UNIVERSIDAD MAYOR DE SAN ANDRES

FACULTAD DE INGENIERIA

CARRERA INGENIERÍA ELECTRÓNICA

PROYECTO DE GRADO

DISEÑO, PLANIFICACIÓN, CABLEADO Y PROTOCOLOS DE RED, PARA EL INSTITUTO DE ELECTRÓNICA APLICADA, CAMPUS UNIVERSITARIO COTA COTA – FACULTAD DE INGENIERÍA

UNIVERSITARIO:

ALFONSO JORGE GALLEGOS GARCIA

TUTOR:

Ing. ROBERTO ZAMBRANA

DOCENTE:

Ing. JOSE CAMPERO

MATERIA: ETN – 1040

LA PAZ – BOLIVIA

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE INGENIERIA

LA FACULTAD DE INGENIERIA DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICTAMENTE ACADÉMICOS.

LICENCIA DE USO

El usuario está autorizado a:

a) Visualizar el documento mediante el uso de un ordenador o dispositivo móvil.
b) Copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.
c) Copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la cita o referencia correspondiente en apego a las normas de redacción e investigación.

El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

AGRADECIMIENTOS

Agradecer y dedicar este proyecto a las personas más especiales que compartieron innumerables acontecimientos en mi vida, a mi madre Ginna que es mi ejemplo de vida, a mis hermanos Fernando y Salvador que son mi fortaleza, a mi novia Carla que me acompaño y apoyo en el camino, a todos mis amigos, a mis docentes de la universidad, a mi querido tutor y a mi impecable docente de proyecto de grado, las palabras no pueden expresar los sentimientos que se generaron, con mucho que expresar les dejo mi más sincero gracias.

Alfonso Jorge Gallegos García

RESUMEN

El proyecto de grado contempla la planificación y el diseño de una red de datos para el Instituto de Electrónica Aplicada, Campus Universitario Cota Cota – Facultad de Ingeniería. En el cual entenderemos la importancia de una red que satisface la necesidad de interactuar.

Las redes de datos son cada vez más una parte esencial de nuestro diario vivir de las cuales dependen nuestras relaciones sociales, negocios, estudios y muchos otros.

Para satisfacer las necesidades del instituto se debe realizar un adecuado diseño y planificación que asegure que se consideren debidamente los requisitos y la selección adecuada de los dispositivos.

Se analiza la interconexión entre dispositivos, los tipos de medios, los factores de interferencia, el esquema de direccionamiento, la infraestructura del edificio y los diferentes cálculos que contribuyen a una red de datos exitosa.

Índice

Índice de figuras

Índice tablas

CAPÍTULO 1

1.1 Introducción

En la actualidad nos encontramos con la constante evolución de las redes, el modo en que las interacciones sociales, comerciales, personales, educativas, políticas y diferentes aspectos que son parte de nuestra vida diaria cambian de forma continua.

Un elemento esencial para la existencia humana es interactuar, la comunicación es vital para desarrollarnos, los métodos de compartir ideas e información avanzan constantemente, y es decisivo el uso de esta tecnología para estar al día.

Las redes proporcionan un acceso rápido a los recursos de información, los cuales son solicitados en cualquier momento y en cualquier lugar, estos recursos no se limitan solo a los tradicionales, se exigen los de voz y video. La necesidad creciente de tecnologías requiere un intercambio de recursos a velocidades mayores y hasta en tiempo real.

Para lograr una conexión rápida, segura y confiable entre los usuarios, los distintos dispositivos de la red deben trabajar en conjunto de manera exitosa, la información debe estar disponible en cualquier momento.

Mediante las redes el significado de mundo cambia, en el cual las fronteras nacionales, las distancias entre los países, las limitaciones físicas y hasta económicas son menos importantes y cada vez son menos problemáticas. Mediante las redes el intercambio de información e ideas aumento la productividad y creó diferentes tipos de oportunidades en todo el planeta, esto se debe a fomentar una comunicación sin límites.

Las redes de datos están aquí para mejorar la calidad de vida de todas las personas, ya que mediante estas se tiene acceso a información que puede ayudar a tomar decisiones, por ejemplo:

- Consultar las condiciones meteorológicas y decidir cómo prepararnos para salir.

- Obtener información de diferentes ubicaciones como hospitales, restaurantes, cines, etc.
- Consultar estados bancarios y realizar pagos.
- Mantener el contacto con personas alrededor de todo el mundo.
- Descargar videos, música, documentos, imágenes, cursos, etc.

Mediante las redes se crearon diferentes herramientas para la comunicación, la mensajería instantánea, blogs, wikis, podcasting, video llamadas, streaming de video y las redes sociales. Las redes cambiaron la forma en la que aprendemos, trabajamos, jugamos y hasta relacionarnos de manera íntima con otras personas.

Los cuatro elementos principales de una red son: las reglas, el medio, los mensajes y los dispositivos.

Para que una red funcione, los diferentes elementos que las componen deben estar interconectados, estas conexiones pueden ser con cables o inalámbricas. Los medios cableados incluyen a los cables de cobre, y estos existen en diferentes tipos como coaxial, par trenzado del cable telefónico, par trenzado UTP, que transmiten señales eléctricas. Y las fibras ópticas, hebras finas de vidrio que transmiten luz. Los medios inalámbricos incluyen conexiones inalámbricas domesticas como un router Wi-Fi, comunicación entre dispositivos de la tierra y satélites, un mensaje puede viajar por una variedad de medios.

Por lo anteriormente mencionado el Instituto de Electrónica Aplicada, Campus Universitario Cota Cota – Facultad de Ingeniería, requiere un acceso a las tecnologías de la información y comunicación, para un manejo eficaz de las herramientas que provee una red de datos.

1.2 Planteamiento del problema

El diseño deficiente o la ausencia de una red de datos, reduce significativamente el intercambio de información, bajos resultados de experiencia, el llegar a más usuarios significa gastos extras, deficiencia en el empleo de equipos y herramientas (computadoras, servidores, equipos de fax, impresoras, software entre otros), datos e información obtenidos en tiempos más prolongados, etc. La cual llevaría al Instituto de Electrónica Aplicada, Campus Universitario Cota Cota – Facultad de Ingeniería a gestiones ineficientes.

1.3 Justificación

Una red se realiza con el fin de facilitar el almacenamiento y procesamiento de la información ya que permite compartir programas, de igual manera, permite establecer los recursos a los que se pueden acceder en la red como: unidades de almacenamiento, Internet, impresoras, entre otros.

Todas estas características, permiten procesar la información y obtener resultados positivos y aprovechar las ventajas que nos ofrecen las redes, además a través de las redes de datos se puede ganar mucho tiempo porque se disponen de varios equipos de cómputo para realizar múltiples tareas.

El proyecto resulta viable ya que con este se daría solución a la necesidad de una red en el Instituto de Electrónica Aplicada, esto implica ahorro de dinero, facilidad de comunicación y poder compartir información. Teniendo en cuenta que compartir la información entre las diferentes áreas del Instituto de Electrónica Aplicada, Campus Universitario Cota Cota – Facultad de Ingeniería es un factor muy importante, esto por supuesto lo soluciona la red.

1.4 Objetivo

Planificar y diseñar la infraestructura de comunicaciones para el flujo de la información del Instituto de Electrónica Aplicada, Campus Universitario Cota Cota – Facultad de Ingeniería.

1.5 Objetivos específicos

- Investigar y analizar las necesidades de comunicaciones del Instituto de Electrónica Aplicada Campus Universitario de Cota Cota – Facultad de Ingeniería.
- Revisar la propuesta arquitectónica para evaluar los requerimientos de conectividad.
- Dimensionar la red cumpliendo los requerimientos.
- Establecer las características de un diseño de red con: escalabilidad, disponibilidad, rendimiento y seguridad.
- Analizar la caracterización del cableado y protocolos.
- Investigar las tecnologías existentes y los estándares relacionados a las redes de área local.
- Analizar y comparar soluciones tecnológicas existentes en el mercado para proponer una como alternativa para la solución propuesta.
- Elaborar el esquema de direccionamiento de red, que luego se aplicará para su diseño.
- Someter a simulación el diseño planteado.

1.6 Alcances

- El desarrollo del diseño contempla las necesidades del Instituto de Electrónica Aplicada Campus Universitario de Cota Cota – Facultad de Ingeniería.
- Examinar la propuesta arquitectónica para satisfacer las necesidades y requerimientos.

- Valorar los requerimientos de la red.
- El diseño debe ser capaz de dar soporte al crecimiento de la red, la disponibilidad se refiere al tiempo en que la red es accesible a los usuarios, el rendimiento se relaciona con los tiempos de respuesta y la seguridad se encarga de proteger la red.
- Comprender el tipo de cableado y la distancia ya que con esta información determinaremos los parámetros para el diseño.
- Conocer las tecnologías y los estándares de las redes de área local.
- Establecer relaciones, diferencias y semejanzas de las tecnologías existentes en el mercado de las redes.
- Seleccionar los instrumentos y dispositivos de la red.
- Evaluar el funcionamiento de la red por simulación.

1.7 Límites

- Las necesidades se contemplan en el ámbito de la red de área local.
- La infraestructura será analizada mediante los planos ya que por el momento no existe de manera física.
- Centrar los requerimientos para la red.
- La escalabilidad, disponibilidad, rendimiento y seguridad, dependen de la tecnología usada, la complejidad de la solución y el coste.
- El cableado depende del tipo de tecnología, la distancia y el coste.
- La investigación se realiza en el mercado local.
- Se analizarán y compararán 3 marcas, mediante sus aspectos técnicos.
- Se especificará solo detalles técnicos que deben cumplir los equipos necesarios para el proyecto.
- La Red de datos (Instituto de Electrónica Aplicada Campus Cota Cota-Facultad de Ingeniera de la UMSA) solo se simulará para su evaluación de funcionamiento.

CAPÍTULO 2

2.1 Marco teórico

La red de datos del Instituto de Electrónica Aplicada (IEA), Campus Universitario Cota Cota – Facultad de Ingeniería, debe satisfacer distintas demandas a través del tiempo, la forma en que los beneficiarios la usarán, las interfaces que coincidan con la tecnología de los dispositivos en la red de área local (Local Area Network, LAN).

Por lo tanto, las características principales de la red LAN es contar con un router que cumplirá la función de Gateway para conectar la LAN a otras redes. Además, la LAN tendrá uno o más switches para conectar los dispositivos finales.

2.2 Identificación del IEA

El IEA tendrá sus nuevas instalaciones ubicada en la ciudad de La Paz, en la Zona de Cota Cota, avenida Andrés Bello, en el campus universitario de la Facultad de Ingeniería.

Visión

El I.E.A. participa en el desarrollo de proyectos de investigación aplicada a nivel internacional, constituyéndose en un referente regional del desarrollo tecnológico.

Misión

Contribuir en el desarrollo y difusión de las telecomunicaciones, sistemas de control, sistemas de computación; realizando investigación, desarrollo e innovación; capacitación y formación especializada, así como, estudios y proyectos para el desarrollo económico y social.

Objetivo

Realizar investigación básica, aplicada, formación especializada, asesoramiento y prestar servicios en las áreas de ingeniería de: control, telecomunicaciones y sistemas; incorporando el desarrollo tecnológico e innovación en los procesos productivos a nivel departamental y nacional.

2.3 Ubicación geográfica.

Ubicación geográfica del Instituto de Electrónica Aplicada, Campus Universitario Cota Cota – Facultad de Ingeniería.

Las coordenadas geográficas aproximadas son:

16°32'20.2"S

68°03'42.4"W

2.4 Dispositivos de la LAN

2.4.1 Dispositivos internetwork

Los dispositivos principales para interconectar las redes son los enrutadores o routers, cada puerto del router se conecta a una red diferente y este realiza el enrutamiento de los paquetes hacia las diferentes redes, los routers tienen la capacidad de dividir los dominios de colisiones y los dominios de broadcast. Los routers pueden utilizarse también para interconectar redes de diferentes tecnologías, además que pueden contar con interfaces LAN y la red de área amplia (Wide Area Network, WAN).

El router y sus interfaces LAN permiten a estos conectarse a lo los medios LAN, para esto se utiliza generalmente cable de par trenzado sin blindaje (Unshielded Twisted Pair, UTP), algunos routers permiten agregar módulos para ampliar sus puertos o para fibra óptica, ya que puede haber diferentes tipos de interfaces para la conexión del cableado WAN y LAN.

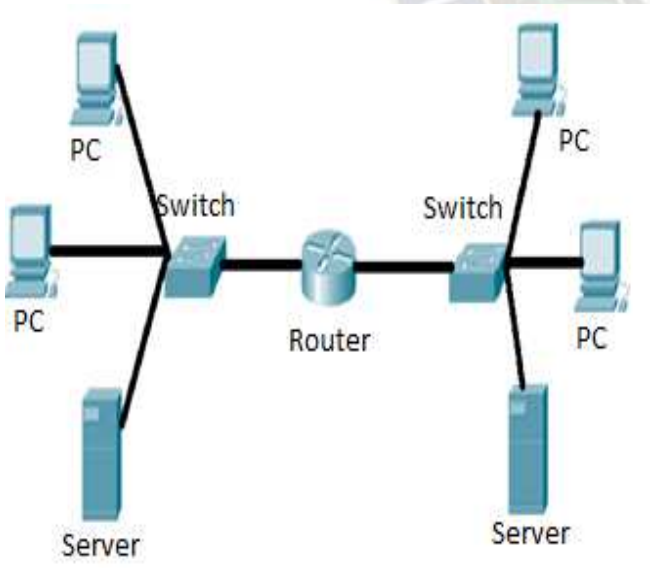


Figura 1: Router interconectando dos LAN.
Fuente: Elaboración propia

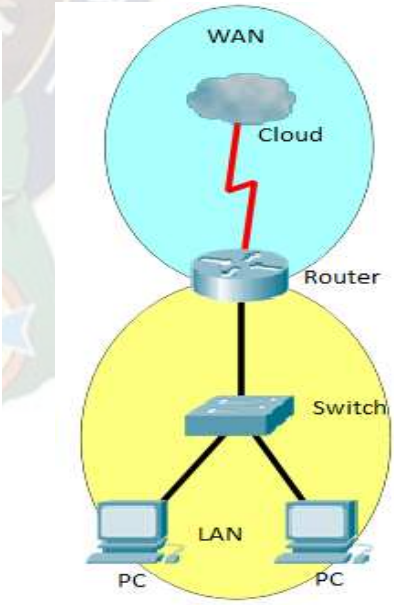


Figura 2:Router interconectando una LAN y Una WAN.
Fuente: Elaboración propia.

2.4.2 Dispositivos intranetwork

Para la LAN es necesario seleccionar de manera correcta los dispositivos para conectar el dispositivo final a la red, comúnmente los dispositivos más usados eran los concentradores como el hub y el switch.

El hub crea un bus lógico, por lo tanto, los puertos utilizan un método de ancho de banda compartido y esto disminuye el rendimiento de la red debido a las colisiones ya que este permanece con un único dominio de colisiones a pesar que se interconecten múltiples hubs. Los hubs son más económicos que los switches[1]. Pero no es conveniente tener hubs en una red ya que es una tecnología antigua.

El switch recibe una trama y regenera la trama en el puerto de destino correspondiente, el switch segmenta una red en múltiples dominios de colisiones, de esta manera reduce las colisiones en una LAN, es decir que cada puerto del switch tiene un dominio de colisiones individual, el switch proporciona un ancho de banda dedicado a cada puerto y así el rendimiento de la LAN aumenta[2].

Los switches son utilizados para conectar dispositivos a una LAN, es confiable y tiene rendimiento mejorado a comparación de un hub.

Existe una variedad de switches disponibles con distintas características que permiten la interconexión de los dispositivos finales.

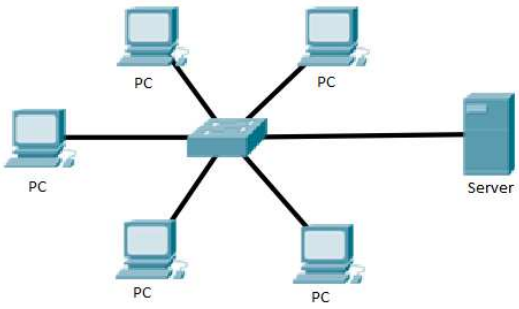


Figura 3: Switch en una LAN
Fuente: Elaboración propia

1 Cisco CCNA Exploration 4.0

2 Nicolás Bonnet, 2014

2.5 Factores de selección

Para cubrir los requisitos de usuario en el IEA se considera los factores que involucrarán la implementación, lo cual se realiza con el diseño y planificación. Estos factores incluyen, entre otros: velocidad y tipos de interfaces, posibilidad de expansión, facilidad de administración, características y servicios.

2.5.1 Velocidad y tipos de interfaces

En una red LAN la velocidad es necesaria, se encuentran ya en el mercado computadoras con NIC incorporadas de 10/100/1000/10000 Mbps. Los dispositivos de capa 2 que tienen mayores velocidades permiten evolucionar a la red manteniendo los dispositivos centrales.

Para la elección de un switch se necesita considerar la cantidad de puertos y el tipo de interfaz, por lo tanto, es importante considerar cuantos puertos necesitarán capacidades de 10 Gbps y cuantos de 100/1000 Mbps.

2.5.2 Elección del router

Para la selección de un router se debe tener en cuenta que las características del equipo cubran con el propósito que tendrá, se debe considerar las velocidades, los tipos de interfaces y los factores adicionales que nos permitan elegirlo de manera correcta como su posibilidad de expansión y las características del SO (sistema operativo).

2.5.3 Expansión

Los routers y switches forman parte de las configuraciones físicas modulares como de las fijas, las fijas tienen una cantidad y un tipo específico de interfaces. Los modulares por otra parte tienen ranuras de expansión que posibilitan la flexibilidad para agregar nuevos módulos cuando aumentan los requisitos, la mayoría de estos dispositivos incluyen una cantidad de puertos fijos y sus ranuras de expansión[3].

3 Cisco CCNA Exploration 4.0

2.5.4 Sistema Operativo

Los sistemas operativos continuamente se mejoran y aparecen nuevas versiones, el router puede admitir determinadas características y servicios, entre ellos tenemos: Seguridad, calidad de servicio (QoS), voz sobre IP (VoIP), enrutamiento en diferentes protocolos, servicios de traducción de direcciones de red (NAT) y protocolos de configuración dinámica de host (DHCP)[4].

2.6 Conexión

La interconexión entre los dispositivos LAN en la instalación se hace por medio del cableado, existen cuatro áreas físicas que se toman en cuenta estas son: Área de trabajo, cuarto de telecomunicaciones, cableado backbone (cableado vertical) y cableado de distribución (cableado horizontal)[5].

2.6.1 Longitud del cable

El estándar internacional para instalaciones UTP ANSI/TIA/EIA-568-B determina que la longitud combinada total del cable que cubre las cuatro áreas mencionadas tendrá una distancia máxima de 100 metros por canal, el estándar establece también que puede utilizarse hasta 5 metros de patch cord para conectar los patch panels y hasta 5 metros de cable desde el punto final del cableado en las tomas de la pared hasta el dispositivo final.

UTP Category	Max. Length	Cable Type	Application
CAT1	-	Twisted Pair	Old Telephone Cable
CAT2	-	Twisted Pair	Token Ring Networks
CAT3	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	100m	Twisted Pair	Token Ring Networks
CAT5	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	100m	Twisted Pair	GigabitEthernet, 10G Ethernet
CAT7	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

Figura 4*:* Diferentes categorías de UTP y especificaciones.
Fuente: firewall.cx (25/07/2016)

4 William Stallings, 2004

5 Cisco CCNA Exploration 4.0

2.6.2 Áreas de trabajo

Las áreas de trabajo son las ubicaciones destinadas para los dispositivos finales los cuáles serán utilizados por usuarios individuales, en el IEA se cuenta con una variedad de laboratorios, salas, aulas, oficinas y otros.

Las áreas que lo requieran contarán con conectores que pueden utilizarse para conectar un dispositivo final a la red. Se utiliza patch cord para conectar los dispositivos finales a estos conectores de pared. El estándar EIA/TIA establece que los patch cords de UTP que sirven para conectar el dispositivo final a los conectores de pared deben tener una longitud máxima de 5 metros.

2.6.3 Cuarto de telecomunicaciones

El cuarto de telecomunicaciones se encuentra en ambos pisos del IEA con el nombre referencial de caseta de telecomunicaciones, es el lugar donde se realizarán las conexiones de los dispositivos intermediarios, estos dispositivos son los switches y routers que conectan la red. Estos dispositivos permiten las transiciones entre el cableado de distribución y el cableado backbone.

En la caseta de telecomunicaciones del IEA se realizan las conexiones entre los patch panels mediante los patch cords, donde terminan los cables de distribución, los patch cords también conectan los dispositivos intermedios.

2.6.4 Cableado de distribución

El cableado horizontal se refiere a los cables que se conectan desde el área de trabajo hasta el cuarto de telecomunicaciones (caseta de telecomunicaciones). La longitud máxima del cable desde el cuarto de telecomunicaciones hasta el de la toma en el área de trabajo no debe superar los 90 metros, a este cableado se lo denomina enlace permanente por que está instalada en la estructura del IEA.

Los medios de distribución parten desde un patch panel en el cuarto de telecomunicaciones a un Jack de pared, los dispositivos se conectan a través de los patch cords[6].

2.6.5 Cableado backbone

El cableado vertical proporciona la interconexión entre los cuartos de entrada de servicios del Instituto de Electrónica Aplicada (IEA) y los cuartos de telecomunicaciones. El cableado del backbone incluye la conexión vertical entre los pisos del edificio, la planta baja y el piso uno del IEA. El cableado backbone es utilizado también para conectar los cuartos de telecomunicaciones a las salas de equipamiento donde suelen ubicarse los servidores.

Los backbones se utilizan para el tráfico agregado, como el tráfico de entrada o de salida de Internet, por lo tanto, generalmente requieren de medios de ancho de banda superiores[7].

2.7 Medios

Los diferentes tipos de medios deben considerarse al seleccionar los cables necesarios para una conexión exitosa.

La capa Física admite múltiples tipos de medios, estos pueden ser: cable UTP (en diferentes categorías), fibra óptica e inalámbrica. Cada tipo de medio tiene ventajas y desventajas[8].

2.8 Ancho de banda

Los dispositivos involucrados en una red presentan requisitos de ancho de banda diferentes, por ejemplo, un servidor generalmente necesita mayor ancho de banda que una laptop que será usada por un único usuario.

6 Cisco CCNA Exploration 4.0

7 Cisco CCNA Exploration 4.0

8 Cisco ICND1 Parte 1, 2013

La tecnología en los medios de cables UTP fueron evolucionando a través del tiempo, así mejorando las velocidades en sus nuevas categorías, con esto se tiene ancho de banda mayores para la LAN.

UTP Category	Data Rate	Cable Type	Application
CAT1	Up to 1Mbps	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	Twisted Pair	GigabitEthernet, 10G Ethernet
CAT7	Up to 10Gbps	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

Figura 5: Diferentes categorías de UTP y especificaciones.
Fuente: firewall.cx (25/07/2016)

2.9 Complejidad de Instalación

La instalación de cableado varía según los tipos de cables y la estructura del edificio, también de las propiedades y el tamaño físico del cable, normalmente se instalan en canales para conductores eléctricos, el cual es un tubo que cubre y protege al cable. El cable UTP tiene la característica de ser relativamente liviano, flexible y tiene un diámetro pequeño, lo cual permite introducirlos en los canales con facilidad. Los conectores RJ-45 son relativamente fáciles de instalar y representan un estándar para las conexiones.

Por otro lado, los cables de fibra óptica contienen una fibra de vidrio delgada, lo cual genera problemas para el radio de curvatura del cable, la cual puede romperse al enroscarse o doblarla mucho, los conectores del cable son mucho más difíciles de instalar y es necesario un equipo especializado.

Las redes inalámbricas requieren de cableado para conectar los dispositivos, como Access Point (AP) a la red LAN, los medios inalámbricos son más fáciles de instalar

que un cable de fibra óptica o un cable UTP, ya que necesita menos cableado, sin embargo, existen varios factores que pueden afectar degradando su funcionamiento[9].

2.10 Conexiones LAN

La Asociación de Industrias Electrónicas y la Asociación de las Industrias de las Telecomunicaciones (EIA/TIA) establecen las conexiones del cableado UTP.

2.10.1 Conector RJ-45

El conector RJ-45 es una interfaz física usada para conectar redes, RJ es un acrónimo del inglés de Registered Jack, es estándar utilizado viene dado por la TIA/EIA-568-B que define la disposición del patillaje de los 4 pares de cable con el que cuenta el cable UTP.

