UNIVERSIDAD SAN PEDRO

VICERRECTORADO ACADÉMICO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERIA INFORMÁTICA Y DE SISTEMAS

Segmentación de la red virtual en la empresa Agro Industrial Paramonga S.A.A.

Tesis para obtener el título profesional de

Ingeniero en informática y de sistemas

AUTOR:

Bach. Elmer Gerard Salazar Cochachin

ASESOR:

Dr. Javier Martínez Carrión

BARRANCA - PERÚ

2019

INDICE

PALABRAS CLAVES

TEMA	VLANS
ESPECIALIDAD	REDES Y COMUNICACIONES

KEYWORDS

THEME	VLANS
SPECIALTY	TIC.

LINEA DE INVESTIGACIÓN

Línea	Infraestructura de tecnología de la información
Sub línea	Redes y comunicaciones
Disciplina	Telecomunicaciones

TÍTULO:

SEGMENTACIÓN DE LA RED VIRTUAL EN LA EMPRESA AGRO INDUSTRIAL PARAMONGA S.A.A.

RESUMEN

El presente proyecto de investigación tuvo como objetivo implementar la segmentación de la red virtual (VLANS), con el apoyo de un Switch CORE y un conjunto de Switch Cisco administrables con mayores capacidades para el uso de aplicaciones y tráfico de datos que requieran mayor carga en la red, tales como la videoconferencia en LAN, copias de respaldo en tiempos menores, uso extensivo de los servicios de intranet (web, correo, multimedia, etc.), telefonía ip, cámaras de seguridad, y todos los Access Point existentes en la red.

La investigación es de tipo descriptivo no experimental con corte transversal, para el desarrollo de la investigación se aplicó la metodología Cisco; el mayor fabricante de equipos de red, donde describe las múltiples fases por las que una red atraviesa utilizando el llamado ciclo de vida de redes PPDIO (Preparación - Planificación – Diseño – Implementación –Operación).

Al incorporar el uso de vlan en la red, permitió que los usuarios accedan a su red respectiva (vlan) a través de sus propias cuentas (id de active Directory), sea cual fuera el puerto de red donde ellos se conecten garantizando la fluidez de las comunicaciones por cable e inalámbricas, dado a los protocolos de seguridad de la información transmitida y recibida.

ABSTRACT

The present project of investigation had as aim implement the segmentation of the virtual network (VLANS), with the support of a Switch CORE and a set of Switch I Dirty administrable with major capacities for the use of applications and traffic of information that need major load in the network, such as the videoconference in LAN, copies of support in minor times, extensive use of the services of intranet (web, mail, multimedia, etc.), telephony ip, safety chambers, and all the existing Access Point in the network.

The Cisco methodology was applied; the largest manufacturer of network equipment, describing the multiple phases through which a network crosses using the so-called PDIOO network lifecycle (Planning - Design - Implementation - Operation - Optimization).

By incorporating the use of vlan in the network, it allows users to access their respective network (vlan) through their own accounts (Active Directory id), regardless of the network port where they connect, guaranteeing the fluidity of cable and wireless communications, given to the security protocols of transmitted and received information.

1. INTRODUCCIÓN

Se revisó la investigación de Céspedes Velasco Jorge Enrique (2012) denominada **"Red De Datos Para Las Comunicaciones En El Hospital Básico De Pelileo".** El presente proyecto de investigación se realizó observando las necesidades del HOSPITAL BÁSICO DE LA CIUDAD DE PELILEO en envió y recepción de datos, en seguridad tanto de equipos como de personas, por lo que nace la necesidad de diseñar una eficiente red de datos. La investigación tiene por objetivo diseñar una red de datos para las comunicaciones en el Hospital Básico de la ciudad de Pelileo. En la cual su prioridad es la comunicación de datos entre las diferentes dependencias del Hospital. Para el presente proyecto se empleó la Metodología CISCO, es una metodología que propone cuatro Fases, para el diseño de redes. El diseño está enfocado en mejorar las comunicaciones internas del Hospital mediante una moderna red de datos, como también facilitar al personal técnico del Hospital en el mantenimiento.

También se revisó la investigación de Omar Jorge Hernández Jiménez, Marco Antonio Huerta Carmona (2014) denominada **"Actualización de una red local plana una red local segura, segmentada con servicios de voz y datos en IFAI".** Desarrolló su tesis en base a la adquisición de nuevos equipos de telecomunicaciones, con la finalidad de proporcionar a una institución una mejora en su plataforma de servicios de voz y datos actuales, los objetivos principales a cumplir son la seguridad, la escalabilidad, la calidad de servicio, teniendo en cuenta la infraestructura actual y un crecimiento a futuro. El uso de la metodología Cisco ayudó a entender todo el diseño físico y lógico de todo el proyecto. Se logró obtener con los equipos de comunicación un mejor control de la administración y seguridad de la red, con la finalidad de proporcionar un servicio integrado de voz y datos, obteniendo así una reducción en los costos, al no instalar los servicios por separado.

También se revisó la investigación de Félix Leonardo Rojas Yovera (2016) denominada **"Propuesta Para La Implementación De La Red De Datos En La Municipalidad Distrital De Tamarindo".** Tuvo como objetivo elaborar una

propuesta para la implementación de la red de datos en la Municipalidad Distrital de Tamarindo, año 2016, para optimizar los servicios de conectividad. La investigación tuvo un diseño no experimental, siendo el tipo de investigación descriptivo y de corte transversal. El modelo de referencia OSI es una base de referencia para la definición de arquitecturas de interconexión de sistemas de comunicación. En este modelo, las funciones de comunicación se distribuyen en un conjunto jerárquico por capas y cada capa realiza un conjunto de tareas relacionadas entre sí. El alcance de esta investigación logró el beneficio de todos los usuarios de la Municipalidad Distrital de Tamarindo. Planteando la propuesta de mejora, en la cual se realizó la propuesta técnica y económica del proyecto

También se revisó la investigación de Ochoa, C. (2012) denominada **"Implementación de un diseño de puente inalámbrico punto multi punto para la mejora de la interconexión de las áreas de la Empresa Plásticos Rímac SRL",** de la Universidad Católica Santo Toribio de Mogrovejo, Chiclayo - Perú. El trabajo se basa en la propuesta de un puente inalámbrico Punto Multipunto que permitirá la mejora de enlazar de las áreas de la empresa Plásticos Rímac S.R.L., entonces con el estudio realizado sobre el análisis de la red actual y equipos con los que cuenta la empresa. La metodología usada para este proyecto fue OSSTMM, Open Source Security Testing Methodology, manual que divide en secciones las cuales se subdividen a su vez en módulos. Se logró un diseño de red que cumpla con los requisitos necesarios para su correcto enlace con las demás sucursales y así logrando reducir gastos generados por el uso de servicios como el internet, teléfono y pasajes de transportes de las áreas de la empresa para el envío de información.

También se revisó la investigación de Liseth Ccelia Bravo Valero (2015) denominada **"Modelo diagnóstico y análisis de la red LAN para la mejora del rendimiento y seguridad en la red de salud Valle del Mantaro".** Este diagnóstico y análisis se realiza con el objetivo de conocer cuáles son los problemas que existen actualmente y proponer una solución a través de un nuevo diseño de red que cumpla con los requerimientos de la institución. Para el desarrollo del proyecto se utiliza la metodología CISCO, que desarrolla en 4 fases fundamentales: Análisis de

requerimientos, Diseño Lógico de la red, Diseño Físico y Pruebas, Optimización y Documentar el diseño de la red. El proyecto permitió abrir y profundizar la investigación tecnológica que brinda la red en la empresa y organización. Comprometiéndose con el buen desempeño laboral de los trabajadores.

La presente investigación se justifica científicamente porque busca conocimientos selectivos y sistematizados para explicar racionalmente como implementar la segmentación de la red virtual (Vlans), y contribuir a la mejora del tráfico de la información, facilitando a los usuarios la comunicación de datos en todas las actividades realizadas en las diferentes áreas de la empresa. Finalmente, la investigación se justifica de manera social, porque busca dar mejora a las actividades realizadas por los usuarios de la empresa Agro Industrial Paramonga, dada a la implementación de la red virtual (Vlans), como también de manera indirecta se verán beneficiados los clientes externos y por ende la sociedad que está en contacto con la organización.

En la Empresa Agro Industrial Paramonga S.A.A. existen diferentes problemas, como:
La infraestructura Tecnológica actual de AIPSAA no cuenta con una gestión y administración de equipos de comunicación óptima, en la actualidad la red no se encuentra gestionada, ya que no existe segmentación (VLANS) ni monitoreo de los eventos que se producen diariamente dentro de la red (identificación de hosts, asignación de direcciones ip, acceso a servicios de red, etc.).
La red de Datos es una red Plana, no se encuentra segmentada y dividida para prestar servicios óptimos de telefonía, transmisión de datos, internet, etc.
Cabe señalar que los Switchs permanecen con la función básica de solo brindar acceso a la red de datos.
También se ha encontrado que conviven 4 segmentos de red IP.
10.100.16.0/23 correspondiente a red de datos (PCS, servidores y otros equipos de cómputo)
10.100.17.0/23 correspondiente a red de datos (PCS y otros equipos de cómputo)
10.100.18.0/22 red utilizada para la red de Switchs administrables
10.100.46.0/24 red correspondiente a los Teléfonos IP

Todas conviven dentro de todo el gran segmento de RED sin ser administradas.
Después de realizar un análisis sobre los problemas que aquejan a la Empresa Agro Industrial Paramonga S.A.A. considero el más importante para la realización del proyecto el siguiente problema: No cuenta con una gestión y administración de equipos de comunicación óptima, ya que no existe segmentación (VLANS), produciendo demora en la comunicación de datos. Frente a este problema es que se formula la siguiente pregunta:
¿Cómo implementar la segmentación de la red virtual Lan (Vlans) para la comunicación de datos en las diferentes áreas de la Empresa Agro Industrial Paramonga S.A.A.?

Para una mejor comprensión de la investigación es importante saber conocer y entender, algunos conceptos que se estarán manejando dentro de este trabajo.

Open Systems Interconnection (1984): Es un modelo de red descriptivo de siete capas definido por la ISO, que asegura compatibilidad e interoperabilidad entre varias tecnologías de red producidas por diferentes compañías, lo que permite trabajar de manera independiente sobre funciones de red separadas y por ende disminuir su complejidad y acelerar su evolución. Este modelo está formado por siete capas, cada una de las cuales realiza funciones diferentes, queson:

CAPA FÍSICA: la más baja del modelo OSI, se encarga de la transmisión y recepción de una secuencia no estructurada de bits sin procesar a través de un medio físico. Describe las interfaces eléctricas/óptica, mecánica y funcional al medio físico, y lleva las señales hacia el resto de las capas superiores. Proporciona:

Codificación de datos: modifica el modelo de señal digital sencilla (1s y 0s) que utiliza el equipo para acomodar mejor las características del medio físico y para ayudar a la sincronización entre bits y trama. Determina:

Qué estado de la señal representa un binario 1
Como sabe la estación receptora cuándo empieza un "momento bit"
Cómo delimita la estación receptora una trama
Anexo al medio físico, con capacidad para varias posibilidades en el medio:

¿Se utilizará un transceptor externo (MAU) para conectar con el medio?
¿Cuántas patillas tienen los conectores y para qué se utiliza cada una de ellas?
Técnica de transmisión: determina si se van a transmitir los bits codificados por señalización de banda base (digital) o de banda ancha (analógica).
Transmisión en el medio físico: transmite bits como señales eléctricas u ópticas adecuadas para el medio físico y determina lo siguiente.
Qué opciones de medios físicos pueden utilizarse
Cuántos voltios/db se deben utilizar para representar un estado de señal en particular mediante un medio físico determinado

CAPA DE VÍNCULO DE DATOS. La capa de vínculo de datos ofrece una transferencia sin errores de tramas de datos desde un nodo a otro a través de la capa física, permitiendo a las capas por encima asumir virtualmente la transmisión sin errores a través del vínculo. Para ello, la capa de vínculo de datos proporciona:
Establecimiento y finalización de vínculos: establece y finaliza el vínculo lógico entre dos nodos.

Control del tráfico en tramas: indica al nodo de transmisión que "dé marcha atrás" cuando no haya ningún búfer de trama disponible.
Secuenciación de tramas: transmite y recibe tramas secuencialmente.
Confirmación de trama: proporciona o espera confirmaciones de trama. Detecta errores y se recupera de ellos cuando se producen en la capa física mediante la retransmisión de tramas no confirmadas y el control de la recepción de tramas duplicadas.

Delimitación de trama: crea y reconoce los límites de la trama.
Comprobación de errores de trama: comprueba la integridad de las tramas recibidas.
Gestión de acceso a medios: determina si el nodo "tiene derecho" a utilizar el medio físico.

CAPA DE RED. La capa de red controla el funcionamiento de la subred, decidiendo qué ruta de acceso física deberían tomar los datos en función de las condiciones de la red, la prioridad de servicio y otros factores. Proporciona:
Enrutamiento: enruta tramas entre redes.

Control de tráfico de subred: los enrutadores (sistemas intermedios de capa de red) pueden indicar a una estación emisora que "reduzca" su transmisión de tramas cuando el búfer del enrutador se llene.

Fragmentación de tramas: si determina que el tamaño de la unidad de transmisión máxima (MTU) que sigue en el enrutador es inferior al tamaño de la trama, un enrutador puede fragmentar una trama para la transmisión y volver a ensamblarla en la estación de destino.

Asignación de direcciones lógico-físicas: traduce direcciones lógicas, o nombres, en direcciones físicas.

Contabilidad del uso de la subred: dispone de funciones de contabilidad para realizar un seguimiento de las tramas reenviadas por sistemas intermedios de subred con el fin de producir información de facturación.

SUBRED DE COMUNICACIONES. El software de capa de red debe generar encabezados para que el software de capa de red que reside en los sistemas intermedios de subred pueda reconocerlos y utilizarlos para enrutar datos a la dirección de destino.

Esta capa libera a las capas superiores de la necesidad de tener conocimientos sobre la transmisión de datos y las tecnologías de conmutación intermedias que se utilizan para conectar los sistemas de conmutación. Establece, mantiene y finaliza las conexiones entre las instalaciones de comunicación que intervienen (uno o varios sistemas intermedios en la subred de comunicación).

En la capa de red y las capas inferiores, existen protocolos entre pares entre un nodo y

su vecino inmediato, pero es posible que el vecino sea un nodo a través del cual se enrutan datos, no la estación de destino. Las estaciones de origen y de destino pueden estar separadas por muchos sistemas intermedios.

CAPA DE TRANSPORTE. La capa de transporte garantiza que los mensajes se entregan sin errores, en secuencia y sin pérdidas o duplicaciones. Libera a los protocolos de capas superiores de cualquier cuestión relacionada con la transferencia de datos entre ellos y sus pares.

El tamaño y la complejidad de un protocolo de transporte dependen del tipo de servicio que pueda obtener de la capa de transporte. Para tener una capa de transporte confiable con una capacidad de circuito virtual, se requiere una mínima capa de transporte. Si la capa de red no es confiable o solo admite datagramas, el protocolo de transporte debería incluir detección y recuperación de errores extensivos.

La capa de transporte proporciona:

Segmentación de mensajes: acepta un mensaje de la capa (de sesión) que tiene por encima, lo divide en unidades más pequeñas (si no es aún lo suficientemente pequeño) y transmite las unidades más pequeñas a la capa de red. La capa de transporte en la estación de destino vuelve a ensamblar el mensaje.

Confirmación de mensajes: proporciona una entrega de mensajes confiable de extremo a extremo con confirmaciones.

Control del tráfico en mensajes: indica a la estación de transmisión que "dé marcha atrás" cuando no haya ningún búfer de mensaje disponible.

Multiplexación de sesión: multiplexa varias secuencias de mensajes, o sesiones, en un vínculo lógico y realiza un seguimiento de qué mensajes pertenecen a qué sesiones (consulte la capa de sesiones).

Normalmente, la capa de transporte puede aceptar mensajes relativamente grandes, pero existen estrictas limitaciones de tamaño para los mensajes impuestas por la capa

de red (o inferior). Como consecuencia, la capa de transporte debe dividir los mensajes en unidades más pequeñas, o tramas, anteponiendo un encabezado a cada una de ellas.

Así pues, la información del encabezado de la capa de transporte debe incluir información de control, como marcadores de inicio y fin de mensajes, para permitir a la capa de transporte del otro extremo reconocer los límites del mensaje. Además, si las capas inferiores no mantienen la secuencia, el encabezado de transporte debe contener información de secuencias para permitir a la capa de transporte en el extremo receptor recolocar las piezas en el orden correcto antes de enviar el mensaje recibido a la capa superior.

Capas de un extremo a otro.
A diferencia de las capas inferiores de "subred" cuyo protocolo se encuentra entre nodos inmediatamente adyacentes, la capa de transporte y las capas superiores son verdaderas capas de "origen a destino" o de un extremo a otro, y no les atañen los detalles de la instalación de comunicaciones subyacente. El software de capa de transporte (y el software superior) en la estación de origen lleva una conversación con software similar en la estación de destino utilizando encabezados de mensajes y mensajes de control.

CAPA DE SESIÓN. La capa de sesión permite el establecimiento de sesiones entre procesos que se ejecutan en diferentes estaciones. Proporciona:

Establecimiento, mantenimiento y finalización de sesión: permite que dos procesos de aplicación en diferentes equipos establezcan, utilicen y finalicen una conexión, que se denomina sesión.

Soporte de sesión: realiza las funciones que permiten a estos procesos comunicarse a través de una red, ejecutando la seguridad, el reconocimiento de nombres, el registro, etc.

CAPA DE PRESENTACIÓN. La capa de presentación da formato a los datos que deberán presentarse en la capa de aplicación. Se puede decir que es el traductor de la red. Esta capa puede traducir datos de un formato utilizado por la capa de la aplicación

a un formato común en la estación emisora y, a continuación, traducir el formato común a un formato conocido por la capa de la aplicación en la estación receptora.

La capa de presentación proporciona:
Traducción del código de caracteres, por ejemplo, de ASCII a EBCDIC. Conversión de datos: orden de bits, CR-CR/LF, punto flotante entre enteros, etc. Compresión de datos: reduce el número de bits que es necesario transmitir en la red. Cifrado de datos: cifra los datos por motivos de seguridad. Por ejemplo, cifrado de contraseñas.

CAPA DE APLICACIÓN. El nivel de aplicación actúa como ventana para los usuarios y los procesos de aplicaciones para tener acceso a servicios de red. Esta capa contiene varias funciones que se utilizan con frecuencia:
Uso compartido de recursos y redirección de dispositivos
Acceso a archivos remotos
Acceso a la impresora remota
Comunicación entre procesos
Administración de la red
Servicios de directorio
Mensajería electrónica (como correo)
Terminales virtuales de red

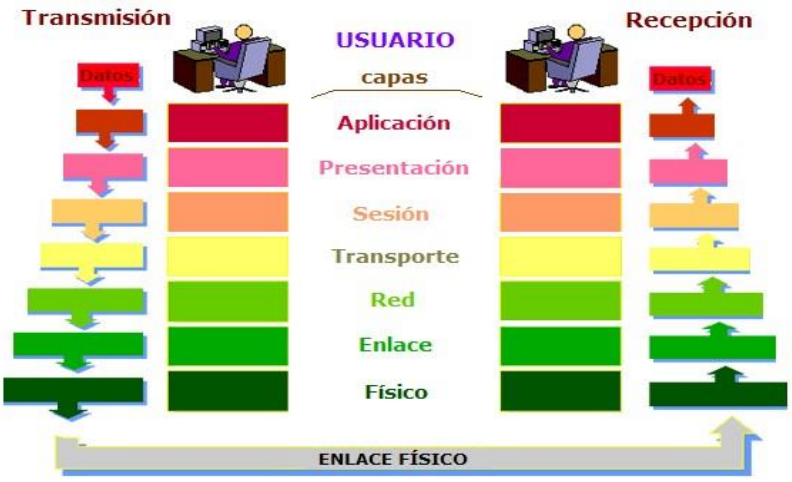


Figura 01: "Las 7 capas del modelo OSI"
Fuente: alegsa.com.ar

Dispositivos de Red

William Stallings (2000). Señala que existen dos clasificaciones, la primera clasificación son los **dispositivos de usuario final,** como por ejemplo computadoras, impresoras, scanners y otros dispositivos que provean servicios directamente al usuario.

Estos dispositivos son conectados físicamente a la red usando una Network Interface Card (NIC) que tiene su propio código o dirección MAC. La segunda clasificación son los dispositivos de red.

Los **dispositivos de red** proveen la comunicación entre dispositivos de usuario final. Como por ejemplo:

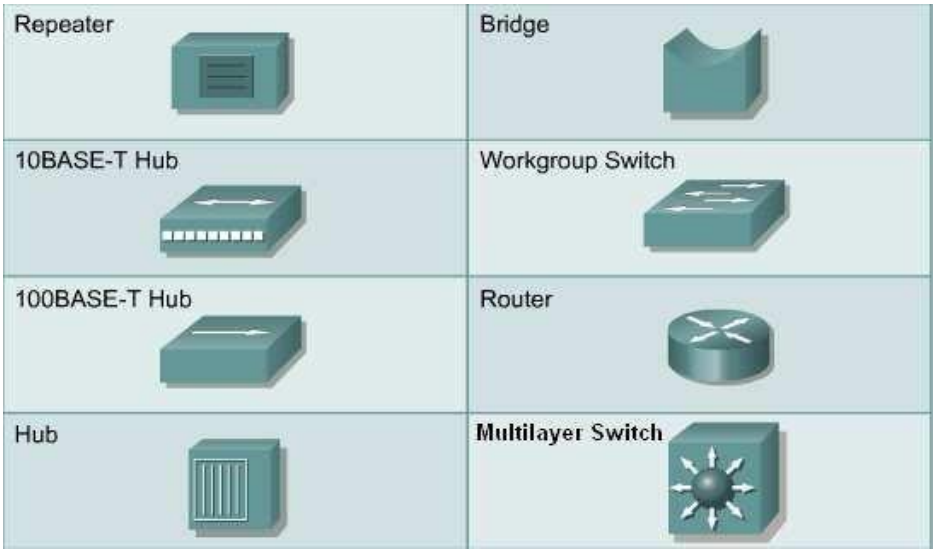


Figura 02: "Iconos de los dispositivos de Red
Fuente: http://www.cisco.com/web/learning/netacad

Repetidor. Es un dispositivo de red usado para regenerar una señal. Regeneran señales analógicas o digitales distorsionadas por la pérdida de transmisión debido a la atenuación. Es un dispositivo de capa 1.

Hub. Dispositivo de capa 1 que permite la concentración de varios dispositivos dentro de un solo dominio de colisión o segmento. Regenera y amplifica las señales de datos para todos los dispositivos conectados, excepto para el dispositivo que originalmente

envió la señal. También es conocido como un repetidor multipuerto, que extiende los dominios de colisión.

Bridge. Es un dispositivo de capa 2 que separa dominios de colisión, porque analiza las direcciones MAC para determinar si las tramas de datos pueden o no cruzar entre dos segmentos de red. Para lograr esto, el bridge aprende las direcciones MAC de los dispositivos en cada segmento conectado. Además, este dispositivo puede convertir formatos de transmisión de datos, lo cual no puede realizar un switch de capa 2.

Switch. Andrew s. Tanenbaum- 4ta. Ed. (2003). Menciona que es un dispositivo de capa 2 y puede ser referido como un bridge multipuerto. Los switches toman las decisiones de envío basadas en las direcciones MAC contenidas dentro de las tramas de datos transmitidas. Los switches aprenden las direcciones MAC de los dispositivos conectados a cada puerto, a través de la lectura de las direcciones MAC origen que se encuentran en las tramas que ingresan al switch, luego esta información es ingresada dentro de la tabla de conmutación que es almacenada en la CAM. Los switches crean un circuito virtual entre dos dispositivos conectados que quieren comunicarse. Cuando este circuito virtual ha sido creado, un camino de comunicación dedicado es establecido entre los dos dispositivos. Esto crea un ambiente libre de colisiones entre el origen y el destino lo cual implica la máxima utilización del ancho de banda disponible.

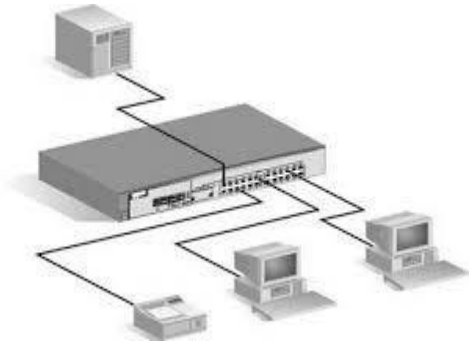


Figura 03: "Transmisiones Simultaneas en un Switch"
Fuente: http://www.cisco.com/web/learning/netacad

Cada puerto del switch representa un solo dominio de colisión, lo cual se conoce como microsegmentación. La desventaja de todos los dispositivos de capa 2, es que ellos envían tramas broadcast a todos los dispositivos conectados a sus puertos.

Router. Cisco Networkers Solutions Forum (2006). Se define como dispositivo de capa 3 que toma decisiones basadas en direcciones de red. Estos utilizan tablas de enrutamiento para almacenar estas direcciones de capa 3. Los routers se encargan de elegir el mejor camino para enviar los datos a su destino y conmutar o enrutar los paquetes al puerto de salida adecuado.

Los routers dividen tanto dominios de broadcast como dominios de colisión. Además, son los dispositivos de mayor importancia para regular el tráfico, porque proveen políticas adicionales para la administración de la red con filtrado de paquetes para la seguridad.

También dan acceso a redes de área amplia (Wan), las cuales están destinadas a comunicar o enlazar redes de área local (Lan's) que se encuentran separadas por grandes distancias.

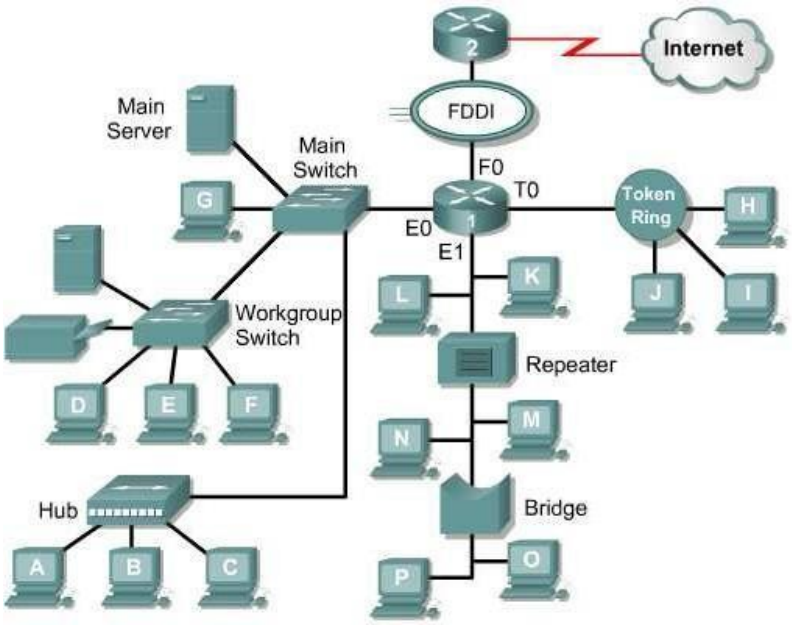


Figura 04: "Interconexión de Dispositivos en Red"
Fuente: http://www.cisco.com

Switch multilayer. Un switch multilayer es la combinación de la conmutación tradicional de capa 2 con la operación de enrutamiento de capa 3 en un solo dispositivo, mediante acciones de hardware de alta velocidad. En tanto que en un router el

enrutamiento se realiza mediante técnicas de software lentas. Este Switch se fundamenta en circuitos del tipo **ASIC**.

Los switches multilayer son más rápidos y baratos que los routers. Aunque algunos switches multilayer carecen de modularidad y flexibilidad que usualmente tienen asociados los routers.

En la actualidad existen switches que pueden manejar información relacionada desde la capa 2 (enlace de datos) hasta la capa 7 (aplicación) del modelo OSI.

Protocolo de Configuración de Hosts Dinámico – DHCP. El DHCP (Protocolo de Configuración de Hosts Dinámico) se basa en el RFC 2131, y trabaja en modo cliente – servidor. El protocolo de configuración de hosts dinámico, habilita a los clientes DHCP, obtener sus configuraciones desde un servidor DHCP, considerando que la opción de configuración de mayor importancia, es la dirección IP asignada al cliente.

El DHCP no se utiliza para la configuración de los switches, routers o servidores. Estos hosts necesitan tener direcciones estáticas.

DHCP usa el UDP como protocolo de transporte. El cliente envía mensajes al servidor sobre el puerto 67, mientras que el servidor envía mensajes al cliente sobre el puerto 68. Los clientes DHCP arriendan la información del servidor por un periodo definido administrativamente. Y cuando el arrendamiento expira, el cliente debe pedir otra dirección, aunque generalmente se le reasigna la misma.

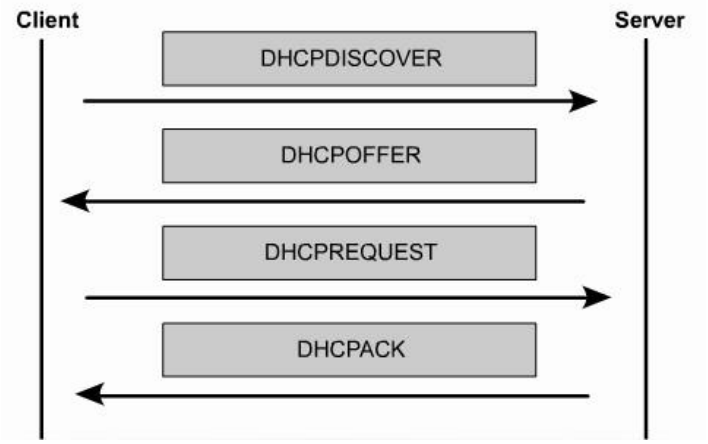


Figura 05: "Orden de Transmisión de Mensajes DHCP"
Fuente: http://www.cisco.com/web/learning/netacad

Ethernet. Ethernet o su estándar equivalente IEEE 802.3, es básicamente una tecnología de transmisión Broadcast, donde los dispositivos como computadoras, impresoras, servidores de archivos, etc.; se comunican sobre un medio de transmisión compartido, lo que quiere decir que ellos se encuentran en una continua competencia por el ancho de banda disponible. Por lo tanto, las colisiones son una natural ocurrencia en redes Ethernet y pueden llegar a ser un gran problema.

La entrega de tramas de datos Ethernet es de naturaleza Broadcast. Ethernet usa el método CSMA/CD (Acceso Múltiple Sensible a Portadora con Detección de Colisión), que le permite a una sola estación transmitir, y puede soportar tasas de transmisión de alta Carrier Sense Multiple Access / Collision Detection velocidad, como: Ethernet: 10 Mbps, Fast Ethernet: 100 Mbps, Gigabit Ethernet: 1000 Mbps y 10- Gigabit Ethernet: 10,000 Mbps.

El desempeño de un medio compartido Ethernet/802.3 puede ser negativamente afectado por factores como: las aplicaciones multimedia con alta demanda de ancho de banda tales como video e Internet, que junto con la naturaleza broadcast de Ethernet, pueden crear congestión en la red; y la latencia normal que adquieren las tramas por viajar a través de los medios de red, atravesar dispositivos de red y los propios retardos de las NICs.

Dominio de Colisión. Es un grupo de dispositivos conectados al mismo medio físico, es decir si dos dispositivos acceden al mismo tiempo al medio, entonces esto resulta en una colisión. Este es un dominio de capa 1.

Dominio de Broadcast. Es un grupo de dispositivos sobre la red que reciben mensajes de broadcast. Este es un dominio de capa 2.

Broadcast y Multicast. Para comunicarse con todos los dominios de colisión, los protocolos usan tramas broadcast y multicast en la capa 2 del modelo OSI. Por lo tanto si un nodo necesita comunicarse con todos los hosts en la red, éste envía una trama broadcast con una dirección MAC de destino 0xFFFFFFFFFFFF. Esta es una dirección a la cual todas las tarjetas NIC deben responder.

