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

L. Félix Autor, C. Vásquez Director
Facultad de Ingeniería en Ciencias Aplicadas, Universidad Técnica del Norte
Ibarra, Ecuador
alfelix@utn.edu.ec cavasquez@utn.edu.ec

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.

Abstract—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.

Índice de Términos — IPv4, IPv6, Transición, Doble pila lite, DNS64, NAT64, CEDIA.

I. INTRODUCCIÓN

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.

II. CONCEPTOS BÁSICOS

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).

A. 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).

- 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.
- 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.

B. 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).

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) Clases de direcciones 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 1 se indica las clases de direcciones IPv4 con su respectiva porción de red y porción de host.

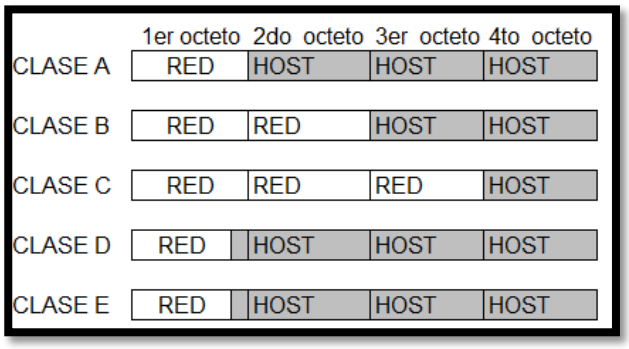

Imagen 1. Asignación de porción de red y host en cada clase de red.

3) Números de host y 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.

número de redes=2^n Ecuación (1)

número de hosts=2^n-2 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

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 cómo se nuestra en la Imagen 2.

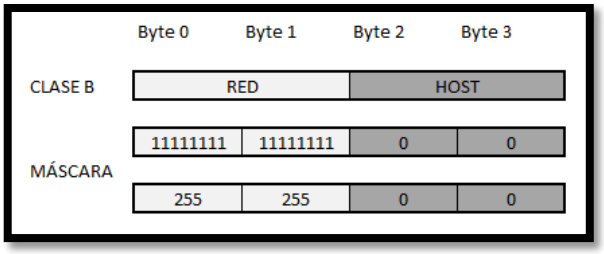

Imagen 2. Máscara de red para una dirección clase B

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).

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

C. 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.

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) 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.

- Datacenter

"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.

- 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.

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.

- 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.

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.

- 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.
- Servidores: 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

D. 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.

1) Capas de una red jerárquica

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

- Capa 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.
- 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.
- Capa 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 3.

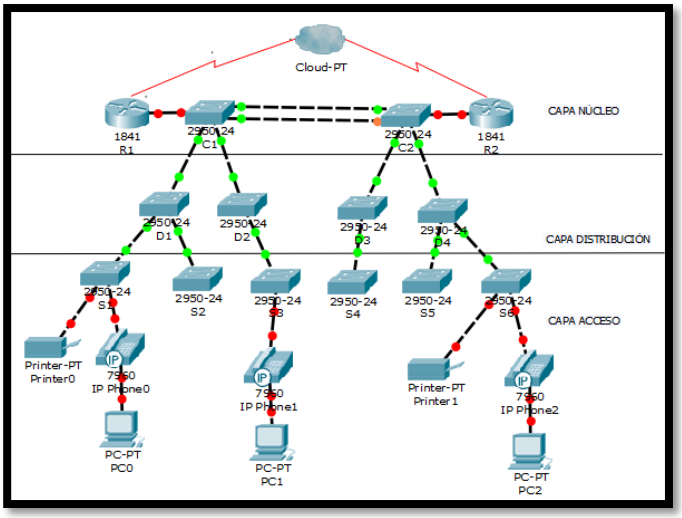

Imagen 3. Capas de una red jerárquica.

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.

3) Principios 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.

- 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.
- 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.
- 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.

E. 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:

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 2:

Tabla 2. 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 a cada VLAN, es conveniente cuando existen

	muchos cambios en la red, configuración compleja.

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

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 3.

Tabla 3. 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.

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 4.