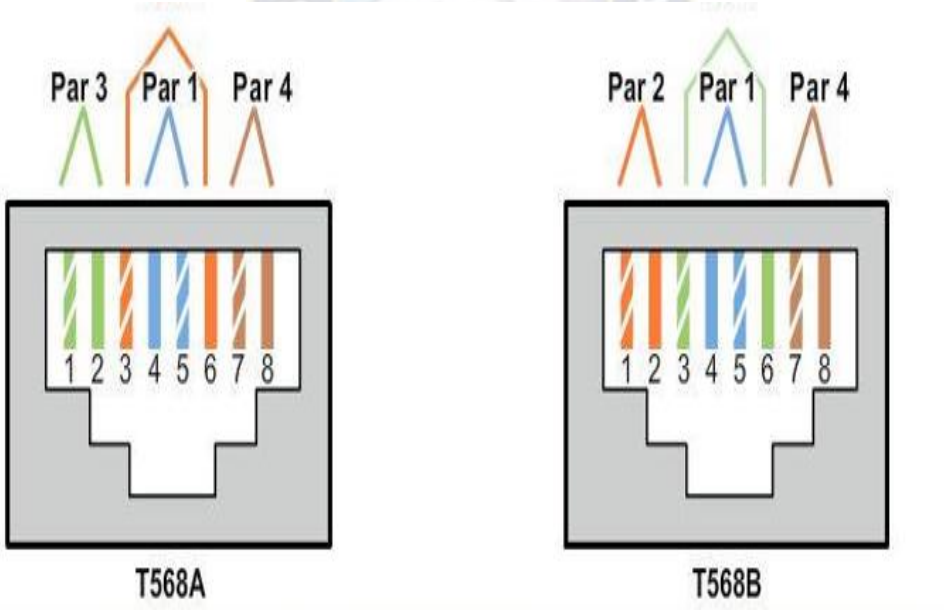


Figura 6: RJ-45 con terminación T568A y T568B
Fuente: CCNA V5.

9 Cisco CCNA Exploration 4.0

2.10.2 Interfaces

En la red LAN, existen dos tipos básicos de interfaces que utiliza el UTP:

MDI (Medium Dependent Interface)

La MDI es la interfaz dependiente del medio y utiliza un diagrama de pines normal, los pines 1 y 2 se utilizan como transmisores y los pines 3 y 6 como receptores, los dispositivos que tendrán conexiones MDI son comúnmente las que cuenten con tarjetas NIC.

MDIX (Medium Dependent Interface Crossover)

La MDI es la interfaz dependiente del medio cruzado, los dispositivos que proporcionan la conectividad a la LAN, por lo general los switches, normalmente utilizan conexiones del tipo MDIX, los cables MDIX intercambian los pares transmisores internamente, esto permite que los dispositivos finales se encuentren conectados a un switch con una conexión directa[10].

Por lo general, cuando se conecta tipos diferentes de dispositivos, se utiliza un cable de conexión directa cuando se conecta dispositivos del mismo tipo, se utiliza un cable de conexión cruzada.

Auto-MDIX

Cuando la interfaz cruzada dependiente del medio automático puede ser habilitada en una interfaz, la interfaz detecta automáticamente el tipo de conexión el directo o el cruzado y configura la conexión adecuada. Con auto-MDIX activada, puede utilizarse cualquier tipo de cable para conectar a otros dispositivos y la interfaz corrige automáticamente cualquier cableado incorrecto[11].

10 Cisco CCNA V5

11 Cisco CCNA V5

Auto-MDIX elimina la necesidad de utilizar cables específicos para cada conexión ya que permite al receptor detectar la señal que está recibiendo y adecuarse a la misma.

2.10.3 Cable UTP

El cableado del par trenzado no blindado (UTP), consiste en cuatro pares de alambres codificados por color que han sido trenzados y cubiertos por un revestimiento de plástico flexible, los códigos de color identifican los pares individuales con sus alambres y sirven de ayuda para la terminación de cables.

El trenzado cancela las señales no deseadas, cuando dos alambres de un circuito eléctrico se colocan uno cerca del otro los campos electromagnéticos externos crean la misma interferencia en cada alambre. Los pares se trenzan para mantener los alambres lo más cerca posible, cuando esta interferencia común se encuentra en los alambres de par trenzado, el receptor los procesa de la misma manera, pero en forma opuesta, como resultado, las señales provocadas por la interferencia electromagnética desde fuentes externas se cancelan de manera efectiva.

Este efecto de cancelación ayuda además a evitar la interferencia proveniente de fuentes internas denominada crosstalk. Crosstalk es la interferencia ocasionada por campos magnéticos alrededor de los pares adyacentes de alambres en un cable. Cuando la corriente eléctrica fluye a través de un alambre, se crea un campo magnético circular a su alrededor. Cuando la corriente fluye en direcciones opuestas en los dos alambres de un par, los campos magnéticos, como fuerzas equivalentes pero opuestas, producen un efecto de cancelación mutua. Además, los distintos pares de cables que se trenzan en el cable utilizan una cantidad diferente de vueltas por metro para ayudar a proteger el cable de la crosstalk entre los pares[12].

12 Cisco CCNA V5

2.10.4 Tipos de cable UTP

El cableado UTP, con una terminación de conectores RJ-45, es un medio común basado en cobre para interconectar dispositivos de red, como computadoras, y dispositivos intermedios, como routers y switches de red.

Según las diferentes situaciones, es posible que los cables UTP necesiten armarse según las diferentes convenciones para los cableados. Esto significa que los alambres individuales del cable deben conectarse en diferentes órdenes para distintos grupos de pines en los conectores RJ-45. A continuación se mencionan los principales tipos de cables que se obtienen al utilizar convenciones específicas de cableado:

• Cable directo de Ethernet

• Cable cruzado de Ethernet

Es posible que la utilización de un cable de conexión cruzada o de conexión directa en forma incorrecta entre los dispositivos no dañe los dispositivos, pero no se producirá la conectividad y la comunicación entre los dispositivos[13].

2.10.5 Cable UTP de conexión directa

Un cable de conexión directa tiene conectores en sus extremos y su terminación es la misma conforme a los estándares T568A o T568B, la identificación del estándar del cable permite determinar si se cuenta con el cable correcto para la conexión.

Los cables directos se utilizan generalmente para las siguientes conexiones: Switch a router, equipo a switch y equipo a hub.

13 Cisco CCNA V5

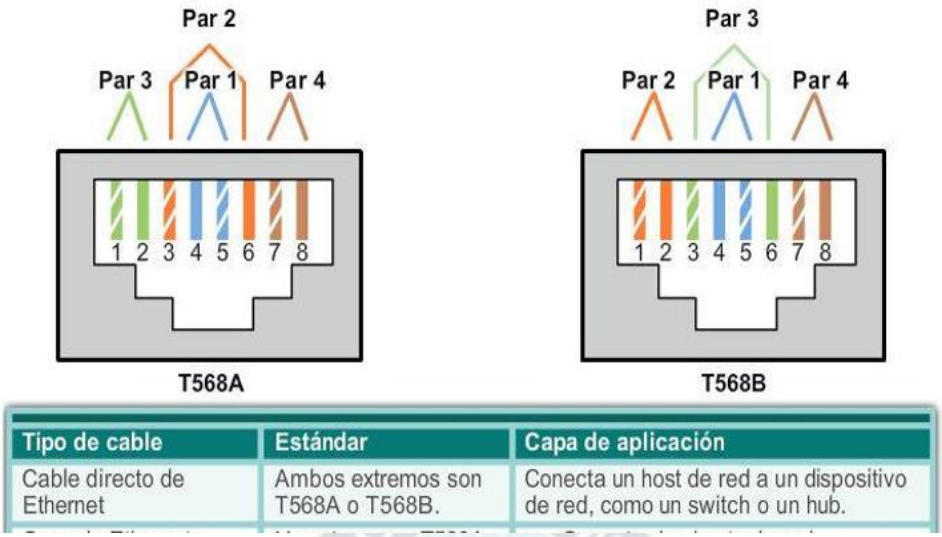


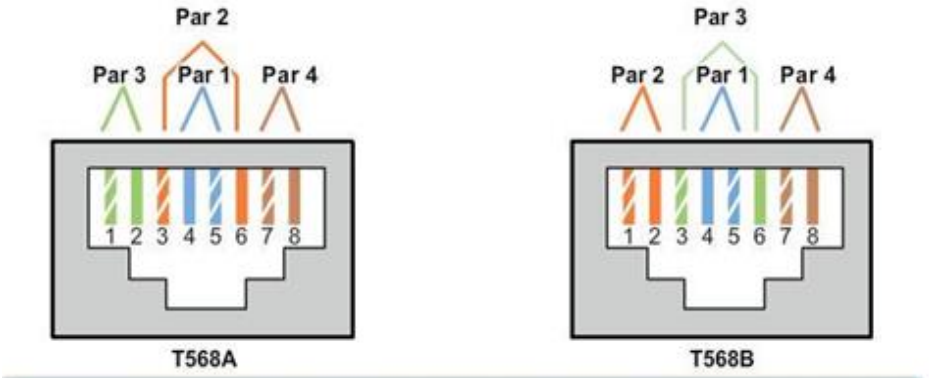
Figura 7: Cables de conexión directa
Fuente: CCNA V5.

2.10.6 Cables UTP de conexión cruzada

Para que los dos dispositivos se comuniquen a través de un cable directamente conectado, el terminal transmisor de uno de los dispositivos necesita conectarse al terminal receptor del otro dispositivo.

El cable debe tener una terminación para que el pin transmisor, Tx, que toma la señal desde el dispositivo A en un extremo, se conecte al pin receptor, Rx, en el dispositivo B. De manera similar, el pin Tx del dispositivo B debe estar conectado al pin Rx del dispositivo A. Si el pin Tx de un dispositivo tiene el número 1 y el pin Rx tiene el número 2, el cable conecta el pin 1 en un extremo con el pin 2 en el otro extremo. Este tipo de cable se denomina "de conexión cruzada" por estas conexiones de pin cruzadas.

Para alcanzar este tipo de conexión con un cable UTP, un extremo debe tener una terminación como diagrama de pin EIA/TIA T568A y el otro, como T568B. Los cables de conexión cruzada conectan generalmente los siguientes dispositivos en una LAN: Switch a switch, switch a hub, hub a hub, router a router (conexión por puertos ethernet), equipo a equipo y equipo a puerto ethernet de router.



Tipo de cable	Estándar	Capa de aplicación
Cruzado Ethernet	Un extremo es T568A, el otro extremo es T568B.	• Conecta dos hosts de red. • Conecta dos dispositivos de red intermediarios (un switch a un switch, o un router a un router).

Figura 8: Cable de conexión cruzada
Fuente: CCNA V5.

2.11 Topología de redes

La topología de red o forma lógica de red se define como la cadena de comunicación que los nodos que conforman una red usan para comunicarse. Es la distribución geométrica de las computadoras conectadas

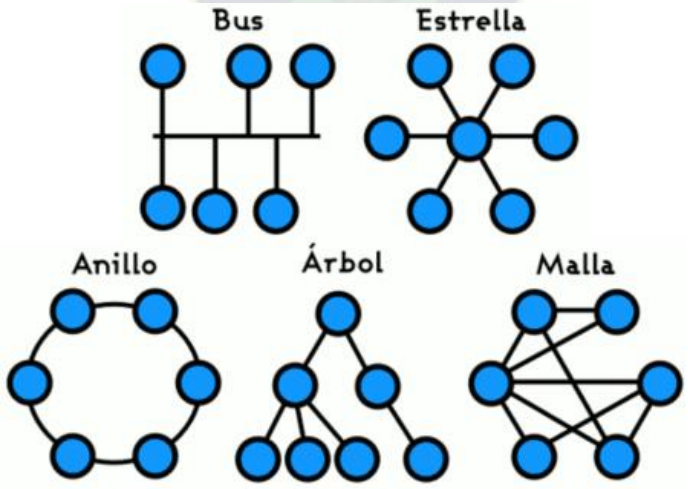


Figura 9: Topologías de red.
Fuente: BICSI, 2002

2.11.1 Red bus

Red cuya topología se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o backbone) al cual se conectan los diferentes dispositivos. De esta forma todos los dispositivos comparten el mismo canal para comunicarse entre sí.

La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre sí. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente. La ruptura del cable hace que los hosts queden desconectados.

Los extremos del cable se terminan con una resistencia de acople denominada terminador, que además de indicar que no existen más ordenadores en el extremo, permiten cerrar el bus por medio de un acople de impedancias[14].

2.11.2 Red estrella

Una red en estrella es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones que han de hacer necesariamente a través de este.

Se utiliza sobre todo para redes locales. La mayoría de las redes de área local que tienen un enrutador (router), un conmutador (switch) o un concentrador (hub) siguen esta topología. El nodo central en estas sería el enrutador, el conmutador o el concentrador, por el que pasan todos los paquetes[15].

2.11.3 Red en anillo

Topología de red en la que cada estación está conectada a la siguiente y la última está conectada a la primera. Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación.

14 Norton, 2000

15 Bigelow, 2003

Cabe mencionar que, si algún nodo de la red deja de funcionar, la comunicación en todo el anillo se pierde.

En un anillo doble, dos anillos permiten que los datos se envíen en ambas direcciones. Esta configuración crea redundancia (tolerancia a fallos), lo que significa que, si uno de los anillos falla, los datos pueden transmitirse por el otro.[16]

2.11.4 Red en malla

La topología en malla es una topología de red en la que cada nodo está conectado a todos los nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos. Si la red de malla está completamente conectada, no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás servidores.

El establecimiento de una red de malla es una manera de encaminar datos, voz e instrucciones entre los nodos. Las redes de malla se diferencian de otras redes en que los elementos de la red (nodo) están conectados todos con todos, mediante cables separados. Esta configuración ofrece caminos redundantes por toda la red de modo que, si falla un cable, otro se hará cargo del tráfico.

Es una opción aplicable a las redes sin hilos (Wireless), a las redes cableadas y a la interacción del software de los nodos.

Una red con topología en malla ofrece una redundancia y fiabilidad superiores. Aunque la facilidad de solución de problemas y el aumento de la confiabilidad son ventajas muy interesantes, estas redes resultan caras de instalar, ya que utilizan mucho cableado. Por ello cobran mayor importancia en el uso de redes inalámbricas (por la no necesidad de cableado) a pesar de los inconvenientes propios del Wireless.

16 Gallo y Hancock, 2002

En muchas ocasiones, la topología en malla se utiliza junto con otras topologías para formar una topología híbrida, está conectada a un servidor que le manda otros computadores[17].

2.11.5 Red en árbol

Topología de red en la que los nodos están colocados en forma de árbol. Desde una visión topológica, la conexión en árbol es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central. En cambio, tiene un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos. Es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones.

La topología en árbol puede verse como una combinación de varias topologías en estrella. Tanto la de árbol como la de estrella son similares a la de bus cuando el nodo de interconexión trabaja en modo difusión, pues la información se propaga hacia todas las estaciones, solo que en esta topología las ramificaciones se extienden a partir de un punto raíz (estrella), a tantas ramificaciones como sean posibles, según las características del árbol. [18]

2.12 VLAN

Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

El rendimiento de la red es un factor importante en la productividad de una organización. Una de las tecnologías que contribuyen a mejorar el rendimiento de la red es la división de los grandes dominios de difusión en dominios más pequeños. Por una cuestión de diseño, los routers bloquean el tráfico de difusión en una interfaz. Sin embargo, los routers generalmente tienen una cantidad limitada de

17 Herrera, 2010

18 Jorge Ghe, 2012

interfaces LAN. La función principal de un router es trasladar información entre las redes, no proporcionar acceso a la red a las terminales.

La función de proporcionar acceso a una LAN suele reservarse para los switches de capa de acceso. Se puede crear una red de área local virtual (VLAN) en un switch de capa 2 para reducir el tamaño de los dominios de difusión, similares a los dispositivos de capa 3. Por lo general, las VLAN se incorporan al diseño de red para facilitar que una red dé soporte a los objetivos de una organización.

Dentro de un entorno de internetwork conmutada, las VLAN proporcionan la segmentación y la flexibilidad organizativa. Las VLAN proporcionan una manera de agrupar dispositivos dentro de una LAN. Un grupo de dispositivos dentro de una VLAN se comunica como si estuvieran conectados al mismo cable. Las VLAN se basan en conexiones lógicas, en lugar de conexiones físicas.

Una VLAN crea un dominio de difusión lógico que puede abarcar varios segmentos LAN físicos. Las VLAN mejoran el rendimiento de la red mediante la división de grandes dominios de difusión en otros más pequeños. Si un dispositivo en una VLAN envía una trama de Ethernet de difusión, todos los dispositivos en la VLAN reciben la trama, pero los dispositivos en otras VLAN no la reciben[19].

2.13 Modelo en capas

Para visualizar la interacción entre varios protocolos, es común utilizar un modelo en capas. Un modelo en capas muestra el funcionamiento de los protocolos que se produce dentro de cada capa, como así también la interacción de las capas sobre y debajo de él.

Existen beneficios al utilizar un modelo en capas para describir los protocolos de red y el funcionamiento.

19 Cisco CCNA V5

2.13.1 Modelos de protocolos y referencias

Existen dos tipos básicos de modelos: modelos de protocolo y modelos de referencia.

Un modelo de protocolo proporciona un modelo que coincide fielmente con la estructura de un protocolo en particular. El conjunto jerárquico de protocolos relacionados representa típicamente toda la funcionalidad requerida para interconectar la red humana con la red de datos. El modelo TCP/IP es un modelo de protocolo porque describe las funciones que se producen en cada capa de los protocolos dentro del conjunto TCP/IP.

Un modelo de referencia proporciona una referencia común para mantener consistencia en todos los tipos de protocolos y servicios de red. Un modelo de referencia no está pensado para ser una especificación de implementación ni para proporcionar un nivel de detalle suficiente para definir de forma precisa los servicios de la arquitectura de red. El propósito principal de un modelo de referencia es asistir en la comprensión más clara de las funciones y los procesos involucrados.

El modelo de interconexión de sistema abierto (OSI) es el modelo de referencia de internetwork más ampliamente conocido. Se utiliza para el diseño de redes de datos, especificaciones de funcionamiento y resolución de problemas[20].

2.13.2 Modelo TCP/IP

El primer modelo de protocolo en capas para comunicaciones de internetwork se creó a principios de la década de los setenta y se conoce con el nombre de modelo de Internet. Define cuatro categorías de funciones que deben tener lugar para que las comunicaciones sean exitosas. La arquitectura de protocolos TCP/IP sigue la estructura de este modelo. Por esto, es común que al modelo de Internet se lo conozca como modelo TCP/IP.

20 Cisco CCNA V5

La mayoría de los modelos de protocolos describen una cantidad de protocolos específicos del proveedor. Sin embargo, puesto que el modelo TCP/IP es un estándar abierto, una compañía no controla la definición del modelo. Las definiciones del estándar y los protocolos TCP/IP se explican en un foro público y se definen en un conjunto de documentos disponibles al público. Estos documentos se denominan Solicitudes de Comentarios (Request For Ccomments, RFC). Contienen las especificaciones formales de los protocolos de comunicación de datos y los recursos que describen el uso de los protocolos. Las RFC también contienen documentos técnicos y organizacionales sobre Internet, incluyendo las especificaciones técnicas y los documentos de las políticas producidos por el Grupo de trabajo de ingeniería de Internet (IETF, Internet Engineering Task Force).

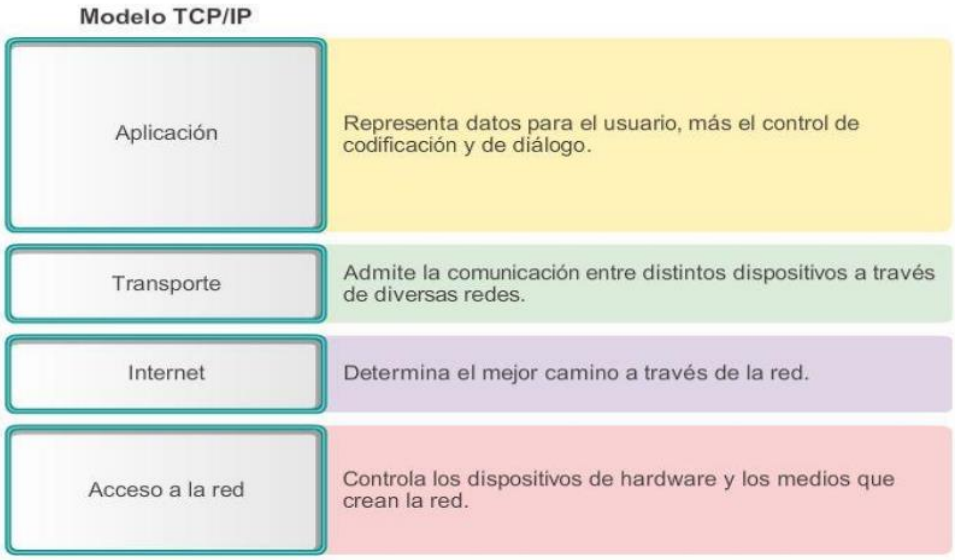


Figura 10: Modelo TCP/IP.
Fuente: CCNA V5.

2.13.3 Modelo OSI

Inicialmente, el modelo OSI fue diseñado por la Organización Internacional para la Estandarización (ISO, International Organization for Standardization) para proporcionar un marco sobre el cual crear una cantidad de protocolos de sistemas abiertos. La visión era que este conjunto de protocolos se utilizara para desarrollar una red internacional que no dependiera de sistemas propietarios.

Lamentablemente, la velocidad a la que fue adoptada la Internet basada en TCP/IP y la proporción en la que se expandió ocasionaron que el desarrollo y la aceptación de los protocolos OSI quedaran atrás. Aunque pocos de los protocolos desarrollados mediante las especificaciones OSI son de uso masivo en la actualidad, el modelo OSI de siete capas ha realizado aportes importantes para el desarrollo de otros protocolos y productos para todos los tipos de nuevas redes.

Como modelo de referencia, el modelo OSI proporciona una amplia lista de funciones y servicios que pueden producirse en cada capa. También describe la interacción de cada capa con las capas directamente por encima y por debajo.

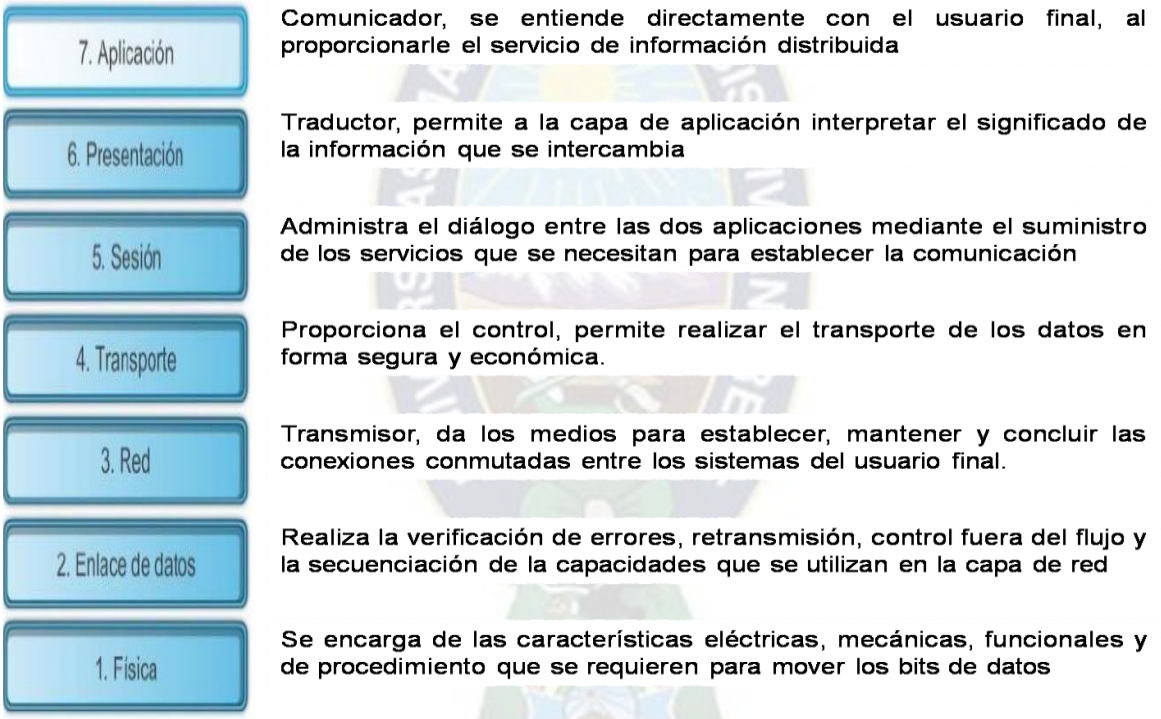


Figura 11: Modelo OSI.
Fuente: CCNA V5.

2.14 DHCP

Todo dispositivo que se conecta a una red necesita una dirección IP única. Los administradores de red asignan direcciones IP estáticas a los routers, a los servidores, a las impresoras y a otros dispositivos de red cuyas ubicaciones (físicas y lógicas) probablemente no cambien. Por lo general, se trata de dispositivos que proporcionan servicios a los usuarios y dispositivos en la red. Por lo tanto, las

direcciones que se les asignan se deben mantener constantes. Además, las direcciones estáticas habilitan a los administradores para que administren estos dispositivos en forma remota. A los administradores de red les resulta más fácil acceder a un dispositivo cuando pueden determinar fácilmente su dirección IP.

Sin embargo, las computadoras y los usuarios en una organización, a menudo, cambian de ubicación, física y lógicamente. Para los administradores de red, asignar direcciones IP nuevas cada vez que un empleado cambia de ubicación puede ser difícil y llevar mucho tiempo. Además, para los empleados móviles que trabajan desde ubicaciones remotas, puede ser difícil establecer de forma manual los parámetros de red correctos. Incluso para los clientes de escritorio, la asignación manual de direcciones IP y otra información de direccionamiento plantea una carga administrativa, especialmente a medida que crece la red.

La introducción de un servidor de protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) en la red local simplifica la asignación de direcciones IP tanto a los dispositivos de escritorio como a los móviles. El uso de un servidor de DHCP centralizado permite a las organizaciones administrar todas las asignaciones de direcciones IP desde un único servidor. Esta práctica hace que la administración de direcciones IP sea más eficaz y asegura la coherencia en toda la organización, incluso en las sucursales[21].

