación teórica y práctica.

Para la simulación de red se ha empleado el switch 3560 como switch de core ya que tiene funcionalidades de capa 3; y los switches 2960 como switches de acceso en toda la red, a continuación se resume los equipos de red por cada planta.

Tabla 68.-Swithes de simulación

EQUIPO	UBICACIÓN	CAPA
1 Switch 3560	Planta alta 1	Núcleo contraído
2 Switches 2960	Planta baja	Acceso
3 Switches 2960	Planta alta 1	Acceso
3 Switches 2960	Planta alta 2	Acceso
1 Switches 2960	PAS	Distribución
4 Switches 2960	PAS	Acceso

Referencia: Basado en investigación teórica y práctica.

Para identificar los equipos dentro de la red se les ha asignado nombres los mismos que se indicó en el capítulo de diseño y se resume a continuación.

Tabla 69.-Nombres de equipos activos de red.

NOMBRE EQUIPO	UBICACIÓN
Switch dos	Planta baja
Switch tres	Planta baja
Switch cuatro	Planta alta 1
Switch cinco	Planta alta 1
Switch seis	Planta alta 1
Switch siete	Planta alta 2
Switch ocho	Planta alta 2
Switch nueve	Planta alta 2
Switch diez	PAS
Switch once	PAS
Switch doce	PAS
Switch trece	PAS
Switch catorce	PAS

Referencia: Basado en investigación teórica y práctica.

Para establecer la conexión física de la red, se ha designado puertos de cada switch para la unión entre equipos, los mismos que se indican a continuación.

Tabla 70.-Interfaces de unión de equipos activos de red.

UNION DE EQUIPOS	INTERFACES
Switch de core- switch dos	Fastethernet 0/1 - Fastethernet 0/1
Switch de core- switch tres	Fastethernet 0/2 - Fastethernet 0/1
Switch de core- switch cuatro	Fastethernet 0/3 - Fastethernet 0/1
Switch de core- switch cinco	Fastethernet 0/4 - Fastethernet 0/1
Switch de core- switch seis	Fastethernet 0/5 - Fastethernet 0/1
Switch de core- switch siste	Fastethernet 0/6 - Fastethernet 0/1
Switch de core- switch ocho	Fastethernet 0/7 - Fastethernet 0/1
Switch de core- switch nueve	Fastethernet 0/8 - Fastethernet 0/1
Switch de core- switch diez	Fastethernet 0/9 - Fastethernet 0/1
Switch diez - switch once	Fastethernet 0/2 - Fastethernet 0/1
Switch diez - switch doce	Fastethernet 0/3 - Fastethernet 0/1
Switch diez - switch trece	Fastethernet 0/4 - Fastethernet 0/1
Switch diez - switch catorce	Fastethernet 0/5 - Fastethernet 0/1

Referencia: Basado en investigación teórica y práctica.

Para establecer la conexión con las estaciones de trabajo, los puertos en los switches de acceso han sido designados a una VLAN y la estación de trabajo con una IP determinada, como se indica a continuación.

Tabla 71.-Interfaces de interconexión estaciones de trabajo.

SWITCH	INTERFAZ	VLAN	DIRECCION IP
Dos	Fastethernet 0/2	16	170.20.16.10
	Fastethernet 0/3	28	170.20.28.10
	Fastethernet 0/4	52	170.20.52.10
Tres	Fastethernet 0/2	30	170.20.30.10
	Fastethernet 0/3	16	170.20.16.20
	Fastethernet 0/4	20	170.20.20.10
	Fastethernet 0/5	48	170.20.48.10
Cuatro	Fastethernet 0/2	8	170.20.8.10
	Fastethernet 0/3	10	170.20.10.10