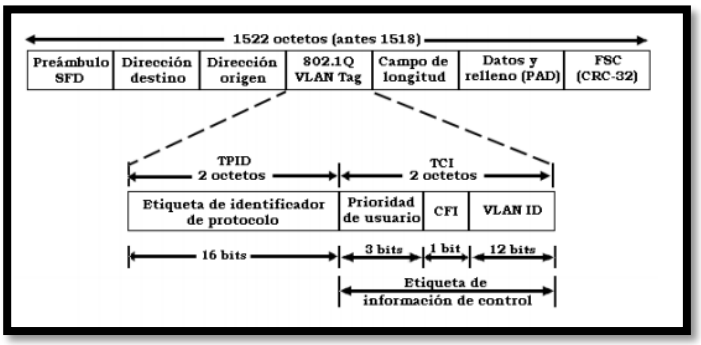

Imagen 4. Trama Ethernet con el protocolo 802.1 Q

Según (Gómez Martín , García Reionoso, & Valera Pintor) "El campo agregado por 802.1Q consta de dos partes el TPID campo de etiqueta de identificador de protocolo y TCI 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.- "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.- Indica el número de VLAN al que pertenece.

El campo TPID consta de 2 octetos y se establece en 0x8100 para especificar que la etiqueta que sigue es 802.1Q

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.

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.

6) Spanning Tree PVST +

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.

7) Listas de control de acceso

Según (Delgado Freire, 2011) "Una ACL 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.

8) 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).

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

Constan los diseños de la topología física y lógica de la red de comunicaciones, basado en los aspectos analizados en el levantamiento de información.

A. Diseño de la topología física de red

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 5 se muestra la nueva topología física para la red de la institución

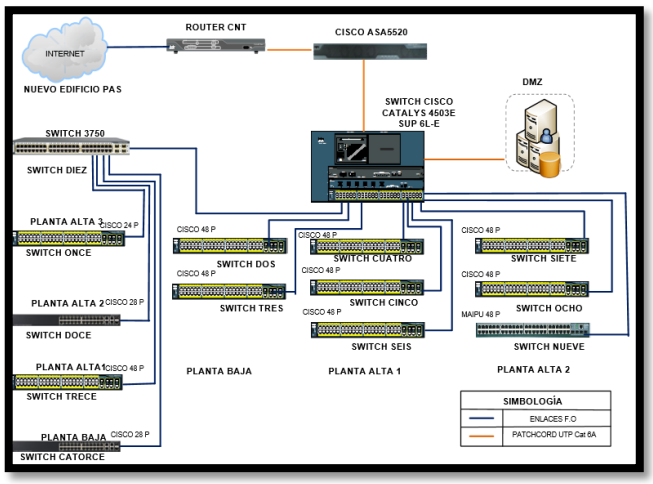

Imagen 5. Nueva topología física de red del GAD Provincial de Imbabura.

1) 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

2) 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.

3) 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) 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.

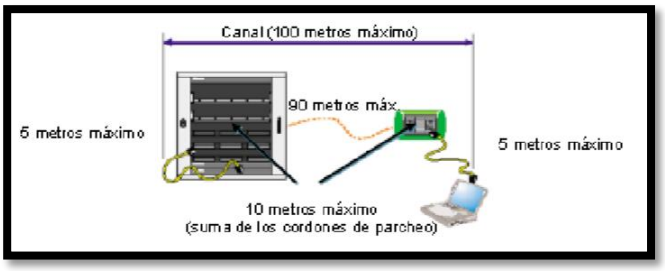

Imagen 6. Distribución horizontal del cableado

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

5) 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.

B. Diseño de la topología lógica de red

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.

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 4.

Tabla 4. 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

2) Topología lógica de red

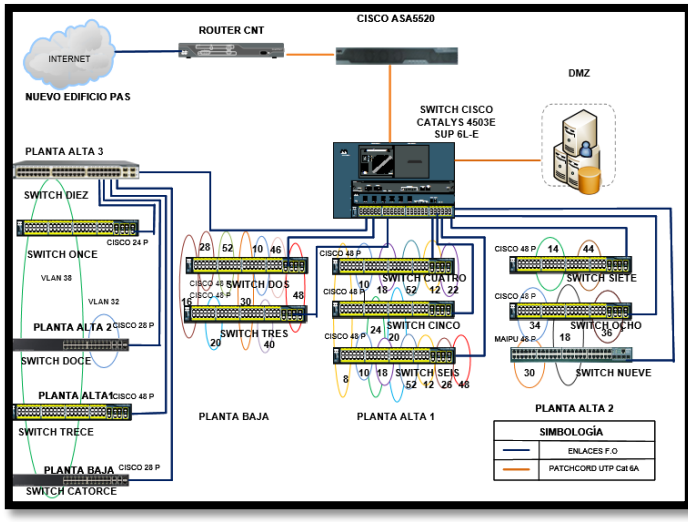

Imagen 7. Diseño de topología lógica de red.

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 Imagen 8.