2.15 Edificio Inteligente

El IEA es una edificación la cual mediante la red de datos tiene la potencialidad de dar un paso adelante en la gestión de sus recursos, la idea de estos conceptos es poder apreciar los alcances de la red de datos del instituto.

Un edificio inteligente es aquella edificación equipada con cableado estructurado para permitir a sus ocupantes controlar remotamente o programar una serie de dispositivos automatizados por medio de un solo comando, es decir que un solo botón pueda realizar varias tareas a la vez.

21Cisco CCNA V5

Para algunos, este concepto de edificio inteligente puede ser aquel que tenga un sistema que ajuste de manera variable la luz, ajuste de temperatura y cambios de humedad todo controlado automáticamente o por dispositivos de control sofisticados.

Un edificio inteligente es aquel que es capaz de crear un ambiente que maximice la eficiencia de los ocupantes mientras que permita una administración efectiva de recursos con el menor costo de tiempo.

Figura 12: Edificio Inteligente.
Fuente: securitysystems.co (05/08/2016)

2.15.1 Inmótica

La inmótica ofrece la posibilidad de monitorear y controlar el funcionamiento general de varios servicios y equipos en el IEA, como balance energético, climatización, iluminación, alarmas de intrusión, detección de incendios y el monitoreo de variables analógicas como temperatura, humedad, etc.

Por inmótica o automatización de edificios entendemos la incorporación al equipamiento de edificios de uso terciario o industrial (oficinas, institutos, edificios

corporativos, hoteleros, empresariales y similares), de sistemas de gestión técnica automatizada de las instalaciones, con el objetivo de reducir el consumo de energía, aumentar el confort y la seguridad de los mismos.

Entenderemos que un edificio es "inteligente" si incorpora sistemas de información en todo el edificio, ofreciendo servicios avanzados de la actividad y de las telecomunicaciones, con control automatizado, monitorización, gestión y mantenimiento de los distintos subsistemas o servicios del edificio, de forma óptima e integrada, local y remotamente. Diseñados con suficiente flexibilidad como para que sea sencilla y económicamente rentable la implementación de futuros sistemas.

Todos estos sistemas son integrables a una red LAN bajo los protocolos de TCP/IP, existen múltiples alternativas de inmótica en el mercado los cuales no son mencionados en el presente proyecto ya que no es el objetivo del mismo.

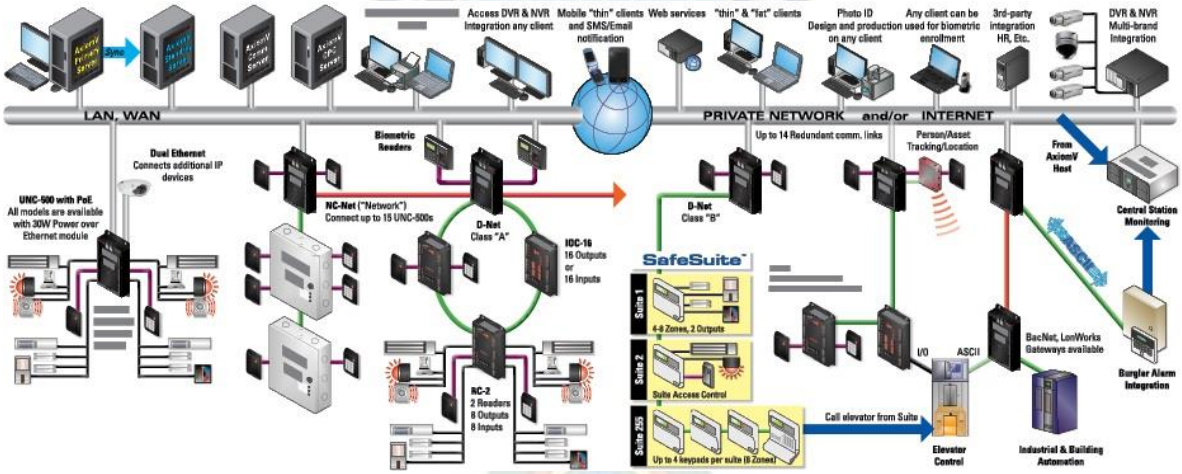


Figura 13: Inmótica conectada a la red
Fuente: rbh-access.com (06/08/2016)

2.15.2 Sistemas de Gestión

El IEA cuenta con diversos ambientes como laboratorios, aulas, biblioteca, cocina, etc. Todos estos sitios necesitan varios sistemas electrónicos de control para su correcto funcionamiento.

Para lograr determinar los sistemas y equipos necesarios para gestionar los diferentes servicios que se puedan presentar en el IEA se divide en tres grupos de gestión de un sistema inmótico:

Gestión de la Seguridad:

- Sistemas de alarmas contra intrusos
- Sistemas de detección de incendios y humo
- Sistema de sonidos o ruidos
- Circuitos cerrados de tv CCTV y video vigilancia
- Controles de acceso: personal y visitantes
- Alarmas técnicas: Control fuga de gas en la cocina, inundaciones etc.
- Parqueo de vehículos
- Supervisión en tiempo real de eventos
- Avisos de mantenimiento preventivo de equipos
- Sistemas biométricos y tarjetas magnéticas.
- Control de activos fijos con tecnología RFID
- Sistema de unidades de respaldo
- Control de acceso perimetral

Gestión del Confort (comodidad):

- Aire acondicionado
- Control de audio y video en auditorios
- Control de persianas
- Manejo de pantallas de proyección
- Control de proyectores, encendido y apagado
- Control de movimiento de proyectores
- Control a distancia

Gestión para ahorro de energía:

- Control en sistemas de iluminación
- Control de motores: bombas de agua, extractores, inyectores

- Control de generadores eléctricos- encendido y apagado remoto
- Control del tanque de combustible

La arquitectura avanzada de un sistema inmótico permite múltiples conexiones a la red LAN entre los diferentes servidores de comunicación y controladores, en el gráfico de la **Figura 13** se puede visualizar todos los servicios que se pueden controlar. Los diferentes equipos, dispositivos y sistemas a gestionar pueden trabajar como subsistemas independientes y se los puede incorporar a un solo sistema dentro de la red por los protocolos de TCP/IP mediante los diferentes dispositivos de entrada – salida de la plataforma que utiliza un sistema inmótico, permitiendo tener un monitoreo centralizado en el IEA.

Figura 14: Sistema de gestión.
Fuente: global-projects.es (07/08/2016)

2.16 Internet de las cosas

El Internet de las Cosas (IdC) o Internet of Things (IoT) consiste en que las cosas tengan conexión a Internet en cualquier momento y lugar. En un sentido más técnico, consiste en la integración de sensores y dispositivos en objetos cotidianos que quedan conectados a Internet a través de redes fijas e inalámbricas. El hecho de que Internet esté presente al mismo tiempo en todas partes permite que la

adopción masiva de esta tecnología sea más factible. Dado su tamaño y coste, los sensores son fácilmente integrables en hogares, entornos de trabajo y lugares públicos. De esta manera, cualquier objeto es susceptible de ser conectado y «manifestarse» en la Red. Además, el IdC implica que todo objeto puede ser una fuente de datos. Esto está empezando a transformar la forma de hacer negocios, la organización del sector público y el día a día de millones de personas.

IoT hace referencia a un mundo conectado hasta el último extremo, donde objetos y seres físicos interaccionan con entornos virtuales de datos en el mismo espacio y tiempo.

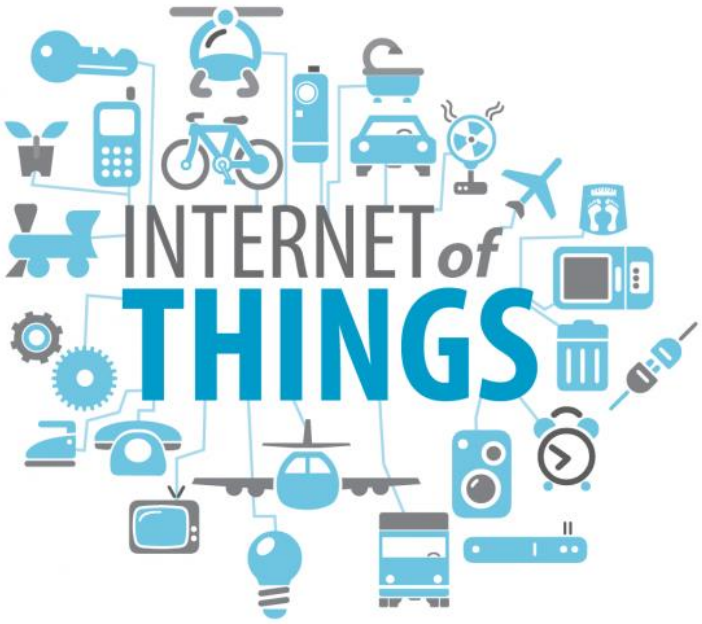


Figura 15: Internet de las cosas.
Fuente: gtt-tech.com (08/08/2016)

2.16.1 IdC en el presente

Antes de analizar el estado actual de IdC, es importante ponerse de acuerdo en una definición. Según el Grupo de soluciones empresariales basadas en Internet (IBSG, Internet Business Solutions Group) de Cisco, IdC es sencillamente el punto en el tiempo en el que se conectaron a Internet más “cosas u objetos” que personas.

En 2003, había aproximadamente 6,3 mil millones de personas en el planeta, y había 500 millones de dispositivos conectados a Internet. Si dividimos la cantidad de dispositivos conectados por la población mundial, el resultado indica que había menos de un dispositivo (0,08) por persona. De acuerdo con la definición de Cisco IBSG, IdC aún no existía en 2003 porque la cantidad de cosas conectadas era relativamente escasa, dado que apenas comenzada la invasión de los dispositivos omnipresentes, como los smartphones.

El crecimiento explosivo de los smartphones y las tablet PC elevó a 12,5 mil millones en 2010 la cantidad de dispositivos conectados a Internet, en tanto que la población mundial aumentó a 6,8 mil millones, por lo que el número de dispositivos conectados por persona es superior a 1 (1,84 para ser exactos) por primera vez en la historia. Si se desglosan aún más estas cifras, Cisco IBSG estima que IdC "nació" en algún punto entre 2008 y 2009.

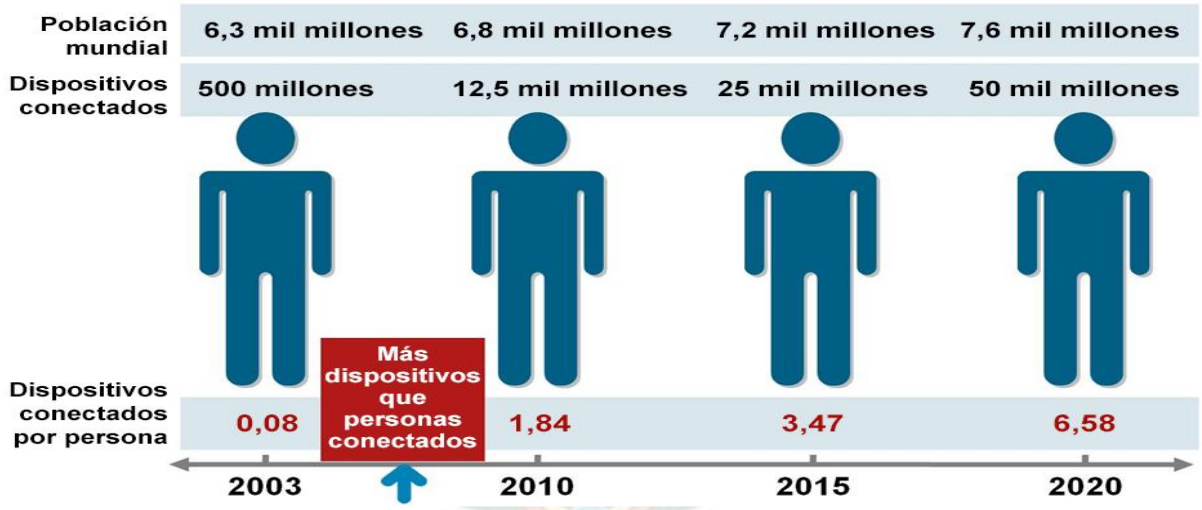


Figura 16: Internet de las cosas.
Fuente: Cisco IBSG, 2011.

2.16.2 Interconexión

Con el Internet de las cosas, el planeta está siendo instrumentado e interconectado, al tiempo que se vuelve más inteligente. Esto ocurre porque los millones de personas y una lista interminable de objetos conectados a Internet (coches, electrodomésticos, teléfonos, cámaras, etc.) ahora pueden interactuar, traspasando

las barreras del tiempo y el espacio. A su alrededor, se construyen entornos “inteligentes” capaces de analizar, diagnosticar y ejecutar funciones.

Cualquier objeto es susceptible de ser conectado y manifestarse en la Red. Las etiquetas RFID (Radio Frequency Identification, en español, identificación por radiofrecuencia) son pequeños dispositivos, similares a una pegatina, que pueden ser adheridos a un producto, persona o animal para almacenar información relevante y dinámica. Mediante radiofrecuencia, la información viaja a un ordenador o dispositivo móvil con acceso a Internet. Dicha información puede ser recibida por un usuario para su interpretación. También existe la posibilidad de que el extremo final sea otra máquina que interprete los datos y actúe según parámetros preestablecidos[22].

Figura 17: Interconexión.
Fuente: wordstream.com (09/08/2016)

2.17 Redes inalámbricas

Las redes inalámbricas, Wireless (sin cables) o WLAN (Wireless LAN) como son más conocidas, son un tipo de redes surgidas de la necesidad de facilitar la

22 Big Data por Luis Joyanes Aguilar, 2013

movilidad de los usuarios. Con ello, en el IEA se evita, entre otros aspectos, el tener que “recablear” un ambiente por la llegada de nuevos usuarios. Gracias a esta nueva tecnología se ha conseguido que los usuarios no dependan de cables que les obliguen a permanecer conectados físicamente a la red.

En la red sin cables se utiliza Wi-Fi como método de acceso. Cuando hablamos de Wi-Fi nos referimos a una de las tecnologías de comunicación inalámbricas más utilizadas hoy en día. Genéricamente las redes inalámbricas son conocidas como WLAN. Wi-Fi es un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11, los cuales serán presentados en los anexos.

El Wi-Fi es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wi-Fi (como una computadora personal, un televisor inteligente, un teléfono inteligente, dispositivos de vigilancia, etiquetas RFDI, etc.) pueden conectarse a internet a través de un punto de acceso de red inalámbrica.

También podemos mencionar la facilidad de implementación o integración de equipamiento en interiores como en exteriores, así como su configuración y puesta en marcha.

El DTIC de la UMSA menciona a las redes inalámbricas como el Wi-Fi como un servicio y a los sistemas que dan acceso las cuales están dirigidas a todos los miembros de la comunidad de la Universidad Mayor de San Andrés, incluyendo: docentes, estudiantes de pre y postgrado, administrativos eventuales y de planta. Ninguna persona deberá realizar cualquier tipo de cobro por el uso de estos servicios o sistemas o negociar de alguna forma con los mismos.

CAPÍTULO 3

3.1 Desarrollo del proyecto

En este capítulo se describen las diferentes etapas que contiene el proyecto, las consideraciones sobre el proyecto, se presenta el análisis de los requerimientos, los detalles del diseño además de los de hardware y software.

3.2 Metodología de diseño

El método para el diseño de la red está basado en la metodología Top-Down Network Design, esta metodología comienza en las capas superiores del modelo de referencia de OSI hacia las inferiores, se concentra en aplicaciones, sesiones y transporte antes de la selección de los routers, switches y medios de las capas inferiores.

El diseño de la red debe ser un proceso que asocie las necesidades del IEA a la tecnología disponible para generar un sistema que maximice el rendimiento del mismo. El diseño consta de tres fases las cuales son las siguientes:

- Fase 1 – Analizar Requisitos
  - Entrevista con el director del Instituto de Electrónica Aplicada, el Ingeniero Wilber Flores Bustillos.
  - Encuestas a los usuarios y miembros del IEA.
  - Revisar la propuesta arquitectónica.
  - Analizar metas técnicas.

- Fase 2 – Diseño Lógico de la Red
  - Diseñar la topología de la red.
  - Diseñar modelos de direccionamiento.
  - Protocolos de conmutación y enrutamiento.
  - Desarrollar estrategias de seguridad para la red.

- Fase 3 – Diseño Físico de la Red
  - Mapa físico de la red.
  - Seleccionar dispositivos para la red.

3.3 Análisis de Requisitos

El Instituto de Electrónica Aplicada participa en el desarrollo de proyectos de investigación aplicada, el cual contribuye al desarrollo y difusión de las telecomunicaciones, sistemas de control, sistemas de computación, realizando investigación, desarrollo e innovación, capacitación y formación especializada.

La nueva infraestructura permite el desarrollo de las actividades realizadas por el IEA en los diferentes ambientes con los que cuenta, los cuales necesitan estar conectados a la red de datos para una eficiente comunicación, y estos presentan diversos requisitos los cuales son recopilados mediante encuestas a los usuarios y la entrevista con el director del Instituto de Electrónica Aplicada, los cuales se encuentran en el **ANEXO 1**.

Los requerimientos que se determinaron se explican a continuación:

- **Cantidad de nodos**

La red de área local del Instituto de Electrónica Aplicada estará conformada por varios dispositivos terminales (PC) conectadas unas a otras en sus dos niveles, planta baja y primer piso, cada computadora de la LAN representará un punto o nodo dentro la red. Los requerimientos de nodos para la red se presentan en la siguiente tabla.

NIVEL	Nº DE NODOS
PLANTA BAJA	32
PRIMER PISO	39

Tabla 1: Cantidad de nodos por nivel del IEA.
Fuente: Elaboración propia.

- **Velocidad**

La necesidad de velocidad está presente en un entorno LAN, se encuentran NIC de 10/100/1000/10000 Mbps, la selección de dispositivos de capa 2 que puedan ajustarse a mayores velocidades permite a la red evolucionar sin reemplazar los dispositivos centrales. Los cables UTP CAT6A, operan a frecuencias de hasta 500 MHz y proveen transferencias de hasta 10 Gbps (10GBASE-T) y soporta una distancia máxima de 100 metros. La nueva especificación mitiga los efectos de la diafonía o crosstalk.

La velocidad de 10 Gbps para una red LAN parece excesivo, pero la necesidad de mayor ancho de banda siempre está presente y en unos años esta será la velocidad que se maneje como estándar.

- **Servicios de red requeridos y de los recursos a compartir**

Desde el punto de vista funcional es necesario establecer los servicios y recursos que la red proveerá a los diferentes usuarios. A continuación, se listan los servicios requeridos y recursos que deberá compartir:

Servicios

- Servicios de archivos e impresión
- Servicios de copia de respaldo y restauración
- Exploración del web en internet
- FTP
- Servicios de seguridad en Internet (Firewall)
- Servicios centralizados de protección contra virus (Firewall)

Recursos

- Documentos
- Mensajes de correo electrónico
- Software de procesamiento de texto
- Ilustraciones, fotografías, videos y archivos de sonido
- Transmisiones en directo de sonido y video

- **Dispositivos y periféricos**

La necesidad de conectar en red dispositivos para compartir su uso, se lista a continuación los dispositivos que se conectaran a la red:

AMBIENTE	DISPOSITIVO
Secretaria	Impresora

Tabla 2: Dispositivo a conectar a la red.
Fuente: Elaboración propia.

- **Usuarios**

Para que la red funcione, es necesario que la misma sea operada por el personal, el cual está conformado por los diferentes usuarios de la red.

los usuarios se detallan en la siguiente tabla:

Nivel Planta Baja

AMBIENTE	CARGO Y/O NOMBRE DEL USUARIO
Recepción	Recepcionista
Grupo de emergencias	Personal por designar
Laboratorio de control	Docente y estudiantes
Laboratorio de electrónica	Docente y estudiantes
Laboratorio de sonido y acústica	Docente y estudiantes
Laboratorio de sistemas digitales	Docente y estudiantes
Taller de mantenimiento	Administrador de la red
Oficina de control	Bibliotecario/Encargado
Sala de computación	Docente y estudiantes

Tabla 3: Usuarios a conectar a la red planta baja IEA.
Fuente: Elaboración propia.

Nivel Primer Piso

AMBIENTE	CARGO Y/O NOMBRE DEL USUARIO
Oficina Director	Ing. Wilber Flores Bustillo
Secretaria	Sria. Ma. Eugenia S. de Mendizábal
Laboratorio de biomédica	Docente y estudiantes
Laboratorio de telecomunicaciones	Docente y estudiantes
Sala de investigadores y reuniones	Docente y estudiantes
Aula tipo 1	Docente
Aula tipo 2	Docente
Auditorio	Por personal autorizado

Tabla 4: Usuarios a conectar a la red primer piso IEA.
Fuente: Elaboración propia (8/11/2016).

- **Seguridad**

En el Instituto de Electrónica Aplicada se debe establecer reglas de seguridad particularmente en los ambientes de las autoridades y de administrativos. También establecer políticas de seguridad en los accesos a la red pública (Internet). Por lo tanto, es necesario que estos ambientes no sean compartidos con los demás ambientes. De esta manera resultaría óptimo la instalación de Routers que brinden el servicio de Firewall, es decir que examinen el tráfico de entrada y salida de estos ambientes, permitiendo solo el paso del tráfico autorizado. De manera similar será necesario el Router que brinde la conexión con el exterior provea un servicio de Firewall para proporcionarle seguridad a toda la red, particularmente al acceso a Internet.

- **Ampliación**

El crecimiento esperado de la red, debido al progresivo aumento de estudiantes y docentes en la nueva infraestructura del IEA implica que el diseño deba extenderse de manera rápida y sencilla sin tener que reemplazar gran parte del hardware y software.

Una solución sencilla y económica para la ampliación de la red es mediante las redes inalámbricas, las cuales pueden ser provistas por un Router Wi-Fi en las áreas requeridas.

- **Administración**

En el IEA cada usuario es responsable del rendimiento de su equipo, los usuarios del instituto tienen conocimientos básicos para encargarse del soporte técnico cuando las cosas no funcionan correctamente en sus estaciones de trabajo, para un correcto funcionamiento se debe tener un experto que se encargue de la administración, supervisión y el mantenimiento de la red.

3.3.1 Propuesta arquitectónica

La estructura del IEA se encuentra ubicado en el Campus Universitario de Cota Cota de la Facultad de Ingeniería, el acceso y salida a este es por medio de una puerta principal y otra secundaria, está distribuido en dos niveles, la planta baja y el primer piso, los cuales se conectan únicamente por gradas.

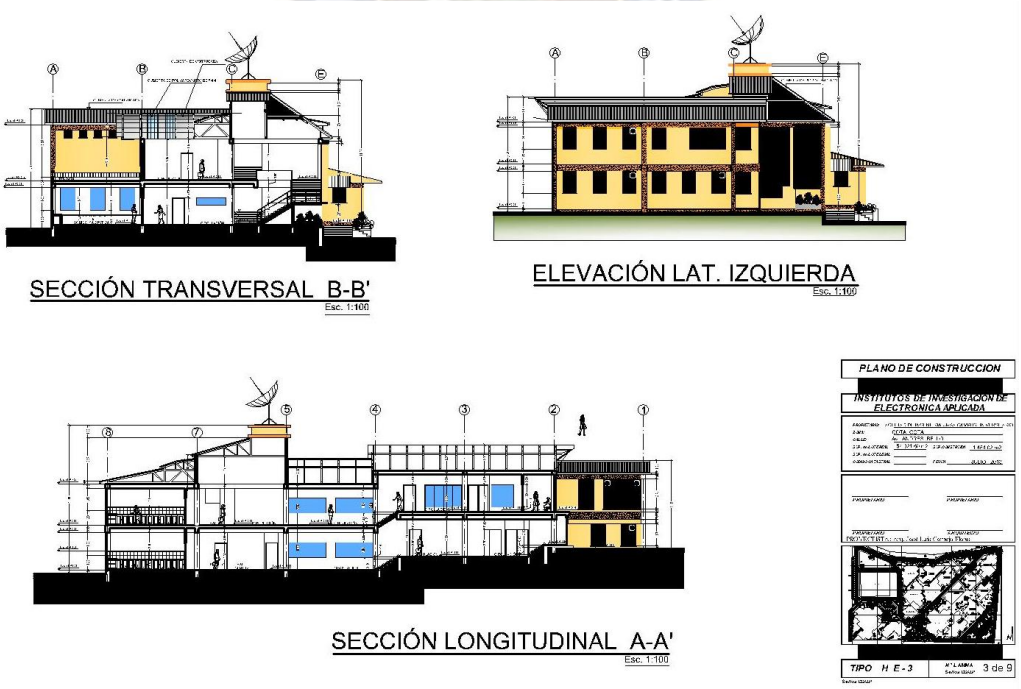


Figura 18: Propuesta arquitectónica IEA.
Fuente: SICOES (29/03/16).