La acumulación de tráfico broadcast y multicast de cada dispositivo de la red es referido como: **radiación de broadcast,** cuya circulación puede saturar la red, es decir que no hay ancho de banda disponible para aplicaciones de datos, resultando en la caída de estas conexiones, situación conocida como una **tormenta de broadcast.**

Causas de Broadcast y Multicast. Existen varias fuentes de broadcast y multicast en redes IP, estas pueden ser: las estaciones de trabajo, los routers, las aplicaciones multicast, el protocolo DHCP, etc. Las estaciones de trabajo envían broadcast de pedidos ARP (Protocolo de Resolución de Direcciones), cada vez que ellos necesitan localizar una dirección MAC que no está en su tabla ARP. Las tormentas de broadcast pueden ser causadas por el pedido de información de un dispositivo dentro de una red que ha crecido mucho. Las aplicaciones multicast, particularmente las aplicaciones de paquetes de video pueden generar una cadena de siete megabytes de datos multicast, que en una red conmutada podría ser enviada a cada segmento, resultando en una severa congestión.

Otra fuente generadora de broadcast es el protocolo DHCP cuando un cliente DHCP usa un pedido de broadcast para localizar el servidor DHCP. Además, estos clientes por lo general repiten este pedido después de un relativo corto "timeout", posiblemente debido a una respuesta lenta del servidor, lo que producen las conocidas **tormentas de**

broadcast; que a su vez producen retardos anormales de otros tráficos cliente / servidor, los cuales también pueden empezar a retransmitir.

MODELO JERÁRQUICO CISCO

Consta de tres capas:

Capa Núcleo: **Backbone**

Capa de Distribución: **Routing**

Capa de Acceso: **Switching**

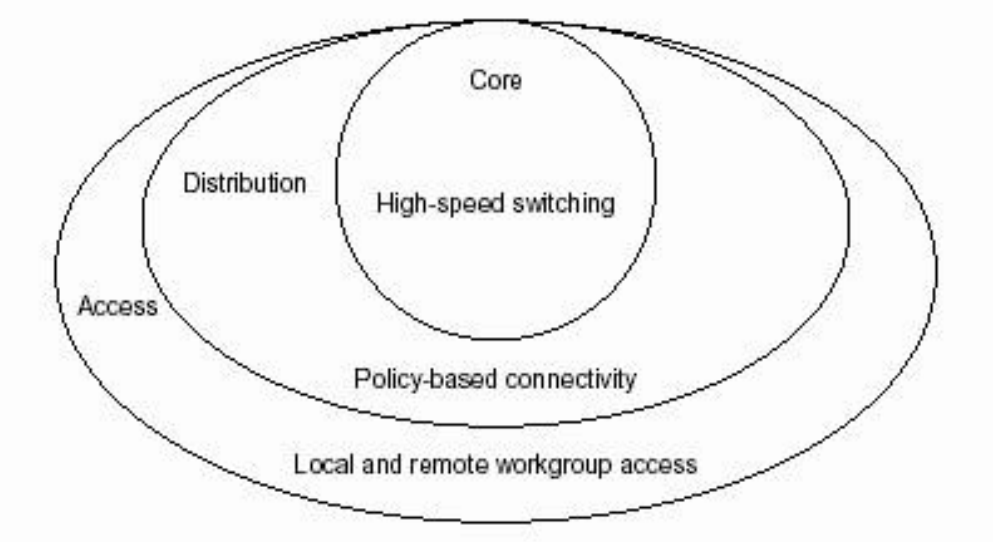


Figura 06: "Capas del Modelo Jerárquico Cisco"
Fuente: www.redesymas.org

Capa Núcleo. Es el backbone de conmutación de alta velocidad que debe ser diseñado para conmutar paquetes lo más rápido posible, es decir es responsable del transporte de grandes cantidades de tráfico en forma confiable y rápida, por lo tanto, la preocupación de esta capa es la velocidad y latencia. Es importante considerar, lo que no debemos hacer en esta capa:

No realizar ningún tipo de manipulación de paquetes, tal como usar listas de control de acceso, enrutamiento entre redes de área local virtuales (VLAN) o filtro de paquetes, lo cual reducirá el tráfico.

No soporta accesos de grupo de trabajo.

Evitar expandir el núcleo o core cuando la red crece. Si el desempeño es un problema en el core, son preferibles las actualizaciones en lugar de las expansiones.

Capa de Distribución. También conocida como "workgroup layer", y es el punto de comunicación entre la capa de acceso y el core. Las principales funciones de la capa de distribución son el proveer enrutamiento, filtros, accesos WAN y determinar cómo los paquetes pueden acceder al core si es necesario.

La capa de distribución es donde se implementan las políticas para la red. Existen algunas acciones que generalmente deben hacerse en esta capa:

Enrutamiento.
Implementación de listas de control de acceso o filtro de paquetes.
Implementación de seguridad y políticas de red, incluyendo traslado de direcciones y firewalls.
Calidad de Servicio, en base a las políticas definidas.
Redistribución entre protocolos de enrutamiento, incluyendo rutas estáticas.
Enrutamiento entre VLan's y otras funciones que soportan los grupos de trabajo.
Definición de dominios de Broadcast y multicast.
Posible punto para acceso remoto.
Traslado de medios de comunicación.

Capa de Acceso. La capa de acceso es el punto en el cual los usuarios finales son conectados a la red. Esta capa puede también usar listas de acceso o filtros para optimizar las necesidades de un grupo particular de usuarios. Los recursos de red de la mayoría de usuarios deben estar disponibles localmente. Esta capa también es conocida como "desktop layer". Estas son algunas de las funciones que incluye esta capa:
Continúa el control de acceso y políticas (desde la capa de distribución)
Creación de dominios de colisión separados (micro- segmentación)
Conectividad de los grupos de trabajo dentro de la capa de distribución.
Habilitar filtros de direcciones MAC.
También es posible tener acceso a grupos de trabajo remotos.

Presta servicios de asignación de VLANs a nivel de capa 2 del modelo OSI.

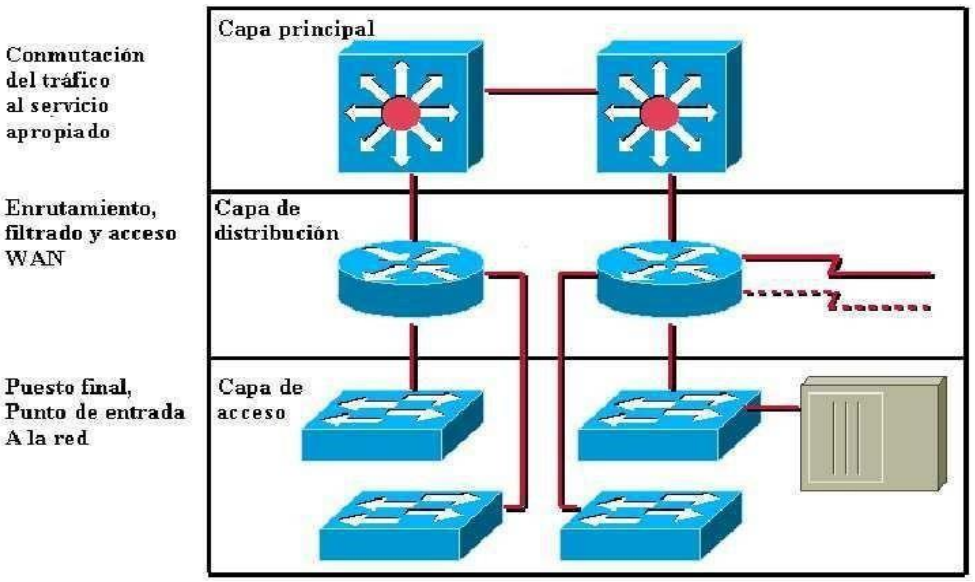


Fig. N° 07: "Estructura de Red definido por Jerarquía"
Fuente: www.geocities.ws

TOPOLOGÍA ESTRELLA.

Una red en estrella es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de este. Los dispositivos no están directamente conectados entre sí, además de que no se permite tanto tráfico de información. Dada su transmisión, una red en estrella activa tiene un nodo central activo que normalmente tiene los medios para prevenir problemas relacionados con el eco.

Figura 08: "Topología Estrella"
Fuente: Cisco.com

La topología estrella es una de las topologías más populares de un LAN (Local Area Network). Es implementada conectando cada computadora a un Hub central. El Hub puede ser *Activo, Pasivo o* Inteligente. Un hub activo es solo un punto de conexión y no requiere energía eléctrica. Un Hub activo (el más común) es actualmente un repetidor con múltiples puertos; impulsa la señal antes de pasarla a la siguiente computadora. Un Hub Inteligente es un hub activo, pero con capacidad de diagnóstico, puede detectar errores y corregirlos.

En una red estrella típica, la señal pasa de la tarjeta de red (NIC) de la computadora que está enviando el mensaje al Hub y este se encarga de enviar el mensaje a todos los puertos. La topología estrella es similar a la Bus, todas las computadoras reciben el mensaje, pero solo la computadora con la dirección, igual a la dirección del mensaje puede leerlo.

Ventajas y desventajas de una topología de red.

Ventajas:

A comparación de las topologías Bus y Anillo, si una computadora se daña el cable se rompe, las otras computadoras conectadas a la red siguen funcionando.
Agregar una computadora a la red es muy fácil ya que lo único que hay que hacer es conectarla al HUB o SWITCH.
Tiene una mejor organización ya que al HUB o SWITCH se lo puede colocar en el centro de un lugar físico y a ese dispositivo conectar todas las computadoras deseadas.

Desventajas.

No es tan económica a comparación de la topología Bus o Anillo porque es necesario más cable para realizar el conexionado.
Si el HUB o SWITCH deja de funcionar, ninguna de las computadoras tendrá conexión a la red.
El número de computadoras conectadas a la red depende de las limitaciones del HUB o SWITCH.

Virtual LAN (Red de área local y virtual)

Es un método que permite crear redes que lógicamente son independientes, aunque estas se encuentren dentro de una misma red física. De esta forma, un usuario podría disponer de varias VLANs dentro de un mismo router o switch. Podría decirse que cada una de estas redes agrupa los equipos de un determinado segmento de red. Crear estas particiones tiene unas ventajas bastante claras a la hora de administrar una red.

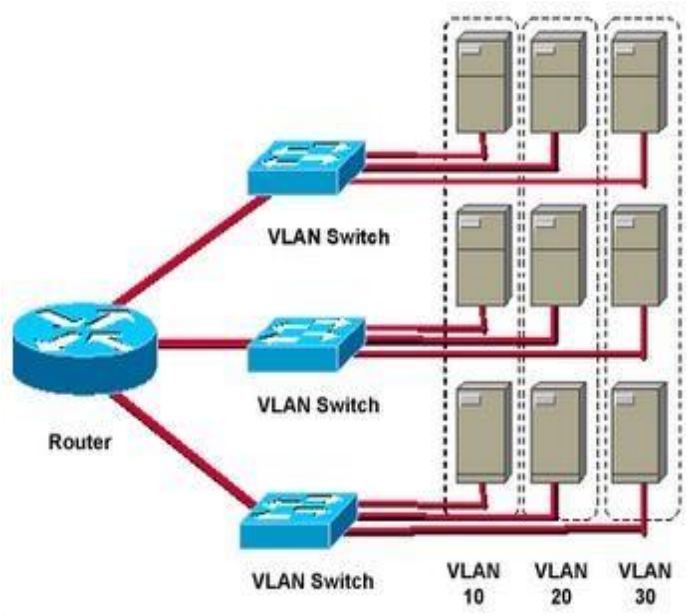


Figura 09: "Lan Virtual"
Fuente: (Xcess Logycs).

USOS Y VENTAJAS

A la fecha se configuran a través de software y poseen grandes beneficios a la hora de garantizar la seguridad y administrar los equipos de forma eficaz, tal y como a hemos puntualizado. En lo que concierne a la seguridad, hay que tener en cuenta que los dispositivos pertenecientes a una VLAN no tienen acceso a los que se encuentren en otras y viceversa. Resulta útil cuando queremos segmentar los equipos y limitar el acceso entre ellos por temas de seguridad.

De lo dicho con anterioridad se deduce que la gestión también será mucho más sencilla, ya que tendríamos a los dispositivos divididos en "clases" aunque pertenezcan a una misma red.

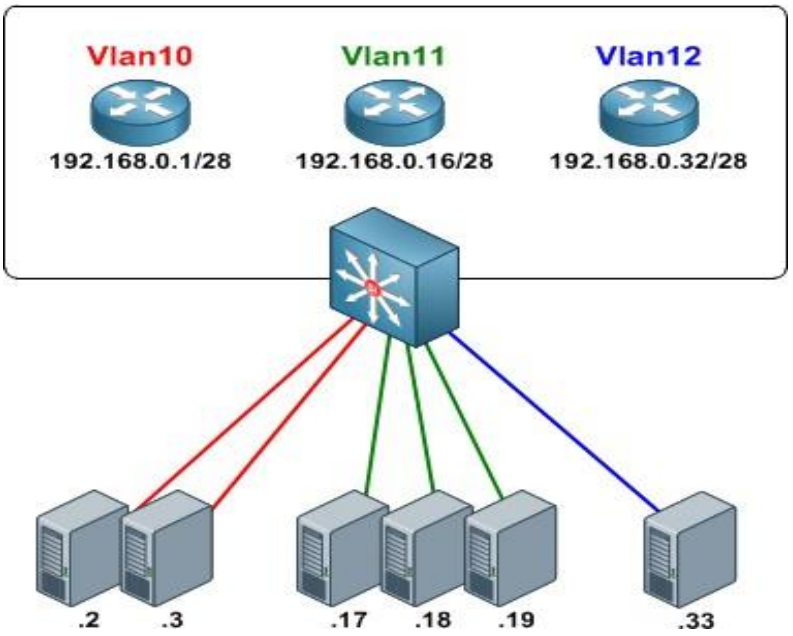


Figura 10: “Lan Virtual”
Fuente: (Servervoip.com).

TIPOS DE VLANS

Dependiendo de la fuente consultada incluso del fabricante se pueden distinguir hasta seis tipos de redes virtuales. Sin embargo, nosotros solo nos vamos a centrar en tres: a nivel de puerto, MAC y aplicación.

Puerto. También conocida como *Port Switching* en los menús de configuración de los routers y switches, se trata de la más extendida y utilizada. Cada puerto se asigna a una VLAN y los usuarios que estén conectados a ese puerto pertenecen a la VLAN asignada. Los usuarios dentro de una misma VLAN poseen de visibilidad los unos sobre los otros, aunque no a las redes virtuales vecinas. El único inconveniente es que no permite dinamismo a la hora de ubicar los usuarios y en el caso de que el usuario cambie de emplazamiento físicamente se debería reconfigurar la red virtual.

Mac: El razonamiento es similar a la anterior, salvo que en vez de ser una asignación a nivel de puerto lo es a nivel de dirección MAC del dispositivo. La ventaja es que permite movilidad sin necesidad de que se tengan que aplicar cambios en la configuración del switch o del router. El problema parece bastante claro: añadir todos los usuarios puede resultar tedioso.

Aplicaciones: Se asignarían redes virtuales en función de la aplicación utilizada, y en este caso intervienen varios factores, como por ejemplo la hora en la que nos encontramos, la dirección MAC o la subred, permitiendo distinguir entre aplicaciones SSH, FTP, Samba o incluso SMTP.

APLICACIONES EN LOS EQUIPOS DOMÉSTICOS

¿Cuántos lectores poseen conexiones FTTH? En este servicio tenemos un claro ejemplo de utilización de VLANs pero a gran escala. Los operadores ubican los diferentes servicios en redes lógicas separadas. Por ejemplo, en el caso de Movistar, el servicio de televisión, VoIP e Internet se encuentran en redes separadas, algo que los usuarios que hagan uso de routers diferentes a los ofrecidos por la operadora conocerán.

Hablando de qué uso se puede dar, resulta bastante claro. Por ejemplo, separar aquellos equipos que acceden a Internet de los que no lo hacen. Esto evita que los intrusos no lleguen a estos y que por ejemplo malware pueda distribuirse gracias a unidades de red que estarían disponibles.

PROTOCOLOS

El protocolo de etiquetado IEEE 802.1Q es el más común para el etiquetado de las VLAN. Antes de su introducción existían varios protocolos propietarios, como el ISL (Inter-Switch Link) de Cisco, una variante del IEEE 802.1Q, y el VLT (Virtual LAN Trunk) de 3Com. El IEEE 802.1Q se caracteriza por utilizar un formato de trama similar a 802.3 (Ethernet) donde solo cambia el valor del campo Ethertype, que en las tramas 802.1Q vale 0x8100, y se añaden dos bytes para codificar la prioridad, el CFI y el VLAN ID. Este protocolo es un estándar internacional y por lo dicho anteriormente es compatible con bridges y switches sin capacidad de VLAN.

CISCO SYSTEM

Cisco es una empresa internacional que diseña y vende soluciones de tecnología de la información como redes de datos y voz, seguridad en redes, así como servicios profesionales de consultoría y soporte. Sus oficinas principales se encuentran en San José California y tiene más de 70, 000 empleados alrededor del mundo. Cisco reportó

cerca de 40 billones de dólares de ingresos en 2010, también está ubicada en el número 16 en la lista de las empresas de tecnología más grandes del mundo.

PRODUCTOS Y SERVICIOS

Actualmente el portafolio de productos y servicios de Cisco está enfocado a tres segmentos de mercado:

Empresas y Proveedores de Servicios

Pequeñas Empresas

Hogar

A continuación, se describe de manera general las soluciones ofrecidas por Cisco.

EMPRESAS Y PROVEEDORES DE SERVICIOS

Borderless Networks: Sistemas de seguridad, aceleración de aplicaciones en redes WAN y sistemas de administración de redes.

Colaboración: Video IP y teléfonos, Tele presencia, Comunicaciones Unificadas, Servicios de Call Center y aplicaciones móviles.

Centros de datos y Virtualización: Computo Unificado, Switches para Centros de Datos y Almacenamiento.

IP NGN (IP NGN (Next Generation Networks): Redes Ruteadas y Switcheadas para Proveedores de Servicio Móvil, Servicios de Televisión contribuidos.

PEQUEÑAS Y MEDIANAS EMPRESAS

WAN y LAN: Routers y Switches.

Seguridad y Vigilancia: Cámaras IP, soluciones de seguridad en redes de datos.

Soluciones de Voz y Conferencia: Teléfonos IP, Gateways, WebEx, Servicios de Video Conferencia.

Redes Inalámbricas: WiFi Access Point, Controladores y Antenas.

Sistemas de Almacenamiento.

HOGAR (USUARIOS FINALES)

Productos de la línea Access Point Linksys

Productos de la línea Switches y Cable Modems Linksys
Cable módems de Banda Ancha
Cisco ūmi para Video Conferencia

La presente investigación es descriptiva, por lo tanto, la hipótesis es implícita. Se presenta el objetivo general. Al realizar la segmentación de la red (VLAN), mejorará la comunicación de datos de todos los trabajos realizado en la Empresa Agro Industrial Paramonga, compartiendo todos los recursos y servicios de manera adecuada, segura, oportuna y rápida.

El objetivo general del proyecto es: Implementar la segmentación de la red virtual Lan (Vlans) para la comunicación de datos entre las diferentes áreas de la Empresa Agro Industrial Paramonga S.A.A.

Los objetivos específicos seleccionados para el desarrollo del informe son: 1) Analizar la situación actual para conocer los requerimientos que conlleva a la construcción de este proyecto, 2) Utilizarla metodología Cisco para el diseño de la segmentación de la red virtual, 3) Implementar la red de área de trabajo para optimizar la comunicación de datos.

2. METODOLOGÍA DE TRABAJO

Definiremos el tipo de investigación de acuerdo a la orientación que se optó por una investigación **Descriptiva** por lo que no se va a generar ninguna nueva modificación teórica en este presente caso de estudio. Y el diseño de investigación se delimita como **No Experimental con corte transversal**, dado que el marco y objeto, que sustenta el problema y la justificación del mismo no se encuentra definida dentro de un proyecto de investigación experimental propiamente dicho.

La población que se involucra para esta investigación son los miembros de la Empresa Agro Industrial Paramonga S.A.A., que son el personal principal para el estudio de nivel de cumplimientos de los lineamientos y estándares internacionales de la seguridad informática. P=9
Por ser una población pequeña se tomará esa cantidad para la muestra. n= 9

Con la finalidad de interrogar y recabar información importante de la población en estudio; considerando que las mismas, será un proceso de comunicación verbal recíproca entre las partes, no estarán sujetas a un estándar formal lo que permitirá un marco de desarrollo abierto y de libertad para la formulación de preguntas y respuestas.

Técnica del Cuestionario, la cual se considera como un medio de comunicación escrito básico, el cual facilita traducir los objetivos y variables de la investigación a través de una serie de preguntas muy particulares, previamente preparadas. Ésta técnica permitirá al encuestado, expresar su punto de vista con respecto a la segmentación de las redes virtuales, problemas e información de relevante interés para la presente investigación.

Técnica de Encuesta, la cual va a permitir a la muestra definida como "Usuario Final" discernir entre un bloque de preguntas orientadas a indagar las necesidades del individuo en torno al uso del servicio de redes virtuales, como parte de la implementación, y finalmente como detector en las necesidades de asistencia objeto de la presente investigación, que permitirá consolidar la propuesta señalada de la presente investigación.

FASES DE LA METODOLOGIA

Metodología Cisco Ciclo de Vida

La metodología exclusiva del ciclo de vida de los Servicios de Cisco define las actividades necesarias en cada fase del ciclo de vida de la red para ayudar a asegurar la excelencia de los servicios.

El enfoque principal de esta metodología es definir las actividades mínimas requeridas, por tecnología y complejidad de red, que permitan asesorar de la mejor forma posible a nuestros clientes, instalando y operando exitosamente las tecnologías Cisco. Así mismo logramos optimizar el desempeño a través del ciclo de vida de su red.

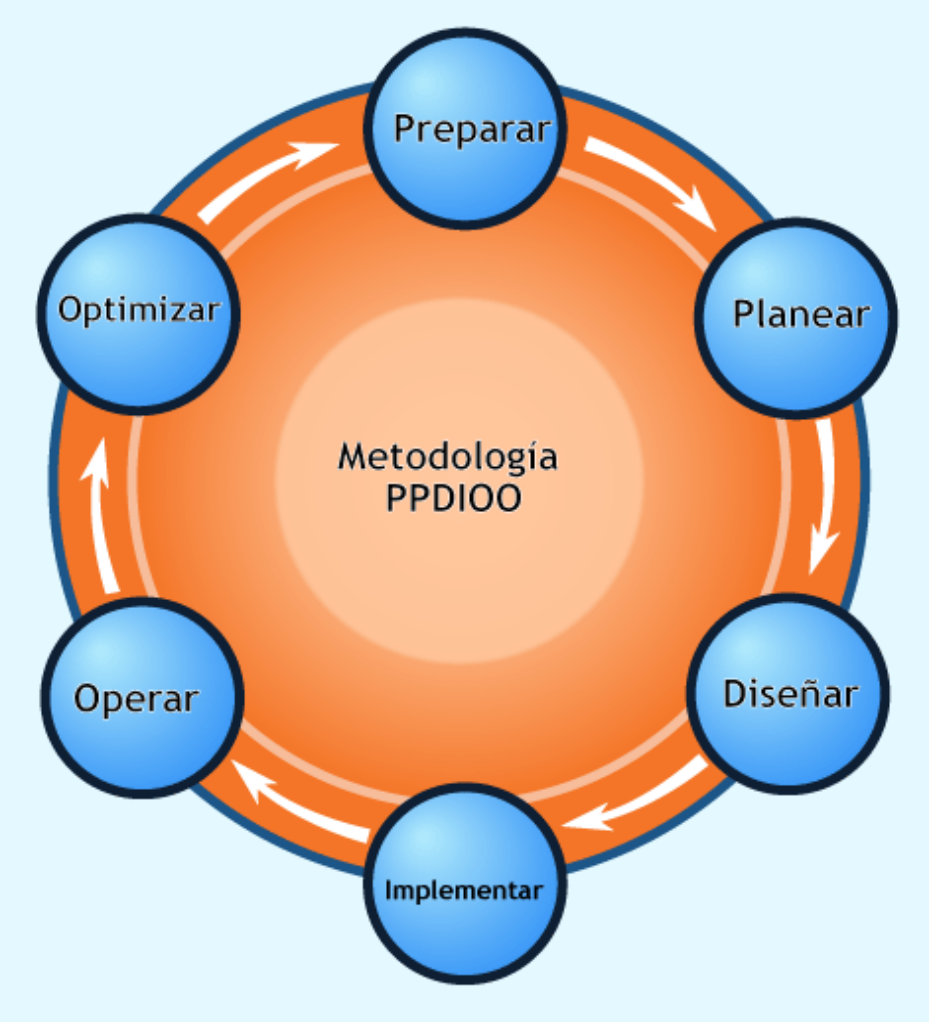


Figura 11: "Metodología Cisco"
Fuente: (Cisco.com).

Preparación

El éxito de un proyecto inicia con la preparación; una visión amplia, los requerimientos y tecnologías necesarias para soportar una solución que sea competitiva. En la fase de preparación una compañía determina un caso de negocio partiendo de las necesidades y del Retorno de Inversión (ROI) al adoptar una nueva tecnología. Se debe tener especial cuidado en las necesidades futuras y en el desarrollo de una estrategia tecnológica y una arquitectura de alto nivel que cubra todas las necesidades de negocio.

Planeación

Una implementación exitosa depende de una evaluación precisa de la red actual, la disposición general de los involucrados en apoyar la solución. En la fase de planeación, una empresa comprueba si tiene recursos suficientes para gestionar un proyecto de implementación de la tecnología desde el inicio hasta el hasta fin. Para evaluar y mejorar la seguridad de la red, una compañía realiza pruebas de su red para que esté preparada para problemas como detección de intrusos y la vulnerabilidad a las redes externas.

La empresa desarrolla un plan detallado del proyecto para identificar los recursos, las posibles dificultades, las responsabilidades individuales y las tareas críticas necesarias para entregar el proyecto final a tiempo y dentro del presupuesto acordado.

Diseño

El desarrollo de un diseño detallado es fundamental para reducir los riesgos, retrasos y el costo total de instalación. Utilizar un diseño de acuerdo con los objetivos de negocio y los requisitos técnicos puede mejorar el rendimiento de la red, mientras se garantiza la alta disponibilidad, confiabilidad, seguridad y escalabilidad. Las operaciones del día a día y los procesos de gestión de red deben ser anticipados, y cuando sea necesario, se crean aplicaciones personalizadas para integrar nuevos sistemas en la infraestructura existente.

La fase de diseño también puede guiar y acelerar la ejecución exitosa con un plan de configuración, protocolos de pruebas y validación de servicios.

Implementación

Una red es esencial para cualquier organización exitosa, esta debe prestar servicios esenciales sin interrupción. En la fase de implementación, una empresa trabaja para integrar los dispositivos y las nuevas capacidades de acuerdo al diseño sin comprometer la disponibilidad de la red o el rendimiento. Después de identificar y resolver problemas potenciales, la empresa intenta acelerar el retorno de inversión con una migración eficiente esto incluye la instalación, configuración, integración, pruebas y la puesta en marcha de la solución. Una vez que la operación es validada, una organización puede empezar a expandir y mejorar las habilidades al personal de TI para aumentar aún más la productividad y reducir el tiempo de inactividad del sistema.

Operación

El funcionamiento de la red representa una porción significativa del presupuesto de TI, así que es importante poder reducir los gastos operativos y al mismo tiempo mejorar el rendimiento.

A lo largo de la fase de operación, una compañía monitorea de forma proactiva la salud de la red para mejorar la calidad del servicio, mitigar las interrupciones y mantener una alta disponibilidad, confiabilidad y seguridad.

Proporcionar un marco eficiente y herramientas operativas para responder a los problemas, una empresa puede evitar el costoso tiempo improductivo y la interrupción del negocio. La participación de personal experto permite a una organización dar cabida a las actualizaciones, adiciones y cambios de manera confiable.

Optimización

Un buen negocio no deja de buscar una ventaja competitiva. Esa es la razón por la mejora continua es uno de los pilares del ciclo de vida de la red. En la fase de optimización, una empresa está continuamente buscando maneras de alcanzar la excelencia operativa a través de un mejor desempeño, ampliación de los servicios y las evaluaciones periódicas de la red.

Toda organización busca optimizar su redy se prepara para adaptarse a las nuevas necesidades de negocio, es aquí donde el Ciclo de Vida comienza de nuevo en busca de una mejora continua.

3. RESULTADOS

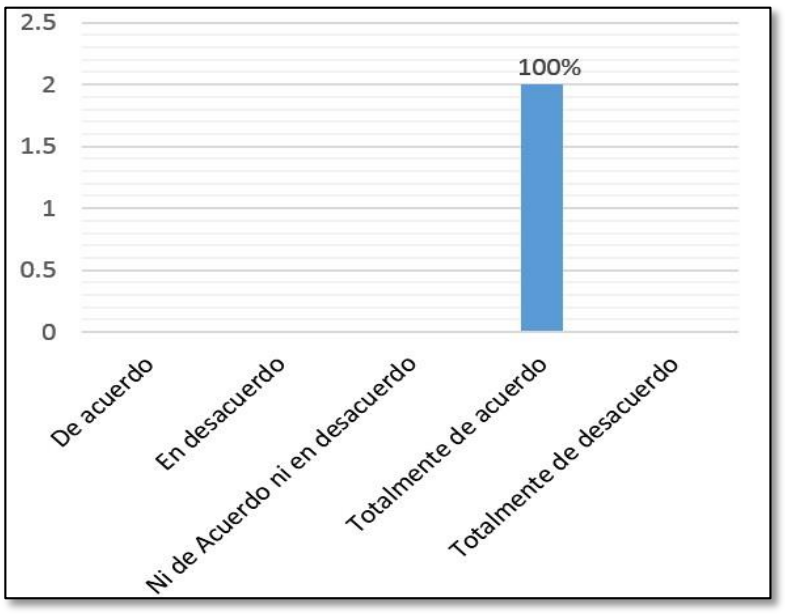
Para el informe de investigación se han aplicado dos encuestas, las cuales se han orientado a los expertos en temas de segmentación de red virtual y a los usuarios finales los cuales serán beneficiados con la implementación.

Aplicada las encuestas a todos los expertos y usuarios finales de la implementación de la red virtual, se obtuvieron los siguientes resultados:

Encuesta a Expertos del tema de Segmentación de Red Virtual

Pregunta Nº 01:

¿Cuán importante considera aplicar la Segmentación de Red Virtual para mejorar la comunicación de datos?



Interpretación:

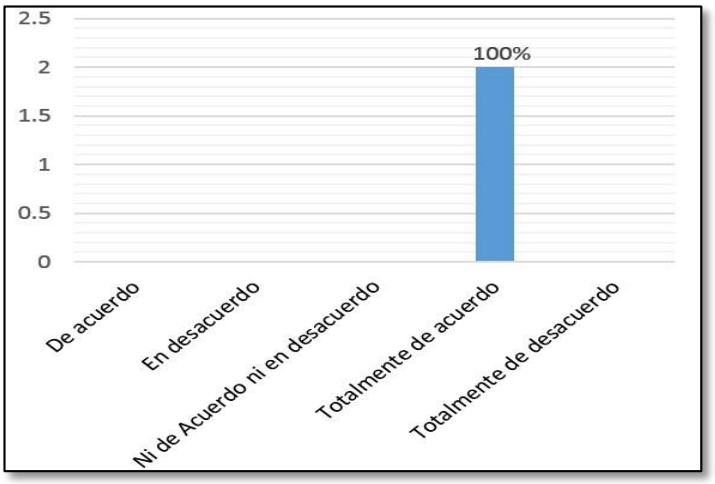
Se aprecia que 100.00% de expertos considera importante implementar la segmentación de Red Virtual para mejorar la comunicación de datos.

Figura 12: "Importancia de la red virtual"

Fuente: Elaboración propia

Pregunta Nº 02:

¿Cree Ud. que la empresa Agro Industrial Paramonga S.A.A. debería implementar la Segmentación de la Red Virtual?