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
ADMINISTRACION	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

Imagen 8. Nuevo direccionamiento IP basado en la creación de nuevas VLANs.

C. 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 5

Tabla 5. Nombres switches de acceso y núcleo contraído

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

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 9.

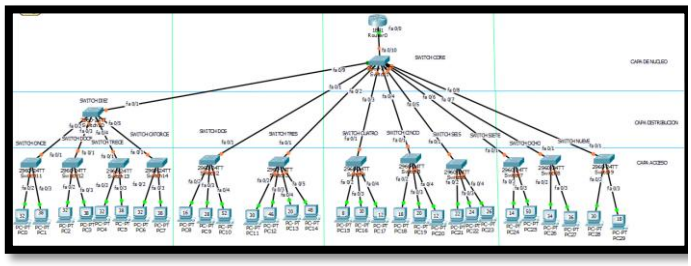

Imagen 9. Modelo jerárquico para la red del GAD Provincial de Imbabura

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 6:

Tabla 6. 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

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.

- VLAN trunking protocol – VTP cliente

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 7.

Tabla 7. 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

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.

- 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.

- 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

- 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 interfaces.

2) Capa núcleo contraído

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.

- 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) quedando las VLANs de la siguiente manera, ver Tabla 8.

Tabla 8. 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

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.

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.

- 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 9 se indica la asignación de los puertos para modo acceso y modo troncal.

Tabla 9. 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

- Protocolo 802.1 Q

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 10 se indica la VLAN y su Gateway de VLAN.

Tabla 10. 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

- 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.

- 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.

IV. IMPLEMENTACIÓN DE LOS NUEVOS DISEÑOS FÍSICO Y LÓGICO DE LA RED

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

A. Cableado estructurado

Las área de cableado estructurado que tienen reestructuración son las siguientes

1) Instalaciones 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 muestra en la Imagen 10.

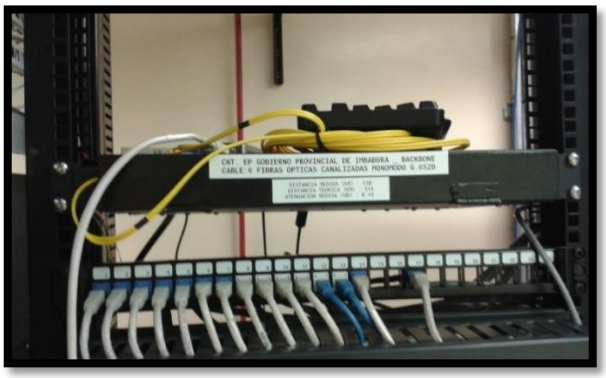

Imagen 10. Conexión hacia el nuevo edificio PAS.

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.

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 11 se indica el techo falso de la planta baja de la institución por donde se pasó el cable de la distribución horizontal

Imagen 11. Distribución horizontal en techo falso

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 12.

Imagen 12. Distribución horizontal en techo falso

4) Área 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 13.

Imagen 13. Instalación puntos de red

B. Configuración 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 11 se indican los equipos con las respectivas configuraciones a implementar:

Tabla 11. 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.

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 14 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 14. Configuración de puertos en modo trunk en switch acceso

Para verificar la configuración del puerto lo realizamos con el comando **show running-config** como se indica en la Imagen 15 o con el comando **show interface trunk** como se indica en la Imagen 15.

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

Imagen 15.- Verificación de puerto en modo trunk en running-config

```
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 16.- Verificación de puerto en modo trunk en interfaces trunk

- Puertos en modo trunk switch de Core

Los puertos en modo trunk son 9, uno para cada switch de acceso de todas las plantas y su configuración se la realiza como se indica en la Imagen 17.

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

Para verificar la configuración del puerto lo realizamos con el comando show running-config o con el comando show interface trunk.

2) VLAN trunking protocol

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

- 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 18.

```
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 18.- Configuración de VTP Server en switch core

- Creación de VLANs

En el switch de core se configura la creación de las VLANs que manejará la red, en la Imagen 19 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 19. Creación de VLANs switch de core.

- 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 20. 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 20. Configuración de Gateway de VLAN para la VLAN PREFECTURA.

- 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 21.

```
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 21. Configuración de VTP Client en switch acceso

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 22 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 22. Verificación de VTP Client en switch acceso

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 23.

```
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 23. Verificación de VLANs propagadas en switch de acceso.

3) Equipos capa de 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:

- 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

- 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 12. 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

La configuración de la interfaz de administración se indica en la Imagen 24 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 24. Configuración de interfaz de administración en switch acceso.