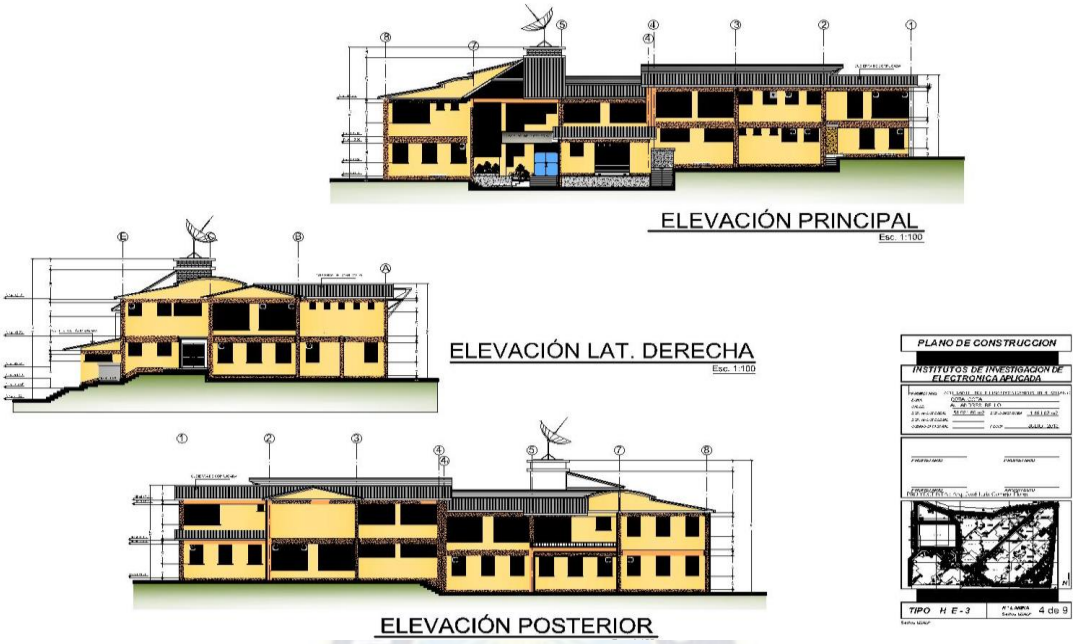


Figura 19: Propuesta arquitectónica IEA.
Fuente: SICOES (29/03/16).

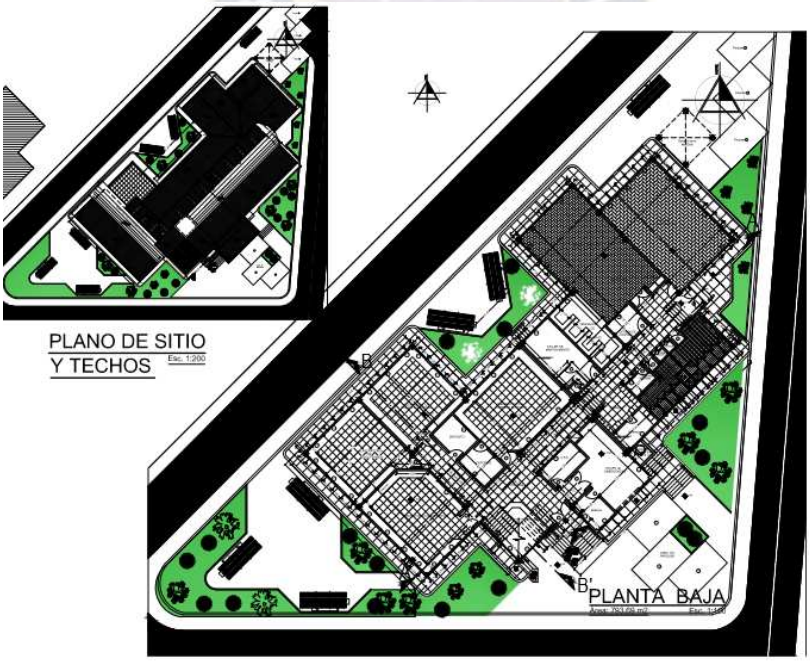


Figura 20: Propuesta arquitectónica IEA.
Fuente: SICOES (29/03/16).

Se describen los ambientes de la planta baja y la cantidad de nodos por ambiente, en la siguiente tabla:

AMBIENTE	Nº DE NODOS
Recepción	1
Grupo de emergencias	2
Laboratorio de control	3
Laboratorio de electrónica	2
Laboratorio de sonido y acústica	3
Deposito 1	0
Deposito 2	0
Laboratorio de sistemas digitales	5
Taller de mantenimiento	2
Casilleros	0
Limpieza	0
Seguridad industrial	0
Baño mujeres	0
Oficina de control	2
Biblioteca y sala de lectura	0
Baño de varones	0
Sala de computación	12
TOTAL	32

Tabla 5: Ambientes y número de nodos planta baja IEA.
Fuente: Elaboración propia.

*En el Taller de mantenimiento se encuentra la caseta de telecomunicaciones.

Se describen los ambientes del primer piso y la cantidad de nodos por ambiente, en la siguiente tabla:

AMBIENTE	Nº DE NODOS
Laboratorio de biomédica	6
Laboratorio de telecomunicaciones	12
Sala de investigadores y área de reuniones	10
Terraza de antenas	0
Aula tipo 1	1
Aula tipo 2	1
Archivo	0
Baño damas	0
Baño varones	0
Cocina	0
Auditorio	2
Secretaria	4
Oficina Director	3
TOTAL	39

Tabla 6: Ambientes y número de nodos planta baja IEA.
Fuente: Elaboración propia

*En el Archivo se encuentra la caseta de telecomunicaciones.

3.3.2 Técnicos

Los requisitos técnicos con los cuales se estructurará la red se describen a continuación.

- **Determinación de la topología**

Para la estructura de la red se propone una topología de estrella jerárquica o de árbol, por medio de concentradores dispuestos en cascada para formar una red jerárquica. Todos los nodos periféricos se pueden comunicar con los demás transmitiendo o recibiendo del nodo central solamente. Un fallo en la línea de conexión de cualquier nodo con el nodo central provocaría el aislamiento de ese nodo respecto a los demás, pero el resto de sistemas permanecería intacto. Los switches de la capa de distribución, los cuales se encuentran en el cuarto de telecomunicaciones de cada piso, dando servicio a las subredes horizontales. La red horizontal de cada planta distribuye las señales desde los switches de distribución hasta las tomas terminales de los usuarios.

- **Red Troncal**

La Red Troncal, Backbone o Red Vertical, se extiende desde el cuarto de comunicaciones de la planta baja del IEA hasta el cuarto de comunicaciones del primer piso. Este conecta al Router principal con los Switches de distribución de cada planta.

- **Selección del medio de comunicación**

Para el enlace físico ente los dispositivos de la red y pensando en una futura expansión y mayor tráfico de la red del IEA, el estándar de red a utilizar es de tipo 10GBASE-T para cable STP categoría 6A, la cual viene dada por la especificación ANSI/TIA/EIA-568-B.2-10.

- **Rack de telecomunicaciones**

Un rack es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para el ancho están normalizadas para que sean compatibles con equipamiento de distintos fabricantes. También son llamados bastidores, cabinas, gabinetes o armarios.
El Rack se puede fijar a la mayoría de las paredes y cuenta con un diseño robusto y compacto que permite colocarlo en prácticamente cualquier lugar sin desperdiciar espacio.
Está diseñado para dar cabida a equipos de red, telecomunicaciones y servidores de 19 pulgadas (ancho), dispone de ventilación para un entorno operativo refrigerado para los equipos.

- **Patch Panel**

Están formados por un soporte metálico y de medidas compatibles para el rack de 19 pulgadas, el patch panel sostiene placas de circuito impreso sobre la que se montan de un lado los conectores RJ45 y del otro los conectores IDC para block tipo 110 que soporten el tipo de cable. Estos vienen en capacidades de 12 a 96 puertos (múltiplos de 12).

- **Rosetas de red**

Usualmente de 2 bocas, aunque existe también la versión reducida de 1 boca. Posee un circuito impreso que soporta conectores RJ45 para conectar los cables UTP que soporten el tipo de cable.

- **Tomas terminales**

Las tomas terminales estarán implementadas mediante conectores hembra RJ45 con 8 contactos. Las conexiones de los cables tanto en las rosetas de usuario como en los paneles de parcheo seguirán el esquema de la norma TIA/EIA 568B.

- **Tipo de tarjeta de interfaz de red**

La tarjeta de interfaz de red (NIC, Network Interface Card), funciona como una interfaz entre el equipo del usuario y el cableado de red. La NIC identifica al equipo en la red y almacena en el búfer los datos entre el equipo y el cable. Cuando los datos son enviados la NIC debe convertir los datos de bytes paralelos a bits en serie y el proceso inverso en la recepción. En la red, la NIC genera las señales eléctricas que viajan a través de la red, administra el acceso a la red y establece la conexión física con el cable.

Los equipos requieren tarjetas de red PCI según el estándar 10GBASE-T o mínimamente 1000BASE-T y que posea conectores RJ45 que soporten el tipo de cable UTP.

3.3.3 Metas técnicas

- **Escalabilidad**

La necesidad del crecimiento de red del IEA es posible al poseer un diseño de cableado estructurado, la topología jerárquica de la red tiene la característica de escalar de manera sencilla. El IEA cuenta con un personal total de 20 usuarios, tanto como docentes, estudiantes y administrativos. En la nueva infraestructura se tiene 71 nodos para usuarios, y su crecimiento futuro puede ser cubierto mediante conexiones inalámbricas.

- **Disponibilidad**

El IEA atenderá de lunes a viernes en horario continuo desde las 8 de la mañana hasta las 4 de la tarde, la red de datos puede ofrecer sus servicios las 24 horas por cada día de la semana.

- **Rendimiento**

El rendimiento de la red del IEA se mejora reduciendo el tamaño del dominio de colisión, los switches logran esto porque cada puerto es un dominio de colisión. El rendimiento también se mejora reduciendo el dominico de difusión, ya que si el número de terminales aumenta el tráfico de difusión también y aumenta el consumo de CPU por procesado de tráfico broadcast no deseado. La manera de reducir eficientemente el dominio de difusión es con la Red de Área Local Virtual (VLAN, Virtual Local Area Network).

- **Seguridad**

Una de las maneras más eficientes de proteger la red es habilitando un firewall en el router ya que este dispositivo protege a los equipos de la red limitando y seleccionando el acceso de la red. Existen otras formas de aumentar la seguridad creando listas de acceso.

3.4 Diseño lógico de la red

El diseño lógico de red es la segunda fase de la metodología adoptada para el proyecto, el primer paso es diseñar la topología de la red, diseñar modelos de direccionamiento, seleccionar protocolos de conmutación y enrutamiento, desarrollar estrategias de seguridad para la red y desarrollar estrategias para el mantenimiento de la red.

3.4.1 Diseño de la topología de red

La topología de red es un mapa que indica los segmentos de red, puntos de interconexión y áreas de usuarios. El objetivo del mapa es mostrar la geometría de la red, no la geografía física o la implementación técnica.

La topología de red, es la Topología Jerárquica esta topología puede ayudar a minimizar gastos, la adquisición de los dispositivos apropiados de funcionamiento entre redes para cada capa jerárquica, así se evitan gastos en características

innecesarias para una capa. La naturaleza modular permite la planificación de cada capa jerárquica.

Las capas de la topología están enfocadas a funciones específicas, permitiendo elegir los correctos sistemas y características para la capa.

La modularidad permite un diseño simple y fácil de entender. La simplicidad minimiza la necesidad de la capacitación extensa para el personal de operaciones de red. El aislamiento de fallas es mejorado y se reconocen fácilmente los puntos de transición en la red y ayuda a aislar los puntos de fallas posibles.

El diseño jerárquico facilita cambios, cuando los elementos de la red lo requieren, el costo está contenido a un pequeño subconjunto de la red total.

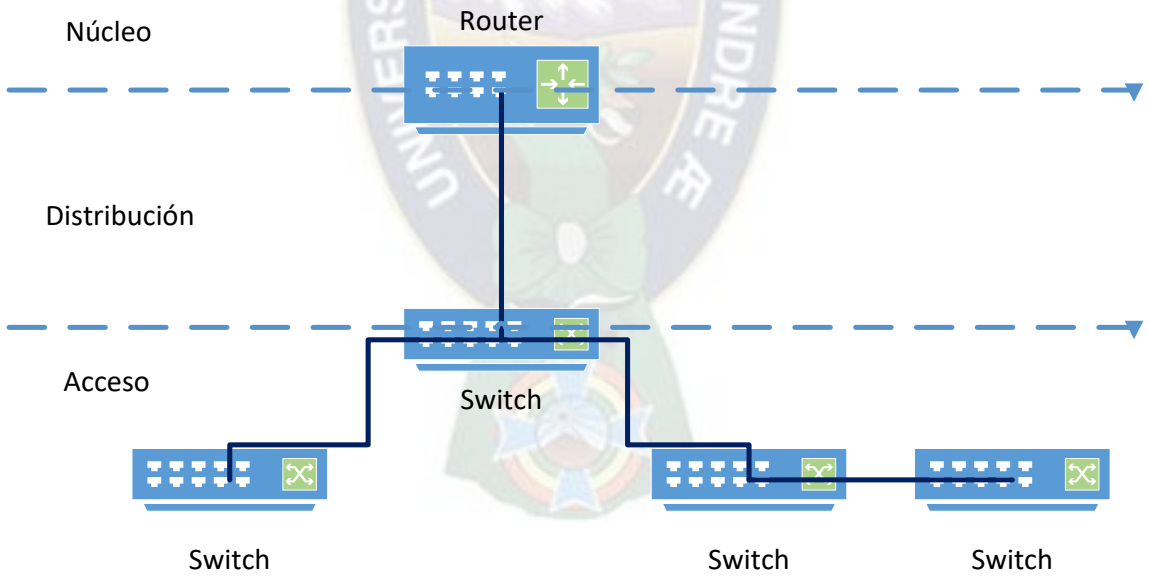


Figura 21: Topología jerárquica.
Fuente: Elaboración propia.

3.4.2 Diseño de direccionamiento de red

Para acelerar la incorporación de nuevos hosts a la red y contribuir a la resolución de problemas, se utiliza direcciones que se ajusten a un patrón común en todas las subredes. Cada uno de los dispositivos del IEA debe asignarse a un bloque lógico de direcciones dentro del rango de direcciones de la red.

Las diferentes categorías para los hosts son:

- Usuarios estudiantes.
- Usuarios docentes.
- Usuarios administrativos.

AMBIENTE PLANTA BAJA	Nº DE NODOS	Administrativos	Docentes	Estudiantes
Recepción	1	1	0	0
Grupo de emergencias	2	2	0	0
Laboratorio de control	3	0	1	2
Laboratorio de electrónica	2	0	1	1
Laboratorio de sonido y acústica	3	0	1	2
Deposito 1	0	0	0	0
Deposito 2	0	0	0	0
Laboratorio de sistemas digitales	5	0	1	4
Taller de mantenimiento	2	2	0	0
Casilleros	0	0	0	0
Limpieza	0	0	0	0
Seguridad industrial	0	0	0	0
Baño mujeres	0	0	0	0
Oficina de control	2	2	0	0
Biblioteca y sala de lectura	0	0	0	0
Baño de varones	0	0	0	0
Sala de computación	12	0	1	11
TOTAL	32	7	8	17

Tabla 7: Cantidad de nodos planta baja por categoría.
Fuente: Elaboración propia.

AMBIENTE PRIMER PISO	Nº DE NODOS	Administrativos	Docentes	Estudiantes
Laboratorio de biomédica	6	0	5	1
Laboratorio de telecomunicaciones	12	0	1	11
Sala de investigadores y área de reuniones	10	0	0	10
Terraza de antenas	0	0	0	0
Aula tipo 1	1	0	1	0
Aula tipo 2	1	0	1	0
Archivo	0	0	0	0
Baño damas	0	0	0	0
Baño varones	0	0	0	0
Cocina	0	0	0	0
Auditorio	2	2	0	0
Secretaria	4	4	0	0
Oficina Director	3	3	0	0
TOTAL	39	9	8	22

Tabla 8: Cantidad de nodos primer piso por categoría.
Fuente: Elaboración propia.

La cantidad y grupos de hosts son:

LAN de estudiantes
Nodos de estudiantes : 39
Router (LAN Gateway) : 1
Switches (administración) : 2
Total, por subred de estudiantes : 42

LAN de docentes
Nodos de instructores : 16
Router (LAN Gateway) : 1
Switches (administración) : 1
Total, por subred de docentes : 18

LAN de administrativos
Nodos de estudiantes : 16
Router (LAN Gateway) : 1
Switches (administración) : 1
Total, por subred de admin. : 18

Los métodos para asignar direcciones a una internetwork son dos. Utilizar la Máscara de Subred de Longitud Variable (VLSM, Variable Length Subnet Masking), donde se asignan el prefijo y los bits de hosts a cada red basándose en la cantidad de hosts de esa red. O utilizar un enfoque distinto a VLSM, en donde las subredes utilizan la misma longitud de prefijo y la misma cantidad de bits del host.

Se asigna el bloque de direcciones 192.168.1.0/24 (máscara de subred 255.255.255.0) a esta internetwork.

Cálculo y asignación de direcciones sin VLSM:

El método de asignación de direcciones sin VLSM, todas las subredes tienen la misma cantidad de direcciones asignadas a ellas. Para proporcionar la cantidad adecuada de direcciones se utiliza de base la cantidad de direcciones más extensa de la red.

En el IEA, la LAN de estudiantes es la red más extensa que requiere 42 direcciones. La fórmula para calcular la cantidad de hosts es:

$$Host\ utilizables\ = 2^n - 2$$

Utilizamos 6 como valor de "n" ya que es la primera potencia de dos, superior a 42 y se restan 2 por la dirección de red y la de broadcast. Por lo tanto, tenemos:

$$Host\ utilizables\ = 2^6 - 2 = 64 - 2 = 62$$

Tenemos 62 direcciones de host utilizables. El cálculo cumple con el requisito de al menos 42 direcciones, con una asignación para el crecimiento. Este cálculo da como resultado 26 bits de red (32 bits totales, 6 bits de host).

Se necesita tres bloques de 62 direcciones cada uno por un total de 186 direcciones ya que existen tres redes en nuestra internetwork. Utilizaremos el bloque de direcciones 192.168.1.0/26. Está es una dirección de Clase C, las direcciones del IP en su primer octeto del 192 al 223 son parte de esta clase.

Nuestro bloque de direcciones 192.168.1.0/26 proporciona las direcciones en un rango de 192.168.1.0 a 192.168.1.255

Cálculos de dirección para las redes:

Dirección : 192.168.1.0
En binario : 11000000.10101000.00000001.00000000
Máscara : 255.255.255.192 = 26
En binario : 11111111.11111111.11111111.11000000

LAN de estudiantes

Para la LAN de estudiantes, los valores son:

192.168.1.1 a 192.168.1.62 hosts con una dirección de subred de 192.168.1.0 y una de broadcast de 192.168.1.63.

LAN de docentes

Para la LAN de docentes, los valores son:

192.168.1.65 a 192.168.1.126 hosts con una dirección de subred de 192.168.1.64 y una de broadcast de 192.168.1.127.

LAN de administrativos

Para la LAN de administrativos, los valores son:

192.168.1.129 a 192.168.1.190 hosts con una dirección de subred de 192.168.1.128 y una de broadcast de 192.168.1.191.

Al utilizar un método con diferente enfoque a VLSM se tienen muchas direcciones sin utilizar, tenemos un bloque desde 198.168.1.192 a 192.168.1.255. El siguiente cuadro nos muestra las direcciones sin utilizar por cada subred:

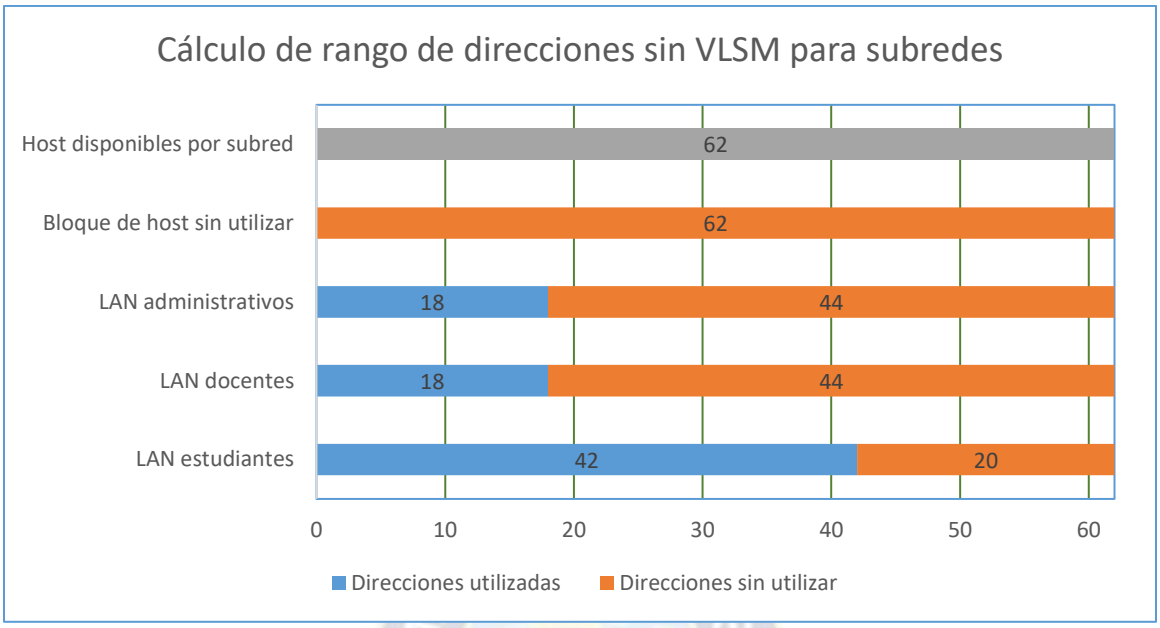


Figura 22: Calculo de rango de direcciones sin VLSM para subredes.
Fuente: Elaboración propia.

Red	Dirección de subred	Rango de dirección de host min.	Rango de dirección de host máx.	Dirección de broadcast.
Estudiantes	192.168.1.0/26	192.168.1.1	192.168.1.62	192.168.1.63
Docentes	192.168.1.64/26	192.168.1.65	192.168.1.126	192.168.1.127
Administrativos	192.168.1.128/26	192.168.1.129	192.168.1.190	192.168.1.191

Tabla 9: Rangos de direcciones sin VLSM por categoría.
Fuente: Elaboración propia.

Cálculo y asignación de direcciones con VLSM:

El método de asignación de direcciones con VLSM, se asigna un bloque de direcciones para cada red lo más adecuado a cada una de ellas. La utilización de VLSM requiere de mayor planificación que el método anterior.

Se asigna el bloque de direcciones 192.168.1.0/24 (máscara de subred 255.255.255.0) a esta internetwork en su totalidad. Se utilizan ocho bits para definir

direcciones host y subredes. Esto produce un total de 256 direcciones locales IPv4 en el rango de 192.168.1.0 a 192.168.1.255

LAN de estudiantes

Para la LAN de estudiantes que es la más extensa se requieren 42 direcciones.

La fórmula para calcular la cantidad de hosts es: $Host\ utilizables\ = 2^n - 2$

Utilizamos 6 como valor de "n" ya que es la primera potencia de dos, superior a 42 y se restan 2 por la dirección de red y la de broadcast. Por lo tanto, tenemos:

$$Host\ utilizables\ = 2^6 - 2 = 64 - 2 = 62$$

Tenemos 62 direcciones de host utilizables. El cálculo cumple con el requisito de al menos 42 direcciones, con una asignación de 20 para el crecimiento.

Al utilizar 6 bits para los hosts da como resultado 2 bits que puede utilizarse localmente para definir las direcciones de subred. La utilización de la dirección disponible más baja da como resultado la dirección de subred de 192.168.1.0/26.

El cálculo de la máscara de subred de estudiantes es:

Dirección : 192.168.1.0
En binario : 11000000.10101000.00000001.00000000
Máscara : 255.255.255.192 = 26
En binario : 11111111.11111111.11111111.11000000

En la red de estudiantes, el rango de host IPv4 es de:

192.168.1.1 a 172.168.1.62 con una dirección de subred de 192.168.1.0 y una de broadcast de 192.168.1.63.

LAN de docentes

Para la LAN de docentes se requieren 18 direcciones.

La fórmula para calcular la cantidad de hosts es: $Host\ utilizables\ = 2^n - 2$

Utilizamos 5 como valor de "n" ya que es la primera potencia de dos, superior a 18 y se restan 2 por la dirección de red y la de broadcast. Por lo tanto, tenemos:

$$Host\ utilizables\ = 2^5 - 2 = 32 - 2 = 30$$

Tenemos 30 direcciones de host utilizables. El cálculo cumple con el requisito de al menos 18 direcciones, con una asignación de 12 para el crecimiento.

El siguiente bloque disponible de direcciones que puede adaptar a los hosts es el bloque 192.168.1.64/27.

Dirección : 192.168.1.64
En binario : 11000000.10101000.00000001.01000000
Máscara : 255.255.255.224 = 27
En binario : 11111111.11111111.11111111.11100000

En la red de docentes, el rango de host IPv4 es de:

192.168.1.65 a 172.168.1.94 con una dirección de subred de 192.168.1.64 y una de broadcast de 192.168.1.95.

LAN de administrativos

Para la LAN de administrativos se requieren 18 direcciones.

La fórmula para calcular la cantidad de hosts es: $Host\ utilizables\ = 2^n - 2$

Utilizamos 5 como valor de "n" ya que es la primera potencia de dos, superior a 18 y se restan 2 por la dirección de red y la de broadcast. Por lo tanto, tenemos:

$$Host\ utilizables\ = 2^5 - 2 = 32 - 2 = 30$$

Tenemos 30 direcciones de host utilizables. El cálculo cumple con el requisito de al menos 18 direcciones, con una asignación de 12 para el crecimiento.

El siguiente bloque disponible de direcciones que puede adaptar a los hosts es el bloque 192.168.1.96/27.