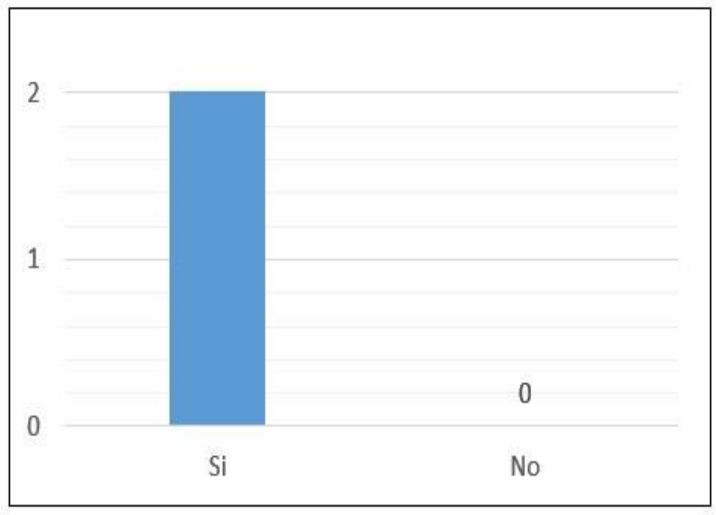


Interpretación:
Se aprecia que 100.00% de expertos considera que la empresa debería de invertir en la segmentación de la Red Virtual.

Figura 13: "Implementación de la red virtual"
Fuente: Elaboración propia

Pregunta Nº 03:

¿Conoce las ventajas y desventajas de la implementación de la Red Virtual?

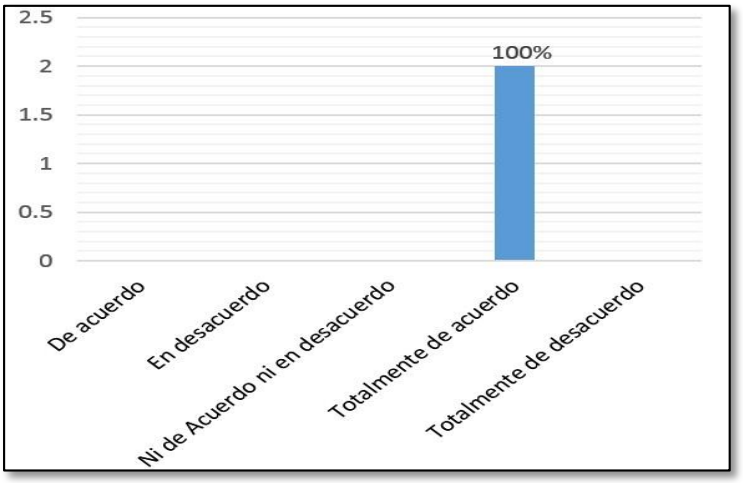


Interpretación:
Se aprecia que 100.00% de expertos conocen o tienen amplia experiencia en temas de segmentación de red virtual.

Figura 14: "Ventajas y desventajas de la red virtual"
Fuente: Elaboración propia

Pregunta N° 04:

¿Cree usted que la segmentación de la red Virtual nos brindará la seguridad de una red confiable?



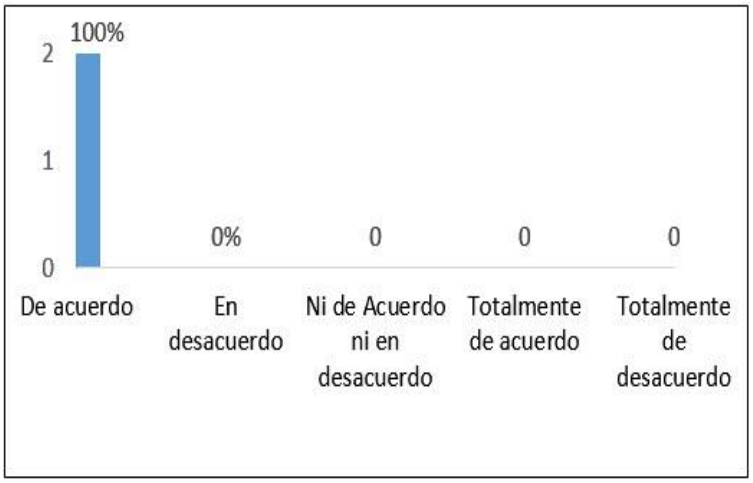
Interpretación:
Se aprecia que 100.00% de expertos consideran que con la segmentación de Red Virtual si nos brindara una red confiable.

Figura 15: "Redes virtuales confiables"

Fuente: Elaboración propia

Pregunta N° 05:

¿La segmentación de la red virtual permitirá mejorar la comunicación de datos en todos los procesos del negocio?



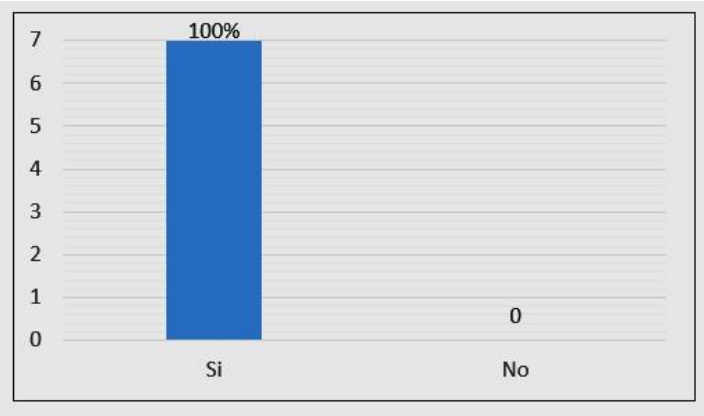
Interpretación:
Se aprecia que 100.00% de expertos consideran que con la segmentación de la red mejorar la comunicación de datos en todos los procesos del negocio.

Figura 16: "Mejora en la comunicación de datos"

Fuente: Elaboración propia

Encuesta a los Usuarios Finales
Pregunta N° 01

¿Tiene conocimiento acerca de lo que es la segmentación de la Red Virtual?

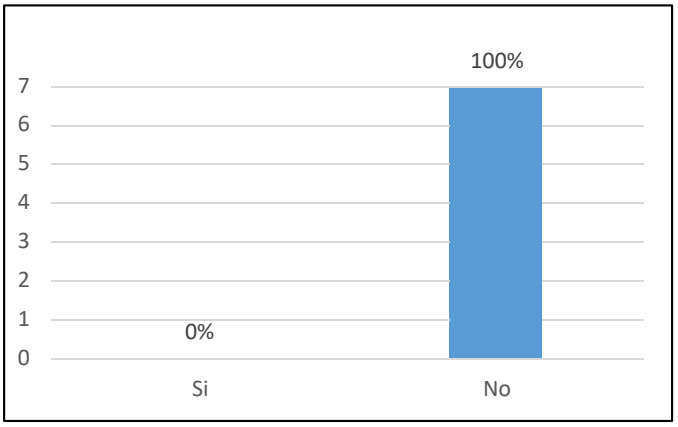


Interpretación:
Se aprecia que 100.00% de los usuarios tienen conocimiento de la segmentación de la Red Virtual.

Figura 17: "Conocimientos sobre la red virtual"
Fuente: Elaboración propia

Pregunta N° 02

¿Cuenta con sus archivos de datos sin demora a la hora de realizar sus actividades diarias?

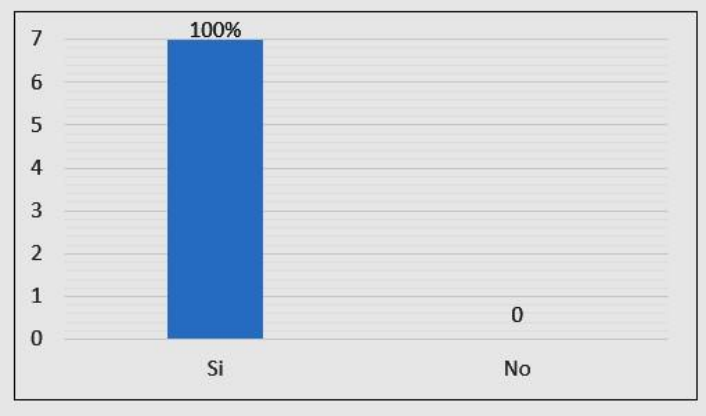


Interpretación:
Se aprecia que 100.00% de los usuarios no cuentan con sus archivos necesarios, dado a las demoras de transferencia de datos.

Figura 18: "Disponibilidad de Archivos"
Fuente: Elaboración propia

Pregunta N° 03

¿Cree usted que la segmentación de la Red Virtual ayudaría a mejorar la comunicación de datos?

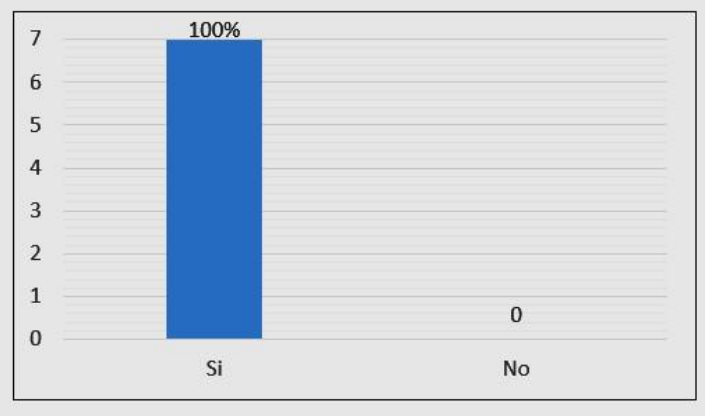


Interpretación:
El 100.00% de los usuarios cree que segmentando la Red mejoraría la comunicación de datos en la Empresa.

Figura 19: "Mejora en la comunicación de datos"
Fuente: Elaboración propia

Pregunta N° 04

¿Estaría dispuesto invertir en un proyecto de segmentación de Red Virtual?

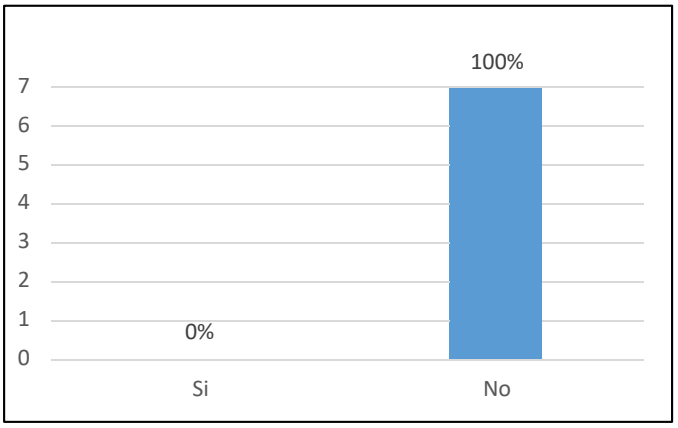


Interpretación:
Se aprecia que el 100.00% de los usuarios están interesados en invertir en la segmentación de la red virtual

Figura 20: "Inversión para la Implementación de redes virtuales"
Fuente: Elaboración propia

Pregunta N° 05

¿Está usted conforme con la velocidad de transferencia de datos (Archivos) que brinda actualmente la red de la empresa?



Interpretación:
Se aprecia que 100.00% de los usuarios no está conforme con la velocidad de transferencia de datos

Figura 21: "Implementación de redes virtuales"
Fuente: Elaboración propia

APLICACIÓN DE LA METODOLOGÍA CISCO

Fases de la Planificación: Este Proyecto tiene como objetivo fundamental reducir costos de operación en todos los procesos que se realizan en la Empresa Agro Industrial Paramonga, facilitando todas las actividades que hasta el día se realizan siendo estos procesos largos e inseguros además se pretende entregar mejores facilidades para hacer un proceso de producción continuo, esto implica el aumentando de la productividad, optimización de los recursos destinados a las personas involucradas; el costo inicial del proyecto será recuperado con el aumento de productividad.

Como también podrá permitir movilidad al personal de la empresa dentro de la misma mediante el uso de la red inalámbrica, y así poder mejorar los procesos para paso de información del resto de departamentos.

Buscar la mejor opción que se adapte a las necesidades de la empresa para brindar un servicio de calidad, pero sobre todo seguir permitiendo el funcionamiento de todas las aplicaciones que son de primordial necesidad para que el negocio siga funcionando en su totalidad.

En esta fase se mostrará todo lo referente a costos que implica el análisis y diseño de la red para la empresa Agro Industrial Paramonga S.A.A., así como también el fundamento del por qué la elección de los equipos que hacen falta o remplazo para el diseño.

Inversión en equipamiento

La inversión en equipamiento se realizará a través de la adquisición de equipos que sirvan para el óptimo funcionamiento de la red y la utilización de equipos ya existentes en la red actual.

Los nuevos equipos que se van a comunicar entre la capa núcleo y capa acceso de la red.

Tabla 01: Detalle costo de equipos de red LAN.

REQUERIMIENTO DE EQUIPOS PARA LA RED LAN			
Cantidad	**Modelo**	**P/U**	**P/T**
3	SWITCH CISCO WS-C2960X-48LPD-L	3.584,90	10.754,70
3	SMARTNET WS-C2960X-48LPD-L	2.218,50	6.655,50
1	SWITCH CISCO WS-C2960X-48TD-L	2.867,40	2.867,40
1	SMARTNET WS-C2960X-48TD-L	1.770,70	1.770,70
5	SWITCH CISCO WS-C2960X-24PD-L	2.354,90	11.774,50
5	SMARTNET WS-C2960X-24PD-L	1.453,80	7.269,00
3	SWITCH CISCO WS-C2960X-24TD-L	1.944,90	5.834,70
3	SMARTNET WS-C2960X-24TD-L	1.202,30	3.606,90
1	SWITCH CISCO WS-C3850-24XS-S	10.762,50	10.762,50
1	SMARTNET WS-C3850-24XS-S	6.655,40	6.655,40
26	MODULO TRANSCEIVER 10 GBASE–SRSFP	333,10	8.660,60
26	PATCH CORD DE FIBRA OPTICA LC	43,80	1.138,80
Monto Total en Dólares			**77.750,70**

Fuente: Elaboración propia.

Estos equipos fueron seleccionados de acuerdo a la necesidad que presenta la nueva topología de red ya que su diseño actual posee una topología de tipo plano y el diseño

planteado es de tipo jerárquico.

Para el segmento inalámbrico los equipos seleccionados se muestran en la siguiente tabla.

Tabla 02: Detalle costo de equipos de red inalámbrica.

REQUERIMIENTO DE EQUIPOS PARA LA RED INALAMBRICA			
Cant.	**Modelo**	**P/U**	**P/T**
13	Cisco Aironet 2700 Series Dual Band	1.033,20	13.431,60
13	SmartNet Cisco 9*5*Ned 802,11AC	142,90	1.858,00
1	Controlador Wireless 2504 Cisco	1.079,80	1.079,80
1	SmartNet Controlador Cisco 8*5*NBD	272,60	272,60
Monto Total en Dólares			**16.642,00**

Fuente: Elaboración propia.

Inversión En Instalación Y Configuración.

Todo el diseño y configuración de equipos requiere su respectiva configuración e instalación es por ello que se describe en la siguiente tabla el valor de los mismos.

Tabla 03: Detalle costo de equipos de red LAN

COSTO DE CONFIGURACION DE EQUIPOS DE RED LAN			
Cant.	**Descripción**	**P/HORA**	**P/T**
3	SWITCH CISCO WS-C2960X-48LPD-L	200,00	600,00
1	SWITCH CISCO WS-C2960X-48TD-L	200,00	200,00
5	SWITCH CISCO WS-C2960X-24PD-L	200,00	1.000,00
3	SWITCH CISCO WS-C2960X-24TD-L	200,00	600,00
1	SWITCH CISCO CORE WS-C3850-24XS-S	500,00	500,00
Monto Total en Dólares			**2.900,00**

Fuente: Elaboración propia.

Tabla 04: Detalle costo de equipos de red inalámbrica.

COSTO DE CONFIGURACION DE EQUIPOS PARA LA RED INALAMBRICA			
Cant.	**Descripción**	**P/HORA**	**P/T**
13	Configuración de dispositivos inalámbricos	150,00	1.950,00
1	Configuración de controlador Wireless	300,00	300,00

Monto Total en Dólares	**2.250,00**

Fuente: Elaboración propia.

Valor del proyecto.

El costo total del proyecto se resume en la siguiente tabla que se presenta a continuación.

Tabla 05: Detalle costo de equipos de red.

VALOR TOTAL DE LA IMPLEMENTACION DE VLAN	
Descripción	**Total**
Requerimientos de equipos para la Red LAN	77.750,70
Requerimientos de equipos para la Red Inalámbricas	16.642,00
Costo de Configuración de equipos de Red LAN	2.900,00
Costo de Configuración de equipos de Red Inalámbricas	2.250,00
Otros gastos en materiales de red	15.000,00
Monto Total en Dólares / IGV incluido	**114.542,70**

Fuente: Elaboración propia.

Densidad de usuarios: La cantidad de usuarios con la cual se encuentra funcionando la empresa se ubican diseminados por todas las áreas, dando un aproximado de 290 usuarios, los usuarios de la empresa por ser esta una pionera a nivel nacional e internacional en la producción y venta del azúcar, tienen como factor común el constante movimiento por las sucursales, así como por todas las áreas en la que se ven involucrados los usuarios.

Número de puntos de red y host: En la siguiente tabla se muestra un detalle de todos los puntos de datos que se encuentran instalados y libres en cada área, así como también se muestra cuantos puntos de datos están siendo ocupados por los usuarios.

Tabla 06: Número de Host por área

AREA	**Nº DE HOST**	**HOST HABILITADOS**
Proyectos	40	37
Fábrica	48	44
Bienestar	48	46
Almacén de productos terminados	16	9

Balanza	8	8
Laboratorio	24	23
Transportes	24	21
Campo	70	50
Sema	16	10
Almacén	20	14
HOST TOTALES	**314**	**262**

Fuente: Elaboración propia.

REQUERIMIENTOS DE LOS USUARIOS A INTERNET: Al ser una empresa cuyo objetivo financiero es la venta de Azúcar a nivel nacional e internacional, los requerimientos de los usuarios en encontrar datos en Internet no son muchos, pero las visitas a sitios con los proveedores si son muy comunes por tal motivo el uso de Internet necesita que tenga un buen ancho de banda ya que los manuales o información son un poco grandes los archivos. Por tal motivo la velocidad es de 1Mbps es suficiente para los usuarios.

Tabla 07: Políticas de acceso a internet.

TIPO	DESCRIPCCION
Gerencial	Acceso a todas las páginas con excepción a páginas prohibidas.
Jefatura A	Acceso a todas las páginas Excepto: a las Páginas prohibidas, Hotmail, Yahoo! y redes sociales.
Jefatura B	Acceso a todas las páginas Excepto: a las Páginas prohibidas, Hotmail, Yahoo! y redes sociales, Streaming: YouTube, vimeo, Spotify, Netflix, Amazon, prime video.
Supervisor	Acceso a las páginas del gobierno, ministerios y entes públicos, google, Gmail, google drive.
Usuario	Acceso a las páginas del gobierno, ministerios y entes públicos.

Fuente: Elaboración propia.

ESCALABILIDAD DE LA RED ACTUAL: Al momento de ser diseñada la red en sus inicios se tuvo en cuenta este factor, pero actualmente con el crecimiento de la empresa y por su puesto el incremento de personal los puntos de datos en cada área fueron escanciando hasta llegar al punto de tener unos cuantos puntos de red

disponibles en todas las áreas, por lo cual no soportaría un incremento excesivo de usuarios, pero si se tuviera proyectado espacio para el incremento de usuarios de forma mesurada y planificada

Los puntos de datos que se encuentran a disponibilidad de la empresa Agro Industrial Paramonga S.A.A. son un total de 314 puntos, los cuales son únicamente para transmisión de datos, esta cantidad de puntos de datos abastecen sin ningún problema a la necesidad de la empresa.

DISPONIBILIDAD DE LA RED ACTUAL: Por políticas de la empresa el mantenimiento que se proporciona a los equipos de comunicación y servidores se realiza varias veces al año dependiendo del área donde se encuentran ubicados, haciendo que el servicio de la red se vea comprometida durante una hora en el tiempo que se realiza dicho mantenimiento, este mantenimiento consiste en verificación de todos los puntos de datos de los equipos de comunicación así como actualizaciones de ciertos procedimientos o programas en los servidores.

El mantenimiento que se da a los equipos es el siguiente:

Mantenimiento de equipos de comunicación y equipos de cómputo dependiendo su ubicación: Mensual, bimestral, trimestral, semestral y Anual.

Mantenimiento de Servidores de forma semestral.

En la siguiente tabla se muestra la ubicación y nombre del archivo descargado, el tiempo de respuesta y el tamaño del archivo, gracias a las estadísticas de la tabla se puede mencionar que el retardo es de 0.30 segundos en la red.

Tabla 08: Prueba de tiempo de respuesta.

Archivo / Directorio	Tiempo (segundos)	Tamaño (Kbytes)
/CPU_SIS_02/doc_user.dat	< 0.4	0.052
/CPU_SIS_02/Dates.dat	< 0.8	1.784
/CPU_SIS_02/Trig.dat	0.055	8.643
/CPU_SIS_02/Dat_ext.dat	0.10	9.842

/CPU_SIS_02/Time.dat	0.12	11.214

Fuente: Elaboración propia.

Números de archivos: 5

Tamaño: 31.535

Tiempo de retardo: 0.30

Velocidad: 14176.853 KB/s

SEGURIDAD

La seguridad para la red de datos en la empresa Agro Industrial Paramonga S.A.A. ha sido dividida en dos partes, la seguridad lógica orientada a la seguridad de aplicaciones o de los servicios que la red actualmente provee y la seguridad física está orientada a la protección de los equipos y el cableado de la red.

SEGURIDAD LOGICA: La seguridad que se encuentra implementada en la Agro Industrial Paramonga S.A.A. se encuentra definida según el recurso que se desee proteger, es decir existen normas de seguridad creadas para el uso del Internet, para accesos a aplicaciones propias de la empresa, para operaciones propias de cada computador.

La empresa Agro Industrial Paramonga S.A.A. denominado como agroparamonga.com cuyo objetivo es tener un control total de la red y así poder otorgar o denegar permisos ya sea para acceso a la red como para impedir que los usuarios puedan instalar o desinstalar las aplicaciones y así poder estropear el normal funcionamiento del computador.

Cada usuario al momento de ingresar al dominio de la empresa se genera un script en el cual se mapeada una unidad y ésta apunta a una carpeta que se encuentra en el servidor de archivos al cual se realizó Backup de forma diaria, cuya finalidad es que los usuarios coloquen toda la información relevante y si ocurre algún percance no se pierda nada.

El uso del Internet se encuentra limitado por 5 tipos de perfiles en general los cuales son según la necesidad u obligaciones que posee con la empresa, esto se lo hace pese

a que todos los usuarios tienen acceso a Internet, a continuación, se detalla cual es el nombre de usuario, así como sus permisos y restricciones:

La restricción de navegador viene dada por el UTM (seguridad perimetral) el cual se encarga de bloquear puertos y de realizar un filtrado del contenido de las páginas que los usuarios desean visitar.

El servidor de correo cuyo agente de transporte de correo que utiliza es Postfix y utiliza la configuración mailbox para almacenar los correos, para evitar spam en los correos electrónicos maneja SpamAssassin; los usuarios para recibir los correos en sus estaciones de trabajo manejan Outlook, Thunderbird y google apps, para que el manejo sea más fácil y conocido.

El servidor de antivirus utiliza Sophos Central Endpoint Antivirus para que las estaciones de trabajo que posean licencias actualicen las definiciones de virus de este servidor. Las actualizaciones de dichas definiciones de virus se almacenan en el servidor y pueden ser utilizadas en cualquier momento.

Todas las estaciones de trabajo para los usuarios manejan el sistema operativo Windows 10 pro, Windows 8.0 pro, Windows 8.1 pro y Windows 7 pro. Permitiendo a las estaciones de trabajo tener un firewall integrado y con mayores seguridades.

SEGURIDAD FISICA: La seguridad de los equipos de comunicación y servidores son óptimas, dado a que existe una sala de servidores y cuartos de rack por cada área.
RED VLAN INALAMBRICA PROPUESTA: Esta implementación tiene como finalidad analizar y diseñar el segmento inalámbrico de la red de datos para la empresa, otorgando así facilidad a los usuarios que necesitan tener movilidad con su equipo por las oficinas de la empresa, este segmento de la red se ve necesaria ya que los usuarios en sus constantes reuniones o movimiento por las diversas áreas no pueden seguir con su trabajo normal.

El diseño que se presenta tiene como objetivo hacer que los usuarios continúen recibiendo todos los servicios que la red les proporciona.

Para presentar una propuesta efectiva se va a realizar pruebas con dispositivos estándar los cuales se encuentran dentro de las mismas capacidades.

CRITERIOS PARA LA IMPLEMENTACION DE LA RED INALAMBRICA:

La propuesta de diseño de red que se presenta, tiene que cumplir los requisitos básicos de conectividad, es decir brindar los servicios que el segmento cableado lo hace; siempre brindando una buena transmisión y recepción de datos.

Brindar soporte a todos los usuarios que realicen uso de este segmento de red, sin ninguna preocupación de saber cuántos usuarios simultáneos se encuentran conectados a la red.

El segmento inalámbrico debe tener la capacidad de llegar a todas las áreas de trabajo de la empresa siempre brindando una óptima calidad de señal, detectar y evitar pérdidas de señal.

Brindar seguridad en el segmento inalámbrico, con el fin de mantener todos los datos de la empresa en total confidencialidad.

Todos los aspectos de red antes mencionados pueden ser solucionados por medio de la buena ubicación de los puntos de acceso y la correcta configuración de los equipos.

Al diseñar una red inalámbrica, el cual va a dar servicio a cada área que la empresa actualmente posee, es decir todos los puntos de acceso van a ser colocados de manera esquemática, esto implica que se tiene que diseñar envidando la interferencia co- canal e interferencias inter-canales de las señales de los dispositivos inalámbricos y así limitar la capacidad de la red inalámbrica.

FASE DE LA PLANEACION: En esta fase se realizará los siguientes análisis:

Análisis de servicios de red y revisión de la topología de red LAN.

Evaluación de esquemas de seguridad (ACL'S, FILTROS, Políticas de Seguridad de firewall, etc.).

Revisión de la estructura de la red de SWITCHS (VLANS, ROUNTING, SPANNING TREE, LOOPBACK DETECTION, 802.1x, etc.)

La Empresa AGRO INDUSTRIAL PARAMONGA, cuenta con una estructura basada en red LAN basada en:

Servicios de acceso LAN a través de Switchs administrables y no administrables D-LINK, CISCO, 3COM y HP.

Servicios de acceso a internet a través de Proxy.

Servicio de acceso inalámbrico WiFi y radio enlaces.

Telefonía IP y Comunicación entre sedes a través del proveedor de servicios VPN

Tabla 09: Relación de equipos de comunicación por ubicación

RELACION DE EQUIPOS DE COMUNICACION POR UBICACION			
AREA	SWITCH	MARCA	ADMINISTRABLE
DATA CENTER	DGS-3120-48PC	DLINK	SI
DATA CENTER	DGS-3450	DLINK	SI
DATA CENTER	CATALYST SERIE	CISCO	SI
DATA CENTER	DGS-3612G	DLINK	SI
LABORATORIO	2952-SFP PLUS	3COM	SI
CAMPO	DES-3028P	DLINK	NO
CAMPO	DES-3028	DLINK	NO
FABRICA	DES-3028	DLINK	SI
SALA DE COMUNICACIONES	DGS-3120-48PC	DLINK	NO
SALA DE COMUNICACIONES	DGS-3120-48PC	DLINK	NO
PROYECTOS	2928 PWR PLUS	HP	NO
PROYECTOS	2928 SFP PLUS	HP	NO
CONTABILIDAD	CATALYST 2960	CISCO	SI
PERSONAL	DES-1024R	DLINK	SI
SEMA	DES-3028	DLINK	SI
BALANZA DE CAÑA	DES-3028	DLINK	NO
LEGAL	DES-3028P	DLINK	SI
LOGISTICA / ALMACEN	2426 PWR PLUS	3COM	SI
TRANSPORTE	DES-3028	DLINK	NO
TALLER ELECTRICO	DES-3526	DLINK	SI
PLANTA DE FUERZA	DGS-3100-24	DLINK	SI
CO-GENERACION	DES-3526	DLINK	SI
TRAPICHE	DES-3028	DLINK	SI

Fuente: Elaboración Propia

DESCRIPCION Y SITUACION ACTUAL DE LOS SERVICIOS DE RED

AIPSA actualmente cuenta con múltiples Switchs administrables y stand-alone **(no administrables),** los cuales se ubican en diferentes áreas, tal y como se indica en el cuadro anterior: Algunos equipos de comunicación son aquellos equipos que nos

son administrables, además he observado que tienen una variedad de marcas como 3COM, CISCO, HP, DLINK, Etc.

Lo recomendado es tener equipos de comunicación de una sola marca para así poder tener un parque homogéneo de equipos y la administración sea una sola para poder asegurar el buen funcionamiento de la red de Datos y la optimización de la misma. Durante el levantamiento de información que se realizó en sus oficinas se pudo observar que muchos de los equipos de comunicación que son administrables se encuentran sin ninguna configuración, no tienen direccionamiento IP, algunos de ellos tenían direcciones IP de fábrica ò de cualquier segmento de red diferente a la de AIPSAA.

En algunas ocasiones generan cierta lentitud al momento de realizar la transmisión de los paquetes de información dentro de la red LAN del cliente.

Según la información obtenida en primera línea y debido a que se tiene que realizar el monitoreo de todos los equipos de la Red, se tuvo que asignar direcciones IP a cada uno de los equipos administrables de marca DLINK, en coordinación con el administrador de toda la infraestructura tecnológica.

A Partir de esta asignación de direcciones IP definimos que el equipo DGS-3612G asignado con IP 10.100.16.2 es el equipo Principal de toda la red de Datos, razón por la cual todos los enlaces de Fibra, Cobre y salida hacia Internet son administrados a través de este equipo.

Cabe resaltar que las funciones del **SWITCH DE CORE (Equipo DGS-3612G)** corresponden a la organización lógica de toda la estructura de red, y por lo tanto es el equipo principal por el cual se transmite toda la información que se produce dentro de la red de datos y voz; debido a que a este equipo llegan todas las conexiones provenientes de los diversos locales de la institución a través de los Switchs de distribución y borde respectivamente.

Figura 22: Gabinete principal
Fuente: Elaboración Propia

Con la información obtenida de cada equipo de comunicación más las visitas que hemos realizado a sus instalaciones podemos concluir en lo siguiente:

El DATACENTER de AIPSAA no está correctamente diseñado para soportar una arquitectura de red compleja, ya que el sistema de cableado estructurado no cuenta con los accesorios de ordenamiento y etiquetado para la identificación de los puntos, no hay sistemas de monitoreo para la red de equipos de comunicación, servidores, sistemas de protección y redundancia de energía eléctrica.

Además, la infraestructura tecnológica actual de AIPSAA no cuenta con una gestión y administración de equipos de comunicación optima, en la actualidad la red no se encuentra gestionada, ya que no existe segmentación **(VLANS)** ni monitoreo de los eventos que se producen diariamente dentro de la red **(identificación de hosts, asignación de direcciones IP, acceso a servicios de red, Etc.).**

La red de Datos es una red Plana, no se encuentra segmentada y dividida para prestar servicios óptimos de telefonía, transmisión de datos, internet, Etc.