Para verificar la configuración de la interfaz de administración se lo realiza con el comando show **running-config** como se indica en la Imagen 25.

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

Imagen 25. Verificación de configuración de interfaz de administración.

- 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 válidas 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 26.- Configuración de puertos en modo access en switch acceso

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 27.- Verificación de puerto en modo access.

- 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 28.

```
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 28.-Configuración de un rango de puertos

- 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 29.

```
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 29.- Configuración de puertos para la VLAN de voz en switch acceso

- 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 30.

```
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 30.- Configuración de default Gateway en switch acceso

- PVST+

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 31.

```
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 31.-Configuración para establecer PVST+ rápido como el modo STP – switch CUATRO

Para verificar la configuración lo realizamos mediante el comando **show running-config** donde se obtiene la siguiente información, ver Imagen 32.

```
!
!
spanning-tree mode pvst
!
```

Imagen 32.-Verificación del PVST+
Referencia: Basado en investigación teórica y práctica.

- 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 33.

```
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 33.-Configuración de port-security mediante sticky secure

Para verificar su configuración se realiza mediante el comando **show running-config** como se indica en la Imagen 34 o con el comando **show port-security**

```
!
interface FastEthernet0/4
 switchport access vlan 16
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/5
 switchport access vlan 28
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/6
 switchport access vlan 52
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
```

Imagen 34.-Verificación de sticky secure antes de reconocer las MAC

En la Imagen 35 se muestra la verificación mediante el comando show running-config luego de que la interfaz haya aprendido la dirección MAC segura.

```
!
interface FastEthernet0/4
 switchport access vlan 16
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00E0.B0ED.0580
!
interface FastEthernet0/5
 switchport access vlan 28
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0001.4311.5258
!
interface FastEthernet0/6
 switchport access vlan 52
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00D0.5831.D080
!
```

Imagen 35.- Verificación de sticky secure después de reconocer las MAC

También podemos verificar mirando la configuración por cada interfaz como se indica en la Imagen 36.

```
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 36.- 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 37.

```
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 37.- Verificación de direcciones MAC aprendidas.

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 38 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.

```
SW_DOS#show port-security interface fastEthernet 0/4
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 00D0.9723.4A6D:16
Security Violation Count   : 1

SW_DOS#
```

Imagen 38.- Violación de puerto

En la Imagen 39 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 39.-Rehabilitación de interfaz

.

4) Equipo capa núcleo contraído

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:

- 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

- 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 40.

```
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 40.- Configuración interfaz de administración switch de core
Referencia: Basado en investigación teórica y práctica.

- DHCP VLAN de voz

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 41.

```
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 41.- Configuración de DHCP para la VLAN inalámbrica

- 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.

- 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 38.

```
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 42.- Configuración para establecer PVST+ rápido como el modo STP – switch de Core

Luego configuramos al switch de Core como primario para las VLANs establecidas como se indica en la Imagen 43.

```
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 43.- Configuración de switch de Core como primario para las VLANs establecidas.

Para verificar la configuración lo realizamos mediante el comando **show running-config** o mediante **show spanning-tree**.

- 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 44.

```
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip access-list standard ACCESO-EQUIPOS
Switch(config-std-nacl)#permit 170.20.8.0 0.0.0.255
Switch(config-std-nacl)#deny any
Switch(config-std-nacl)#exit
Switch(config)#end
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#line vty 0 4
Switch(config-line)#access-class ACCESO-EQUIPOS in
Switch(config-line)#login local
Switch(config-line)#transport input ssh
Switch(config-line)#end
Switch#
```

Imagen 44.-Configuración de lista de acceso

V. CONCLUSIONES Y RECOMENDACIONES

A. 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.

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.

B. 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.

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.

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.

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.

VI. REFERENCIAS

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.

PÁGINAS 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

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

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.

Amada Félix Autor Nació en Pablo Arenas Urcuquí el 22 de octubre de 1992, reside en Ibarra provincia de Imbabura. Realizo sus estudios secundarios en el colegio Nacional "Ibarra", obteniendo el título de bachiller en la especialidad de Físico Matemático. Actualmente, es egresada de la Universidad Técnica del Norte en la Carrera de Ingeniería en Electrónica y Redes de Comunicación.

Ing. C. Vásquez Director Es un profesional en Ingeniería Electrónica y Telecomunicaciones. Actualmente es docente de la Facultad de Ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte en áreas como: Networking, WLAN, Fibra Óptica entre otras áreas relacionadas.