Dirección : 192.168.1.96
En binario : 11000000.10101000.00000001.01100000
Máscara : 255.255.255.224 = 27
En binario : 11111111.11111111.11111111.11100000

En la red de administrativos, el rango de host IPv4 es de:

192.168.1.97 a 172.168.1.126 con una dirección de subred de 192.168.1.96 y una de broadcast de 192.168.1.127.

Si es necesario adaptar el crecimiento futuro, aún se encuentran disponibles las direcciones en el rango de 192.168.1.128 a 192.168.1.255.

Una de las funciones de VLSM es descentralizar las redes y de esta forma conseguir redes más seguras y jerárquicas. El otro método con una máscara de subred de tamaño fijo, todas las subredes tienen el mismo tamaño, en el caso anterior la subred más grande necesita 48 hosts, y todas las demás subredes tiene el mismo tamaño de 64 direcciones IP.

En el siguiente cuadro se muestra el cálculo de direcciones con rangos de direcciones VLSM para subredes:

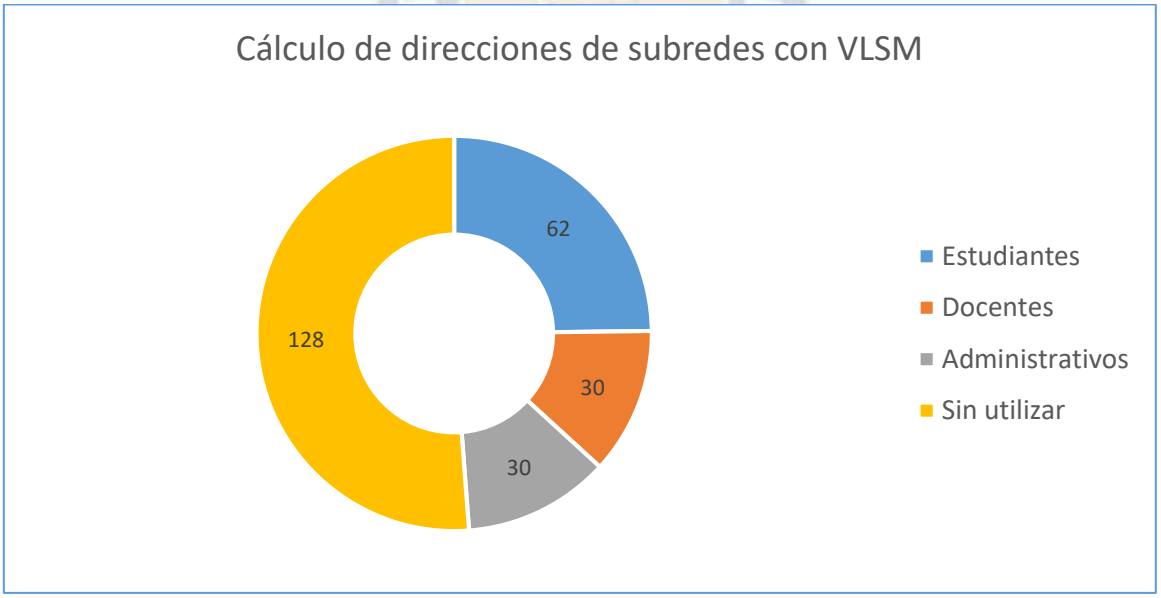


Figura 23: Cálculo de rango de direcciones con VLSM para subredes.
Fuente: Elaboración propia

Red	Dirección de subred	Rango de dirección de host min.	Rango de dirección de host máx.	Dirección de broadcast.
Estudiantes	192.168.1.0/26	192.168.1.1	192.168.1.62	192.168.1.63
Docentes	192.168.1.64/27	192.168.1.65	192.168.1.94	192.168.1.95
Administrativos	192.168.1.96/27	192.168.1.97	192.168.1.126	192.168.1.127

Tabla 10: Rangos de direcciones con VLSM por categoría.
Fuente: Elaboración propia.

Red de área local virtual

Una Red de área local virtual (VLAN, Virtual Local Area Network) es un método para crear redes lógicas independientes dentro de una misma red física. Las VLAN pueden coexistir en un conmutador físico, son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local, en el IEA se separan en las de Estudiantes, Docentes y Administrativos, que no deberían intercambiar datos usando la red local, aunque pueden hacerlo a través de un enrutador.

Como se mostró anteriormente en el cálculo de direcciones con VLSM es más eficiente y desperdicia menos direcciones de red, se utilizarán los rangos de red calculados con el método de VLSM para el diseño de las VLAN del IEA, segmentando las redes con su respectivo ID, está segmentada mediante tres VLAN, Estudiantes, Docentes y Administrativos.

Los segmentos lógicos a separar están dados por la siguiente tabla:

Segmento de red	VLAN
Estudiantes	10
Docentes	20
Administrativos	30

Tabla 11: Asignación de VLAN por segmento de Red.
Fuente: Elaboración propia.

Se debe crear las VLAN asignando un numero de ID válido, los cuales se encuentran en la tabla anterior, posterior a su creación el siguiente paso es asignar puertos a la VLAN.

Enlace Troncal de la VLAN

Un enlace trocal de VLAN es un enlace de capa 2 del modelo OSI entre switches que transporta el tráfico para todas las VLAN.

Para configurar un puerto de switch se debe configurar los comandos en el switch en su respectivo puerto que será la interfaz en modo troncal. La encapsulación de la configuración de los enlaces troncales es la 802.1Q, si la configuración del enlace troncal no tiene la misma encapsulación en los extremos, se registran errores y no se podrá enviar el tráfico de las VLAN mediante el enlace.

3.4.3 Protocolos de conmutación y enrutamiento

VLAN Trunking Protocol (VTP)

El instituto de electrónica aplicada la red será segmentada en las diferentes VLANs descritas, por lo tanto, el VTP (Protocolo troncal de VLAN), es un protocolo de nivel 2 usado para configurar y administrar VLANs. Permite centralizar y simplificar la administración en un domino de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos. El protocolo VTP en el IEA permite gestionar la red cuando de manera manual es inabordable y también facilita la administración en redes pequeñas como es el caso del IEA.

IEEE 802.1Q

El protocolo IEEE 802.1Q, también conocido como dot1Q, es un mecanismo que permite a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking). Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en la red del IEA.

Todos los dispositivos de interconexión que soportan VLAN deben seguir la norma IEEE 802.1Q que especifica con detalle el funcionamiento y administración de redes virtuales.

DHCP

DHCP (Dynamic Host Configuration Protocol) en español protocolo de configuración dinámica de host, es un servidor que usa protocolo de red de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. Así los clientes de una red IP pueden conseguir sus parámetros de configuración automáticamente.

Las computadoras y los usuarios del IEA, a menudo, cambian de ubicación, física y lógica. Para los administradores de red, asignar direcciones IP nuevas cada vez que un empleado cambia de ubicación puede ser difícil y llevar mucho tiempo. Incluso para los usuarios de escritorio, la asignación manual de direcciones IP y otra información de direccionamiento plantea una carga administrativa, especialmente a medida que crece la red.

3.4.4 Estrategias de Seguridad

Firewall

Un firewall o en español cortafuegos es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Un firewall es un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Un firewall puede ser hardware, software o ambos.

ACL

Una lista de control de acceso o ACL (Access Control List) se refiere a una lista de reglas que detallan puertos de servicio o nombres de dominios (de redes) que están disponibles en una terminal u otro dispositivo de capa de red, cada uno de ellos con

una lista de terminales y/o redes que tienen permiso para usar el servicio. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

3.5 Diseño físico de la red

El diseño físico de la red se realizó en base a los planos del IEA, donde se muestra la ubicación de cada nodo y el cableado estructurado desde las casetas de telecomunicaciones de cada nivel a los puntos de conexión.

El diseño de la infraestructura del sistema de cableado estructurado de la red, se fundamenta en la norma ISO (International Organization for Standardization) la que encargo al grupo de trabajo ISO/IEC/SC25/WG3 realizar las normas internacionales basándose en TIA/EIA – 568. Específicamente, el estándar TIA/EIA-568-B que sustituye al conjunto de estándares TIA/EIA-568-A que han quedado obsoletos.

3.5.1 Mapa físico de la red

El mapa físico de la red está representado por dos planos uno por cada nivel del IEA, es decir: un plano de la planta baja y el otro de la planta del primer piso.

Cada plano muestra la ubicación física de los elementos involucrados en la red, en cada uno se puede apreciar las siguientes características:

- Ubicación física de los nodos en los diferentes ambientes del IEA.
- Casetas de telecomunicaciones (distribución del cableado horizontal).
- Trazado del cableado (construcción de las rutas y ubicaciones del cableado).
- Identificación de los símbolos utilizados en la representación física de la red.

Los planos y los puntos descritos se encuentran en el **ANEXO 2.**

3.5.2 Selección de dispositivos de la red.

Los dispositivos de red son los que transportan los datos que deben transferirse entre dispositivos de usuario final. Los dispositivos de red proporcionan el tendido de las conexiones de cable, la concentración de conexiones, la conversión de los formatos de datos y la administración de transferencia de datos. En el IEA se requieren de dos tipos de dispositivos de red un Router y Switches.

El Router debe contar con las siguientes características:

Puertos y servicios	
Puertos RJ-45 Gigabit Ethernet 10/100/1000	2
Firewall	Si
DHCP	Si
Access list	Si
Encapsulación dot1Q	Si
IPv4, IPv6	Si

Tabla 12: Características que debe tener el Router.
Fuente: Elaboración propia.

Los Switches deben contar con las siguientes características:

Puertos y servicios	
Puertos RJ-45 Gigabit Ethernet 10/100/1000	24
VLAN	Si
VTP	Si
Telnet	Si
Encapsulación dot1Q	Si
IPv4, IPv6	Si

Tabla 13: Características que deben tener los Switches.
Fuente: Elaboración propia.

3.5.2.1 Selección de Router.

Se hizo la selección del router comparando 3 marcas, las especificaciones técnicas de los equipos comparados se encuentran en el **ANEXO 3**.

El Router es el: Cisco 1941 Integrated Services Router.

Se requiere un Router.

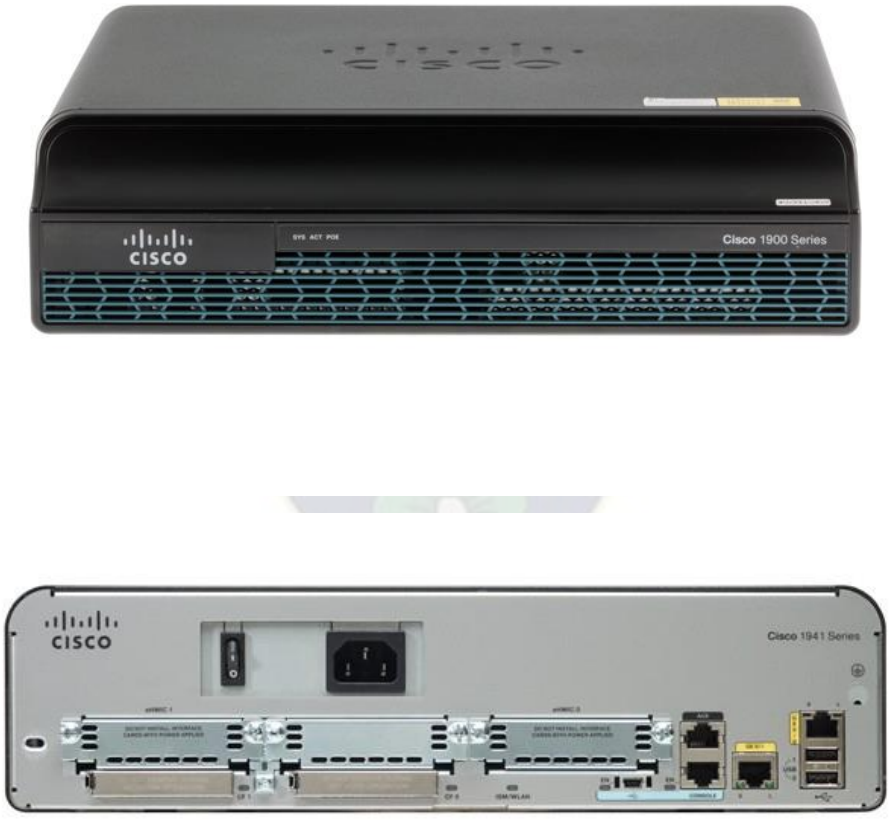


Figura 24: Router Cisco 1941.
Fuente: http://www.cisco.com/ (28/10/16).

3.5.2.2 Selección de Switch.

Se hizo la selección del switch comparando 3 marcas, las especificaciones técnicas de los equipos comparados se encuentran en el **ANEXO 3**.

El Switch es el: Cisco Catalyst 3650-24TS-S Switch.

Se requieren cuatro Switches.

Figura 25: Cisco Catalyst 3650-24TS.
Fuente: http://www.cisco.com/ (28/10/16).

CAPÍTULO 4

4.1 Pruebas y simulación.

Cisco Packet Tracer es un software propiedad de Cisco System Inc., diseñado para la simulación de redes basada en los equipos de la marca. Es la principal herramienta de trabajo para pruebas y simulación. Se usa la versión 2016 de Cisco Packet Tracer. El simulador no cuenta con todos los dispositivos de la marca, por lo tanto, se tiene dispositivos standard con el cual se cubren todas las necesidades para realizar la simulación de la red del IEA, en el CAPÍTULO 3 se seleccionó los dispositivos reales y sus especificaciones técnicas se encuentran en el **ANEXO 3**.

4.2 Pruebas.

Se realiza las pruebas de cómo funciona un switch cuando se envía tráfico de broadcast en los siguientes casos:

- Switch configuración por defecto.
- Switch configurado con VLANs

De esta manera se observa la eficiencia de las VLANs al reducir el dominio de difusión.

4.2.1 Switch configuración por defecto.

En esta prueba se tiene 5 PCs conectadas a un Switch, se asigna las direcciones IP a las PCs. La PC0 a la PC2 pertenecen a la misma subred y desde la PC3 a la PC4 a otra subred.

Direcciones IP:

PC0 a PC2: de 192.168.1.2 a 192.168.1.4 con máscara de 255.255.255.0

PC3 a PC4: de 192.168.2.2 a 192.168.2.4 con máscara de 255.255.255.0

Todos los puertos del switch pertenecen a la VLAN 1 (VLAN por defecto), y no se realiza ninguna configuración sobre el switch.

Se crea un PDU (Protocol Data Unit) de broadcast el cual se visualiza en el modo de simulación de Cisco Packet Tracer para ver su propagación por la red.

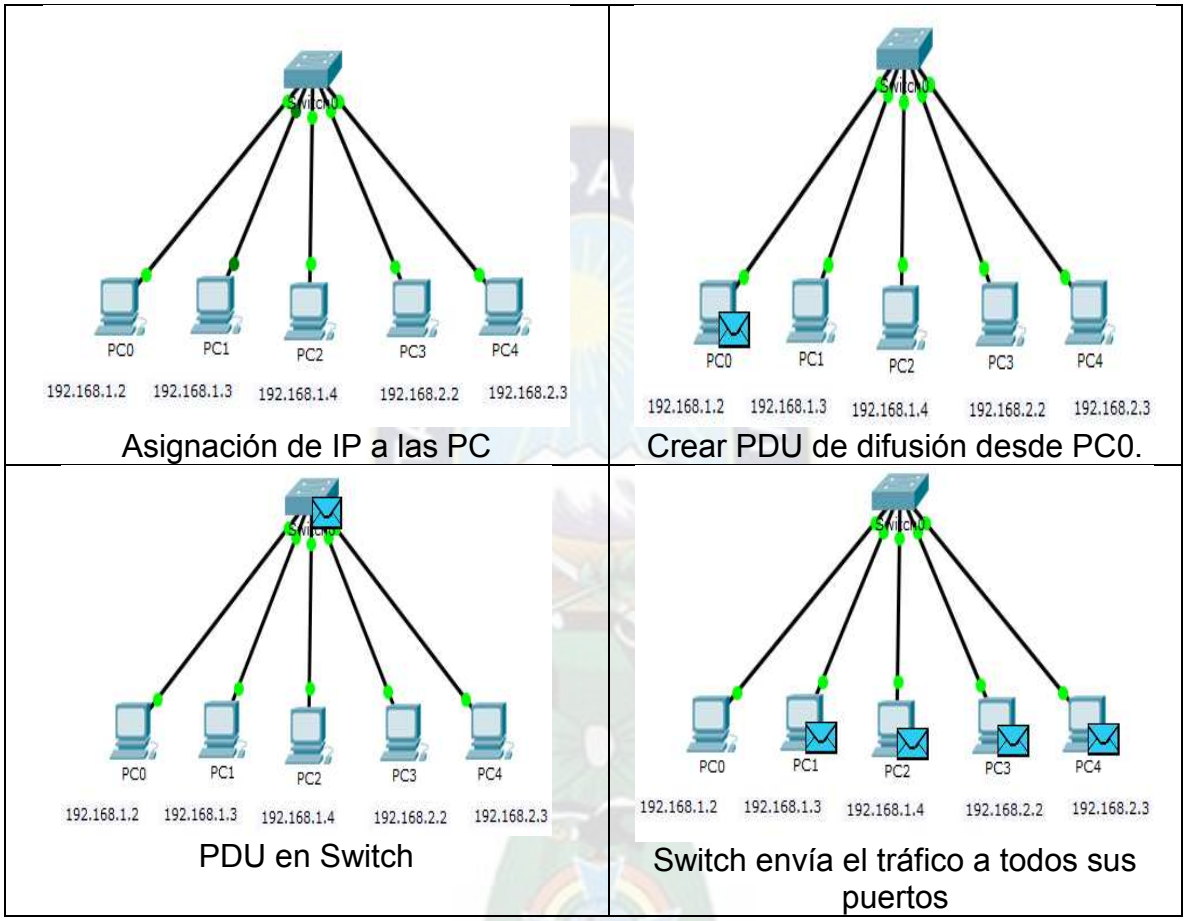


Figura 26: Prueba Switch por defecto.
Fuente: Elaboración propia.

Como se aprecia en la simulación el dominio de broadcast es único y envía el tráfico hacia todas las terminales reduciendo la eficiencia y saturando la red.

4.2.2 Switch configurado con VLANs.

De similar manera que en la prueba anterior se asigna las mismas direcciones IP, pero en este caso se configura dos VLANs, una para cada subred:

También se crea el PDU para el tráfico de broadcast y lo enviamos desde la PC0 y se observa el comportamiento del tráfico en la simulación.

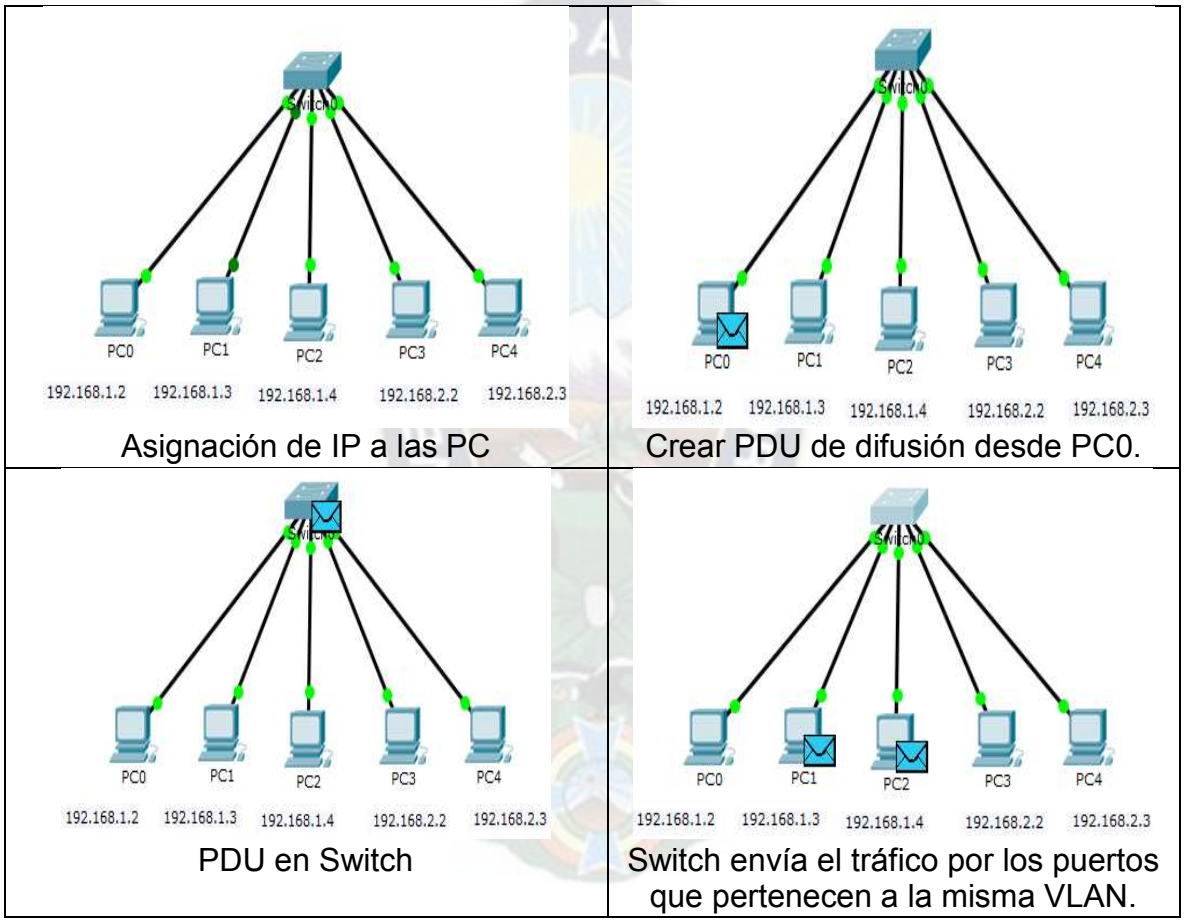


Figura 27: Prueba Switch con VLAN.
Fuente: Elaboración propia.

Como se puede apreciar el dominio de broadcast de dividió en dos, una por cada VLAN creada. Se redujo el tamaño del dominio de difusión y la red es más fácil de administrar. PC0 a PC2 pertenecen a la VLAN 10 y PC3 a PC4 pertenecen a la VLAN 20. La configuración del switch de esta prueba se encuentra en el **ANEXO 4**.

4.3 Simulación de la Red.

En el Instituto de Electrónica Aplicada existen dos pisos planta baja y primer piso, por lo tanto, se distribuyen las diferentes VLANs a lo largo de todos los ambientes que lo requieran. Se usa el protocolo VTP para distribuir y administrar las VLANs, reduciendo la necesidad de configurar las VLAN en cada uno de los dispositivos y reduciendo errores de configuración.

Además, se configura los servicios de DHCP y listas de acceso para asignar direcciones IP de manera dinámica y bloquear el acceso no autorizado respectivamente.

Mediante el análisis y el dimensionamiento se requieren de cuatro Switches y un Router para cubrir los nodos del IEA. La configuración de los dispositivos seguirá los siguientes puntos:

Configuración Switches

- Configurar switch servidor VTP.
- Configurar el resto de los switches en modo cliente.
- Asignación de puertos a las VLANs y a los enlaces troncales.
- Configurar contraseñas en los switches.
- Crear anuncio de alerta.
- Configurar Telnet (Acceso Remoto).

Configuración Router

- Configurar el servicio de DHCP.
- Creación de sub-interfaces para cada VLAN.
- Configurar listas de acceso.
- Configurar Firewall.
- Configurar contraseña.
- Crear anuncio de alerta.

4.4 Configuración switches.

4.4.1 Configuración switch servidor VTP.

Crear cuatro switches en Cisco Packet Tracer, seleccionar a uno que será el servidor de VTP en este caso el SW1IEA y se configura.

Los comandos de configuración del Switch se encuentran en **ANEXO 4**.

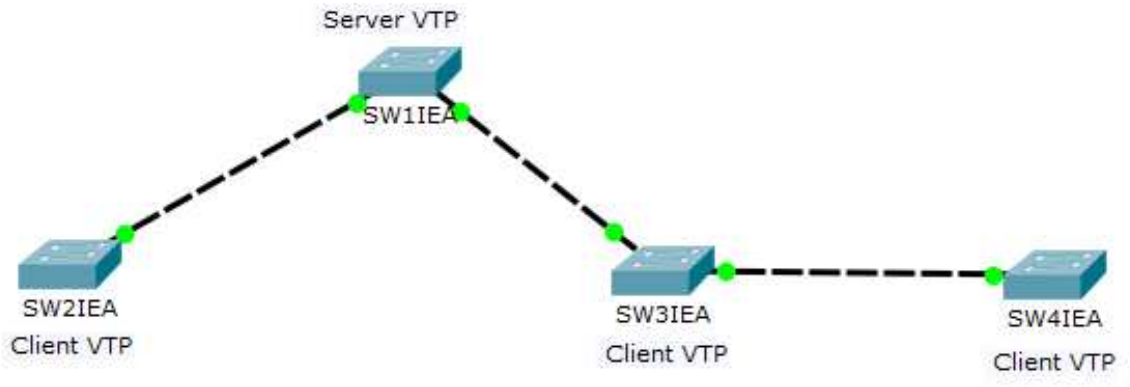


Figura 28: Switches Server y Client VTP.
Fuente: Elaboración propia.

4.4.2 Configuración switches Cliente VTP.

Los switches SW2IEA, SW3IEA y SW4IEA se configuran en modo cliente, como se ve en la **Figura 28**, todos los enlaces son troncales entre los switches y la configuración de los switches se encuentran en **ANEXO 4**.