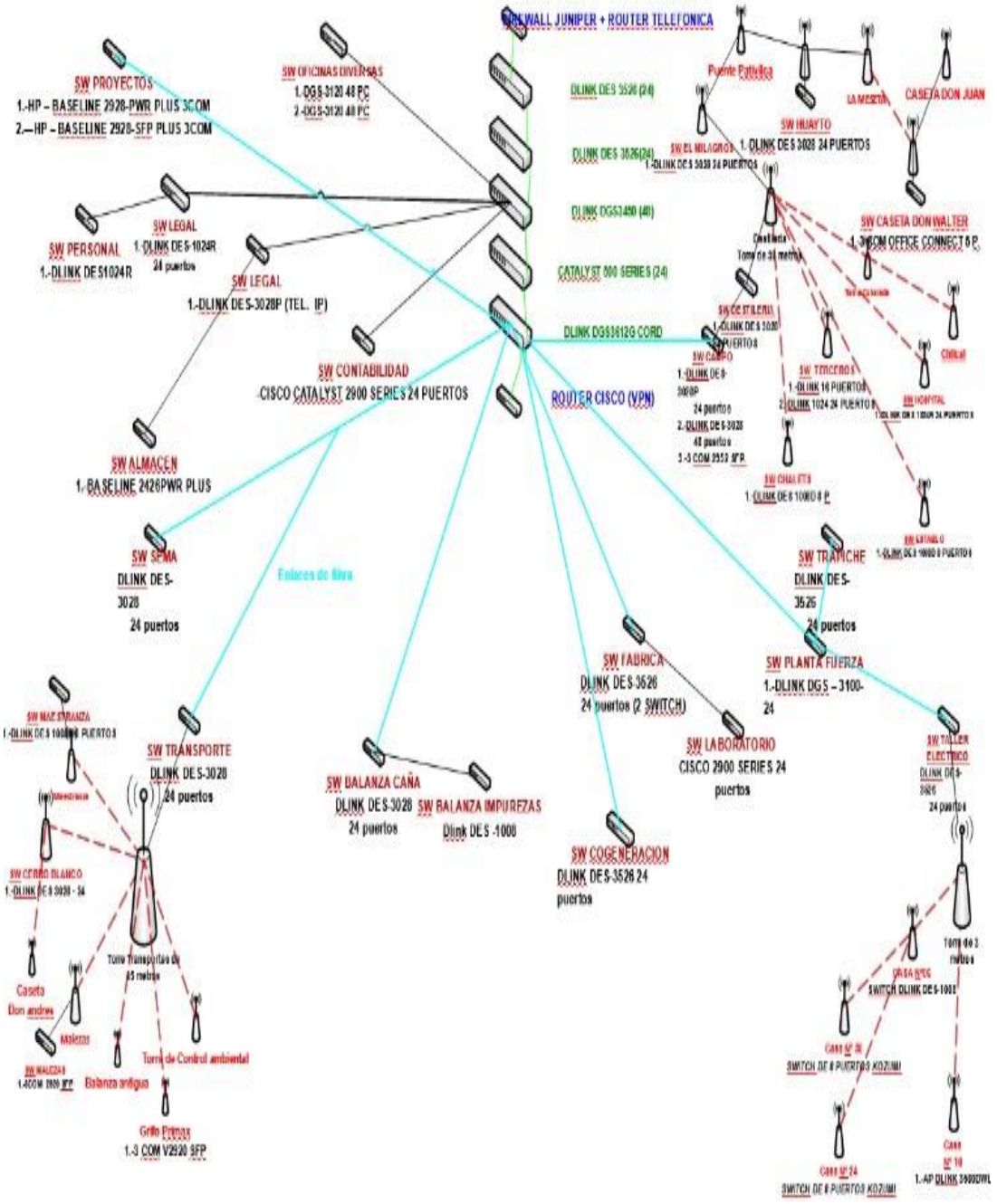


Figura 23: Plano de red AIPSA

Fuente: Elaboración propia

Cabe señalar que los Switchs permanecen con la función básica de solo brindar acceso a la red de datos

El cableado estructurado que tienen actualmente no tiene categoría y está expuesto a

presentar fallas y errores de trasmisión de paquetes, desde la malformación de una cabecera del paquete a ser transmitido desde el inicio hasta la recepción del mismo, además pueden presentar loop de datos dentro de su misma RED, lentitud, etc.

Figura 24: Gabinete Torre Principal
Fuente: Elaboración propia

Se puede observar que el equipo de comunicación está expuesto al Polvo, humedad, inclemencia del clima y además no cuenta con un Patch Panel, los puntos de Red llegan de manera directa al Switch, y no se encuentran identificados ni certificados, estos tipos de problemas son los que mayormente hacen que la red sea inestable y lenta.

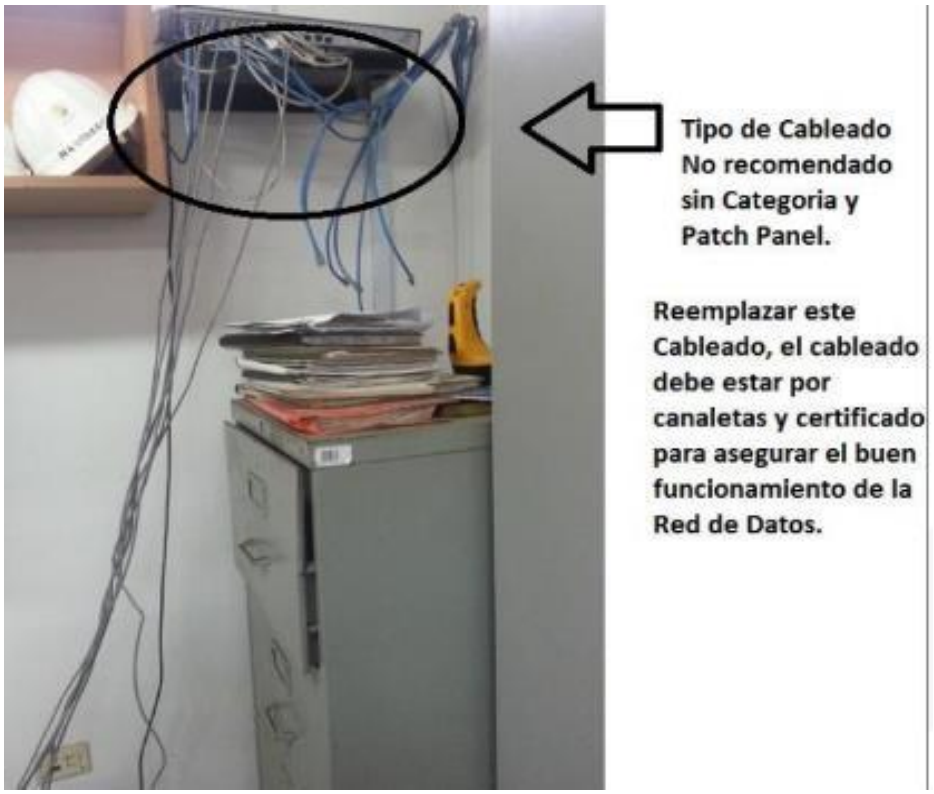


Figura 25: Switch de Transporte
Fuente: Elaboración propia.

Otro Gabinete expuesto a ser manipulado por cualquier usuario, además se puede observar que el cableado que alimenta al equipo de comunicación no cuenta con los estándares mínimos para brindar un buen servicio de red.

Además, proliferan equipos pequeños no administrables en la red, que dadas sus características solamente son usados para apalear el problema de escasez de puntos de red o en todo caso cubrir mayores distancias, tal es el caso de los equipos ubicados en todas las áreas.

Ninguno de los equipos de comunicación cuenta con un gabinete debidamente acondicionado.

No existe un sistema de cableado estructurado, tal y como se muestra en las fotografías los enlaces de los puntos de red, llegan directamente hacia los puertos de los Switchs, sin pasar por los Patch panel.

No se cuenta con un DATACENTER alterno (BACKUP), el cual garantice la operatividad de los servicios de red LAN, internet y telefonía de las demás sucursales en caso suceda alguna caída de servicios (corte de energía, colapso de las líneas de fibra óptica, mantenimiento físico de los equipos, etc.).

La red no cuenta con servicios extensivos de uso de la INTRANET (vlans, routing LAN, calidad de servicio, segmentación de ancho de banda, etc), y aun así ya se avizoran futuros proyectos para la implementación del mismo hacia todos los usuarios de la red, tanto administrativos, operativos e invitados (actualmente con soporte a 700 y próximamente a 1500 usuarios) lo cual exigirá mayor cantidad de proceso y almacenamiento tanto en la red de servidores como en los equipos de comunicación (principalmente el Switchs core).

OTROS SERVICIOS QUE FORMAN PARTE DE LA INFRAESTRUCTURA TECNOLOGICA DE AIPSAA.

INTERNET. Los mecanismos de seguridad para el acceso a internet se dan desde el servidor PROXY (control de acceso a páginas web), el firewall (control de acceso por puertos de servicio) y el Switchs controlador wireless (seguridad por MAC).

No se establecen cuotas de consumo ni horarios de acceso hacia dichos servicios, tanto para la red de los usuarios administrativos, producción e invitados.

No existe un sistema de respaldo (Backup) y contingencia (redundancia) en caso fallen los equipos que proporcionan los accesos, particularmente se menciona el firewall y el proxy.

SERVICIO DE ACCESO INALAMBRICO. AIPSA cuenta con servicios de acceso inalámbrico a la red a través de Access Points DWL-3200AP.

Estos equipos funcionan de manera independiente (diferentes configuraciones por equipo) en toda la red de la institución.

OBSERVACIONES. Los mecanismos de seguridad empleados corresponden a un sistema basado en WPA – PSK también conocido como WPA casero.

No existe el roaming entre los Access point.

La seguridad inalámbrica se da a través de las direcciones MAC de los usuarios, esto condiciona a que solamente se puedan ingresar hasta un máximo de 16 direcciones por Access Point.

Los usuarios inalámbricos registrados acceden de forma libre y espontánea a todos los servicios de la red LAN sin ningún tipo de restricción.

Actualmente no existe un mecanismo eficiente para medir el ancho de banda consumido por estos usuarios.

Algunas áreas de la institución no cuentan con un servicio de acceso inalámbrico adecuado, debido a que su estructura física contiene hierro y concreto reforzado, ocasionando que la señal de los equipos inalámbricos se debilite y por lo tanto no atienda a las solicitudes de conexión.

TELEFONIA IP. AIPSA cuenta con el servicio de telefonía ip, los cuales son gestionados desde LIMA, en una red paralela a la red de datos.

OBSERVACIONES. Los teléfonos IP, trabajan a una velocidad de 10/100 Mbps a ellos se conectan las estaciones de trabajo, ello permite el uso de la red de datos y telefonía sobre un mismo puerto.

EVALUACION DE ESQUEMAS DE SEGURIDAD

SITUACION ACTUAL. Los sistemas de seguridad de acceso en la red se encuentran gobernados desde los siguientes frentes:

Internet: a través del servidor proxy y el firewall JUNIPER 55GS.

Red LAN no existen VLAN´S y políticas ACL sobre la red.

LAN Inalámbrica: seguridad WPA-PSK.

Las políticas del servidor proxy incluyen la denegación de acceso hacia determinadas direcciones web, mas no se usan las funciones avanzadas tales como proxy caché).

El proxy solo gobierna las conexiones de la red de los usuarios administrativos más

no la de los usuarios inalámbricos.

El firewall solamente se utiliza para brindar acceso hacia determinados servicios de internet a través de listas de puertos TCP/UDP.

El firewall no se utiliza para publicación de servicios ni para el control de consumo máximo de ancho de banda, por lo tanto, muchas de sus funciones no se están aplicando.

El acceso a la red inalámbrica está condicionado a utilizar un sistema de seguridad basado en wpa y filtro de direcciones MAC.

La capacidad máxima de direcciones MAC que admite cada Access point es de 16.

Este método de seguridad, no permite una actualización eficiente de los accesos ya que constantemente hay que evaluar que usuarios acceden a los servicios y cuáles no para eliminarlos de la base de datos.

No existen herramientas de software implementadas en la red, que permitan monitorear los equipos que se ubican en la red.

RECOMENDACIONES. A continuación, detallaremos todas las mejoras que se deben implementar para mejorar y optimizar la RED de Datos de AIPSAA.

Realizar el cambio total de su cableado de RED por una cableada Estructurada categoría 6ª, el mismo que debe está certificado en cada uno de sus Puntos.
Acondicionamiento de su Data Center de manera óptima, el cual deberá contemplar lo siguiente:
Cableado estructurado categoría 6a
Gabinete independiente para los equipos de comunicación.
Red de energía independiente con su propio tablero de energía estabilizada.
Estabilizador de Ultra aislamiento.
Tomas de energía estabilizada y con toma a tierra.
Instalación de un UPS para futuros corte de energía.
Contar con aire acondicionado de precisión.
Contar con un sistema de Seguridad y Monitoreo de todos los equipos principales de la Red de Datos.
Contar con piso técnico y falso techo.

Contar con un Switchs de chasis de CORE **(De preferencia)** con mayor capacidad de proceso **(CPU y MEMORIA)**, que pueda atender las necesidades futuras de la institución, para lo cual la siguiente línea de productos en el fabricante D-LINK corresponde al Switchs DGS-6608, como se muestra en la imagen.
La otra opción más económica contemplaría el uso de 2 unidades correspondientes a la serie de Switchs DGS-3620, los cuales se colocarían en stack (formando un enlace de 10 Gigabytes).

A continuación, un comparativo entre los Switchs recomendados (DGS-3620 y DGS-6608) y el Switchs core actual DGS-3612.

Dada la capacidad de dichos equipos de poder trabajar en slots, se recomienda trabajar con opciones modulares es decir adquiriendo solo los módulos que se necesitan y luego ir agregando según las necesidades de la institución.
Contar con un Data Center alterno.

Las futuras adquisiciones de Switchs de distribución y/o borde deberán contemplar puertos POE (power over Ethernet) ya que estos equipos permiten energizar sobre el mismo cableado a otros equipos que usan la red tales como teléfonos IP, AP, etc. Ello evitaría el uso de un cableado eléctrico por equipo.

Eliminar de forma definitiva el uso de equipos no administrables en la red, (Cascadas) en el caso de requerir poca densidad de puertos se puede optar por la línea Smart de dlink , como el DGS-1210P o cualquiera en la línea de dichos productos.
Actualizar las versiones de firmware de todos los equipos, esto permitirá agregar nuevas funciones a los equipos, así como también solucionar problemas de funcionalidad reportados por otros usuarios en diversas localidades del mundo donde el fabricante opera.

Elaborar documentos de uso interno, donde se explique a detalle el funcionamiento y la operación de cada equipo, principalmente el Switchs de CORE, ya que la misma gobierna la red y si en algún momento se pierde la configuración, se podrá entregar

al personal que se encargara de la implementación, el manual conteniendo toda la información actualizada del mismo.

Realizar backups de las configuraciones de todos los equipos en la red.
Capacitar al personal en el uso de las diversas tecnologías implementadas en la red de AIPSA.

Asignar un mayor número de personal para el uso y mantenimiento de los sistemas involucrados en la red (switching, servidores, wireless, etc.).

Implementar y capacitar al personal involucrado en el uso de sistemas de monitoreo de red, ya que dichos sistemas permitirán informar en tiempo real el status de operación de los equipos.

VENTAJAS PARA LA INSTITUCION. La implementación de un Switchs de CORE con mayores capacidades, permitirá el uso de aplicaciones que requieran mayor carga en la red tales como videoconferencia en LAN, copias de respaldo en tiempos menores, uso extensivo de los servicios de intranet (web, correo, streaming, multimedia, etc.), crecimiento modular (se pueden ir agregando más puertos al Switchs de acuerdo a los slots libres), etc.

Al contar con soluciones de Backup y redundancia se asegura la continuidad de los servicios de red sin que se afecte en mayor medida la productividad de la institución.

El uso de sistemas de cableado estructurado permitirá una mayor organización y orden en las instalaciones del Data Center (etiquetado de cables, identificación de puntos, fácil tendido de nuevos puntos, etc.).

SERVICIOS DE ACCESO INALAMBRICO

RECOMENDACIONES. Considerar la implementación de un Switchs Controlador inalámbrico (DWS- 4026) el cual será el encargado de gestionar todos los Access Point de la red (DWL-6600AP).

Mejorar la forma de registro de los usuarios a través de sistemas basados en "portal cautivo", que utilicen las credenciales de acceso del usuario (según directorio activo) y no las direcciones MAC de sus tarjetas de red inalámbricas, ya que dicho método ofrece poca seguridad para el acceso (mediante determinado software se puede clonar la MAC y se brinda acceso a usuarios ajenos a la red).

Considerar el uso de antenas sectoriales en los Access points ubicados en los bordes perimetrales de AIPSA, ya que actualmente cuentan con antenas omnidireccionales, debido a ello la señal es percibida fuera del perímetro de la institución.
Para las zonas donde no se tenga cobertura inalámbrica, se plantea el uso de más Access points.

Para las zonas donde exista una pobre señal de cobertura, se plantea la redistribución de los Access points más cercanos (verificar cercanía a objetos que causen interferencia como columnas, puertas metálicas, etc) y/o utilizar antenas externas de mayor potencia (las actuales son de 5dbi de ganancia).

VENTAJAS PARA LA INSTITUCION. Hoy en día la disponibilidad de los servicios de comunicación inalámbrica en muchas instituciones garantiza el acceso inmediato a los datos y recursos de red en lugares donde por múltiples razones no se puede usar red cableada.

El uso de sistemas de portal cautivo donde el usuario solo tiene que ingresar sus credenciales (usuario y password) a través de un portal web institucional que a la vez sea informativo generara una muy buena acogida, como ya lo es en muchos lugares del mundo, además de garantizar la seguridad de la información transmitida y recibida.

Se garantizará la fluidez de las comunicaciones inalámbricas en la institución a través de mayor cantidad de Access points y/o antenas de mayor potencia.

TELEFONIA IP. AIPSA cuenta con el servicio de telefonía ip, los cuales son

gestionados desde LIMA, en una red paralela a la red de datos

OBSERVACIONES. Los teléfonos IP, trabajan a una velocidad de 10/100 Mbps a ellos se conectan las estaciones de trabajo, ello permite el uso de la red de datos y telefonía sobre un mismo puerto.

RECOMENDACIONES. Verificar si todos los teléfonos pueden trabajar con vlans. Para las estaciones de trabajo que requieran mayor ancho de banda, contar con teléfonos ip que incluyan puertos Gigabit (ejm. Polycom Soundpoint IP 560) o en todo caso contar con puntos de red cableada adicional.

VENTAJAS PARA LA INSTITUCION. Contar con teléfonos IP que soporten vlans en su configuración, permitirá segmentar la red de datos con respecto a la red de telefonía.

Contar con conexiones de mayor velocidad permitirá aplicar nuevas funciones en los sistemas de telefonía, tales como video llamada.

Una mayor velocidad en los puertos de los teléfonos también permitirá que las PC´s conectadas al mismo accedan a la red con mayor eficiencia.

FASES DE DISEÑO.

En esta fase se realiza el diseño de redes de área local virtual, para mejorar el rendimiento de la red, proveer seguridad, segmentación, mejor administración de red, reducción de costos, uso adecuado y jerárquico cumpliendo con todos los estándares de red. La infraestructura tecnológica con que se cuenta dentro de las instalaciones de la empresa, permite soportar Redes Virtuales, permitiendo así implementar toda la gama de configuraciones para mejorar el desempeño de la LAN.