	Fastethernet 0/4	12	170.20.12.10
Cinco	Fastethernet 0/2	8	170.20.8.20
	Fastethernet 0/3	20	170.20.20.20
	Fastethernet 0/4	24	170.20.24.10
Seis	Fastethernet 0/2	12	170.20.12.20
	Fastethernet 0/3	24	170.20.24.20
	Fastethernet 0/4	26	170.20.26.10
Siete	Fastethernet 0/2	14	170.20.14.10
	Fastethernet 0/3	44	170.20.44.10
Ocho	Fastethernet 0/2	34	170.20.34.10
	Fastethernet 0/3	36	170.20.36.10
Nueve	Fastethernet 0/2	20	170.20.20.30
	Fastethernet 0/3	18	170.20.18.10
Once	Fastethernet 0/2	32	170.20.32.10
	Fastethernet 0/3	38	170.20.38.10
Doce	Fastethernet 0/2	32	170.20.32.20
	Fastethernet 0/3	38	170.20.38.20
Trece	Fastethernet 0/2	32	170.20.32.30
	Fastethernet 0/3	38	170.20.38.30
Catorce	Fastethernet 0/2	32	170.20.32.40
	Fastethernet 0/3	38	170.20.38.40

Referencia: Basado en investigación teórica y práctica.

Para el acceso a los equipos activos, en el diseño de red se determinó diferentes contraseñas que garanticen el acceso confiable, las mismas que se resumen en la tabla siguiente.

Tabla 72.-Contraseñas de equipos activos de red.

EQUIPOS	CONSOLA	ENABLE	ENABLE SECRET	TELNET	SSH
CORE	C0re@2016	C0re@2016	C0re#2016	Cor3#@2016	Gpi#71
SW_DOS	Gpi2@2016	Gpi2@2016	Gpi2#2016	Gpi2#@2016	Gpi#72
SW_TRES	Gpi3@2016	Gpi3@2016	Gpi3#2016	Gpi3#@2016	Gpi#73
SW_CUATRO	Gpi4@2016	Gpi4@2016	Gpi4#2016	Gpi4#@2016	Gpi#74
SW_CINCO	Gpi5@2016	Gpi5@2016	Gpi5#2016	Gpi5#@2016	Gpi#75
SW_SEIS	Gpi6@2016	Gpi6@2016	Gpi6#2016	Gpi6#@2016	Gpi#76

SW_SIETE	Gpi7@2016	Gpi7@2016	Gpi7#2016	Gpi7#@2016	Gpi#77
SW_OCHO	Gpi8@2016	Gpi8@2016	Gpi8#2016	Gpi8#@2016	Gpi#78
SW_NUEVE	Gpi9@2016	Gpi9@2016	Gpi9#2016	Gpi9#@2016	Gpi#79
SW_DIEZ	Gpi10@2016	Gpi10@2016	Gpi10#2016	Gpi10#@2016	Gpi#710
SW_ONCE	Gpi11@2016	Gpi11@2016	Gpi11#2016	Gpi11#@2016	Gpi#711
SW_DOCE	Gpi12@2016	Gpi12@2016	Gpi12#2016	Gpi12#@2016	Gpi#712
SW_TRECE	Gpi13@2016	Gpi13@2016	Gpi13#2016	Gpi13#@2016	Gpi#713
SW_CATORCE	Gpi14@2016	Gpi14@2016	Gpi14#2016	Gpi14#@2016	Gpi#714

Referencia: Basado en investigación teórica y práctica.

- **CONFIGURACIONES**

Una vez establecida la topología física de la red contemplando todos los datos antes mencionados sobre sus puertos de conexión, se procede a realizar los parámetros de diseño planteados con el siguiente orden para garantizar que las configuraciones se realicen de forma correcta.

1. Realizamos las configuraciones básicas de los equipos activos de red que son:
    - Nombre
    - Banner
    - Contraseñas
        - Consola
        - Enable
        - Enable secret
        - Habilitación telnet
        - Ssh
        - Contraseña encriptada

- Copiar configuración a NVRAM
- Desactivar la búsqueda DNS

2. Configuración de las interfaces entre switches en modo trunk.
3. Establecimiento VTP
    - VTP server
    - VTP cliente
    - Creación de VLANs
4. Configuración de las interfaces entre switches de acceso y equipos finales en modo acceso.
5. Configuración de la tarjeta de red de los equipos finales.
6. Configuración de gateway de VLAN
7. Establecimiento del default gateway
8. Configuración de interfaces de administración
9. Establecimiento de Pvst+
10. Definición de la seguridad por puertos (port security)
11. Configuración de Access-list.
12. Configuración de DHCP para la VLAN inalámbrica.