4.4.3 Asignación de puertos.

Los puertos tipo troncal o trunk, se utilizan para realizar conexiones entre switches y entre switches y routers, un puerto trunk puede transportar tráfico de múltiples VLANs por un solo enlace físico.

Los puertos tipo acceso, se utilizan para conectar dispositivos finales, los puertos de acceso solo transportan tráfico de una VLAN.

Puertos modo troncal

Switch	Puertos
SW1IEA	G0/1, G0/2, F0/1
SW2IEA	G0/1
SW3IEA	G0/1, G0/2
SW4IEA	G0/2

Tabla 14: Puertos Troncales de los switches.
Fuente: Elaboración propia.

Puertos modo acceso

VLAN	SW1IEA	SW2IEA	SW3IEA	SW4IEA
10 Estudiantes	----	Fa0/1 a Fa0/17	Fa0/1 a Fa0/22	----
20 Docentes	Fa0/2 a Fa0/10	----	----	Fa0/1 a Fa0/8
30 Administrativos	Fa0/11 a Fa0/18	----	----	Fa0/9 a Fa0/17
99 Telnet	Fa0/24	Fa0/24	Fa0/24	Fa0/24
Puertos disponibles	Fa0/19 a Fa0/23	Fa0/18 a Fa0/23	Fa0/23	Fa0/18 a Fa0/23

Tabla 15: Puertos de acceso de los switches.
Fuente: Elaboración propia.

La configuración de los puertos se encuentra en el **ANEXO 4**.

Se incluye una PC por cada VLAN de cada switch, según la **Tabla 15**. Se les asigna la dirección IP estática correspondiente y se simula un ping entre ordenadores.

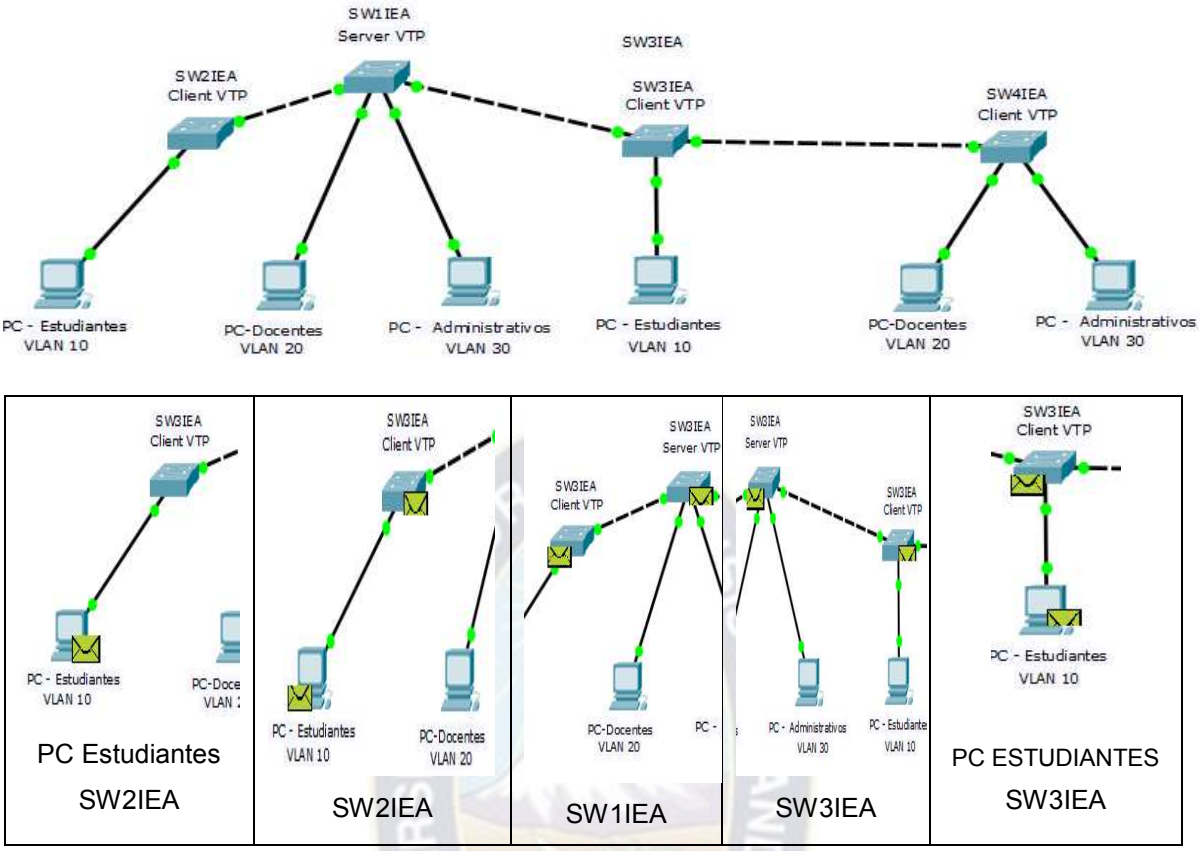
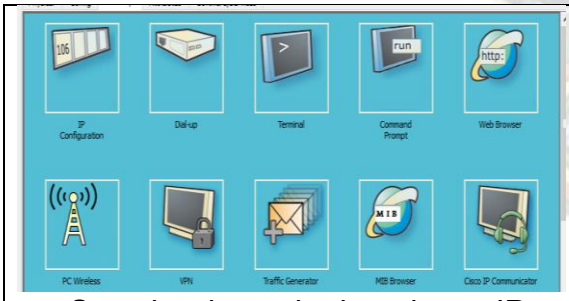
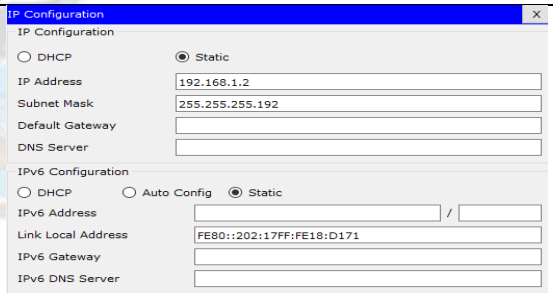


Figura 29: Ping PC estudiante SW2IEA a PC estudiante SW3IEA.
Fuente: Elaboración propia.

La dirección IP estática en la PC se asigna de la siguiente manera. Clic izquierdo en la PC y seguir los pasos de la **Figura 30.**



Se selecciona el primer icono IP Configuration.



Seleccionar Static e introducir la Dirección y la Máscara.

Figura 30: Asignación de dirección IP estática a las PCs.
Fuente: Elaboración propia.

4.4.4 Seguridad de acceso.

Para tener acceso a la configuración del switch, se configura contraseñas para ingresar al modo privilegiado, contraseña de consola y la contraseña vty que permite el acceso remoto por telnet. La configuración se encuentra en el **ANEXO 4**.

4.4.5 Banner de advertencia.

Se incluye un banner (anuncio) de alerta al momento de entrar al CLI (Command Line Interface) de los switches. La configuración se encuentra en el **ANEXO 4**.
El mensaje es el siguiente:

!!!!!!!!!ALERTA!!!!!!!!!

SOLO PERSONAL AUTORIZADO IEA

4.4.6 Telnet.

Para el acceso remoto se configura Telnet con vty, se crea la vlan 99 para el acceso por el puerto fa0/24 de cada switch, este se encuentra en una red diferente y por seguridad solo hay dos direcciones de host. La red que se creó para Telnet en cada switch es:

dirección de red 192.168.1X.0 con máscara 255.255.255.252 = /30

El switch tiene la primera dirección: 192.168.1X.1/30

La PC debe tener la segunda dirección: 192.168.1X.2/30

Donde X es el número de switch 1, 2, 3 o 4. La dirección asignada a la PC debe ser estática. La configuración se encuentra en el **ANEXO 4**.

4.5 Configuración Router.

Sin el router las VLANs no pueden comunicarse entre ellas, además se debe asignar de manera manual la dirección IP a cada una de las PC, lo que puede ocasionar errores, por ejemplo: asignar la misma dirección IP a más de una PC, asignar direcciones IP que no correspondan a la VLAN del puerto conectado o simplemente no saber qué dirección IP introducir en las PCs.

Lo más conveniente es tener un servidor DHCP que asigne de manera dinámica las direcciones IP, y el router seleccionado cumple con este protocolo y servicio.

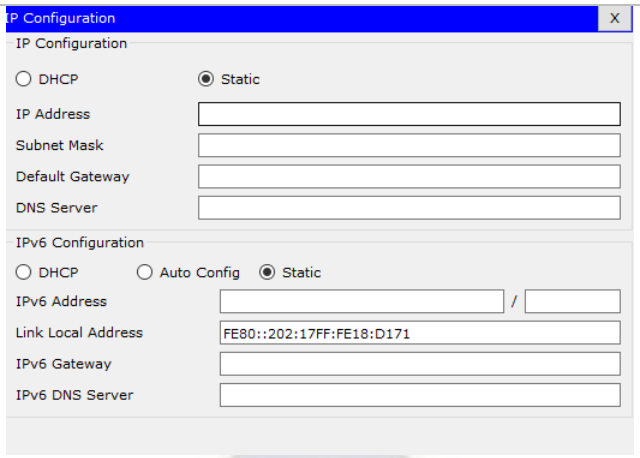
4.5.1 Configuración DHCP.

Para la configuración de protocolo DHCP se configura un pool de direcciones para cada una de las VLANs, para cada VLAN se asigna la red y la máscara, posteriormente se configura el Gateway por defecto, que es la primera dirección de cada una de nuestras subredes. La configuración se encuentra en el **ANEXO 5**.

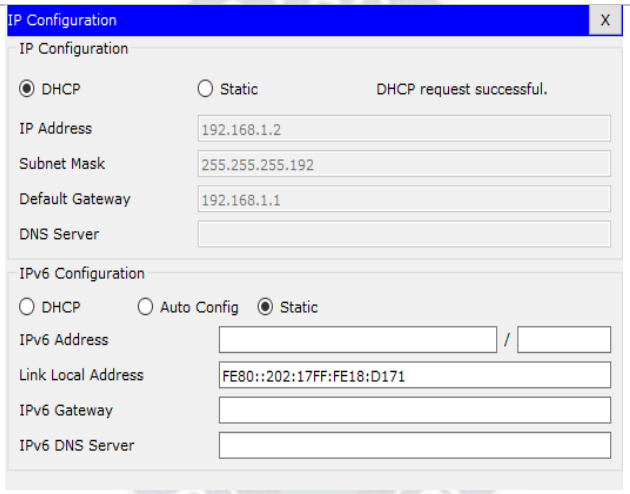
4.5.2 Configuración de sub-interfaces.

Mediante el protocolo de encapsulación IEEE802.1Q o dot1Q se crean sub interfaces, el primer paso es crear una sub-interfaz por cada VLAN, luego se incluye la encapsulación dot1Q seguido del ID de la VLAN y por ultimo debe ingresarse la IP del Gateway de cada VLAN. Después se levanta la interfaz física para que todas las sub-interfaces también se levanten (cambien de estado a up). La configuración se encuentra en el **ANEXO 5**.

El protocolo DHCP es uno de los más importantes en una red ya que los usuarios no permanecerán siempre en un mismo ambiente, les permite conectarse a la red sin sufrir conflictos de direcciones IP y usar diferentes máquinas de manera inmediata. Además, que el asignar direcciones IP de manera estática es muy moroso y le quita eficiencia a la red.



Dirección Estática vacía.



DHCP solicitud de dirección exitosa.

Figura 31: Asignación de dirección por DHCP.
Fuente: Elaboración propia.

4.5.3 Configuración de Access Control List (ACL).

Mediante la configuración realizada todas las VLANs pueden comunicarse entre ellas, lo ideal es que los Estudiantes no se comuniquen con la VLAN de Administrativos. Para eso es necesario crear una lista de control de acceso (ACL) que bloquee el tráfico entre los Estudiantes y los Administrativos, se realiza creando una lista de acceso denegando la IP de red y su Wildcard, se ingresa a la sub-interfaz de la VLAN de estudiantes y se configura el grupo de acceso. En la simulación se ve el antes y después del ACL. La configuración e imágenes de la simulación se encuentra en el **ANEXO 5**.

4.5.4 Configuración de Firewall.

El Firewall (cortafuegos) es una parte de la red que bloquea el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. En la simulación se configura un Firewall para negar el acceso del protocolo ICMP al servidor y permitiendo el acceso solo por HTTP. Por lo tanto, se crea el servidor que simulará el acceso a internet y tendrá una dirección IP de 192.168.100.10. La configuración e imágenes de la simulación se encuentra en el **ANEXO 5**.

4.5.5 Seguridad de acceso.

Para tener acceso a la configuración del router, se configura contraseñas para ingresar al modo privilegiado y contraseña de consola. La configuración se encuentra en el **ANEXO 5**.

4.5.6 Banner de advertencia.

Se incluye un banner (anuncio) de alerta al momento de entrar al CLI (Command Line Interface) del router. La configuración se encuentra en el **ANEXO 5**. El mensaje es el siguiente:

!!!!!!!!!ALERTA!!!!!!!!!

SOLO PERSONAL AUTORIZADO IEA

4.6 Guardar la configuración.

Las configuraciones actuales del router y switches son almacenadas en la memoria RAM, este tipo de memoria pierde el contenido al apagarse el equipo. Para que esto no ocurra es necesario hacer una copia a la NVRAM. El comando: copy running-config startup-config. Copia la configuración de la RAM a la NVRAM. Los datos de configuración almacenados en la memoria no volátil no son afectados por la falta de alimentación. La configuración se encuentra en el **ANEXO 5**.

4.7 Diagrama de topología.

La siguiente figura muestra la topología de red del Instituto de Electrónica Aplicada, el cuadro izquierdo representa los equipos dispuestos en la Planta Baja, y el cuadro derecho los equipos del Primer Piso. Se identifica cada VLAN con un recuadro de color, verde para VLAN de Estudiantes, naranja para VLAN de Docentes y amarillo para VLAN de Administrativos. Existe una VLAN 99 para acceso Telnet la cual no se representa en la figura, esta VLAN solo tiene un puerto de acceso en cada uno de los switches, por el puerto 24.

Se identifica en cada recuadro de color la cantidad de PCs que tiene cada VLAN en cada piso del IEA.

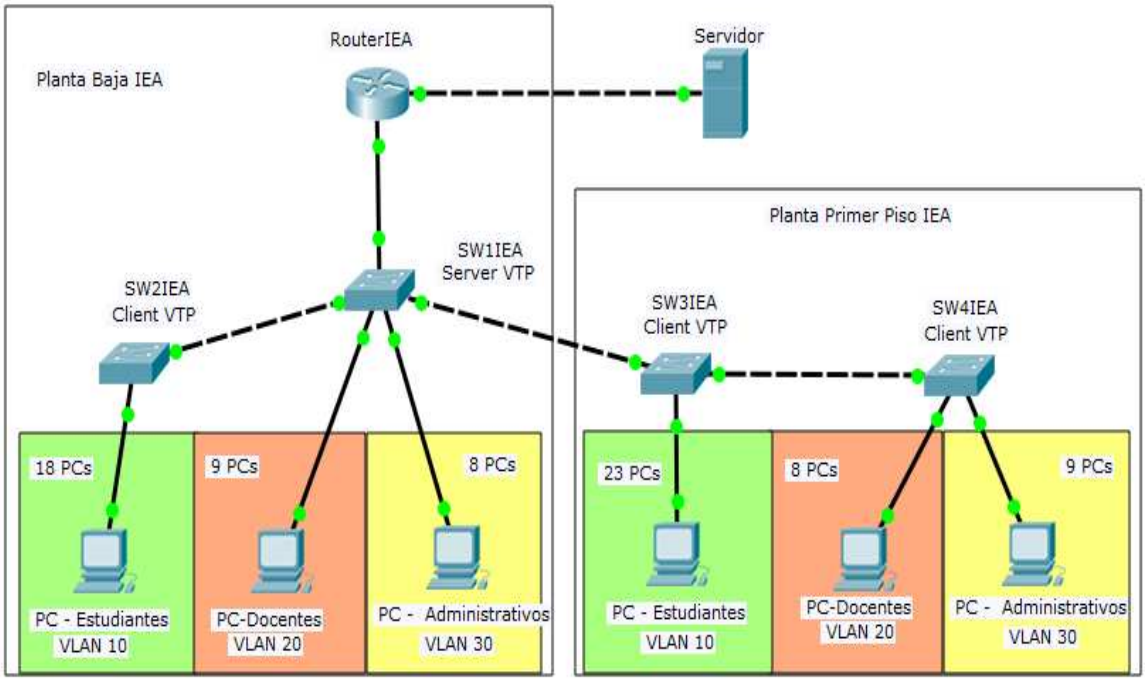


Figura 32: Diagrama de la topología de red del IEA.
Fuente: Elaboración propia.

CAPÍTULO 5

5.1 Conclusiones y recomendaciones

Las conclusiones y recomendaciones del presente proyecto de grado se encuentran sustentadas por el estudio teórico, las pruebas, simulaciones y por los estudios de campo que se realizaron.

5.2 Conclusiones

Para lograr investigar y analizar las necesidades de comunicaciones del Instituto de Electrónica Aplicada, se empleó la estrategia de encuestas a los estudiantes y docentes, como una entrevista con el Director del IEA. Se analizó los datos obtenidos y se determinaron los requisitos que debe cumplir la red.

A partir de planos arquitectónicos y visitas en sitio de los ambientes del IEA se revisó la propuesta arquitectónica, la cantidad de nodos que requiere cada ambiente, la ubicación de las casetas de telecomunicaciones (cuarto de telecomunicaciones) en donde se alojarán los dispositivos y los canales de distribución del cableado estructurado. Con la información recopilada se diseñó y modificó los planos para presentar la propuesta de este documento. Además, se presenta los planos realizados en AutoCAD del diseño de red en formato digital.

Mediante el análisis de los requerimientos se dimensiona las diferentes variables necesarias para la red de datos: la cantidad de puertos, las direcciones IP, la cantidad de VLANs, la velocidad y tipos de interfaces, el tipo de conectores, la topología de red, entre otros. Todos para un correcto y eficiente funcionamiento de la red de datos.

Al ser una red de topología jerárquica, permite la planificación de cada capa y estas están enfocadas a funciones específicas. La naturaleza modular permite un diseño simple y fácil de entender. Por lo tanto, la estabilidad para el crecimiento de la red se logra con los puertos disponibles en los dispositivos de acceso y es fácil de aumentar más de estos dispositivos en los armarios de comunicaciones. La red

proporciona una disponibilidad constante a los usuarios. El rendimiento es mejorado debido a la reducción de los dominios de colisión y dominios de difusión gracias al switch y las VLANs. Se implementan técnicas de seguridad mediante listas de acceso, configuración de firewall y contraseñas en los dispositivos para que solo personal autorizado acceda a ellos.

El cableado de la red se caracterizó por su velocidad y distancia para cubrir los requerimientos actuales y futuros, ya que al menos debe cubrir dos migraciones de dispositivos para mejorar el rendimiento de la red. Los protocolos de enrutamiento, de conmutación, de servicios y encapsulación se basaron en los requerimientos de la red.

Las tecnologías relacionadas con el área local se analizaron por sus especificaciones técnicas y por los servicios que pueden proveer. Los estándares relacionados a las redes de área local están considerados dentro del proyecto y se siguen las recomendaciones para el diseño de la red.

Las soluciones tecnológicas que se analizaron como alternativas para la propuesta fue mediante una comparación de sus especificaciones técnicas y de servicios. La comparación se realizó con tres diferentes marcas y se seleccionó los dispositivos que cumplan con las necesidades y requerimientos identificados para el IEA.

El esquema de direccionamiento está basado en IPv4, se usó el método de VLSM asignando un bloque de direcciones adecuado para a la red. La asignación de las direcciones IP de los dispositivos se desarrolló cubriendo satisfactoriamente cada uno de los nodos del IEA del diseño propuesto.

El diseño propuesto se simuló mediante el software de Cisco Packet Tracer, es uno de los programas de simulador de redes más completo. En la simulación se configuro cada uno de los dispositivos: switches, router, PCs y servidor. En cada uno de ellos se introdujo la configuración correcta para el funcionamiento de la red de manera satisfactoria. Se hicieron pruebas en el simulador enviando paquetes PDU, pings, TCP y otros entre los dispositivos para verificar el funcionamiento con resultados exitosos en cada uno de los casos.

5.3 Recomendaciones

Instalar una herramienta de análisis de protocolos, que permita ver todo el tráfico que pasa a través de la red del IEA. Una herramienta puede ser el Wireshark.

Realizar un “Plan de Contingencias”, que contenga los procedimientos necesarios que se deben tomar cuando exista alguna falla en la red de datos del IEA.

Instalar un sistema de puesta a tierra para la protección de las personas que manipulan los diferentes equipos electrónicos y armarios de cableado, ante averías fortuitas que pueden provocar que las masas metálicas de los elementos anteriores queden bajo tensión. Para la protección de los equipos electrónicos activos ante descargas eléctricas provocadas por fenómenos atmosféricos y la protección de los equipos electrónicos y del propio cableado estructurado ante interferencias electromagnéticas.

El personal de mantenimiento y administración de la red, debe estar capacitado y certificado para cubrir las necesidades de la red, así podrá brindar un mejor soporte a la red y a los usuarios.

Asegurar que exista garantía de los dispositivos y elementos de red, que este contemplada por el fabricante y no solo por el distribuidor.

Dar mantenimiento de manera frecuente a los dispositivos y revisar el estado físico de los mismos cada cierto tiempo.

El Internet de las Cosas (IoT) se convertirá en un elemento vital para las organizaciones. Se puede evaluar cómo el IoT puede traer valor al lugar de trabajo. Ya sea a través de iluminación inteligente, servicios de geolocalización en sitio o sistemas interconectados de aire acondicionado, seguridad, gestión de recursos eléctricos, de agua y datos. El IEA podrá aprovechar los innumerables usos que tiene IoT originando una mayor consolidación de servicios.

La seguridad en redes evoluciona y se mueve hacia la nube. Nuevas oportunidades surgen gracias a los sistemas de auto aprendizaje (o machine learning). En el futuro

veremos modelos de seguridad en redes con capacidades enriquecidas para la resolución de problemas. Al ofrecer estas capacidades desde la nube y aprovechar las experiencias agregadas de un conjunto más amplio de redes, los procesos de diagnóstico y remediación serán mejores y más rápidos.

Crear una Red Privada Virtual (VPN, Virtual Private Network) entre el Instituto de Electrónica Aplicada que se encuentra en el 7mo piso de la Facultad de Ingeniería ubicado en la Av. Mariscal Santa Cruz frente al Obelisco y el de Cota Cota. Una conexión VPN lo que permite es crear una red local sin necesidad que sus integrantes estén físicamente conectados entre sí, sino a través de Internet. Se obtienen las ventajas de la red local con una mayor flexibilidad, pues la conexión es a través de Internet.

Crear contenido de multimedia: cursos, tutoriales, talleres, etc. Para los docentes, estudiantes y población en general, para ser transmitida por streaming, esto difundirá de manera más eficiente los avances que se desarrollen en el instituto y puede ser un generador de recursos económicos cobrando por la certificación a los usuarios.

El IEA puede convertirse en un Proveedor de Servicios de Internet (ISP, Internet Service Provider) siendo una entidad que ofrece acceso a Internet para vender (re-vender) a los demás institutos e infraestructuras en el Campus Universitario de la UMSA con proyecciones de expansión fuera del Campus.

El crear un Cluster de Servidores permite tener un buen rendimiento en cuanto al tráfico o uso de aplicaciones alojadas en los servidores, el Cluster es un grupo de múltiples ordenadores unidos mediante una red de alta velocidad, de tal forma que el conjunto es visto como un único ordenador mucho más potente.

BIBLIOGRAFÍA

Tanenbaum, Wetherall. (2012). Redes de computadoras. Pearson. Mexico

Bigelow, S. (2003). Localización de averías, reparación, mantenimiento y optimización de redes. McGraw-Hill. España.

CCNA V5.0. (2014). Cisco Systems, Inc. USA

CVD. (2014). Campus Wired LAN, Technology Desing Guide. Cisco Validated Designs. USA

Dave Evans. (2011). The Internet of Things How the Next Evolution of the Internet Is Changing Everything. IBSG. USA

Gallo, M. Y Hancock, W. (2002). Comunicación entre computadoras y tecnologías de redes. THOMSON. México.

Hallberg, B. (2003). Fundamentos de redes. McGraw-Hill. México.

Horak, R. (2000). Communications Systems & Networks. Prentice Hall. Boston.

Huidobro, J. M. (1992). Comunicaciones de empresa. Paraninfo. Madrid.

ICND1-2. (2013). Cisco Systems,Inc. USA

James D. McCabe (2007). Network Analysis, Architecture, and Design. Morgan Kaufmann. USA

José María Barceló Ordinas, Jordi Íñigo Griera, Ramón Martí Escalé, Enric Peig Olivé, Xavier Perramon Tornil. (2004). Software Libre Redes de computadoras. UOC. Barcelona.

Priscilla Oppenheiner (2011) Top-Down Network Design. Cisco Systems, Inc. USA.

Sheldom, T. (2000). Diseño de Sistemas de Teleproceso. Marcombo. Barcelona.

Willian Stallings. (2004), Comunicaciones y Redes de Computadoras. Pearson Prentice Hall. Madrid.

Glosario

Arquitectura de comunicaciones La estructura hardware y software que Implementan las funciones de comunicación.

Autenticación Proceso usado para verificar la integridad de los datos transmitidos, especialmente mensajes

Byte Grupo de 8 bits, con el que normalmente se opera como una entidad.