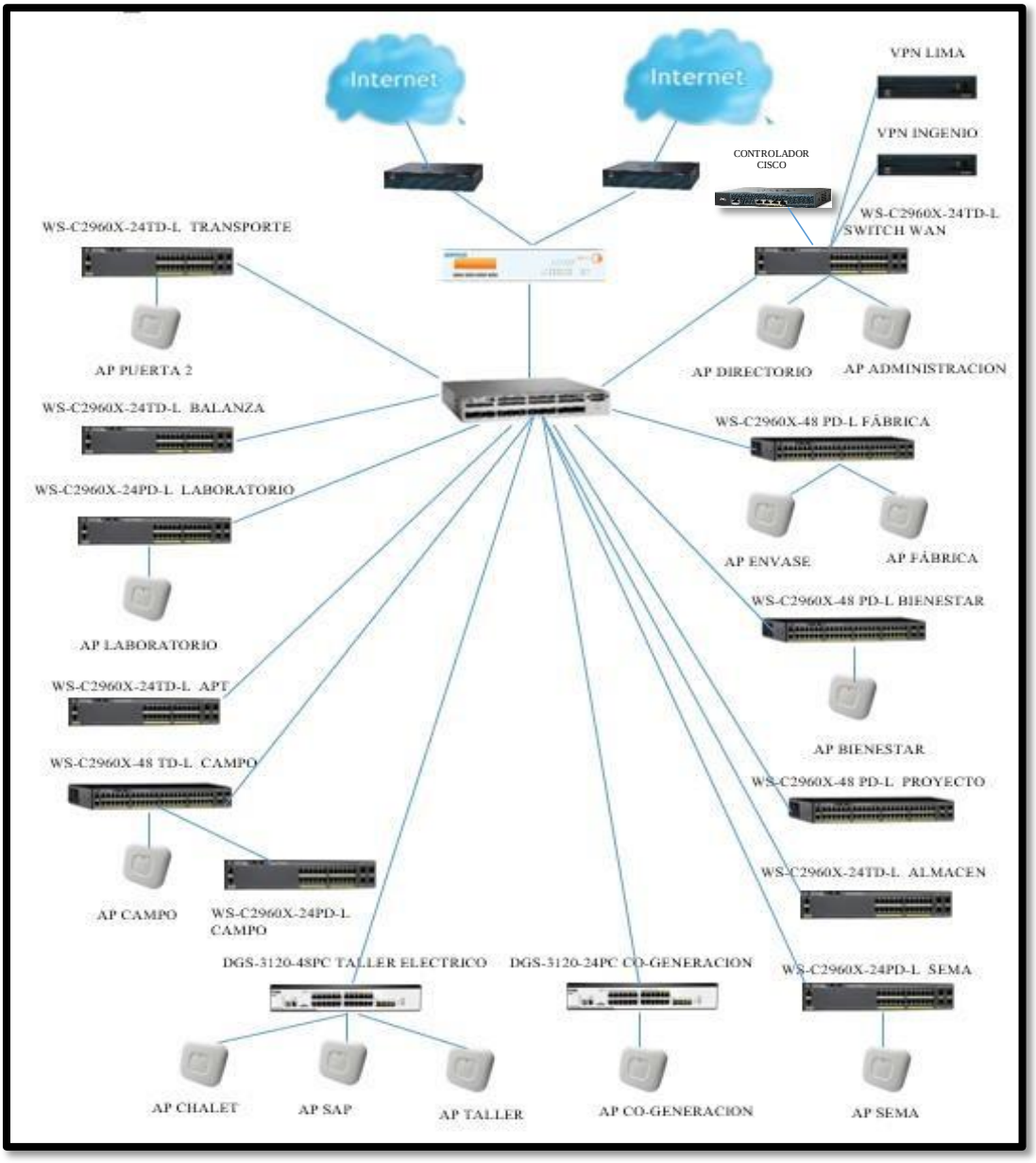


Figura 26: Diseño de Red

Fuente: Elaboración Propia

DISEÑO DE RED SWITCH WS-C3850-24XS-S CORE DATA CENTER

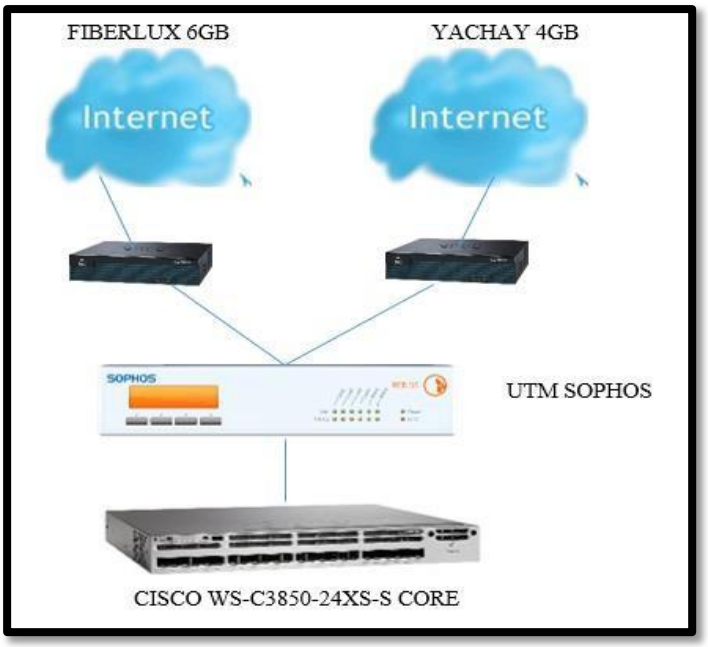


Figura 27: Diseño de red Switchs Core

Fuente: Elaboración Propia

DISEÑO DE RED SWITCH WS-C2960X-24TD-L WAN

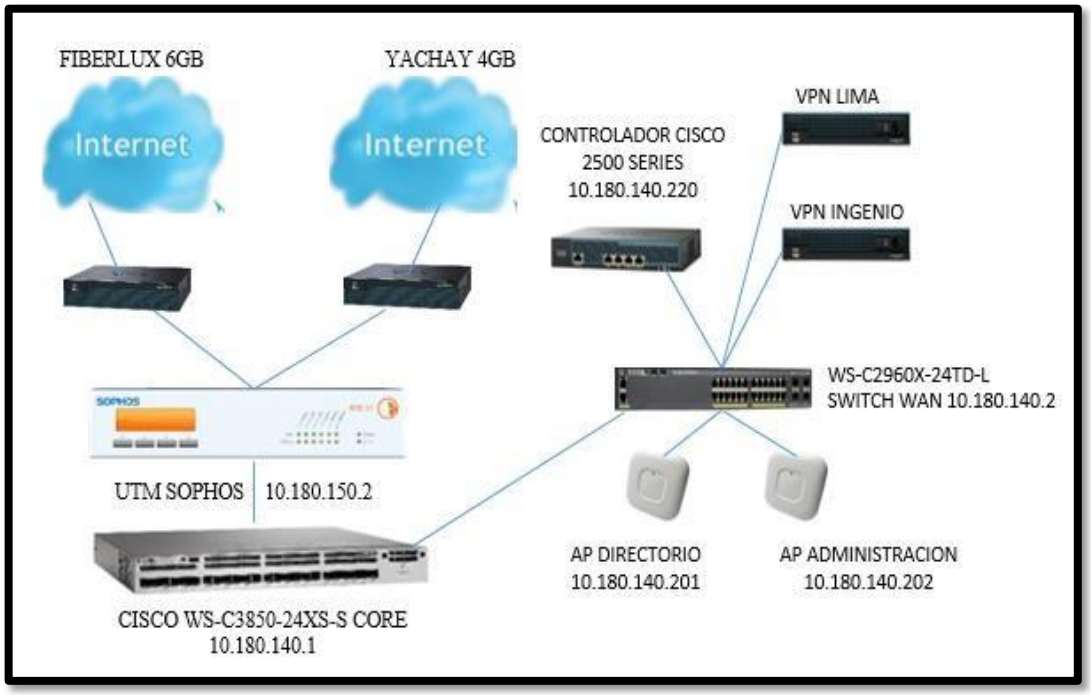


Figura 28: Diseño de red Switchs Wan

Fuente: Elaboración Propia

DISEÑO DE RED SWITCH WS-C2960X-48 PD-L PROYECTO

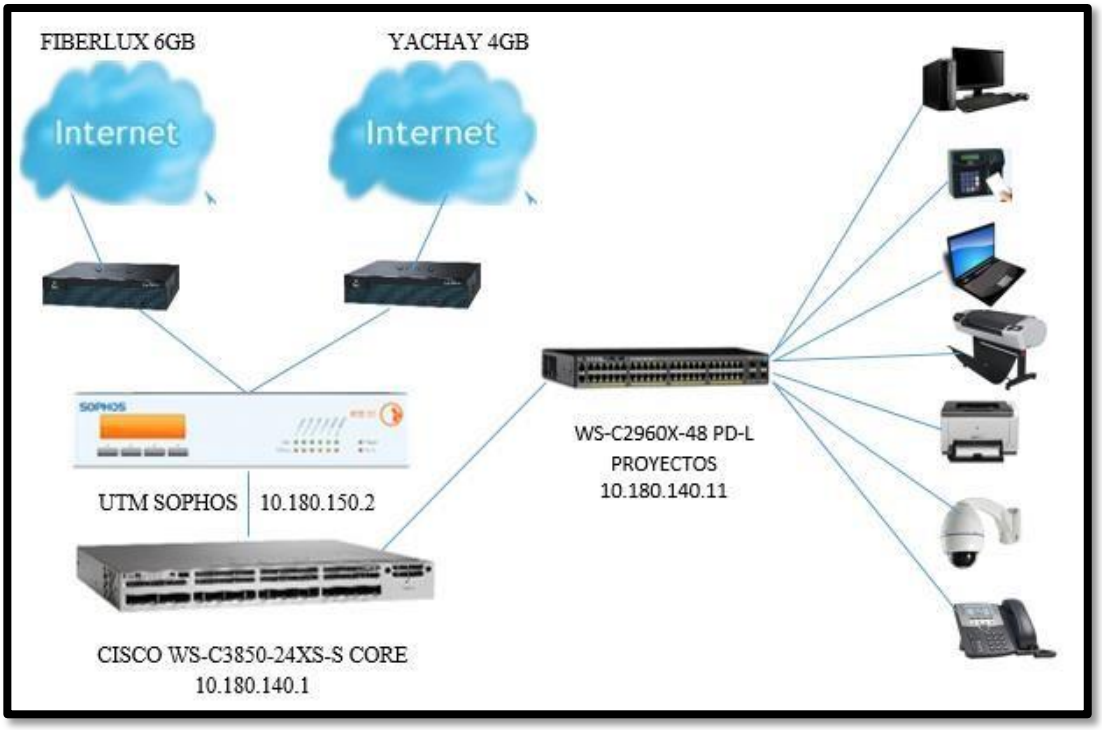


Figura 29: Diseño de red Switchs Proyectos

Fuente: Elaboración Propia

DISEÑO DE RED SWITCH WS-C2960X-48 PD-L FÁBRICA

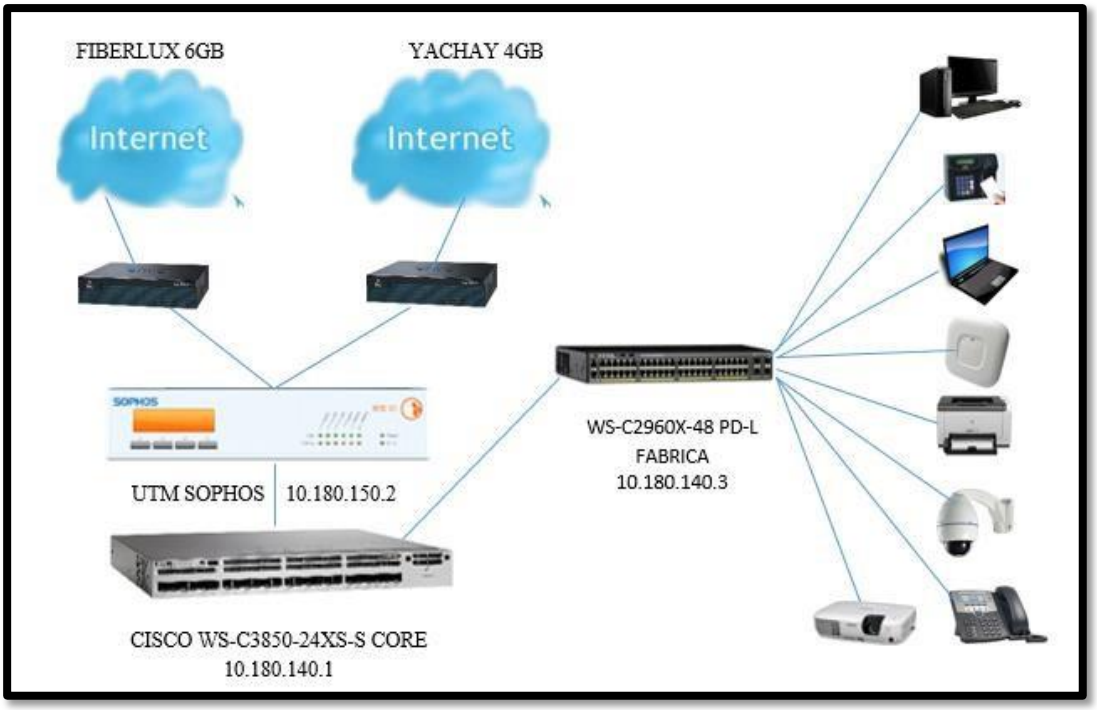


Figura 30: Diseño de red Switchs Fábrica

Fuente: Elaboración Propia

DISEÑO DE RED SWITCH WS-C2960X-48 PD-L AREAS DIVERSAS

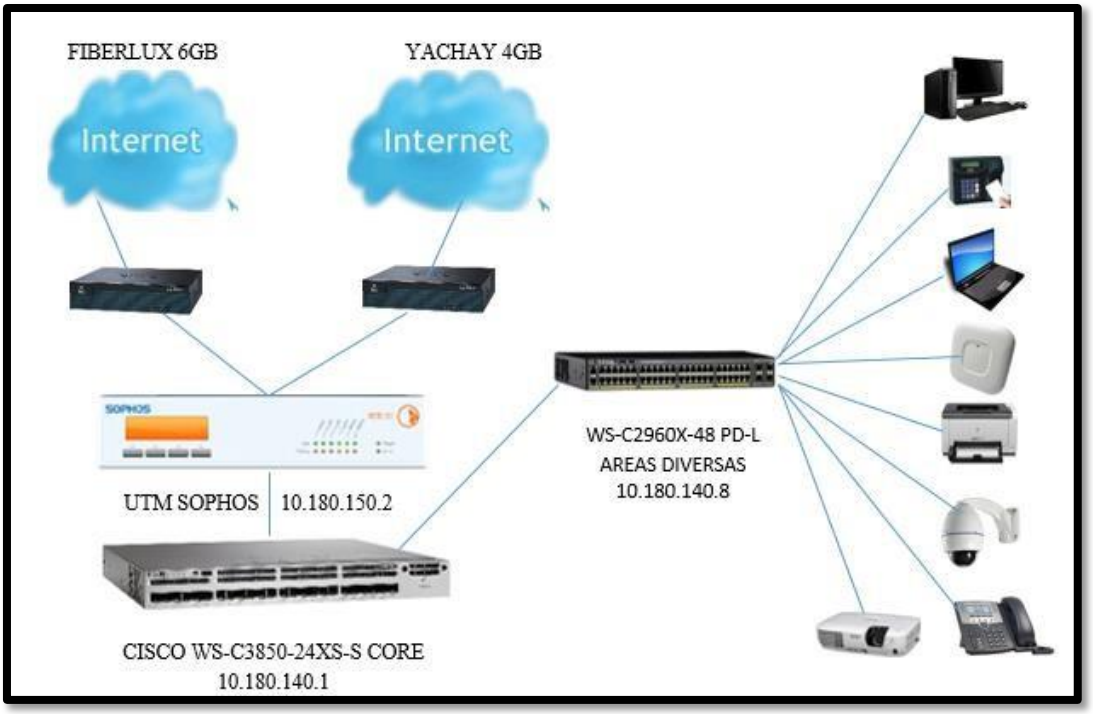


Figura 31: Diseño de red Switchs Áreas Diversas

Fuente: Elaboración Propia

DISEÑO DE RED SWITCH WS-C2960X-24 PD-L APT

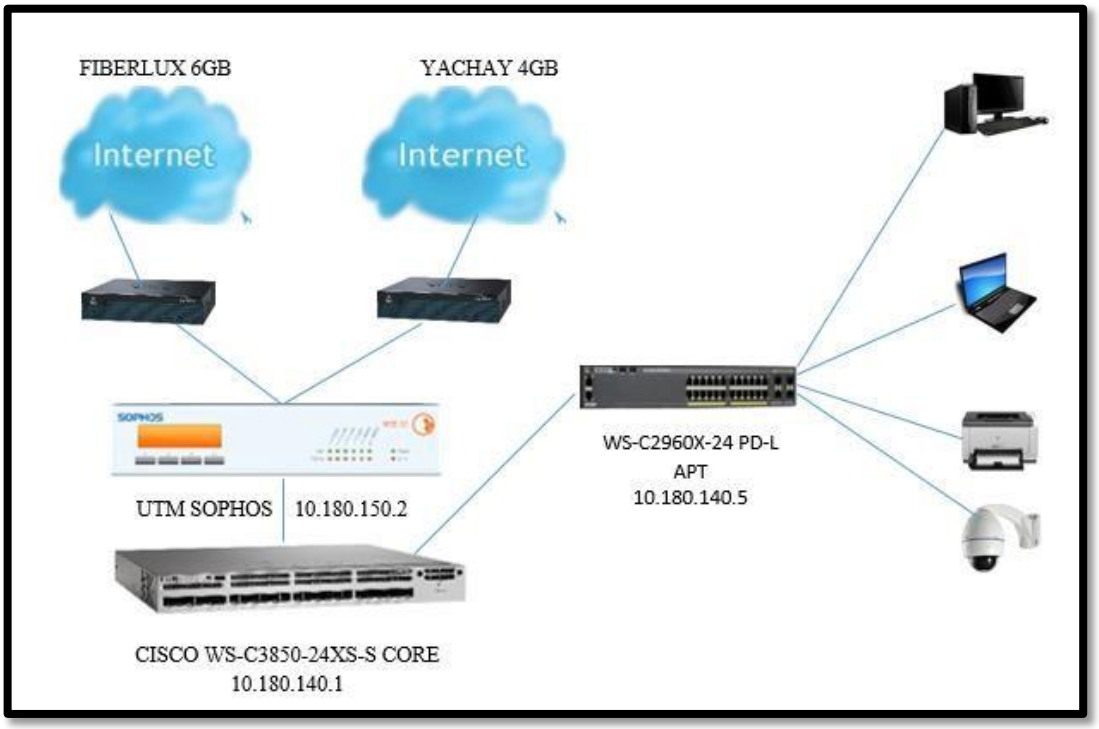


Figura 32: Diseño de red Switchs Apt

Fuente: Elaboración Propia

DISEÑO DE RED SWITCH WS-C2960X-24 PD-L BALANZA

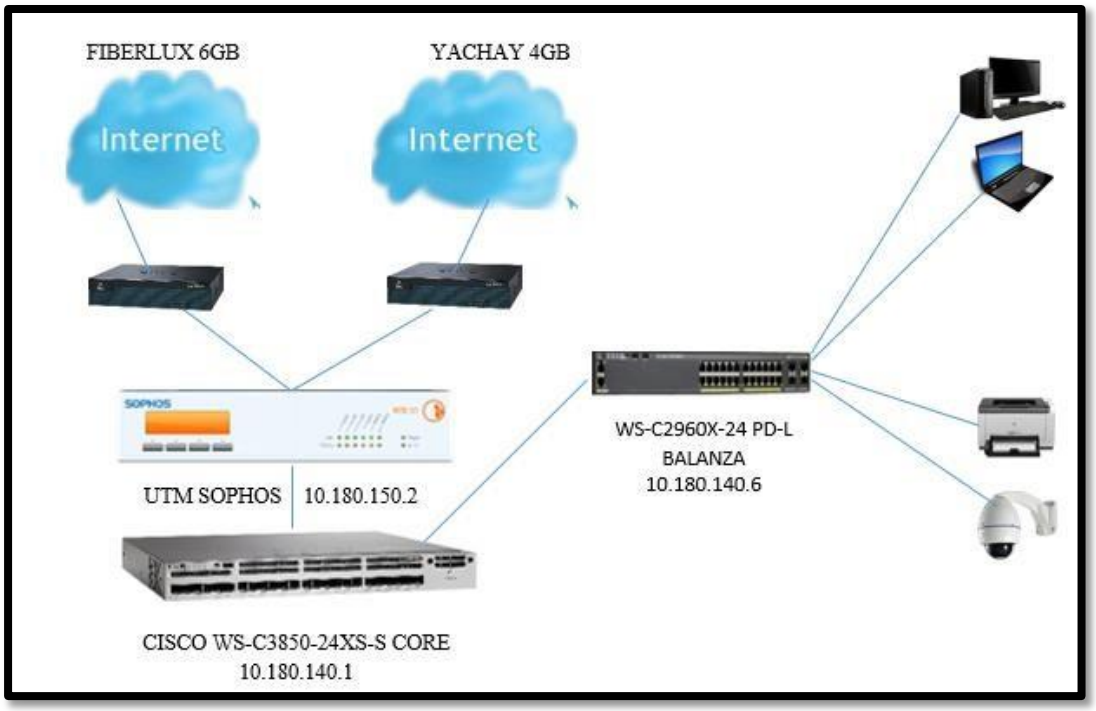


Figura 33: Diseño de red Switchs Balanza

Fuente: Elaboración Propia

DISEÑO DE RED SWITCH WS-C2960X-24 PD-L LABORATORIO

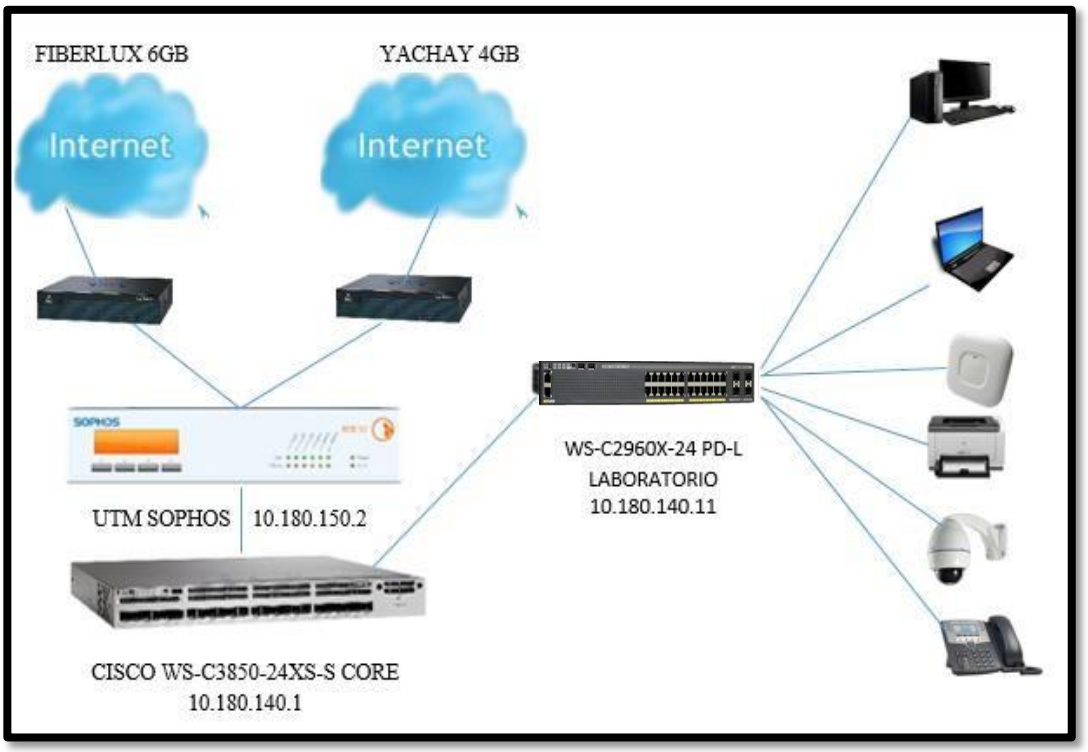


Figura 34: Diseño de red Switchs Laboratorio

Fuente: Elaboración Propia

DISEÑO DE RED SWITCH WS-C2960X-24 TD-L TRANSPORTE

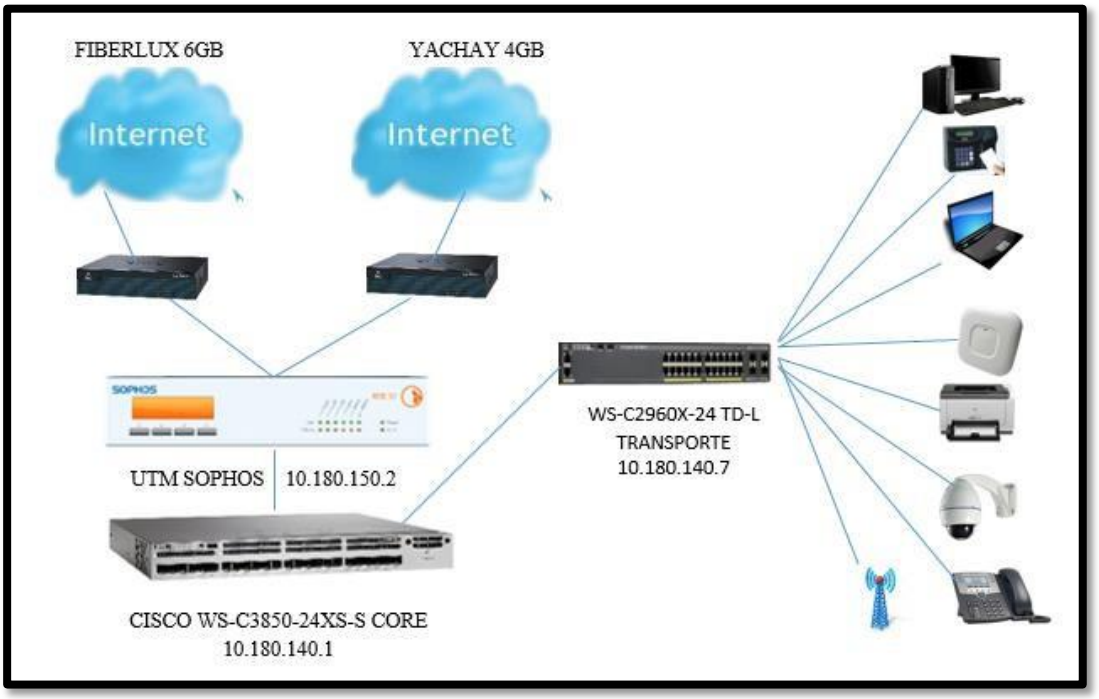


Figura 35: Diseño de red Switchs Transporte

Fuente: Elaboración Propia

DISEÑO DE RED SWITCH WS-C2960X-24 PD-L / C2960X-48 TD-L CAMPO

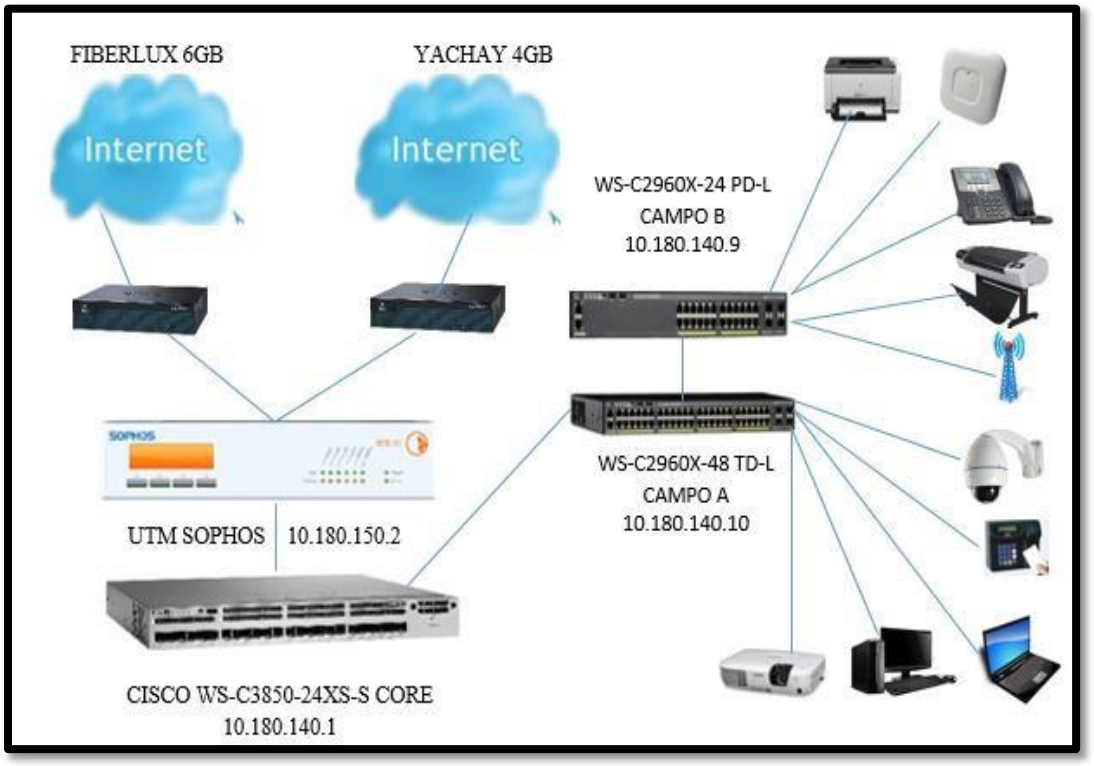


Figura 36: Diseño de red Switchs Campo

Fuente: Elaboración Propia

DISEÑO DE RED SWITCH WS-C2960X-24 PD-L SEMA

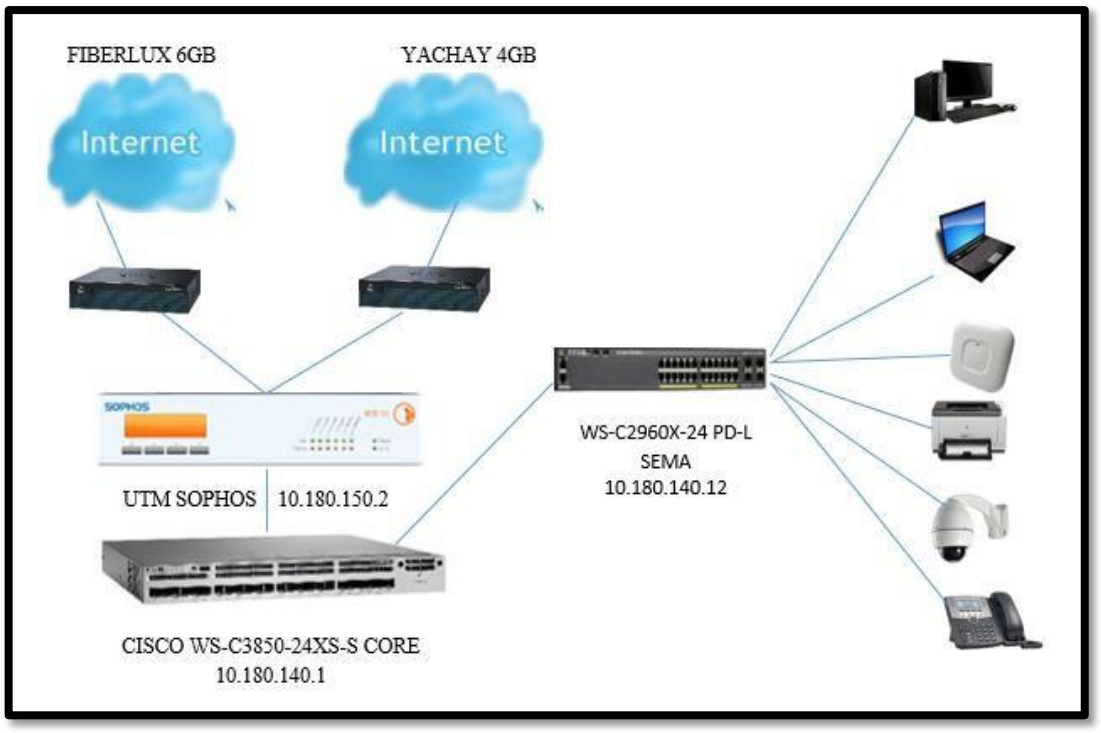


Figura 37: Diseño de red Switchs Sema

Fuente: Elaboración Propia

DISEÑO DE RED SWITCH WS-C2960X-24 TD-L ALMACEN

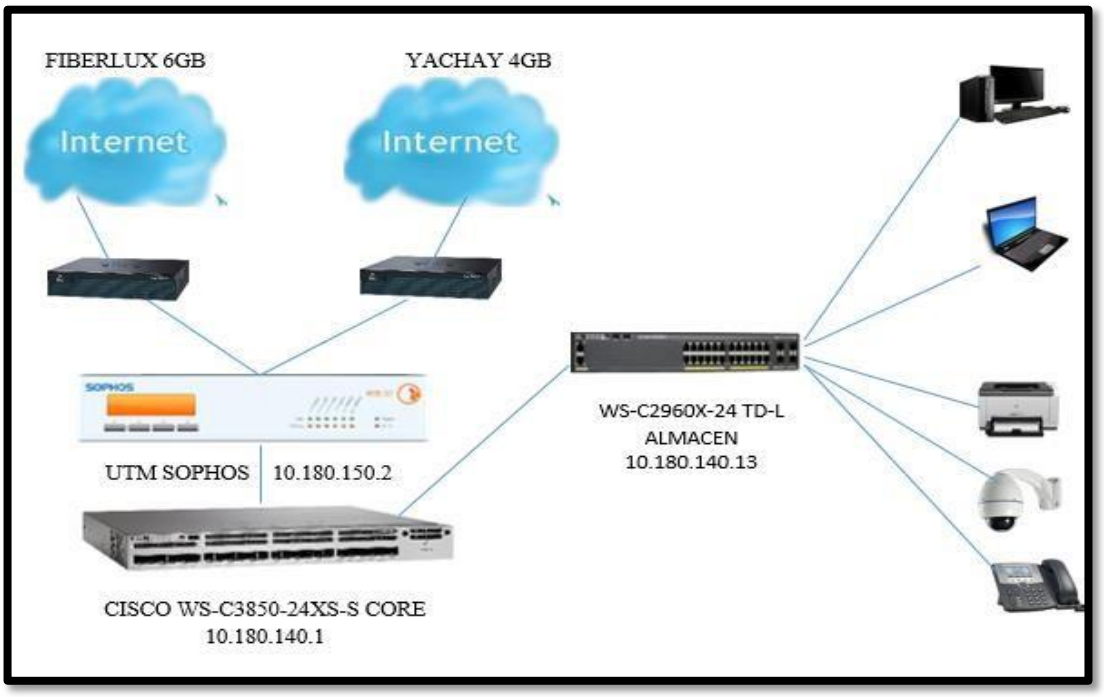


Figura 38: Diseño de red Switchs Almacén

Fuente: Elaboración Propia

DISEÑO DE RED INALAMBRICA

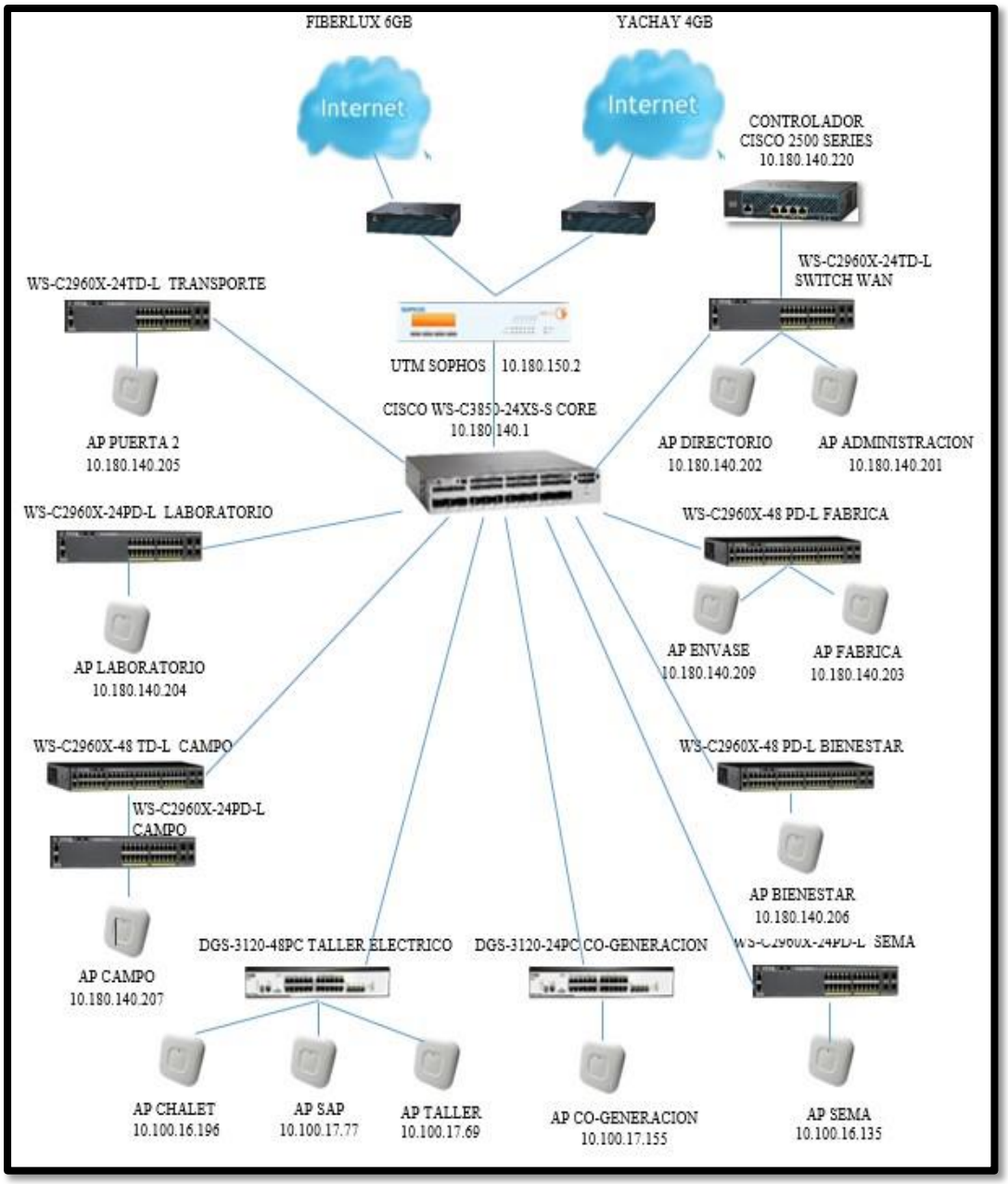


Figura 39: Diseño de red Inalámbrica

Fuente: Elaboración Propia

FASE DE IMPLEMENTACION

Un factor que se debe considerar y que se debe tener especial énfasis, ya que es el tema en el cual radica el proyecto es en la creación de VLAN, tecnología que permite crear dominios de difusión más pequeños reduciendo considerablemente afectaciones en la red local, una característica que hace viable y atractiva la implementación de VLAN es la mejora en el aspecto de seguridad en la red local, permitiendo crear grupos de VLAN según su función en una misma red local.

Las redes VLAN agrupan a las redes de forma lógica en vez de física lo que permite que los usuarios y grupos de trabajo estén en diferentes ubicaciones geográficas. Al disminuir los usuarios de un mismo grupo lógico distribuidos en diferentes segmentos se aumenta el ancho de banda para el grupo de usuarios. Con los nuevos segmentos se pueden implementar diferentes topologías y protocolos para cada uno, permitiendo el control absoluto del tráfico de entrada y salida de las VLAN hacia otras.

La implementación de las VLAN en los segmentos de usuarios, servidores y voz, garantiza una mejor distribución y seguridad en la red, permitiendo localizar rápidamente posibles problemas a futuro además de minimizar los dominios de broadcast.

Para este proyecto, la implementación de VLAN se desarrolló en toda la instalación de la empresa AGRO INDUSTRIAL PARAMONGA, la asignación sería de la siguiente manera.

Tabla 10: Vlans por tipo

TIPO	**N° VLAN**
SERVIDORES	1
RED LAN 1	10
RED LAN 1	20
RED DE IMPRESORAS	30
RED DE TELEFONIA IP	40
UPS (Proyectado)	50
CAMARAS	60
DATA CUARTO CONTROL (Proyectado)	70

SERVIDORES (Proyectado)	80
RED WI-FI	90
CELDA DE ENERGIA (Proyectado)	100
EQUIPOS BALANZA (Proyectado)	110
ACCESOS PUERTAS	120
VIDEO CONFERENCIA	130
SWITCH	140
ENLACES ISP (Proyectado)	150
	160

Fuente: Elaboración propia

Las VLAN y ACL son creadas en el switch core de capa 3 que cuenta con la capacidad de gestionar grandes cantidades de tráfico por ser un equipo robusto, en este switch mantendrá un constante flujo de tráfico, ya que será responsable de la comunicación entre usuarios locales y servicios internos como también usuarios locales y servicio a Internet, este dispositivo será capaz de la comunicación entre las diferentes VLAN.

Figura 40: Switch Core – sala de servidores

Fuente: Elaboración propia

INSTALACION DEL SWITCH WAN

Equipo modelo Catalyst 2960 x de 24 puertos no PoE, este equipo permite el enlace entre las diferentes sedes de la empresa como: El Ingenio, Andahuasi, Paramonga y la Corporación Lima. A través de servicios VPN, servicios contratados al proveedor como Movistar.

Los servicios VPN son usados para la comunicación entre la corporación Lima y la

Empresa Agro Industrial Paramonga. Servicio brindado por el proveedor Movistar. El enlace Lan to Lan es utilizado para la comunicación de datos entre la Empresa El Ingenio y La Empresa Agro Industrial Paramonga, Empresa Andahuasi y la Empresa Agro Industrial Paramonga. Servicio brindado por el proveedor FiberLux.

Figura 41: Switch Wan
Fuente: Elaboración propia

INSTALACION DEL SWITCH EN EL GABINETE DEL AREA DE PROYECTO

Equipo modelo Catalyst 2960 x de 48 puertos PoE marca Cisco, este equipo ayudará a optimizar el tráfico, mejorar la seguridad, en resumen, se tiene la flexibilidad para reaccionar ante el crecimiento de la red, mejorando la confiabilidad y disponibilidad de la red. Este Switch está instalado en el gabinete del área de Proyectos donde se conectan los siguientes equipos:

25 computadoras (Vlan 10)

3 Laptops (Vlan 10, Vlan 90)

1 impresora Láser (Vlan 30)

1 ploter (Vlan 30)

2 teléfonos ip (Vlan 40)

4 cámaras (Vlan 60)

1 Acceso recepción (Vlan 120)

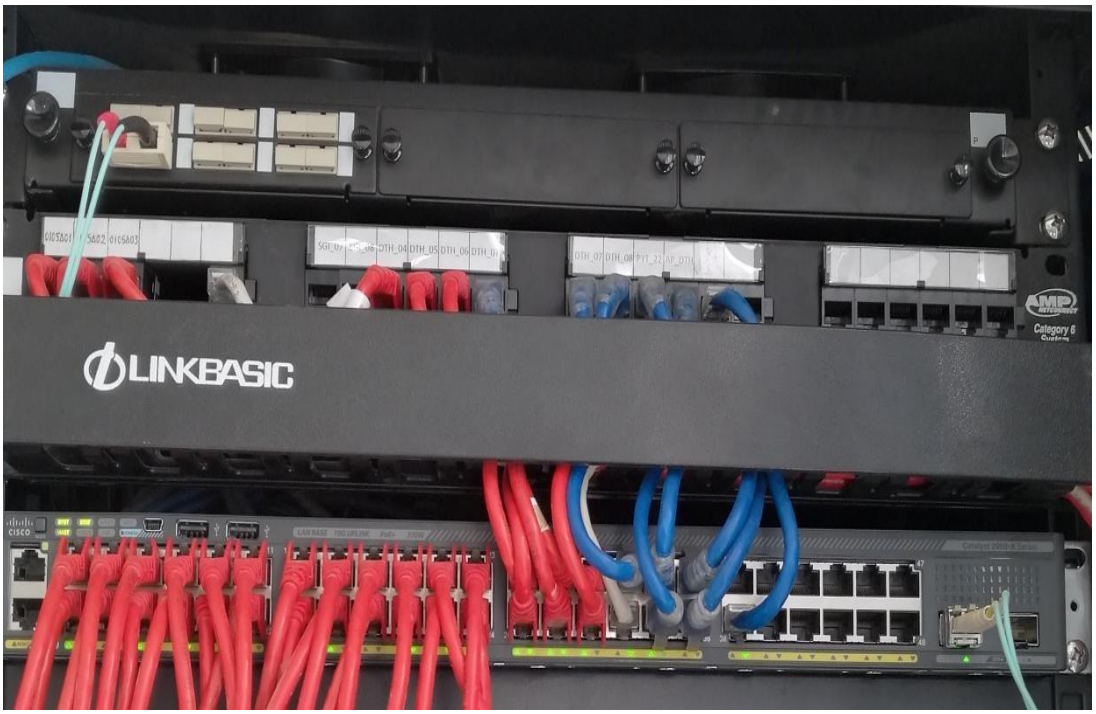


Figura 42: Switch del área de Proyectos
Fuente: Elaboración propia

INSTALACION DEL SWITCH EN EL GABINETE DEL AREA DE FÁBRICA

Equipo modelo Catalyst 2960 x de 48 puertos PoE marca Cisco, este equipo ayudará a optimizar el tráfico, mejorar la seguridad, en resumen, se tiene la flexibilidad para reaccionar ante el crecimiento de la red, mejorando la confiabilidad y disponibilidad de la red. Este Switch está instalado en el gabinete del área de Fábrica donde se conectan los siguientes equipos:

28 computadoras (Vlan 10)

4 Laptops (Vlan 10, Vlan 90)

1 impresora Láser (Vlan 30)

3 teléfonos ip (Vlan 40)

3 cámaras (Vlan 60)

1 proyector (Vlan 90)

3 Access Point Cisco (Vlan 140)

1 Reloj Marcador (Vlan 160)

Figura 43: Switch del área de Fábrica
Fuente: Elaboración propia

INSTALACION DEL SWITCH EN EL GABINETE DE AREAS DIVERSAS

Equipo modelo Catalyst 2960 x de 48 puertos PoE marca Cisco, este equipo ayudará a optimizar el tráfico, mejorar la seguridad, en resumen, se tiene la flexibilidad para reaccionar ante el crecimiento de la red, mejorando la confiabilidad y disponibilidad de la red. Este Switch está instalado en el gabinete de diversas áreas como Bienestar, Comunicaciones, Activo Fijo, Control Documentario, Seguridad Industrial, Asuntos Ambientales, Recepción y Seguridad Patrimonial; donde se conectan los siguientes equipos:

31 computadoras (Vlan 10)

4 Laptops (Vlan 10, Vlan 90)

1 impresora Láser (Vlan 30)

1 impresora de código de barras (Vlan 30)

5 teléfonos ip (Vlan 40)

1 cámaras (Vlan 60)

1 proyector (Vlan 90)

1 Access Point Cisco (Vlan 140)

1 Reloj Marcador (Vlan 160)

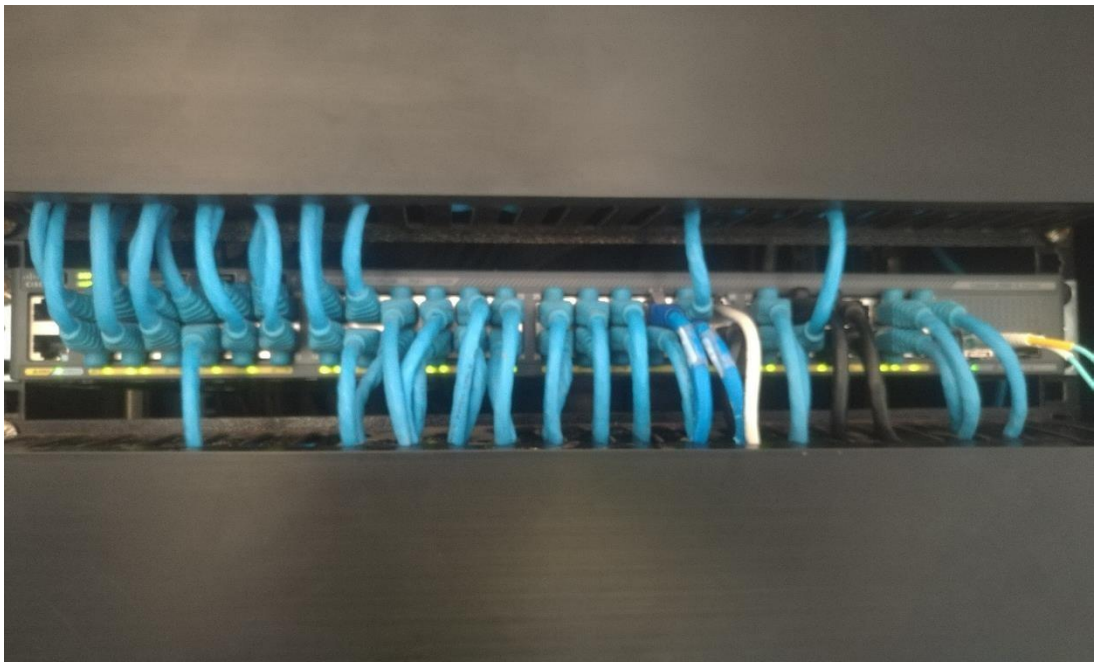


Figura 44: Switch de área diversas

Fuente: Elaboración propia

INSTALACION DEL SWITCH EN EL GABINETE DE APT

Equipo modelo Catalyst 2960 x de 24 puertos PoE, marca Cisco, este equipo ayudará a optimizar el tráfico, mejorar la seguridad, en resumen, se tiene la flexibilidad para reaccionar ante el crecimiento de la red, mejorando la confiabilidad y disponibilidad de la red. Este Switch está instalado en el gabinete de APT; donde se conectan los siguientes equipos:

2 computadoras (Vlan 10)

1 impresora Láser (Vlan 30)

1 impresora de código de barras (Vlan 30)

5 cámaras (Vlan 60)

Figura 45: Switch del área APT

Fuente: Elaboración propia

INSTALACION DEL SWITCH EN EL GABINETE DE BALANZA DE CAÑA

Equipo modelo Catalyst 2960 x de 24 puertos PoE marca Cisco, este equipo ayudará a optimizar el tráfico, mejorar la seguridad, en resumen, se tiene la flexibilidad para reaccionar ante el crecimiento de la red, mejorando la confiabilidad y disponibilidad de la red. Este Switch está instalado en el gabinete de Balanza de Caña; donde se conectan los siguientes equipos:

3 computadoras (Vlan 10)

1 impresora Láser (Vlan 30)

1 impresora Código de Barras (Vlan 30)

3 cámaras (Vlan 60)

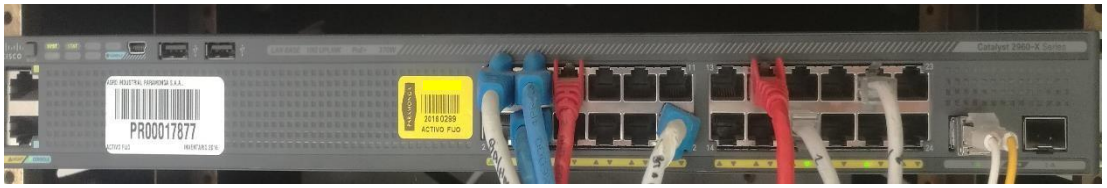


Figura 46: Switch de Balanza de Caña

Fuente: Elaboración propia

INSTALACION DEL SWITCH EN EL GABINETE DE LABORATORIO

Equipo modelo Catalyst 2960 x de24 puertos PoE marca Cisco, este equipo ayudará a optimizar el tráfico, mejorar la seguridad, en resumen, se tiene la flexibilidad para reaccionar ante el crecimiento de la red, mejorando la confiabilidad y disponibilidad

de la red. Este Switch está instalado en el gabinete de Laboratorio; donde se conectan los siguientes equipos:

6 computadoras (Vlan 10)

5 Laptops (Vlan 10, Vlan 90)

1 impresora Láser (Vlan 30)

1 Access Point Cisco (Vlan 90)

1 Teléfono IP (Vlan 40)

9 cámaras (Vlan 60)

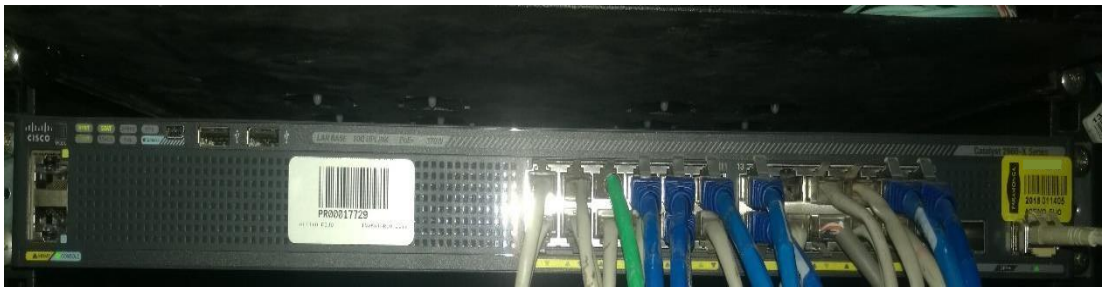


Figura 47: Switch Laboratorio

Fuente: Elaboración propia

INSTALACION DEL SWITCH EN EL GABINETE DE TRANSPORTE

Equipo modelo Catalyst 2960 x de 24 puertos no PoE marca Cisco, este equipo ayudará a optimizar el tráfico, mejorar la seguridad, en resumen, se tiene la flexibilidad para reaccionar ante el crecimiento de la red, mejorando la confiabilidad y disponibilidad de la red. Este Switch está instalado en el gabinete del área de Transportes; donde se conectan los siguientes equipos:

3 computadoras (Vlan 10)

1 Laptops (Vlan 10, Vlan 90)

1 impresora Láser (Vlan 30)

1 Access Point Cisco (Vlan 90)

1 Teléfono IP (Vlan 40)

6 cámaras (Vlan 60)

7 Enlaces Inalámbricos (Vlan 1)

1 Reloj Marcador (Vlan 160)

Figura 48: Switch Oficina de Transportes

Fuente: Elaboración propia

INSTALACION DEL SWITCH EN EL GABINETE DE CAMPO

Equipo modelo Catalyst 2960 x de 24 puertos PoE marca Cisco y Equipo modelo Catalyst 2960 x de 48 puertos no PoE marca Cisco, estos equipos ayudarán a optimizar el tráfico, mejorar la seguridad, en resumen, se tiene la flexibilidad para reaccionar ante el crecimiento de la red, mejorando la confiabilidad y disponibilidad de la red. Estos Switch están instalados en el gabinete del área de Campo; donde se conectan los siguientes equipos:

25 computadoras (Vlan 10)

6 Laptops (Vlan 10, Vlan 90)

2 Impresoras Láser (Vlan 30)

1 Ploter (Vlan 30)

1 Access Point Cisco (Vlan 90)

4 Teléfonos IP (Vlan 40)

6 cámaras (Vlan 60)

1 Reloj Marcador (Vlan 160)

4 Enlaces Inalámbricos (Vlan 1)

Figura 49: Switch Oficina de Campo

Fuente: Elaboración propia

INSTALACION DEL SWITCH EN EL GABINETE DE SEMA

Equipo modelo Catalyst 2960 x de 24 puertos PoE marca Cisco, este equipo ayudará a optimizar el tráfico, mejorar la seguridad, en resumen, se tiene la flexibilidad para reaccionar ante el crecimiento de la red, mejorando la confiabilidad y disponibilidad de la red. Este Switch está instalado en el gabinete del área de Sema; donde se conectan los siguientes equipos:

4 computadoras (Vlan 10)

3 Laptops (Vlan 10, Vlan 90)

1 Impresoras Láser (Vlan 30)

1 Access Point Cisco (Vlan 90)

1 Teléfonos IP (Vlan 40)

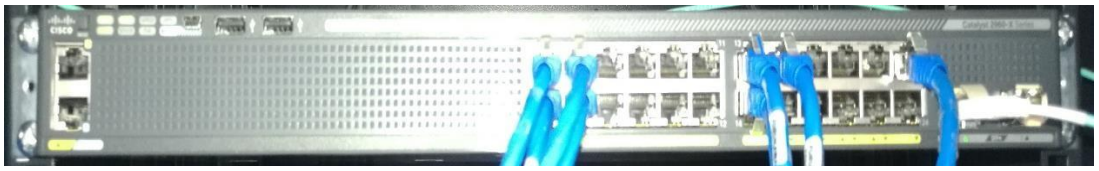


Figura 50: Switch Oficina de Sema

Fuente: Elaboración propia

INSTALACION DEL SWITCH EN EL GABINETE DE ALMACEN

Equipo modelo Catalyst 2960 x de 24 puertos no PoE marca Cisco, este equipo ayudará a optimizar el tráfico, mejorar la seguridad, en resumen, se tiene la flexibilidad para reaccionar ante el crecimiento de la red, mejorando la confiabilidad y disponibilidad de la red. Este Switch está instalado en el gabinete del área de Almacén de Materiales; donde se conectan los siguientes equipos:

9 computadoras (Vlan 10)