Capa Grupo de servicios, funciones y protocolos, completo desde un punto de vista conceptual, que constituye uno de entre un conjunto de grupos dispuestos jerárquicamente y que se extiende a través de todos los sistemas que conforman la arquitectura de la red.

Colisión Situación en la que dos paquetes se transmiten a través de un medio al mismo tiempo. Su interferencia hace a ambos ininteligibles.

Diafonía Fenómeno por el que una señal transmitida en un circuito o canal de un sistema de transmisión crea un efecto indeseado en otro circuito o canal.

Difusión Transmisión simultánea de datos a varias estaciones.

Enrutamiento Determinación del camino o ruta que atravesarán las unidades de datos (tramas, paquetes, mensajes, etc.) desde la fuente al destino.

Encapsulado Adición de información de control por una entidad de protocolo sobre datos obtenidos de un usuario del protocolo

Medio de transmisión Camino físico entre transmisores y receptores en un sistema de comunicación

Nodo Unión de red o punto de conexión. la notación de la Capa 2 para dispositivos de red conectados a un medio común

Paquete Grupo de bits que incluye datos e información adicional de control. Generalmente se refiere a una unidad de datos del protocolo de la capa de red (capa 3 de OSI).

Protocolo Internet Protocolo de interconexión de redes que proporciona servicios sin conexión a través de múltiples redes de conmutación de paquetes.

Protocolo Conjunto de reglas que gobiernan la operación de unidades funcionales para llevar a cabo la comunicación.

Red de área local Red de comunicación que proporciona interconexión entre varios dispositivos de comunicación de datos en un área pequeña.

ANEXO 1

Encuesta para el Instituto de Electrónica Aplicada Campus Cota Cota.

La siguiente encuesta fue realizada a 7 miembros del instituto de electrónica aplicada, entre estudiantes y docentes de investigación. Se colocará un número al lado de las opciones que representa la cantidad de personas que contestaron esa respuesta.

Lea atentamente cada pregunta y a continuación encierre su respuesta.

Parte I: Usuarios

1) _____ **¿Cuál es su nivel del uso de la red?**

   a. Baja **4**
   b. Media **3**
   c. Alta

2) _____ **¿Para que usa la red?**

   a. Transportar los datos.
   b. Compartir información y recursos
   c. Acceso a internet y otros servicios **5**
   d. Todas las anteriores **2**

3) _____ **¿Cuánto tiempo aproximadamente usa la red?**

   a. Menos de 1 hora
   b. Más de 1 hora menos de 5 horas **7**
   c. Más de 5 horas

Parte II: Importancia

1) _____ **¿Cuán importante es la red de datos para el instituto?**

   a. Nada importante
   b. Poco importante
   c. Importante **2**
   d. Muy importante **5**

2) _____ **¿Qué considera que es lo más importante de una red?(corregir)**

a. Transportar los datos.

b. Compartir información y recursos

c. Acceso a internet y otros servicios **5**

d. Todas las anteriores 2

4) _____ **¿Para la seguridad de la red, cuál considera necesaria?**

a. Restricción de páginas WEB **2**

b. Restricción a descargas **1**

c. Restricción de los recursos (Impresoras, fax y otros). **4**

d. todas las anteriores

5) ¿Tu acceso a la red es con un equipo personal?

a) Si **2**

b) No **5**

6) ¿Tu acceso a la red es de manera inalámbrica?

a) Si

b) No **7**

7) ¿Cuantos dispositivos usas con la red del IEA?

1 **7**

6) ¿Con que frecuencia estarás en el IEA?

2 veces por semana **5**

3-4 veces por semana **2**

Entrevista del Instituto de Electrónica Aplicada Campus Cota Cota.

Las siguientes preguntas fueron realizadas al Director del Instituto de Electrónica Aplicada, el Ing. Wilber Flores Bustillos. La entrevista se llevó a cabo en fecha de 29/06/16.

Parte I: Usuarios

1) ¿En qué horarios funcionará el instituto y que días?

   El instituto cumplirá con el horario continuo, desde las 8:00 hasta las 16:00 y los días serán de lunes a viernes.

2) ¿Sistemas de control de acceso al instituto están considerados? (Credenciales, biométricos otros)

   No, el instituto no cuenta con ningún tipo de sistema de control digital. Cuenta con una lista de control de firmas y asistencia manual.

3) ¿Quiénes usaran la red?

   Los usuarios serán los estudiantes, docentes y administrativos.

4) ¿Cuál será el nivel de uso de la red? (Videoconferencia, blogs, datos, video, etc.)

   La mayor carga será de datos, pero sería optimo contar con una red hábil para realizar videoconferencias y otros.

5) ¿Cuántos usuarios aproximadamente tendrá el instituto por cada ambiente?

   Un total de 20 personas en el instituto, y en la hora más cargada se llega a tener unos 12 usuarios de la red, los docentes y estudiantes no ocupan los ambientes todos los días ni en todo el horario.

Parte II: Importancia

1) ¿Que considera que es lo más importante de una red? (Transportar datos, compartir información y recursos, accesos a internet y otros servicios)

   La capacidad de ancho de banda, no estar restringidos en la última conexión para tener la capacidad de transmitir datos en la intranet, para realizar VoIP, videoconferencias, en realidad no estar restringidos a ninguna aplicación.

2) ¿La seguridad de la red, con restricción de páginas web y otros?

   Si la red debe tener una gestión para que los usuarios puedan comunicarse, el utilizar un firewall para restringir ciertos accesos y los estudiantes no deberían poder comunicarse con la red de los administrativos para no interferir con el trabajo.

3) ¿Considera necesario el uso de redes Wi-Fi y en que ambientes?

   Considero necesario el uso de redes inalámbricas y en todos los ambientes.

4) ¿El uso de cámaras IP para la seguridad?

   Si el instituto debería contar con un sistema de seguridad, pero debido a no ser considerado en el proyecto inicial y por el tema de presupuesto no es una realidad inmediata

5) ¿La comunicación por VoIP entre oficinas?

   Sí, es algo que se debe realizar. Además de tener comunicación con los diferentes ambientes y no solo en las oficinas sino también en laboratorios.

Parte III: Aspectos técnicos

1) ¿Cuál es la expectativa de crecimiento del IEA, tanto en equipos como en personal?

   Al contar con la nueva infraestructura se espera un crecimiento de cantidad de personal administrativos, de estudiantes y docentes, debido a que tendremos cinco laboratorios. Pero no se puede dar un porcentaje inicial de crecimiento y lo primero es equipar los laboratorios.

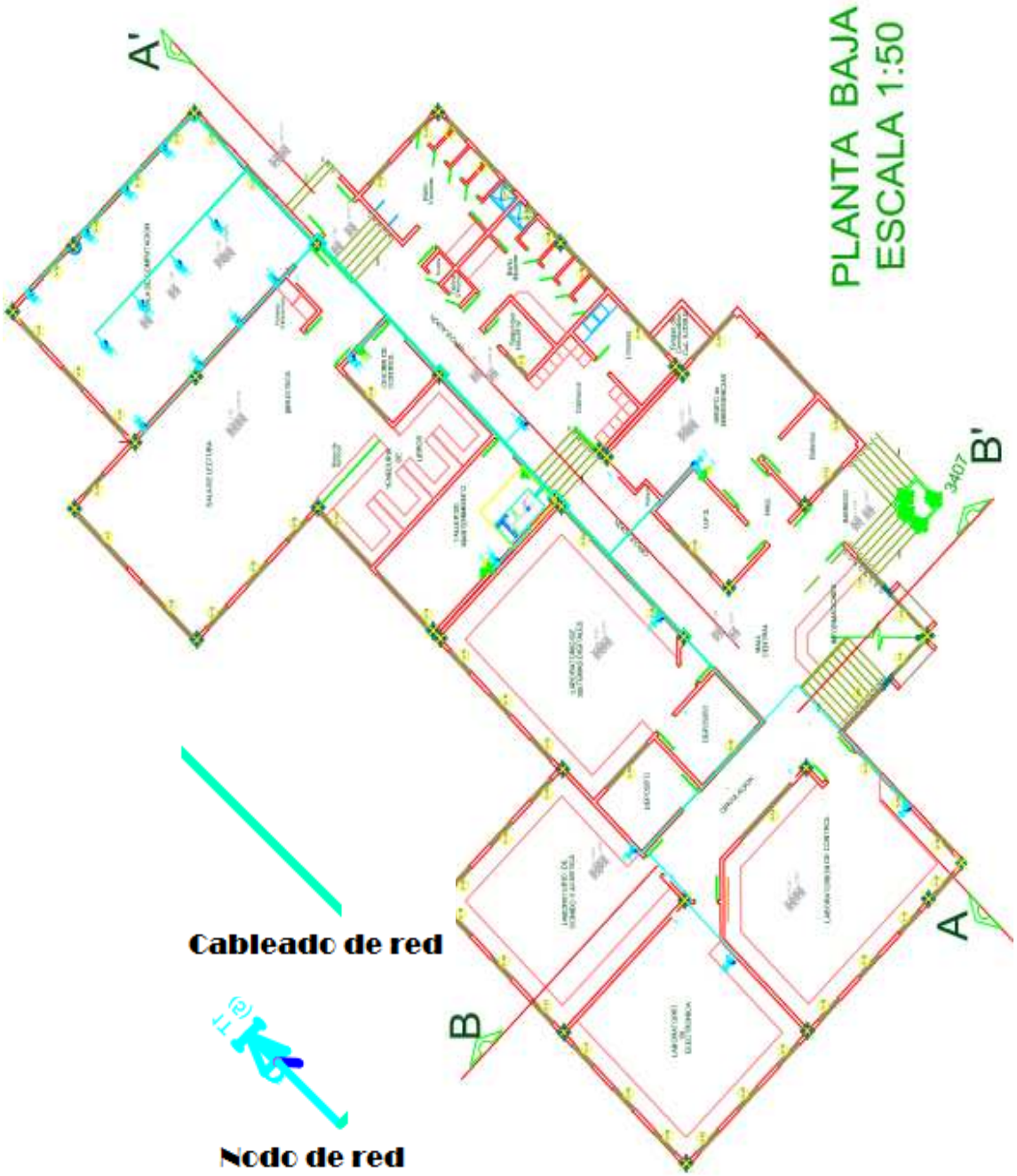
2) ¿Se consideró un laboratorio de redes para el IEA?

   No existe un laboratorio de redes como tal, pero existe un laboratorio de telecomunicaciones en los que se realizaran las actividades pertinentes a las redes, además que el IEA cuenta con una maestría de redes y se implementará

ANEXO 2

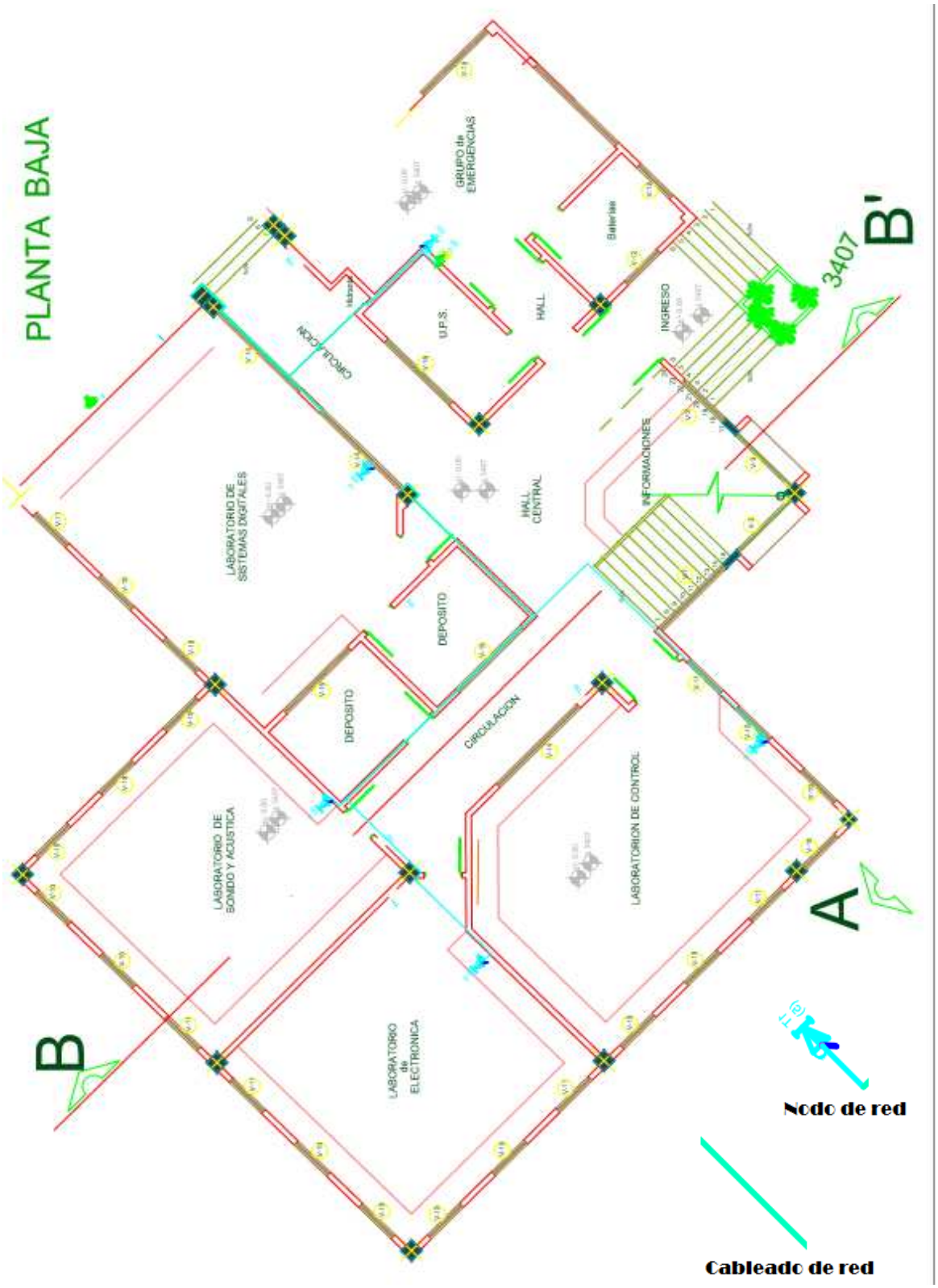
MAPA FISICO DE LA RED

PLANTA BAJA

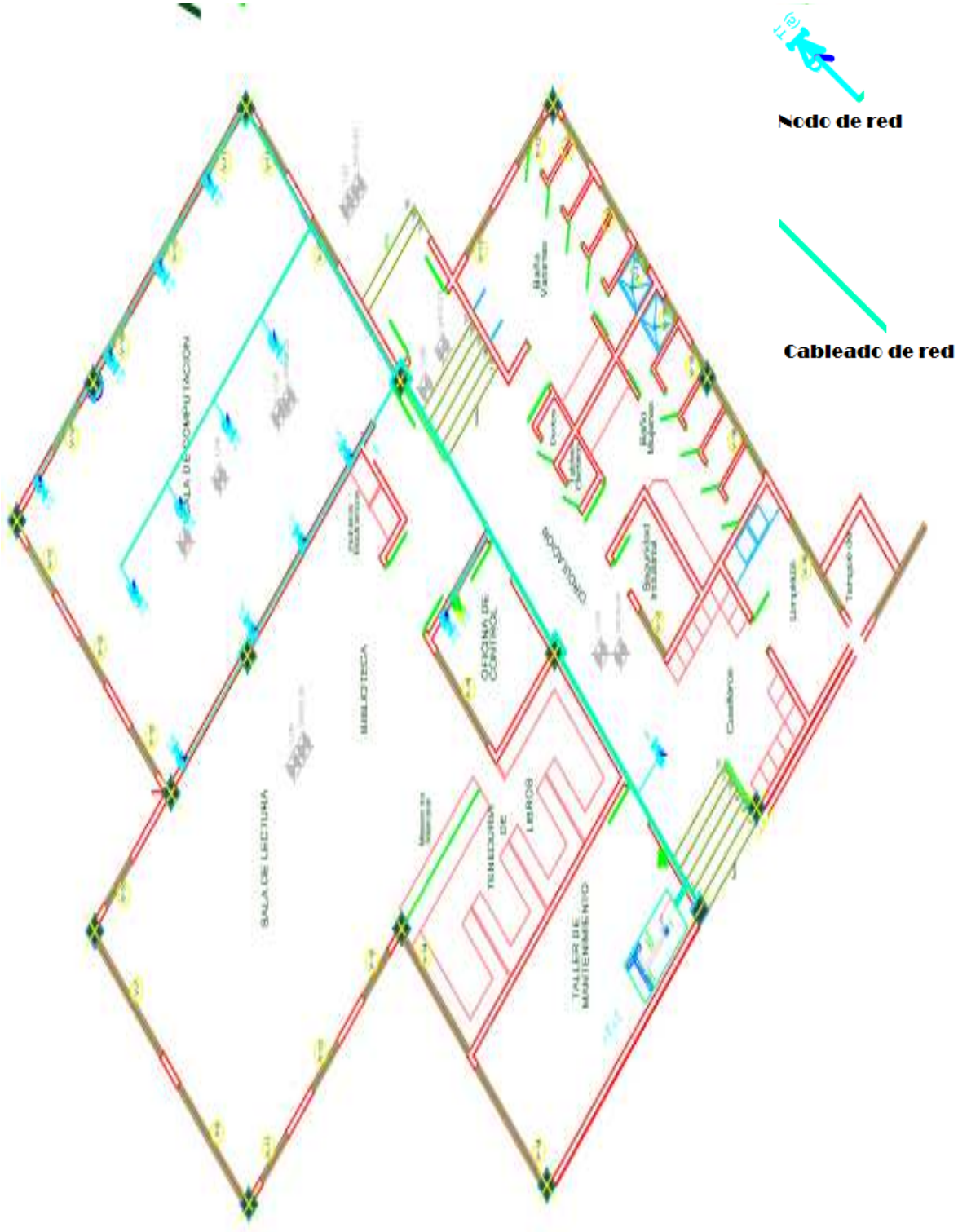


PRIMER PISO

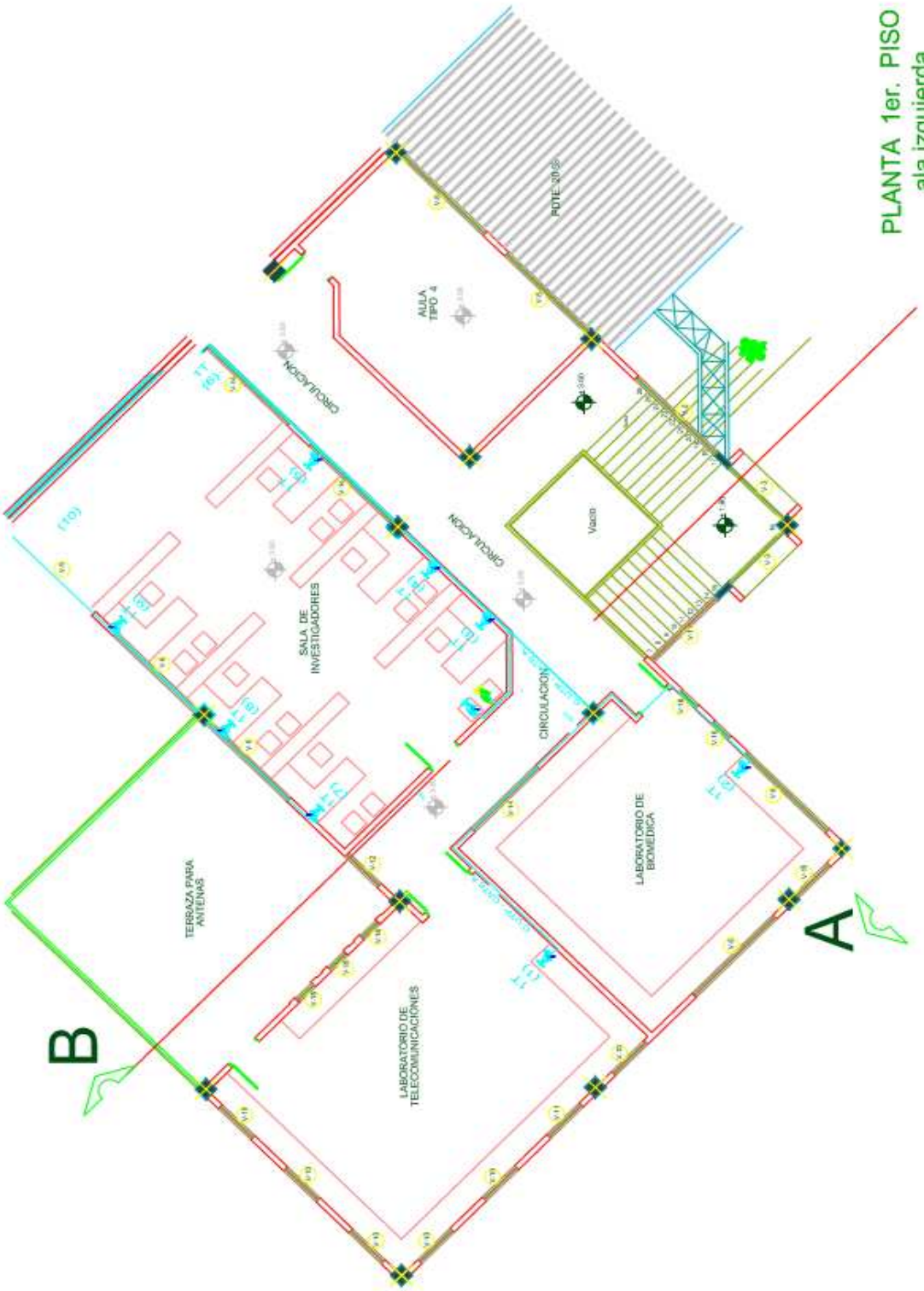
PLANTA BAJA ALA IZQUIERDA



PLANTA BAJA ALA DERECHA



PRIMER PISO ALA IZQUIERDA



PRIMER PISO ALA DERECHA

ANEXO 3

3.1 TP-LINK

Switch TP-LINK T2600G-28MPS

PoE+ Features Standard: 802.3at/af compliant PoE+ Ports: 24 Ports Power Supply: 384W L2 and L2+ Features Static routing L2PT Link Aggregation Control Protocol (LACP) STP/RSTP/MSTP IGMP Snooping Loopback Detection Quality of Service Support IEEE 802.1P 8 priority queues DSCP QoS Rate limit feature Security Strategies AAA Access Control List (IPv4/IPv6) IP-MAC-Port Binding ARP Inspection IP Source Guard 802.1x and RADIUS/TACACS+ Authentication Support DoS defend	IPv6 Support Dual IPv4/IPv6 Stack MLD Snooping PMTU Discovery IPv6 Neighbor Discovery IPv6 ACL DHCPv6 Snooping IPv6 Interface OAM 802.3ah Ethernet Link OAM Device Link Detect Protocol(DLDP) Management Web-based GUI Command Line Interface Telnet Dual Image DHCP Server DHCP Relay sFlow LLDP, LLDP-MED SNMP v1/v2c/v3 RMON (1,2,3,9 group)

Router TP- LINK TL-ER6120

- Hasta 100 túneles VPN IPsec, rendimiento VPN IPsec de 130 Mbps
- IPsec, PPTP, L2TP, L2TP sobre IPsec
- IPsec NAT Traversal (NAT-T)
- Encriptación DES, 3DES, AES128, AES192, AES256
- Autenticación MD5, SHA1
- Modo de gestión de claves manual e IKE
- VPN IPsec red a red, cliente a red
- Servidor/cliente VPN PPTP/L2TP
- Puerto DMZ basado en hardware
- NAT uno a uno
- ALG FTP/H.323/SIP/IPsec/PPTP
- Bloqueo de aplicaciones de mensajería instántanea y P2P
- Filtrado de URLs y palabras clave
- Filtrado de contenido web (Java, ActiveX, cookies)
- Inspección ARP
- Defensa contra ataques DoS/DDoS
- Balanceo inteligente de carga
- Política de enrutamiento
- Respaldo de enlace (tiempo de espera, recuperación de errores)
- Control de ancho de banda según la IP
- Ancho de banda garantizado y limitado
- Límite de sesión según la IP
- Puerto VLAN, puerto espejo
- Enrutamiento estático, RIP v1/v2
- Servidor PPPoE
- E-Bulletin

3.2 CISCO

SWITCH CISCO Catalyst 3650-24TS-S

Switch Capacity	
Type:	IPv4 routes
Value:	24000
Type:	NetFlow entries
Type:	Virtual interfaces (VLANs)
Value:	1000
Type:	Switched virtual interfaces (SVIs)
Dimensions & Weight	
Depth:	17.6 in
Height:	1.7 in
Weight:	15.15 lbs
Width:	17.5 in
Environmental Parameters	
Humidity Range Operating:	5 - 96% (non-condensing)
Max Operating Temperature:	113 °F
Max Storage Temperature:	158 °F
Min Operating Temperature:	23 °F
Min Storage Temperature:	-40 °F
Flash Memory	
Installed Size:	2 GB
Header	
Brand:	Cisco
Compatibility:	PC
Manufacturer:	Cisco Systems
Model:	3650-24TS-S
Packaged Quantity:	1
Product Line:	Cisco Catalyst
Interface Provided	
Connector Type:	RJ-45
Qty:	24
Type:	1000Base-T
Connector Type:	Type A