1 Impresoras Láser (Vlan 30)

4 Teléfonos IP (Vlan 40)

Figura 51: Switch Oficina de Sema

Fuente: Elaboración propia

INSTALACION DEL CONTROLADOR INALAMBRICO CISCO 2500 SERIES

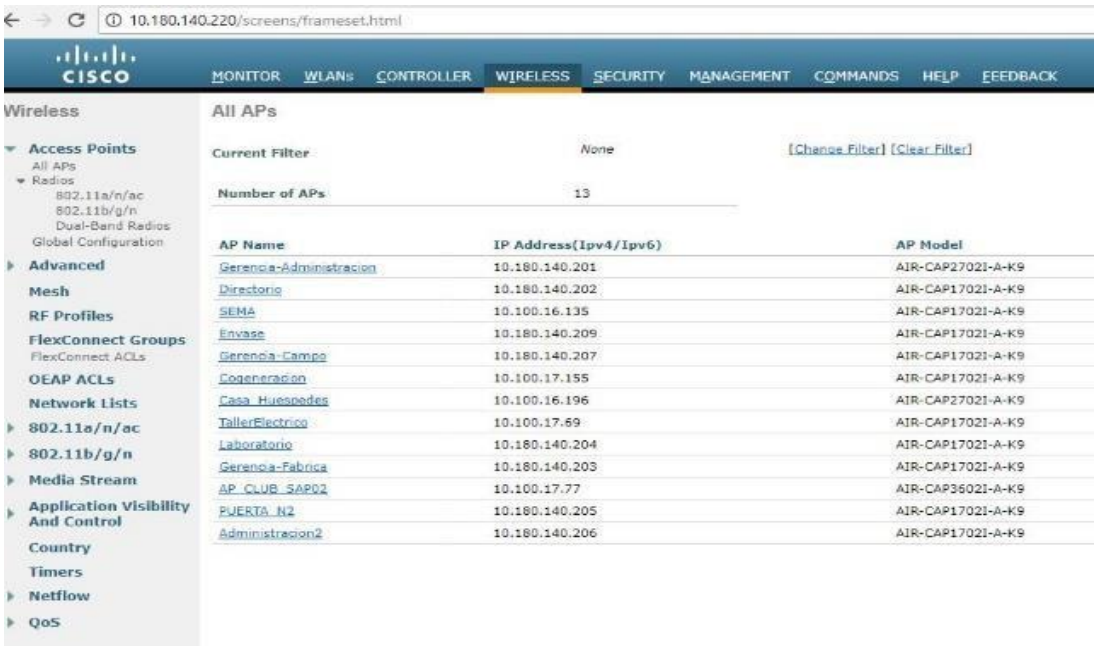


Figura 52: Controlador Inalámbrico Cisco

Fuente: Elaboración propia

MONITOR DEL CONTROLADOR INALAMBRICO CISCO 2500 SERIES

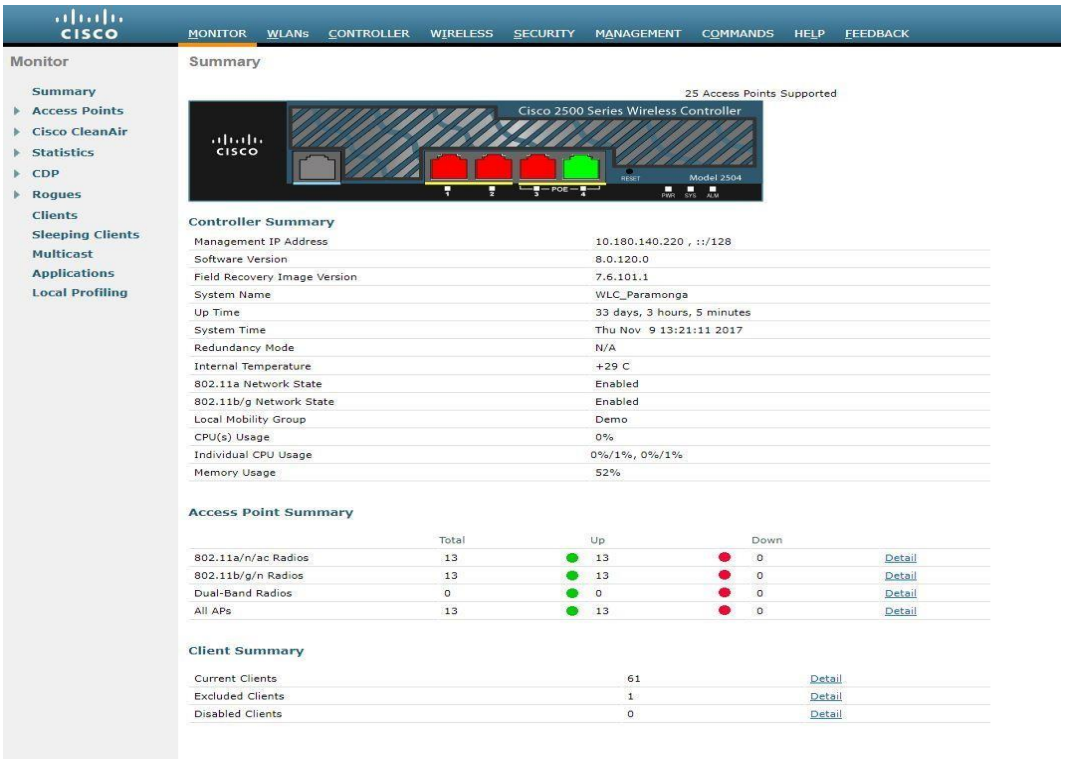


Figura 53: Monitor del Controlador Inalámbrico Cisco

Fuente: Elaboración propia

VLANS EN EL CONTROLADOR INALAMBRICO CISCO 2500 SERIES

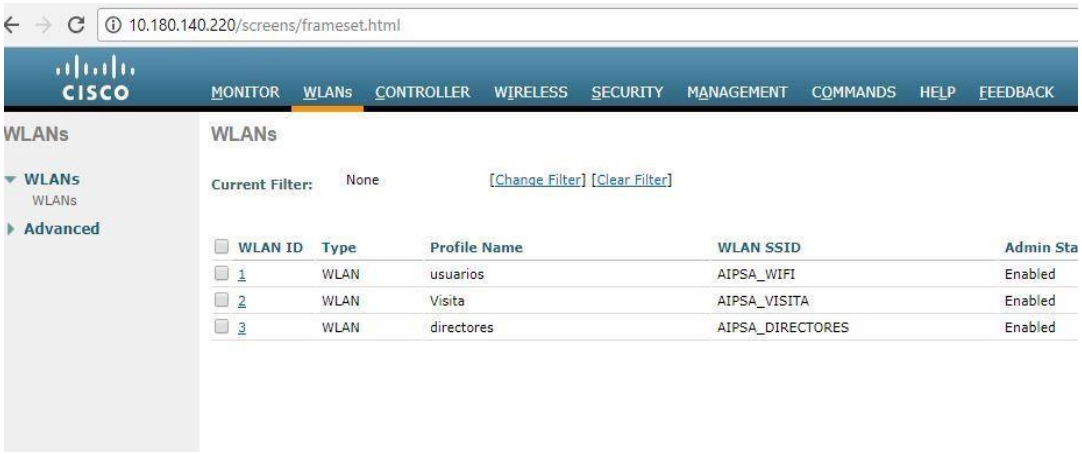


Figura 54: Vlans en el Controlador Inalámbrico Cisco

Fuente: Elaboración propia

INSTALACION DEL AP EN LA OFICINA DE ADMINISTRACION

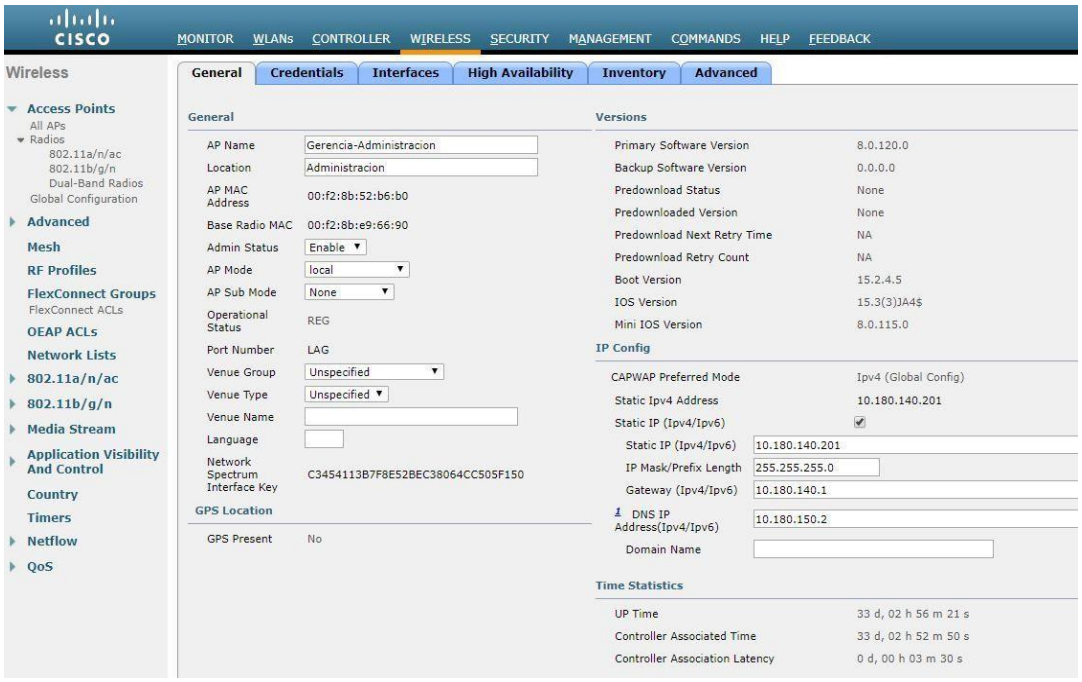


Figura 55: Access Point de Administración

Fuente: Elaboración propia

INSTALACION DEL AP EN LA OFICINA DE BIENESTAR

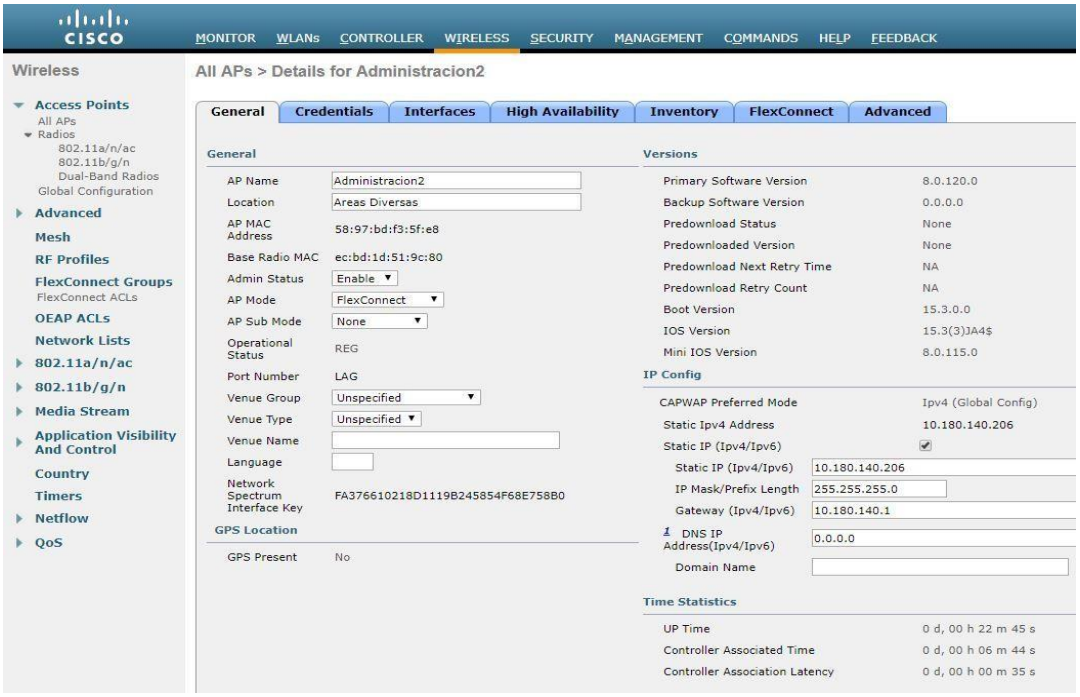


Figura 56: Access Point de Bienestar

Fuente: Elaboración propia

INSTALACION DEL AP EN LA OFICINA DE CAMPO

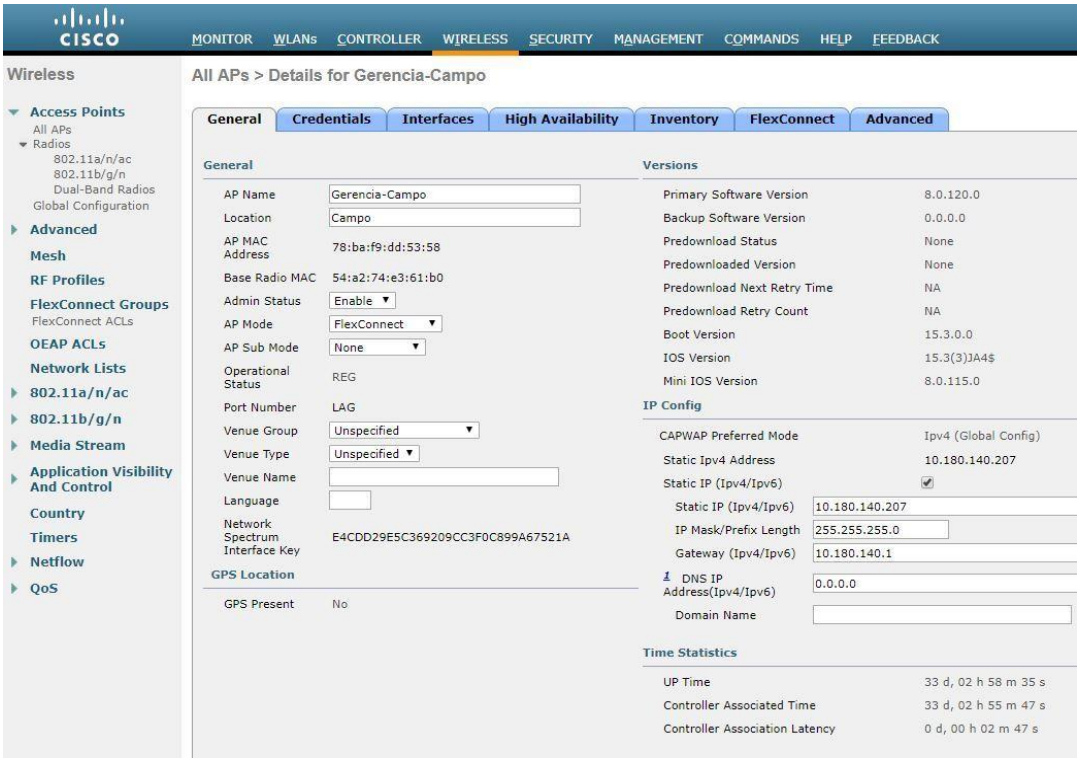


Figura 57: Access Point de Campo

Fuente: Elaboración propia

INSTALACION DEL AP EN LA OFICINA DE COGENERACION

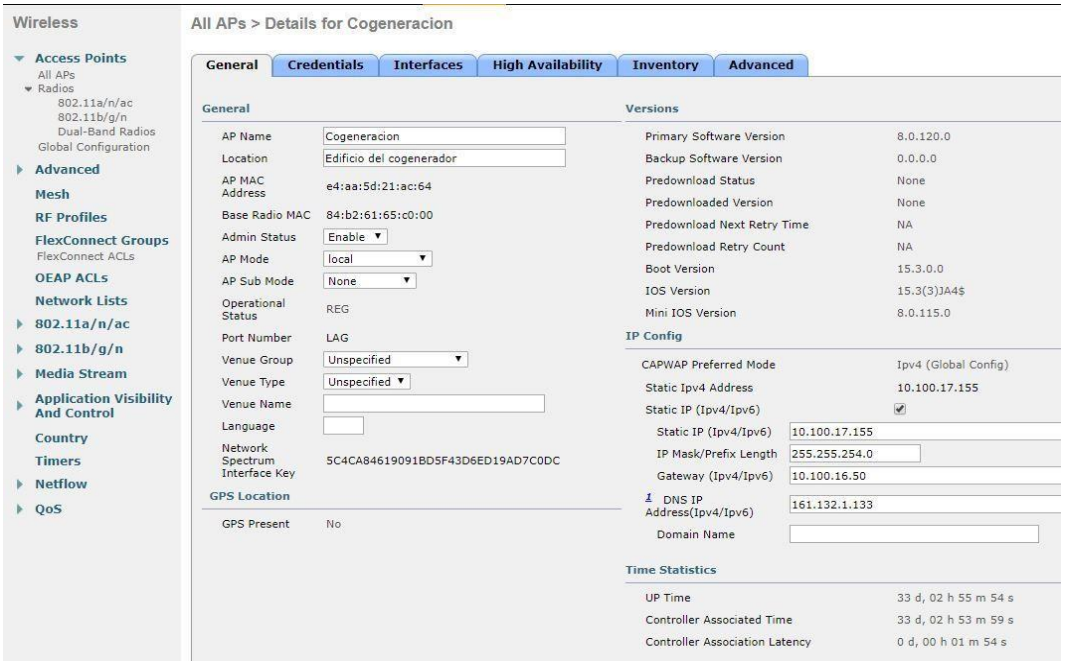


Figura 58: Access Point de Cogeneración

Fuente: Elaboración propia

INSTALACION DEL AP EN LA OFICINA DEL DIRECTORIO

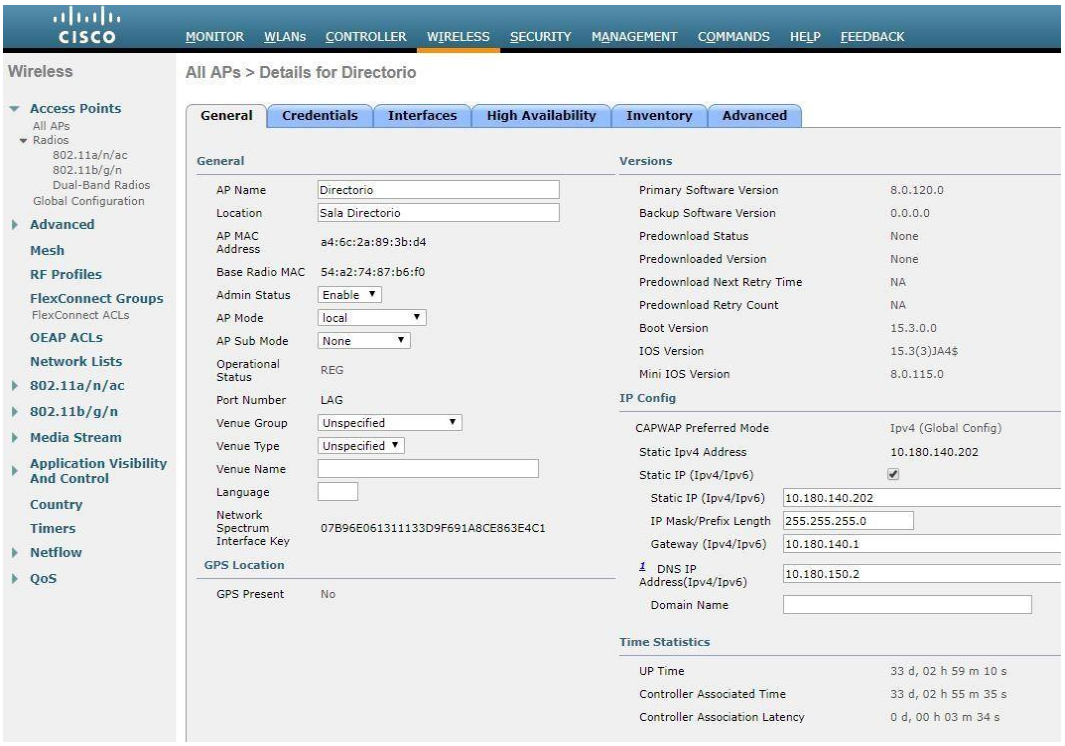


Figura 59: Access Point del Directorio

Fuente: Elaboración propia

INSTALACION DEL AP EN LA OFICINA DE ENVASE

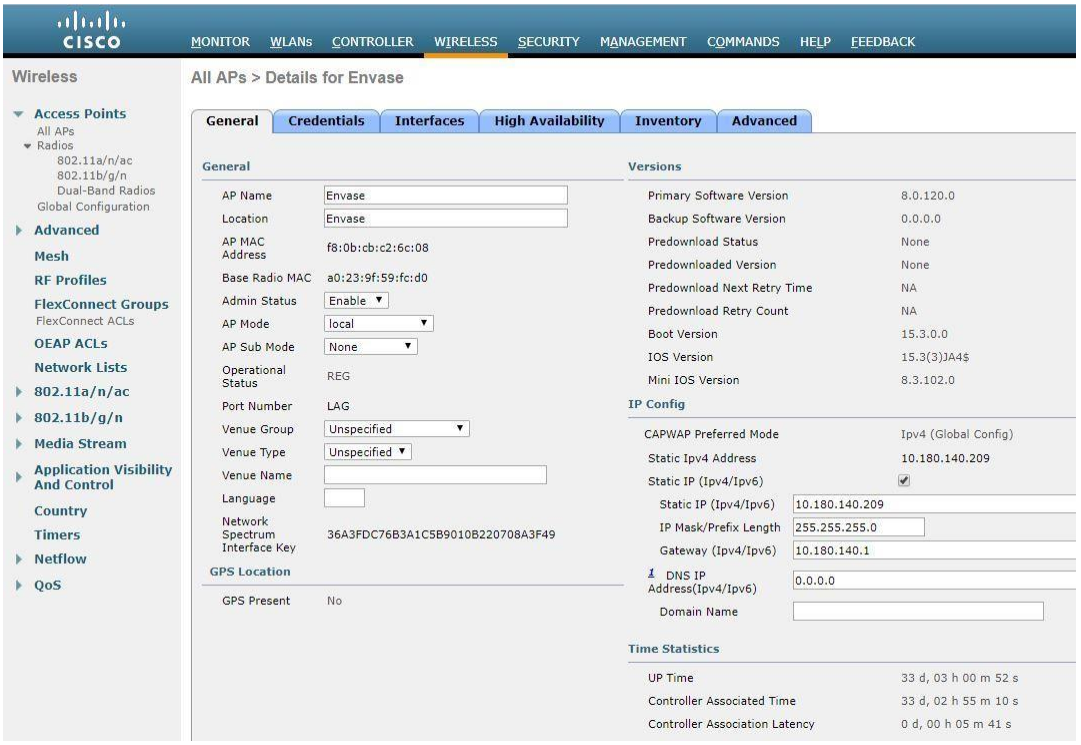


Figura 60: Access Point de Envase

Fuente: Elaboración propia

INSTALACION DEL AP EN LA OFICINA DE FABRICA

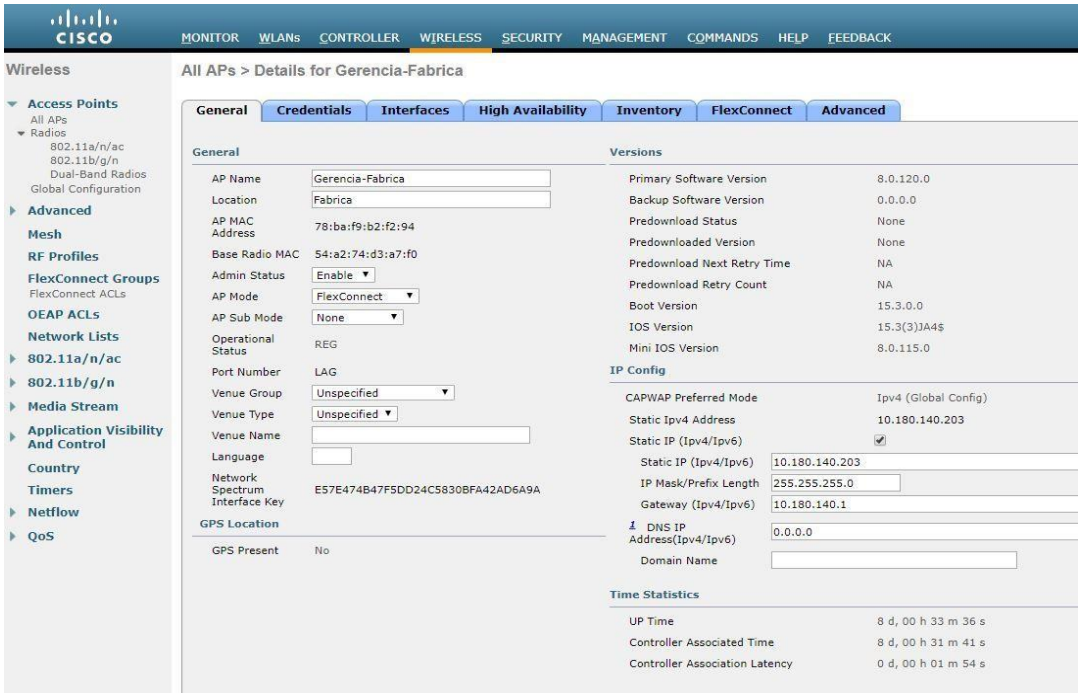


Figura 60: Access Point de Fábrica

Fuente: Elaboración propia

INSTALACION DEL AP EN LA OFICINA DE LABORATORIO

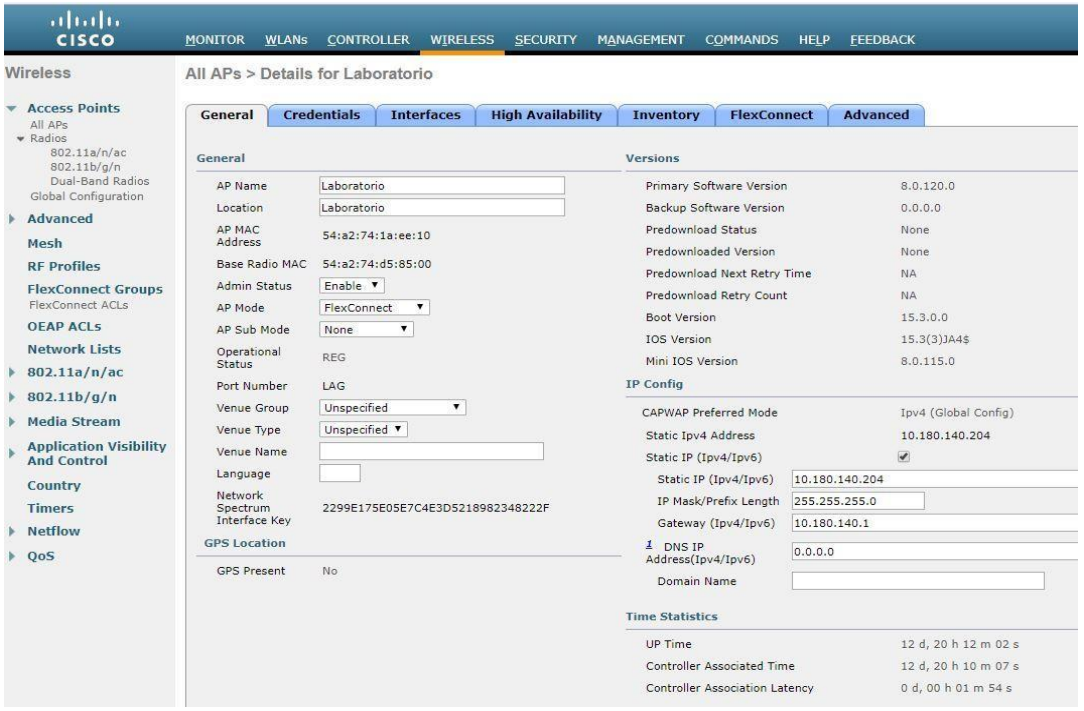


Figura 61: Access Point de Laboratorio

Fuente: Elaboración propia

INSTALACION DEL AP EN LA OFICINA DE CASETA 2

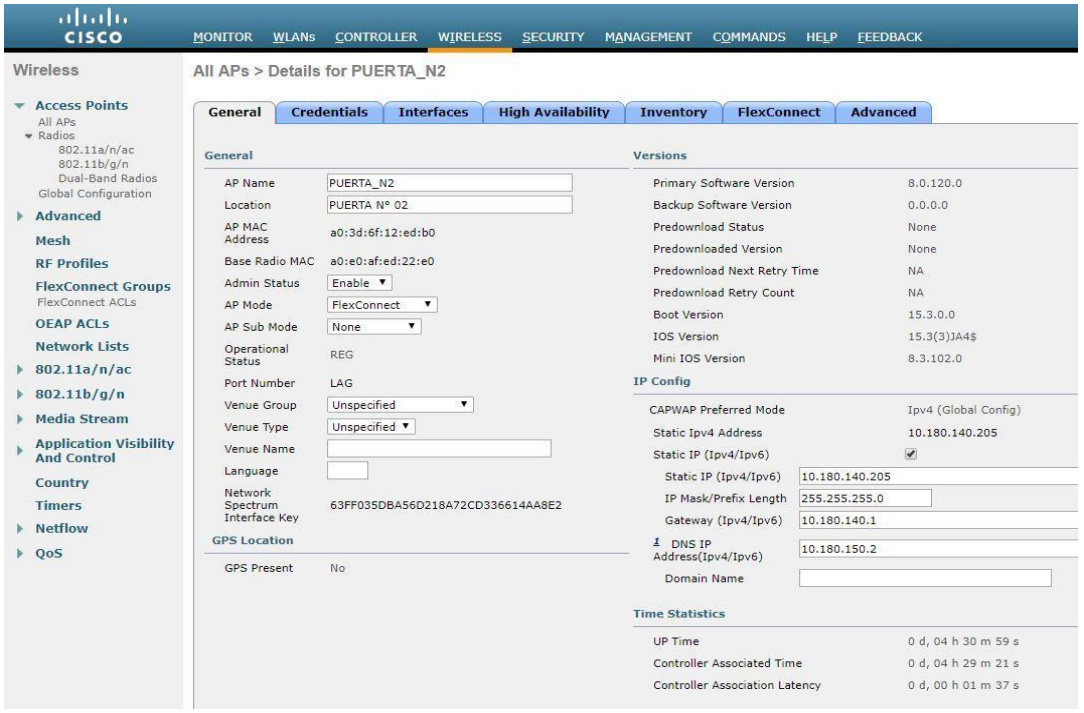


Figura 62: Access Point de Caseta 2

Fuente: Elaboración propia

INSTALACION DEL AP EN LA OFICINA DE PROYECTO SAP

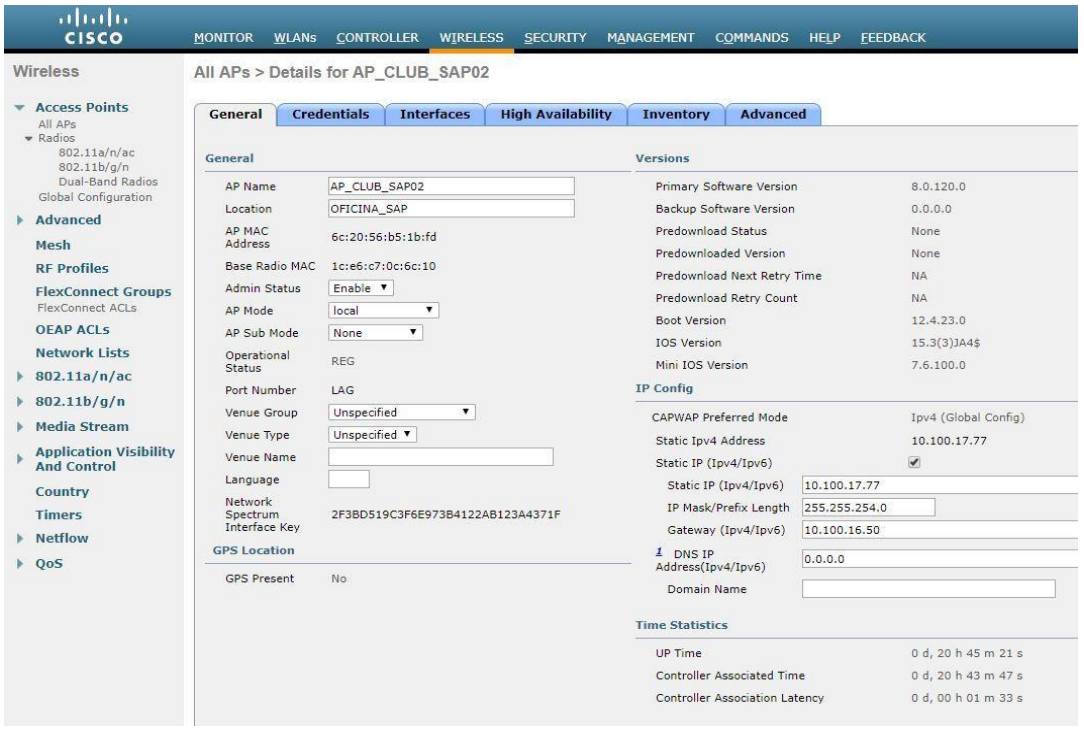


Figura 63: Access Point de Proyecto Sap

Fuente: Elaboración propia

INSTALACION DEL AP EN LA OFICINA DE SEMA

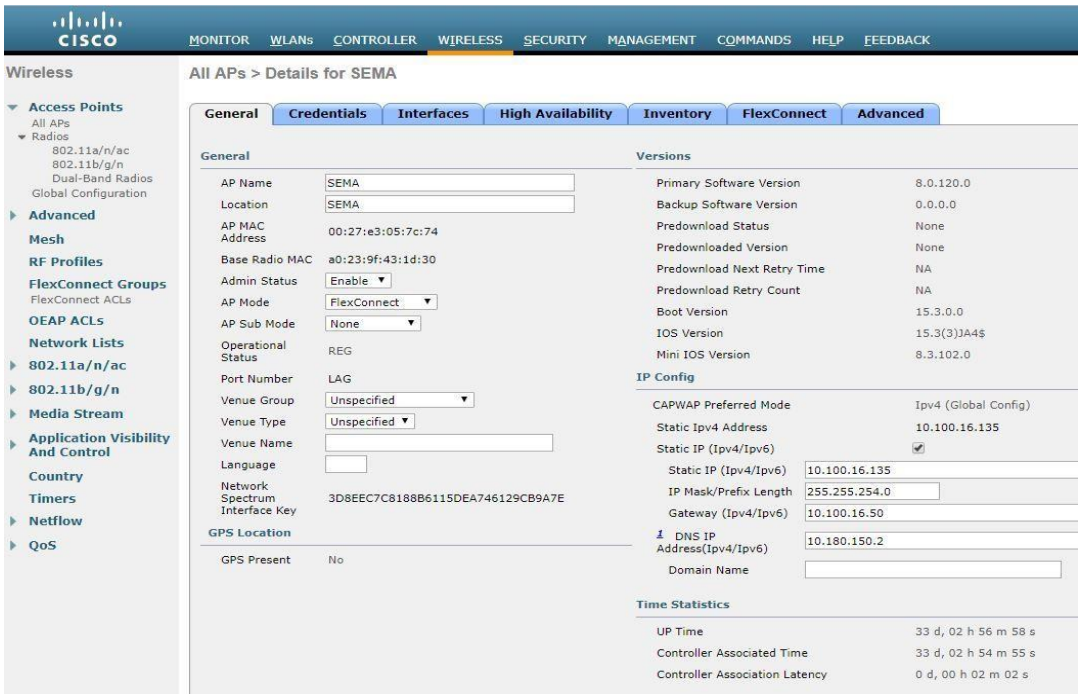


Figura 64: Access Point de Sema

Fuente: Elaboración propia

INSTALACION DEL AP EN LA OFICINA DE TALLER ELECTRICO

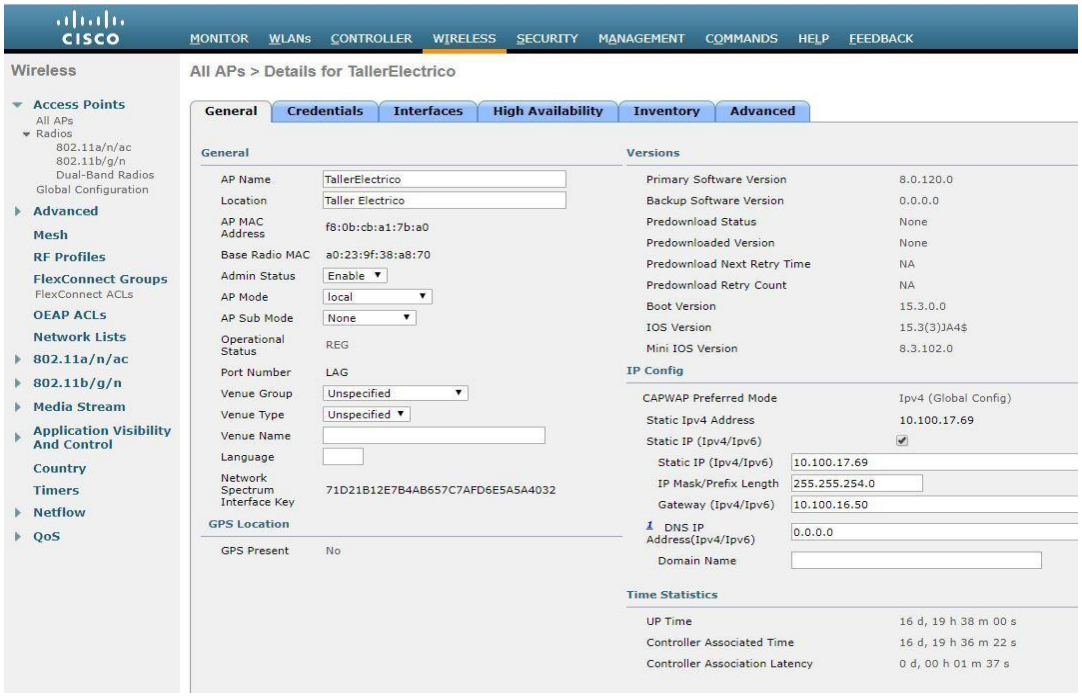


Figura 65: Access Point de Sema

Fuente: Elaboración propia

INSTALACION DEL AP EN LA OFICINA DE CHALET HUESPED

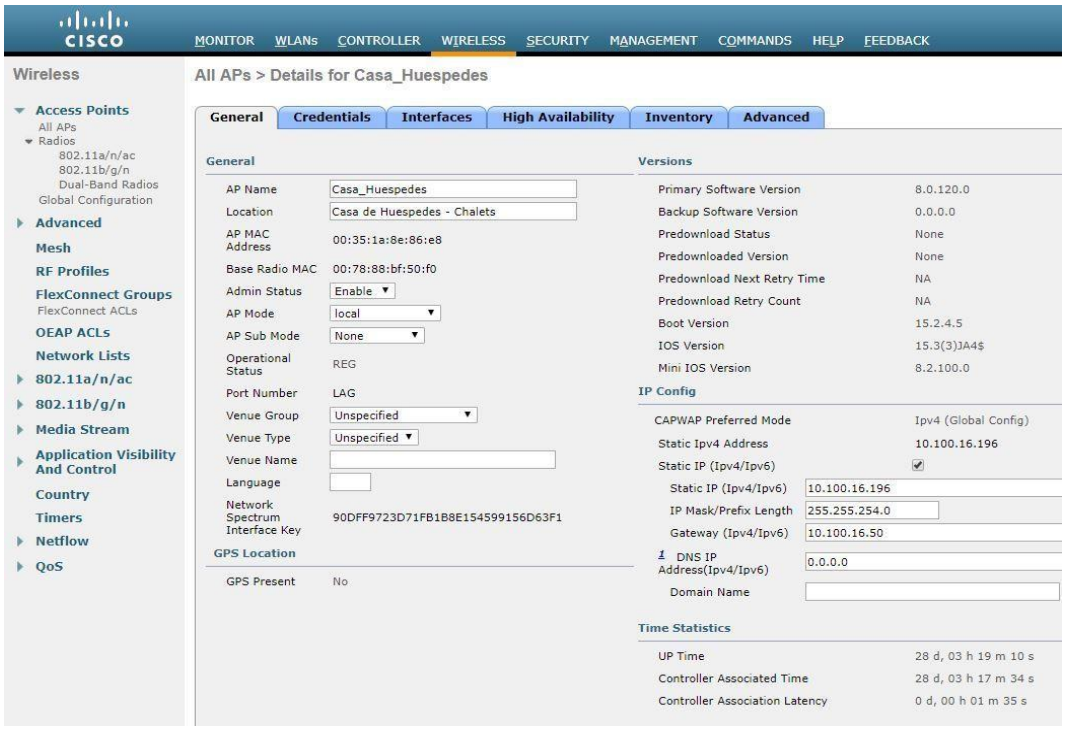


Figura 66: Access Point de Sema

Fuente: Elaboración propia

FASE DE OPERACIÓN

Para examinar la calidad de un enlace de red se pueden realizar diferentes pruebas con los protocolos TCP (Protocolo de control de Transmisión) y UDP (Protocolo de Datagramas de Usuario). La calidad de una red puede ser examinada bajo las siguientes maneras:

Latencia: que es el tiempo de respuesta o round.trip time (RTT) y puede medirse usando el comando Ping.

Se realizaron pruebas de latencia de diferentes estaciones de trabajo hacia el servidor de red, y como muestra la imagen no tenemos perdida de paquetes, tiempo aproximado de respuesta es de Mínimo = 0ms, Máximo = 4ms, Media = 0ms

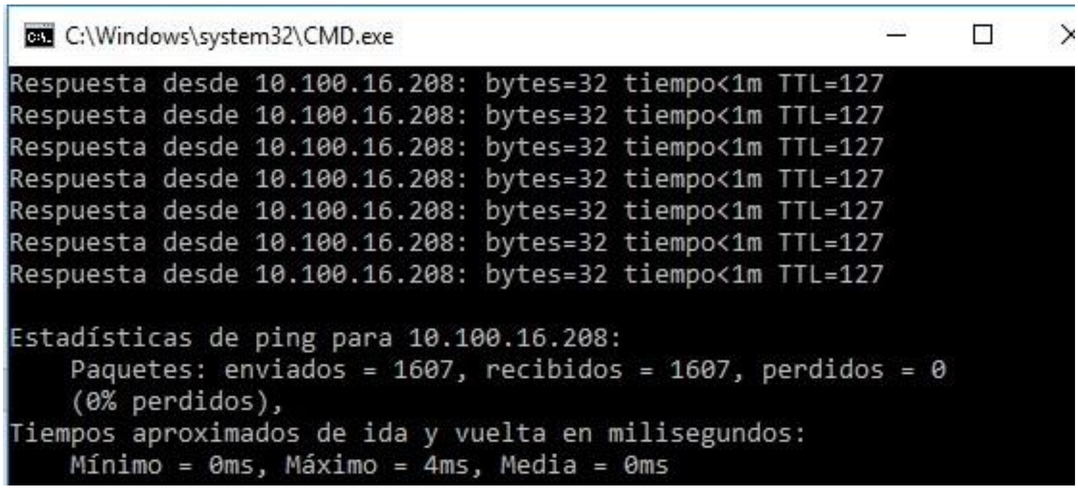


Figura 67: Ping al Servidor de Red

Fuente: Elaboración propia

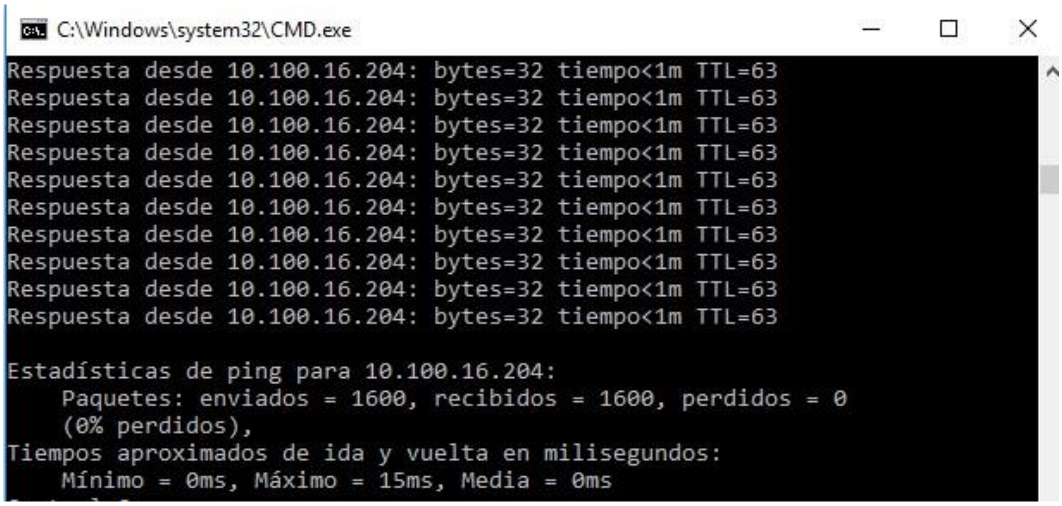


Figura 68: Ping al Servidor de Base de Datos

Fuente: Elaboración propia

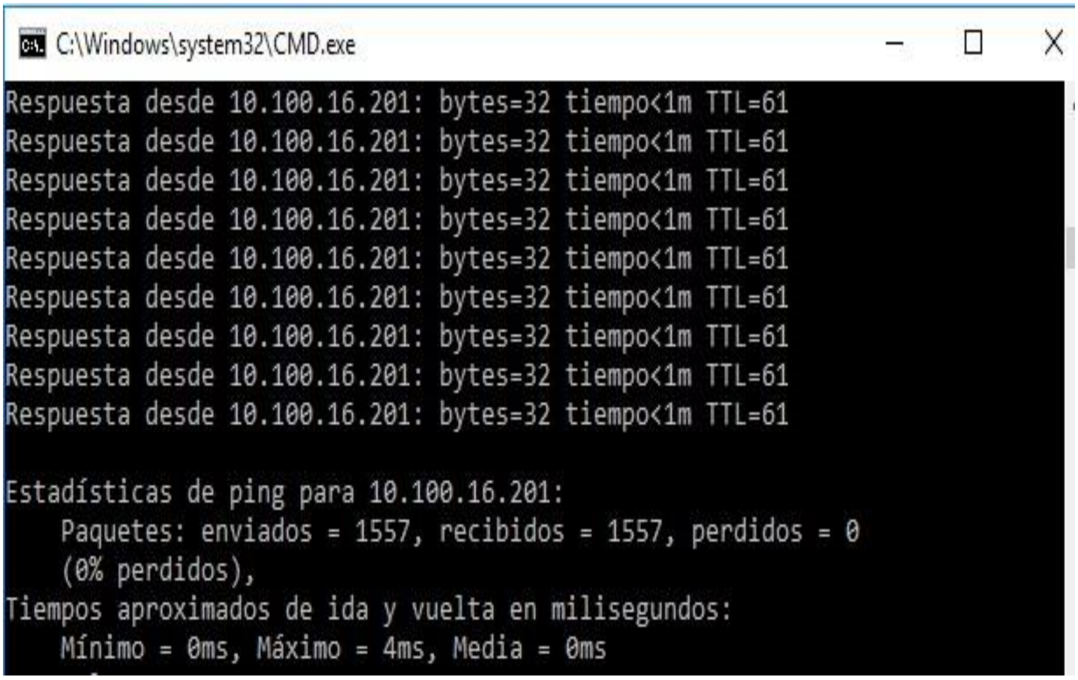


Figura 69: Ping al Servidor de Correo

Fuente: Elaboración propia

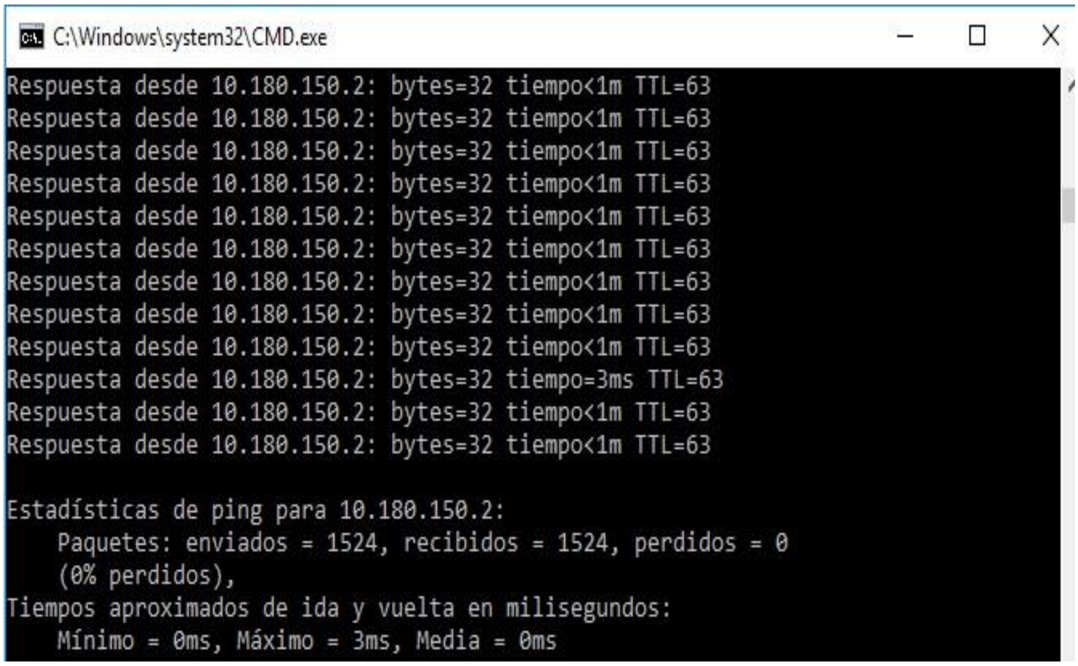


Figura 70: Ping al Servidor de Sophos

Fuente: Elaboración propia

Prueba de transferencia de archivos de 11.5 GB de una estación de trabajo hacia el Servidor de Red

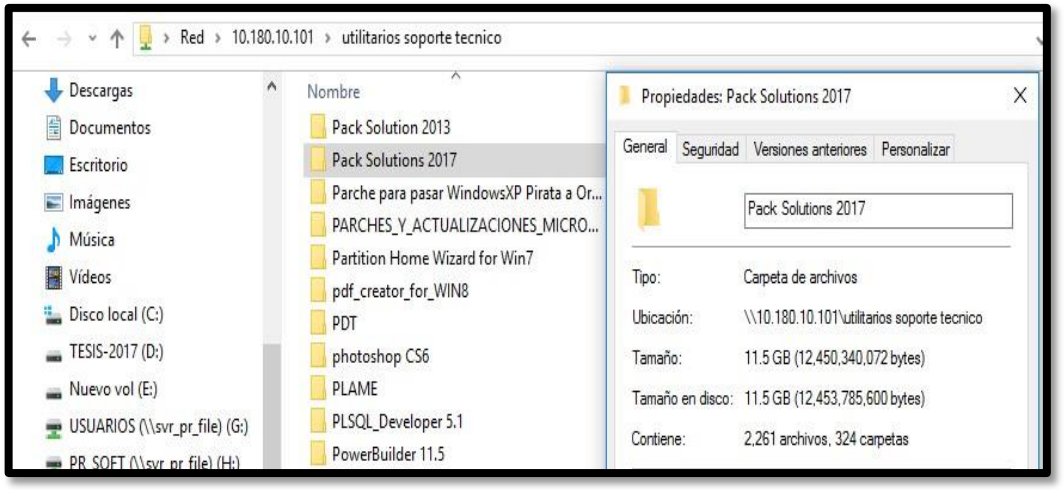


Figura 71: Archivo de 11.5 GB

Fuente: Elaboración propia

La transferencia del archivo se completó en 00:01:15 minutos, llegando entre 90 y 105 MB/s

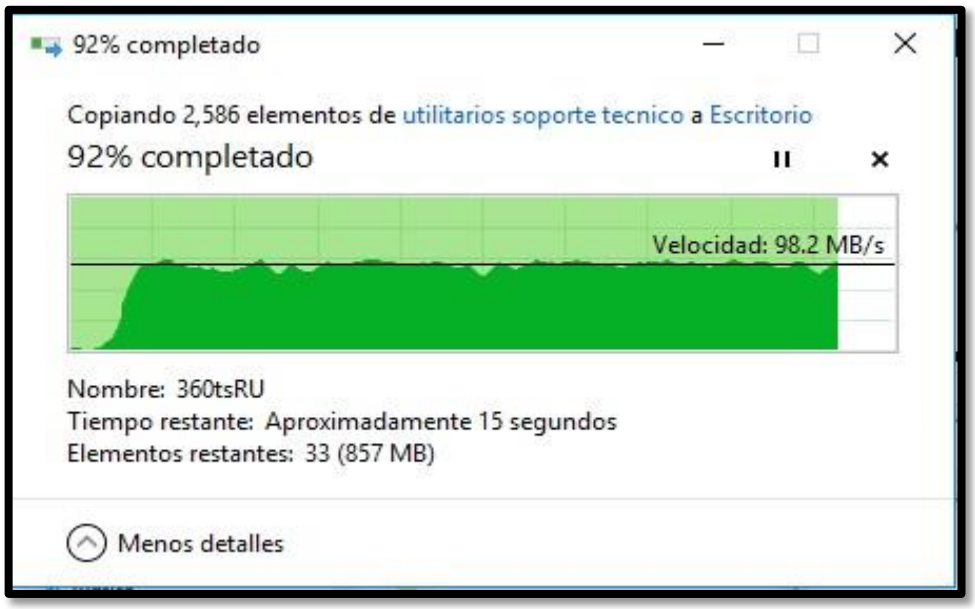


Figura 72: Velocidad de Transferencia de archivos

Fuente: Elaboración propia

4. ANALISIS Y DISCUSION

De los resultados obtenidos del análisis de la situación actual de la empresa, se llegó a la conclusión, la necesidad de implementar la red virtual en la empresa AGRO INDUSTRIAL PARAMONGA S.A.A, para mejorar la eficiencia de la misma, lo que conduce a la investigación a ser altamente factible

También se observa como en la investigación de Liseth Ccelia Bravo Valero en su tesis denominada **"Modelo diagnóstico y análisis de la red LAN para la mejora del rendimiento y seguridad en la red de salud Valle del Mantaro".** Donde también se utilizó la metodología Cisco para el diagnóstico y análisis, con el objetivo de conocer cuáles son los problemas que existen y así proponer una solución a través de un nuevo diseño de red que cumpla con los requerimientos de la institución. Permitiendo abrir y profundizar la investigación tecnológica que brinda la red en la empresa y organización.

El implementar la red de área de trabajo, el acceso a los servicios y recursos compartidos de la red se han visto reforzados como consecuencia de la configuración de tecnologías de seguridad, propias de nuevos equipos con garantía mundial en el mercado como es la marca Cisco. Estos nuevos mecanismos han permitido elevar el nivel de seguridad en un 95%, mejoras que satisfacen las exigencias y lineamientos estratégicos de la empresa. Así mismo estas mejoras se ven reforzadas por el uso del UTM (Seguridad Perimetral), logrando un nivel de seguridad superior.

5. CONCLUSIONES

En base al desarrollo del plan de trabajo del proyecto, para la implementación de la Red Virtual LAN y red inalámbrica de la empresa Agro Industrial Paramonga S.A.A, se puede concluir que:

Se logró analizar la situación actual de las áreas críticas, permitiendo visualizar los requerimientos de diseño e implementación de la red física y virtual para la satisfacción de los usuarios al acceder a sus archivos de trabajo, dado que en la actualidad es muy necesario ya que permite una alta velocidad de acceso a los datos por parte de los usuarios.

Se logró una implementación de trabajo ordenado para obtener una solución de red virtual con el uso de la metodología Cisco.

Se logró la implementación de la red virtual en la Empresa Agro Industrial Paramonga que nos permite gran movilidad de datos, reducción de costos y además una gran escalabilidad de la red entre otros; Tomando en cuenta la seguridad, ya que la confidencialidad en estas es vulnerable y los equipos Cisco son los más recomendados por su nivel de seguridad.

6. RECOMENDACIONES

El personal encargado del área de tecnología de la información debe preocuparse por analizar y proteger las redes de la empresa contra intrusos, programas maliciosos y spam, e implementar restricciones orientadas a bloquear el ingreso a páginas que consuman una gran cantidad de ancho de banda como son video en línea, y radios por Internet, como también:

Definir derechos de usuarios adecuados para las distintas tareas.

Descargas de archivos solo en sitios de confianza.

Realizar auditorías con frecuencia de los recursos compartidos de red.

Vigilar las conexiones de red.

Vigilar el rango de direcciones IP predeterminados para cada equipo.

Controlar los puertos abiertos de la red con frecuencia, y bloquear los que no se utilicen.

Controlar periódicamente los puntos de acceso a su red.

Probar los programas nuevos en una red distinta antes de utilizarlos.

Desactivar los puertos USB no utilizados.

Se debe capacitar a los usuarios sobre el buen uso de los equipos de cómputo, portátiles, educando a que los usuarios no abusen de los recursos compartidos que otros computadores pueden proporcionar.

Los encargados del área tecnológica deben tener en claro cómo funciona el diseño jerárquico de la red, diferenciando para que sirve cada capa para así poder implementar nuevas tecnologías o añadir nuevos requerimientos de la red.

La lectura y análisis de los archivos de registro de sucesos o log’s generados por el servidor de autenticación para así poder analizar sobre amenazas que ha sufrido el segmento LAN o inalámbrico.

7. REFERENCIAS BIBLIOGRAFICAS

Bravo Valero, Liseth Celia (2015). *Modelo diagnóstico y análisis de la red LAN para la mejora del rendimiento y seguridad en la red de salud Valle del Mantaro.* Huancayo, Perú.

Cabezas Avalos, Edwin Samuel y Castillo Narváez, Braulio Cristopher (2013) *Análisis de la red de datos Ministerio de Relaciones Laborales (Edificio Torreazul – Administrativo.* Quito, Ecuador.

Céspedes Velasco, Jorge Enrique (2012). *Red De Datos Para Las Comunicaciones en Hospital básico de Pelileo.* Ecuador.

CISCO (2006).*Networkers Solutions Forum Routed Fast Converence and High Availability*

Comer, Douglas (1996). *Redes Globales de Información con Internet y TCP/IP.* México: Prentice–Hall.

Hernández Jiménez, Omar y Huerta Carmona, Marco (2014). *Actualización de una red local plana una red local segura, segmentada con servicios de voz y datos en IFAI*. México, D.F.

Kenneth, D., Stewart III y Audrey Adams. (2015). *Desingning and Supporting Computer Networks.* California, Estados Unidos.: Cisco Networking Academy.

Ochoa Saavedra, Cesar Ramiro (2012). *Implementación de un diseño de puente Inalámbrico punto multipunto para la mejora de la enlazar de las áreas de la empresa plásticos Rímac SRL.* Chiclayo Perú.

Rojas Yovera, Félix Leonardo (2016). *Propuesta Para La Implementación de La Red de Datos en la Municipalidad Distrital de Tamarindo.* Perú.

REFERENCIAS ELECTRONICAS

Castañeda, Luis. “Simuladores de Redes Cisco.”(Citado el 23 de Setiembre de 2017) disponible en http://www.slideshare.net/aaron12/simuladores-de-redes-cisco

Della, Jorge. “Modelo de Referencia OSI.”(Citado el 28 de Setiembre del 2017) editado por Mario Navarro: disponible en http://www.frm.utn.edu.ar/comunicaciones/modelo_osi.html

Medina, Luis. “Diseño de Redes, Modelo Jerárquico.”(Citado el 06 de Octubre de 2017) disponible en: http://www.redesymas.org/2011/05/diseno-de-redes-modelo- jerarquico.html

Metodología CISCO PPDIO. (Citado el 25 de Agosto Del 2017) https://http//www.cisco.com/c/es_co/index.html?.

Redes Virtuales VLANs. (Citado el 16 de Setiembre de 2017]) Disponible en http://www.textoscientificos.com/redes/redes-virtuales

Tecnología CISCO, Productos y Servicios para Empresas. (Citado el 03 de Agosto Del 2017) https://www.cisco.com/c/en/us/products/index.html

8. ANEXOS

Encuesta a Expertos del tema de Segmentación de Red Virtual

Pregunta Nº 01:

- **¿Cuán importante considera aplicar la Segmentación de Red Virtual para mejorar la comunicación de datos?**

  ( ) Muy Importante

  ( ) Importante

  ( ) Poco Importante

  ( ) Sin Importancia

Pregunta Nº 02:

- **¿Cree Ud. que la empresa Agro Industrial Paramonga S.A.A. debería implementar la Segmentación de la Red Virtual?**

  ( ) De acuerdo

  ( ) En desacuerdo

  ( ) Ni de acuerdo, ni en desacuerdo

  ( ) Totalmente de Acuerdo

  ( ) Totalmente de desacuerdo

Pregunta Nº 03:

- **¿Conoce las ventajas y desventajas de la implementación de la Red Virtual?**

  ( ) Si

  ( ) No

Pregunta N° 04:

- **¿Cree usted que la segmentación de la red Virtual nos brindará la seguridad de una red confiable?**

  ( ) De acuerdo

  ( ) En desacuerdo

  ( ) Ni de acuerdo, ni en desacuerdo

  ( ) Totalmente de Acuerdo

( ) Totalmente de desacuerdo

Pregunta N° 05:

- **¿La segmentación de la red virtual permitirá mejorar la comunicación de datos en todos los procesos del negocio?**

  ( ) De acuerdo

  ( ) En desacuerdo

  ( ) Ni de acuerdo, ni en desacuerdo

  ( ) Totalmente de Acuerdo

  ( ) Totalmente de desacuerdo

Encuesta a los Usuarios Finales

Pregunta N° 01

- **¿Tiene conocimiento acerca de lo que es la segmentación de la Red Virtual?**

  ( ) Si

  ( ) No

  ( ) Np

Pregunta N° 02

- **¿Cuenta con sus archivos de datos sin demora a la hora de realizar sus actividades diarias?**

  ( ) No

  ( ) Si

  ( ) Np

Pregunta N° 03

- **¿Cree usted que la segmentación de la Red Virtual ayudaría a mejorar la comunicación de datos?**

  ( ) No

  ( ) Si

  ( ) Np

Pregunta N° 04

- **¿Estaría dispuesto invertir en un proyecto de segmentación de Red Virtual?**

  ( ) No

  ( ) Si

  ( ) Np

Pregunta N° 05

- **¿Está usted conforme con la velocidad de transferencia de datos (Archivos) que brinda actualmente la red de la empresa?**

  ( ) No

  ( ) Si

  ( ) Np

CONFIGURACION DEL SWITCH CORE

```
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 no ip address
 negotiation auto
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
!
interface TenGigabitEthernet1/0/3
 switchport mode trunk
!
interface TenGigabitEthernet1/0/4
!
interface TenGigabitEthernet1/0/5
 switchport mode trunk
!
interface TenGigabitEthernet1/0/6
 switchport mode trunk
!
interface TenGigabitEthernet1/0/7
!
interface TenGigabitEthernet1/0/8
!
interface TenGigabitEthernet1/0/9
 switchport mode trunk
!
interface TenGigabitEthernet1/0/10
 switchport mode trunk
!
interface TenGigabitEthernet1/0/11
 switchport mode trunk
!
interface TenGigabitEthernet1/0/12
!
interface TenGigabitEthernet1/0/13
!
interface TenGigabitEthernet1/0/14
!
interface TenGigabitEthernet1/0/15
!
interface TenGigabitEthernet1/0/16
!
interface TenGigabitEthernet1/0/17
!
interface TenGigabitEthernet1/0/18
```

```
!
interface TenGigabitEthernet1/0/19
!
interface TenGigabitEthernet1/0/20
!
interface TenGigabitEthernet1/0/21
 switchport mode trunk
!
interface TenGigabitEthernet1/0/22
 switchport mode trunk
!
interface TenGigabitEthernet1/0/23
 switchport mode trunk
!
interface TenGigabitEthernet1/0/24
 switchport mode trunk
!
interface TenGigabitEthernet1/1/1
!
interface TenGigabitEthernet1/1/2
!
interface TenGigabitEthernet1/1/3
!
interface TenGigabitEthernet1/1/4
!
interface TenGigabitEthernet1/1/5
!
interface TenGigabitEthernet1/1/6
!
interface TenGigabitEthernet1/1/7
!
interface TenGigabitEthernet1/1/8
!
interface FortyGigabitEthernet1/1/1
!
interface FortyGigabitEthernet1/1/2
!
interface Vlan1
 ip address 10.100.16.1 255.255.254.0 secondary
 ip address 10.100.56.1 255.255.255.0 secondary
 ip address 10.100.18.1 255.255.255.0 secondary
 ip address 10.100.16.50 255.255.254.0 secondary
 ip address 10.100.46.1 255.255.255.0
 ip policy route-map CORREO
!
interface Vlan10
 description Salida Cliente 10 Cpu
 ip address 10.180.10.1 255.255.255.0
```

```
!
interface Vlan20
 description Salida Cliente 20
 ip address 10.180.20.1 255.255.255.0
!
interface Vlan30
 description Salida Cliente 30 Impresoras
 ip address 10.180.30.1 255.255.255.0
!
interface Vlan40
 description Puntos de data para Telefonia IP
 ip address 10.180.40.1 255.255.255.0
!
interface Vlan50
 description Vlan para el monitoreo de Ups
 ip address 10.180.50.1 255.255.255.0
!
interface Vlan60
 description sistema de Video Vigilancia y Camaras IP - (200 Camaras)
 ip address 10.180.60.1 255.255.255.0
!
interface Vlan70
 description Puntos de Data para cuarto de control
 ip address 10.180.70.1 255.255.255.0
!
interface Vlan80
 description Vlan Servidores
 ip address 10.180.80.1 255.255.255.0
!
interface Vlan90
 description Puntos de Acceso Wifi
 ip address 10.180.90.1 255.255.255.0
!
interface Vlan100
 description Medidores de Celda de Energia
 ip address 10.180.100.1 255.255.255.0
!
interface Vlan110
 description Equipos de Automatizacion, balanzas
 ip address 10.180.110.1 255.255.255.0
!
interface Vlan120
 description Sistema de Control de Acceso,Puertas
 ip address 10.180.120.1 255.255.255.0
!
interface Vlan130
 description Video Conferencia
 ip address 10.180.130.1 255.255.255.0
```

```
!
interface Vlan140
 ip address 10.180.140.1 255.255.255.0
!
interface Vlan150
 description Enlaces ISP
 ip address 10.180.150.1 255.255.255.0
!
interface Vlan160
 ip address 10.180.160.1 255.255.255.0
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.180.150.2
ip route 1.0.0.0 255.255.0.0 10.180.150.3
ip route 10.0.0.0 255.0.0.0 10.180.150.3
ip route 10.100.13.0 255.255.255.0 10.180.150.4
ip route 172.20.0.0 255.255.0.0 10.180.150.3
ip route 192.168.0.0 255.255.0.0 10.180.150.3
!
ip access-list extended CORREO_PARAMONGA
 deny   ip host 10.100.16.201 10.100.16.0 0.0.1.255
 deny   ip host 10.100.16.201 10.100.46.0 0.0.0.255
 deny   ip host 10.100.16.201 10.100.56.0 0.0.0.255
 deny   ip host 10.100.16.201 10.100.18.0 0.0.0.255
 permit ip host 10.100.16.201 any
!
!
route-map CORREO permit 1
 match ip address CORREO_PARAMONGA
 set ip next-hop 10.180.150.3
!
!
!
line con 0
 stopbits 1
 line aux 0
 stopbits 1
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
wsma agent exec
```

```
 profile httplistener
 profile httpslistener
!
wsma agent config
 profile httplistener
 profile httpslistener
!
wsma agent filesys
 profile httplistener
 profile httpslistener
!
wsma agent notify
 profile httplistener
 profile httpslistener
!
!
wsma profile listener httplistener
 transport http
!
wsma profile listener httpslistener
 transport https
!
ap group default-group
end

SW-CORE# 967731520967731520
```

CONFIGURACION DEL SWITCH WAN

```
errdisable recovery cause security-violation
errdisable recovery cause channel-misconfig (STP)
errdisable recovery cause pagp-flap
errdisable recovery cause dtp-flap
errdisable recovery cause link-flap
errdisable recovery cause sfp-config-mismatch
errdisable recovery cause gbic-invalid
errdisable recovery cause psecure-violation
errdisable recovery cause port-mode-failure
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause pppoe-ia-rate-limit
errdisable recovery cause mac-limit
errdisable recovery cause vmps
errdisable recovery cause storm-control
errdisable recovery cause inline-power
errdisable recovery cause arp-inspection
errdisable recovery cause loopback
errdisable recovery cause small-frame
errdisable recovery cause psp
errdisable recovery interval 30
```

```
!
vlan internal allocation policy ascending
!
vlan 10
 name Data10
!
vlan 20
 name Data20
!
vlan 30
 name Data30
!
vlan 40
 name Telefonia_Ip
!
vlan 50
 name UPS_CtoComunicacion
!
vlan 60
 name CCTV
!
vlan 70
 name Centro_de_Control
!
vlan 80
 name Servidores
!
vlan 90
 name WIFI_CORP
!
vlan 100
 name MEDIDORES_ELECTRICOS
!
vlan 110
 name Automatizacion
!
vlan 120
 name Asistencia_Personal
!
vlan 130
 name Video_Conferencia
!
vlan 140
 name Gestion_Equipos_Red
!
vlan 150
 name Enlace-WAN
!
```

```
vlan 160
!
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet1/0/1
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/2
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/3
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/4
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/5
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/6
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/7
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/8
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/9
 description AP DIRECTORIO
```

```
 switchport access vlan 140
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/10
 description AP GERENCIA-ADM
 switchport access vlan 140
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/11
 description AP CISCO
 switchport access vlan 140
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/12
 description AP CISCO
 switchport access vlan 140
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/13
 spanning-tree portfast
!
interface GigabitEthernet1/0/14
 spanning-tree portfast
!
interface GigabitEthernet1/0/15
 spanning-tree portfast
!
interface GigabitEthernet1/0/16
 switchport access vlan 130
 spanning-tree portfast
!
interface GigabitEthernet1/0/17
 spanning-tree portfast
!
interface GigabitEthernet1/0/18
 spanning-tree portfast
!
interface GigabitEthernet1/0/19
 description Trunk to SW-CUARTO-2
 switchport trunk native vlan 140
 switchport mode trunk
 spanning-tree portfast
!
interface GigabitEthernet1/0/20
```

```
 switchport access vlan 150
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/21
 switchport access vlan 150
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/22
 switchport trunk native vlan 140
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/0/23
 switchport access vlan 150
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/24
 spanning-tree portfast
!
interface GigabitEthernet1/0/25
!
interface GigabitEthernet1/0/26
!
interface TenGigabitEthernet1/0/1
 switchport mode trunk
!
interface TenGigabitEthernet1/0/2
!
interface Vlan1
 no ip address
!
interface Vlan140
 ip address 10.180.140.2 255.255.255.0
!
ip default-gateway 10.180.140.1
ip http server
ip http authentication local
ip http secure-server
!
!
line con 0
line vty 0 4
 login local
 transport input ssh
line vty 5 15
```

```
 login local
 transport input ssh
!
end

SW-WAN#
```

CONFIGURACION DEL SWITCH EN EL AREA DE PROYECTO

```
!
vlan internal allocation policy ascending
!
vlan 10
 name Data10
!
vlan 20
 name Data20
!
vlan 30
 name Data30
!
vlan 40
 name Telefonia_Ip
!
vlan 50
 name UPS_CtoComunicacion
!
vlan 60
 name CCTV
!
vlan 70
 name Centro_de_Control
!
vlan 80
 name Servidores
!
vlan 90
 name WIFI_CORP
!
vlan 100
 name MEDIDORES_ELECTRICOS
!
vlan 110
 name Automatizacion
!
vlan 120
 name Asistencia_Personal
!
vlan 130
```

```
 name Video_Conferencia
!
vlan 140
 name Gestion_Equipos_Red
!
vlan 150
 name Enlace-WAN
!
vlan 160
 name VISITAS
!
!
!
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet1/0/1
 switchport access vlan 10
!
interface GigabitEthernet1/0/2
 switchport access vlan 40
!
interface GigabitEthernet1/0/3
!
interface GigabitEthernet1/0/4
!
interface GigabitEthernet1/0/5
 switchport access vlan 10
!
interface GigabitEthernet1/0/6
 switchport access vlan 10
!
interface GigabitEthernet1/0/7
 switchport access vlan 10
!
interface GigabitEthernet1/0/8
 switchport access vlan 10
!
interface GigabitEthernet1/0/9
 switchport access vlan 10
!
interface GigabitEthernet1/0/10
 switchport access vlan 10
!
interface GigabitEthernet1/0/11
 switchport access vlan 30
```

```
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
 switchport access vlan 10
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
 switchport access vlan 10
!
interface GigabitEthernet1/0/18
 switchport access vlan 10
!
interface GigabitEthernet1/0/19
 switchport access vlan 10
!
interface GigabitEthernet1/0/20
 switchport access vlan 10
!
interface GigabitEthernet1/0/21
 switchport access vlan 10
!
interface GigabitEthernet1/0/22
 switchport access vlan 30
!
interface GigabitEthernet1/0/23
 switchport access vlan 10
!
interface GigabitEthernet1/0/24
 switchport access vlan 10
!
interface GigabitEthernet1/0/25
 switchport access vlan 10
!
interface GigabitEthernet1/0/26
 switchport access vlan 40
!
interface GigabitEthernet1/0/27
 switchport access vlan 10
!
interface GigabitEthernet1/0/28
 switchport access vlan 40
!
```

```
interface GigabitEthernet1/0/29
 switchport access vlan 30
!
interface GigabitEthernet1/0/30
!
interface GigabitEthernet1/0/31
!
interface GigabitEthernet1/0/32
!
interface GigabitEthernet1/0/33
 switchport access vlan 10
!
interface GigabitEthernet1/0/34
 switchport access vlan 10
!
interface GigabitEthernet1/0/35
!
interface GigabitEthernet1/0/36
 switchport access vlan 10
!
interface GigabitEthernet1/0/37
!
interface GigabitEthernet1/0/38
!
interface GigabitEthernet1/0/39
!
interface GigabitEthernet1/0/40
!
interface GigabitEthernet1/0/41
!
interface GigabitEthernet1/0/42
!
interface GigabitEthernet1/0/43
!
interface GigabitEthernet1/0/44
!
interface GigabitEthernet1/0/45
!
interface GigabitEthernet1/0/46
!
interface GigabitEthernet1/0/47
!
interface GigabitEthernet1/0/48
!
interface GigabitEthernet1/0/49
!
interface GigabitEthernet1/0/50
!
```

```
interface TenGigabitEthernet1/0/1
 switchport mode trunk
!
interface TenGigabitEthernet1/0/2
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan140
 ip address 10.180.140.11 255.255.255.0
!
ip default-gateway 10.180.140.1
ip http server
ip http authentication local
ip http secure-server
!
!
!
line con 0
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
end

SW-PROYECTO#
```

CONFIGURACION DEL SWITCH EN EL AREA DE FÁBRICA

```
switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/11
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/12
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/13
 switchport access vlan 10
```

```
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/14
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/15
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/16
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/17
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/18
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/19
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/20
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/21
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/22
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
```

```
interface GigabitEthernet1/0/23
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/24
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/25
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/26
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/27
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/28
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/29
 switchport access vlan 30
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/30
 switchport access vlan 110
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/31
 switchport access vlan 110
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/32
 switchport access vlan 140
 switchport mode access
```

```
 spanning-tree portfast
!
interface GigabitEthernet1/0/33
 switchport access vlan 40
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/34
 switchport access vlan 40
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/35
 switchport access vlan 40
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/36
 switchport access vlan 120
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/37
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/38
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/39
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/40
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/41
 switchport access vlan 140
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/42
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
```

```
interface GigabitEthernet1/0/43
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/44
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/45
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/46
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/47
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/48
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/49
!
interface GigabitEthernet1/0/50
!
interface TenGigabitEthernet1/0/1
 switchport mode trunk
!
interface TenGigabitEthernet1/0/2
!
interface Vlan1
 ip address dhcp
!
interface Vlan140
 ip address 10.180.140.3 255.255.255.0
!
ip default-gateway 10.180.140.1
ip http server
ip http authentication local
```

```
ip http secure-server
!
!
!
line con 0
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
end
```
SW-FABRICA-OFICINA#

CONFIGURACION DEL SWITCH EN EL AREA DE ADMINISTRACION 2

```
lan 60
 name CCTV
!
vlan 70
 name Centro_de_Control
!
vlan 80
 name Servidores
!
vlan 90
 name WIFI_CORP
!
vlan 100
 name MEDIDORES_ELECTRICOS
!
vlan 110
 name Automatizacion
!
vlan 120
 name Asistencia_Personal
!
vlan 130
 name Video_Conferencia
!
vlan 140
 name Gestion_Equipos_Red
!
vlan 150
 name Enlace-WAN
!
```

```
vlan 160
 name VISITAS
interface FastEthernet0
no ip address
 shutdown
!
interface GigabitEthernet1/0/1
 switchport access vlan 10
!
interface GigabitEthernet1/0/2
 switchport access vlan 10
!
interface GigabitEthernet1/0/3
 switchport access vlan 10
!
interface GigabitEthernet1/0/4
 switchport access vlan 10
!
interface GigabitEthernet1/0/5
 switchport access vlan 10
!
interface GigabitEthernet1/0/6
 switchport access vlan 10
!
interface GigabitEthernet1/0/7
 switchport access vlan 10
!
interface GigabitEthernet1/0/8
 switchport access vlan 10
!
interface GigabitEthernet1/0/9
 switchport access vlan 10
!
interface GigabitEthernet1/0/10
 switchport access vlan 10
!
interface GigabitEthernet1/0/11
 switchport access vlan 10
!
interface GigabitEthernet1/0/12
 switchport access vlan 10
!
interface GigabitEthernet1/0/13
 switchport access vlan 10
!
interface GigabitEthernet1/0/14
 switchport access vlan 10
!
```

```
interface GigabitEthernet1/0/15
 switchport access vlan 10
!
interface GigabitEthernet1/0/16
 switchport access vlan 10
!
interface GigabitEthernet1/0/17
 switchport access vlan 10
!
interface GigabitEthernet1/0/18
 switchport access vlan 40
!
interface GigabitEthernet1/0/19
 switchport access vlan 10
!
interface GigabitEthernet1/0/20
 switchport access vlan 10
!
interface GigabitEthernet1/0/21
 switchport access vlan 10
!
interface GigabitEthernet1/0/22
 switchport access vlan 10
!
interface GigabitEthernet1/0/23
 switchport access vlan 10
!
interface GigabitEthernet1/0/24
 switchport access vlan 10
!
interface GigabitEthernet1/0/25
 switchport access vlan 10
!
interface GigabitEthernet1/0/26
 switchport access vlan 10
!
interface GigabitEthernet1/0/27
 switchport access vlan 10
!
interface GigabitEthernet1/0/28
 switchport access vlan 10
!
interface GigabitEthernet1/0/29
 switchport access vlan 10
!
interface GigabitEthernet1/0/30
 switchport access vlan 10
!
```

```
interface GigabitEthernet1/0/31
 switchport access vlan 10
!
interface GigabitEthernet1/0/32
 switchport access vlan 10
!
interface GigabitEthernet1/0/33
 switchport access vlan 30
!
interface GigabitEthernet1/0/34
 switchport access vlan 40
!
interface GigabitEthernet1/0/35
!
interface GigabitEthernet1/0/36
 switchport access vlan 140
!
interface GigabitEthernet1/0/37
 switchport access vlan 40
!
interface GigabitEthernet1/0/38
 switchport access vlan 40
!
interface GigabitEthernet1/0/39
 switchport access vlan 10
!
interface GigabitEthernet1/0/40
 switchport access vlan 30
!
interface GigabitEthernet1/0/41
 switchport access vlan 10
!
interface GigabitEthernet1/0/42
 switchport access vlan 10
!
interface GigabitEthernet1/0/43
 switchport access vlan 140
!
interface GigabitEthernet1/0/44
 switchport access vlan 60
!
interface GigabitEthernet1/0/45
 switchport access vlan 120
!
interface GigabitEthernet1/0/46
 switchport access vlan 120
!
interface GigabitEthernet1/0/47
```

```
 switchport access vlan 120
!
interface GigabitEthernet1/0/48
 description Trunk to SW_WAN
 switchport trunk native vlan 140
 switchport mode trunk
!
interface GigabitEthernet1/0/49
!
interface GigabitEthernet1/0/50
!
interface TenGigabitEthernet1/0/1
 switchport mode trunk
!
interface TenGigabitEthernet1/0/2
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan140
 ip address 10.180.140.8 255.255.255.0
!
ip default-gateway 10.180.140.1
ip http server
ip http authentication local
ip http secure-server
!
!
!
!
line con 0
login local
line vty 0 4
login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
end

SW-CUARTO-2#


errdisable recovery cause pagp-flap
errdisable recovery cause dtp-flap
```

```
errdisable recovery cause link-flap
errdisable recovery cause sfp-config-mismatch
errdisable recovery cause gbic-invalid
errdisable recovery cause psecure-violation
errdisable recovery cause port-mode-failure
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause pppoe-ia-rate-limit
errdisable recovery cause mac-limit
errdisable recovery cause vmps
errdisable recovery cause storm-control
errdisable recovery cause inline-power
errdisable recovery cause arp-inspection
errdisable recovery cause loopback
errdisable recovery cause small-frame
errdisable recovery cause psp
errdisable recovery interval 30
!
vlan internal allocation policy ascending
!
vlan 10
 name Data10
!
vlan 20
 name Data20
!
vlan 30
 name Data30
!
vlan 40
 name Telefonia_Ip
!
vlan 50
 name UPS_CtoComunicacion
!
vlan 60
 name CCTV
!
vlan 70
 name Centro_de_Control
!
vlan 80
 name Servidores
!
vlan 90
 name WIFI_CORP
!
vlan 100
 name MEDIDORES_ELECTRICOS
```

```
!
vlan 110
 name Automatizacion
!
vlan 120
 name Asistencia_Personal
!
vlan 130
 name Video_Conferencia
!
vlan 140
 name Gestion_Equipos_Red
!
vlan 150
 name Enlace-WAN
!
!
!
!
!
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet1/0/1
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/2
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/3
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/4
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/5
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
```

```
!
interface GigabitEthernet1/0/6
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/7
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/8
 switchport access vlan 30
 spanning-tree portfast
!
interface GigabitEthernet1/0/9
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/10
 switchport access vlan 140
 spanning-tree portfast
!
interface GigabitEthernet1/0/11
 spanning-tree portfast
!
interface GigabitEthernet1/0/12
 spanning-tree portfast
!
interface GigabitEthernet1/0/13
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/14
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/15
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/16
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
```

```
!
interface GigabitEthernet1/0/17
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/18
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/19
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/20
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/21
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/22
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/23
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/24
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/25
 switchport mode trunk
!
interface GigabitEthernet1/0/26
 switchport mode trunk
!
interface TenGigabitEthernet1/0/1
```

```
 switchport mode trunk
!
interface TenGigabitEthernet1/0/2
 switchport mode trunk
!
interface Vlan1
 no ip address
!
interface Vlan140
 ip address 10.180.140.5 255.255.255.0
!
ip default-gateway 10.180.140.1
ip http server
ip http authentication local
ip http secure-server
!
!
!
!
line con 0
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
end

SW-APT#
```