Rack Mounting Kit:	Included
Networking	
Advanced Switching:	Layer 3
Compliant Standards:	IEEE 802.1ab (LLDP) , IEEE 802.1D , IEEE 802.1p , IEEE 802.1Q , IEEE 802.1s , IEEE 802.1w , IEEE 802.1x , IEEE 802.3 , IEEE 802.3ab , IEEE 802.3ad (LACP) , IEEE 802.3u , IEEE 802.3x , IEEE 802.3z
Connectivity Technology:	Wired/Wireless
Features:	Access Control List (ACL) support , ARP support , DHCP snooping , Dynamic ARP Inspection (DAI) , EIGRP Stub Routing , Energy Efficient Ethernet , Flexible NetFlow (FNF) , IGMP snooping , Layer 2 support
Form Factor:	Desktop , Rack-mountable
Jumbo Frame Support:	9198 bytes
MAC Address Table Size:	32000 entries
Manageable:	Yes
Ports Qty:	24
Power Over Ethernet (PoE):	No
Remote Management Protocol:	CLI , RMON 1 , RMON 2 , RMON 3 , RMON 9 , SNMP 1 , SNMP 2c , SNMP 3 , SSH , Telnet
Routing Protocol:	OSPF , RIP-1 , RIP-2 , RIPng , Static IP routing
Stackable:	Stackable
Status Indicators:	Active , Port duplex mode , Port transmission speed , Status , System

Qty: 1 Type: USB Comments: Management Type: Serial (console) Type: Management (Gigabit LAN) Connector Type: Type B Type: Management (mini-USB) Comments: Uplink Connector Type: SFP Qty: 4 Type: 1000Base-X Miscellaneous Authentication Method: RADIUS , Secure Shell (SSH) , TACACS+ Color Category: Black Compliant Standards: BSMI CNS 13438 Class A , CISPR 22 Class A , CISPR 24 , CSA C22.2 No. 60950-1 Second Edition , EN 60950-1 Second Edition , EN 61000-3-2 , EN 61000-3-3 , EN55022 Class A , EN55024 , FCC Part 15 A , GOST , ICES-003 Class A , IEC 60950-1 Second Edition , ISO 7779 , KCC , KN22 Class A , KN24 , NOM , RoHS , UL 60950-1 Second Edition , VCCI Class A Height (Rack Units): 1 MTBF: 661,800 hours switching , Link Aggregation Control Protocol (LACP) , MLD snooping , Multiple Spanning Tree Protocol (MSTP) support , Port Aggregation Protocol (PAgP) support , Virtual Trunking Protocol (VTP), Quality of Service (QoS) , RADIUS support , Rapid Per-VLAN Spanning Tree Plus (PVRST+) , Rapid Spanning Tree Protocol (RSTP) support , Remote Switch Port Analyzer (RSPAN) , Trunking , Uni-Directional Link Detection (UDLD) , VLAN	Subcategory: Network hubs and switches Subtype: Gigabit Ethernet Type: Switch Performance Type: Switching capacity Value: 88 Gbps Type: Forwarding performance Value: 65.47 Mpps Ports Qty: 24 Type: 10/100/1000 Ports (2nd) Qty: 4 Type: SFP (mini-GBIC) Power Device Frequency Required: 50/60 Hz Hot-Plug: Hot-plug Installed Qty: 1 Max Supported Qty: 2 Nominal Voltage: AC 120/230 V Power Provided: 250 Watt Power Redundancy: Optional Power Redundancy Scheme: 1+1 (with optional power supply) Type: Internal power supply RAM Installed Size: 4 GB Service Support Details Full Contract Period: Lifetime Support Details Service Included: Replacement Support Details Type: Limited warranty Support Details Full Contract Period: 90 days Support Details Service Included: Phone consulting Support Details Type: Technical support Service & Support Type: Limited lifetime warranty Service & Support Details Response Time: Next business day Slot Provided Free Qty: 1 Total Qty: 1 Type: Stacking Module slot

ROUTER Cisco 1941 Integrated Services Router

Tipo de dispositivo Router Tipo incluido Sobremesa, montaje en rack - modular - 2U Tecnología de conectividad Cableado Protocolo de interconexión de datos Ethernet, Fast Ethernet, Gigabit Ethernet Red / Protocolo de transporte IPSec, PPPoE, L2TPv3 Protocolo de direccionamiento OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, enrutamiento IPv4 estático, enrutamiento IPv6 estático, enrutamiento basado en reglas (PBR), MPLS, Bidirectional Forwarding Detection (BFD),DHCP, IPv4-to-IPv6 Multicast Protocolo de gestión remota SNMP, RMON Algoritmo de cifrado SSL Características Protección firewall, asistencia técnica VPN, soporte de MPLS, soporte para Syslog, filtrado de contenido, soporte IPv6, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Dynamic Multipoint VPN (DMVPN), Web Services Management Agent (WSMA), NetFlow Cumplimiento de normas IEEE 802.3, IEEE 802.1Q, IEEE 802.3af, IEEE 802.3ah, IEEE 802.1ah, IEEE 802.1ag, ANSI T1.101, ITU-T G.823, ITU-T G.824 , CISPR 22 clase A, CISPR 24, EN55024, EN55022 clase A, EN50082-1, AS/NZS 60950-1, ICES-003 clase A, CS-03,	limitada - 1 año Parámetros de entorno Temperatura mínima de funcionamiento 0 °C Temperatura máxima de funcionamiento 40 °C Ámbito de humedad de funcionamiento 10 - 85% USB 2 x External USB flash memory slots (type A) 1 x USB console port (type B) (up to 115.2 kb/s) Memory DDR2 ECC DRAM Memory: Default 512 MB DDR2 ECC DRAM Memory: Maximum 2 GB Compact Flash (External)-Default : Slot 0: 256 MB Compact Flash (External)-Maximum : Slot 0: 4 GB Slot 1: 4 GB Ports 2 x Total onboard Gigabit Ethernet 10/100/1000 WAN 2 x RJ-45 1 x Serial console (up to 115.2 kb/s) 1 x Serial auxiliary (up to 115.2 kb/s) Slots 2 x EHWIC 1 x Double-wide EHWIC (Use of a double-wide EHWIC slot will consume two EHWIC slots) 1 x ISM Acceleration Embedded hardware-based crypto acceleration (IPSec): Yes Power Specifications

R&TTE, FCC CFR47 Part 15, EN300-386, UL 60950-1, IEC 60950-1, EN 60950-1, BSMI CNS 13438, AS/NZS 3548 clase A, CAN/CSA C22.2 No. 60950-1, VCCI V-3, EN 61000, TIA/EIA/IS-968 Memoria RAM 512 MB (instalados) / 2 GB (máx.) Memoria Flash 256 MB (instalados) / 8 GB (máx.) Indicadores de estado Actividad de enlace, alimentación Expansión / Conectividad Interfaces 2 x 10Base-T/100Base-TX/1000Base-T - RJ-45 Administración: 1 x consola - RJ-45 Administración: 1 x consola - mini USB tipo B Serial: 1 x auxiliar - RJ-45 USB: 2 x USB de 4 clavijas Tipo A Ranuras de expansión 2 (total) / 2 (libre) x EHWIC 2 (total) / 1 (libre) x CompactFlash 1 (total) / 1 (libre) x ISM Alimentación Dispositivo de alimentación Fuente de alimentación eléctrica Voltaje necesario CA 120/230 V (50/60 Hz) Diverso Kit de montaje en bastidor Incluido Software / Requisitos del sistema OS prorporcionado Cisco IOS IP Base Medidas y peso Anchura 34.3 cm Profundidad 29.2 cm Altura 8.9 cm Peso 5.4 kg Garantía del fabricante Servicio y mantenimiento Garantía	Power Supply AC, PoE Typical Power (No Modules): 35 W AC Input Voltage: 100 to 240 V Frequency: 47 to 63 Hz Current Range AC Power Supply (Maximum): 1.5 to 0.6 A Surge Current:<50 A Power Capacity AC Power Supply: 110 W PoE Power Supply (Platform Only): 110 W PoE Device with PoE Power Supply: 80 W Environmental Operating Conditions Temperature 5906' (1800 m) Maximum Altitude: 32 to 104˚F (0 to 40˚C) Temperature 9843' (3000 m) Maximum Altitude: 32 to 77˚F (0 to 25˚C) Altitude: 10000' (3000 m) Relative Humidity: 10 to 85% Acoustic: Sound Pressure (Typ/Maximum) 26/46 dBA Acoustic: Sound Power (Typ/Maximum) 36/55 dBA Storage Conditions Temperature: -40 to +158˚F (-40 to +70˚C) Relative Humidity: 5 to 95% Altitude: 15000' (4570 m) Regulatory Compliance Safety UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1 EMC 47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A Telecom Standards TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3

3.3 MIKOTIK

MIKOTIK CRS226-24G-2S+IN

Details	
Product code	CRS226-24G-2S+IN
SFP DDMI	Yes
CPU nominal frequency	400 MHz
CPU core count	1
Architecture	MIPS-BE
Size of RAM	64 MB
10/100/1000 Ethernet ports	24
Power Jack	1
Supported input voltage	8 V - 30 V
PoE in	Yes
Voltage Monitor	Yes
PCB temperature monitor	Yes
Dimensions	285x145x45mm
Operating System	RouterOS
Tested ambient temperature	-35C to +65C
License level	4
CPU	QCA8519
Max Power consumption	21W
SFP+ ports	2
Serial port	RJ45
Storage type	NAND
Storage size	128 MB

Licencia Level 4

Initial Config Support	15 days
Wireless AP	yes
Wireless Client and Bridge	yes
RIP, OSPF, BGP protocols	yes
EoIP tunnels	unlimited
PPPoE tunnels	200
PPTP tunnels	200
L2TP tunnels	200
OVPN tunnels	200
VLAN interfaces	unlimited
HotSpot active users	200
RADIUS client	yes
Queues	unlimited
Web proxy	yes
User manager active sessions	20

MIKROTIK CRS226-24G-2S+IN

Details	
Product code	CRS226-24G-2S+RM
SFP DDMI	Yes
CPU nominal frequency	400 MHz
CPU core count	1
Size of RAM	64 MB
Architecture	MIPS-BE
10/100/1000 Ethernet ports	24
Power Jack	1
PoE in	Yes
Supported input voltage	8 V - 30 V
Voltage Monitor	Yes
PCB temperature monitor	Yes
Dimensions	443x145x45mm
Operating System	RouterOS
Tested ambient temperature tested	-35C to +65C
License level	5
CPU	QCA8519
Max Power consumption	21W
SFP+ ports	2
Supported Voltage	8-30V on Ether1
Serial port	RJ45
Storage type	NAND
Storage size	128 MB

Licencia Level 5	
Wireless AP	yes
Wireless Client and Bridge	yes
RIP, OSPF, BGP protocols	yes
EoIP tunnels	unlimited
PPPoE tunnels	500
PPTP tunnels	500
L2TP tunnels	500
OVPN tunnels	unlimited
VLAN interfaces	unlimited
HotSpot active users	500
RADIUS client	yes
Queues	unlimited
Web proxy	yes
User manager active sessions	50
Number of KVM guests	Unlimited

Comentarios de la selección.

Se eligió los dispositivos de cisco por su características y especificaciones técnicas, además de ser el propietario del protocolo VTP para gestionar de manera más eficiente, sencilla y optima la red. Estos dispositivos son los que cumplen con todos los requerimientos del CAPÍTULO 3 en su subtitulo 3.5.2.

ANEXO 4

CONFIGURACION SWITCHES

4.1 Prueba

```
Switch>enable
Switch#configure terminal
Switch(config-vlan)#vlan 10
Switch(config-vlan)#name Estudiantes
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name docentes
Switch(config-vlan)#exit
Switch(config)#interface range f0/1-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#interface range f0/4-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
```

4.2 Configuración SW1IEA server VTP

```
Switch#enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW1IEA
SW1IEA(config)#vtp mode server
Device mode already VTP SERVER.
SW1IEA(config)#vtp domain IEA
Changing VTP domain name from NULL to IEA
SW1IEA(config)#vtp password UMSAIEA
Setting device VLAN database password to UMSAIEA
SW1IEA(config)#vlan 10
SW1IEA(config-vlan)#name Estudiantes
SW1IEA(config-vlan)#vlan 20
SW1IEA(config-vlan)#name Docentes
SW1IEA(config-vlan)#vlan 30
SW1IEA(config-vlan)#name Administrativos
SW1IEA(config-vlan)#exit
SW1IEA(config)#interface range g0/0-1
interface range not validated - command rejected
SW1IEA(config)#interface range g0/1-2
SW1IEA(config-if-range)#switchport mode trunk
SW1IEA(config-if-range)#interface f0/1
SW1IEA(config-if)#switchport mode trunk
SW1IEA(config-if)#exit
```

4.3 Configuración SW2IEA, SW3IEA y SW4IEA client VTP

Configuración SW2IEA client VTP

```
Switch>en
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW2IEA
SW2IEA(config)#vtp domain IEA
Changing VTP domain name from NULL to IEA
SW2IEA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW2IEA(config)#vtp password UMSAIEA
Setting device VLAN database password to UMSAIEA
SW2IEA(config)#inter g0/1
SW2IEA(config-if)#switchport mode trunk
```

Configuracion SW3IEA client VTP

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW3IEA
SW3IEA(config)#vtp domain IEA
Domain name already set to IEA.
SW3IEA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW3IEA(config)#vtp password UMSAIEA
Setting device VLAN database password to UMSAIEA
SW3IEA(config)#interface range g0/1-2
SW3IEA(config-if-range)#switchport mode trunk
```

Configuracion SW4IEA client VTP

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW4IEA
SW4IEA(config)#vtp domain IEA
Domain name already set to IEA.
SW4IEA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW4IEA(config)#vtp password UMSAIEA
Setting device VLAN database password to UMSAIEA
SW4IEA(config)#interface g0/2
SW4IEA(config-if)#switchport mode trunk
```

4.4 Asignación puertos en los Switches

Asignación puertos SW1IEA

```
SW1IEA>enable
SW1IEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1IEA(config)#interface range fa0/2-10
SW1IEA(config-if-range)#switchport mode access
SW1IEA(config-if-range)#switchport access vlan 20
SW1IEA(config-if-range)#interface range fa0/11-18
SW1IEA(config-if-range)#switchport mode acces
SW1IEA(config-if-range)#switchport access vlan 30
SW1IEA(config-if-range)#exit
```

Asignación puertos SW2IEA

```
SW2IEA>enable
SW2IEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW2IEA(config)#interface range f0/1-17
SW2IEA(config-if-range)#switchport mode acces
SW2IEA(config-if-range)#switchport acces vlan 10
SW2IEA(config-if-range)#exit
```

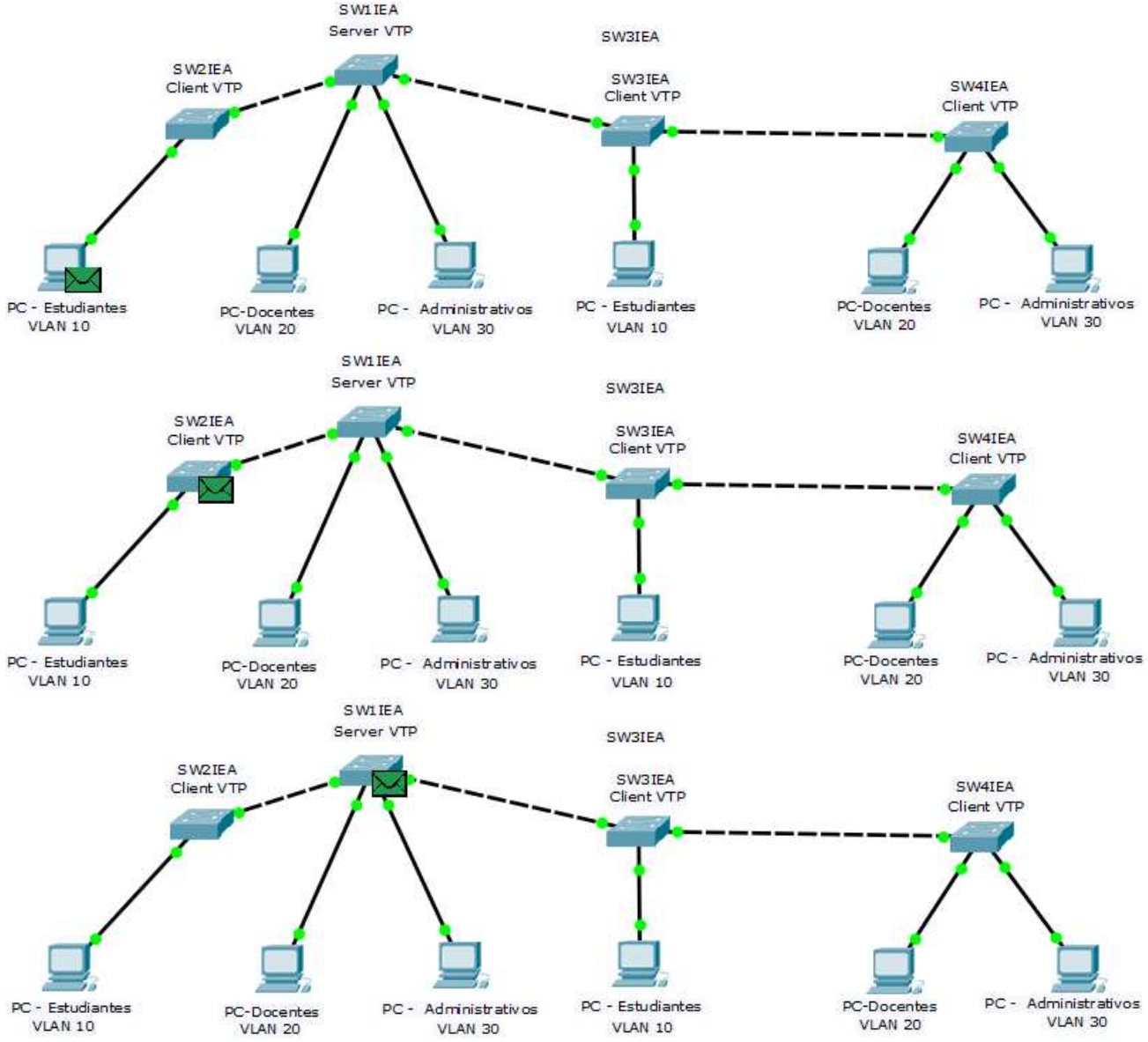
Asignación puertos SW3IEA

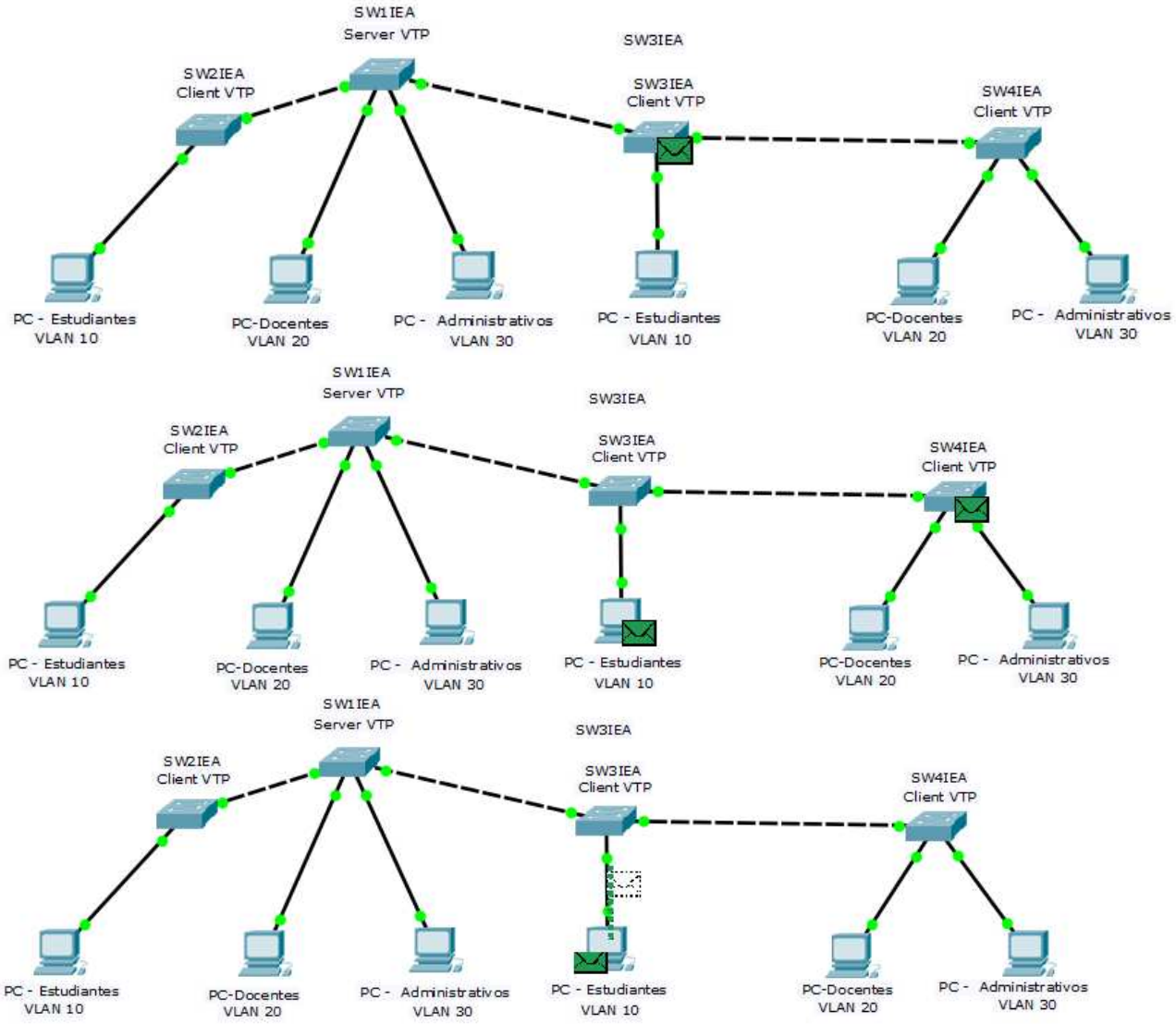
```
SW3IEA>enable
SW3IEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW3IEA(config)#interface range fa0/1-22
SW3IEA(config-if-range)#switchport mode access
SW3IEA(config-if-range)#switchport access vlan 10
SW3IEA(config-if-range)#exit
```

Asignación puertos SW4IEA

```
SW4IEA#enable
SW4IEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW4IEA(config)#interface range f0/1-8
SW4IEA(config-if-range)#switchport mode access
SW4IEA(config-if-range)#switchport access vlan 20
SW4IEA(config-if-range)#interface range f0/9-17
SW4IEA(config-if-range)#switchport mode access
SW4IEA(config-if-range)#switchport access vlan 30
SW4IEA(config-if-range)#exit
```

4.5 Trafico Broadcast desde PC Estudiantes de SW2IEA





El trafico solo llega a los dispositivos dentro de la misma VLAN, reduciendo eficientemente el dominio de broadcast.

4.6 Configuración password para modo privilegiado, consola y vty.

SW1IEA

```
SW1IEA>en
SW1IEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1IEA(config)#enable password IEA
SW1IEA(config)#enable secret UMSA
SW1IEA(config)#line console 0
SW1IEA(config-line)#password IEA
SW1IEA(config-line)#login
```

SW1IEA(config-line)#line vty 0 15
SW1IEA(config-line)#password IEA
SW1IEA(config-line)#login
SW1IEA(config-line)#exit
SW1IEA(config)#service password-encryption

SW2IEA
SW2IEA>enable
SW2IEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW2IEA(config)#enable password IEA
SW2IEA(config)#enable secret UMSA
SW2IEA(config)#line console 0
SW2IEA(config-line)#password IEA
SW2IEA(config-line)#login
SW2IEA(config-line)#line vty 0 15
SW2IEA(config-line)#password IEA
SW2IEA(config-line)#login
SW2IEA(config-line)#exit
SW2IEA(config)#service password-encryption

SW3IEA
SW3IEA>enable
SW3IEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW3IEA(config)#enable password IEA
SW3IEA(config)#enable secret UMSA
SW3IEA(config)#line console 0
SW3IEA(config-line)#password IEA
SW3IEA(config-line)#login
SW3IEA(config-line)#line vty 0 15
SW3IEA(config-line)#password IEA
SW3IEA(config-line)#login
SW3IEA(config-line)#exit
SW3IEA(config)#service password-encryption

SW4IEA
SW4IEA>enable
SW4IEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW4IEA(config)#enable password IEA
SW4IEA(config)#enable secret UMSA
SW4IEA(config)#line console 0
SW4IEA(config-line)#password IEA
SW4IEA(config-line)#login
SW4IEA(config-line)#line vty 0 15
SW4IEA(config-line)#password IEA
SW4IEA(config-line)#login
SW4IEA(config-line)#exit
SW4IEA(config)#service password-encryption

4.7 Banner de advertencia

SW1IEA
SW1IEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1IEA(config)#banner motd $!!!!!!!!!ALERTA!!!!!!!!!
Enter TEXT message. End with the character '$'.
SOLO PERSONAL AUTORIZADO IEA$

SW2IEA
SW2IEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1IEA(config)#banner motd $!!!!!!!!!ALERTA!!!!!!!!!
Enter TEXT message. End with the character '$'.
SOLO PERSONAL AUTORIZADO IEA$
SW3IEA
SW3IEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1IEA(config)#banner motd $!!!!!!!!!ALERTA!!!!!!!!!
Enter TEXT message. End with the character '$'.
SOLO PERSONAL AUTORIZADO IEA$

SW4IEA
SW4IEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1IEA(config)#banner motd $!!!!!!!!!ALERTA!!!!!!!!!
Enter TEXT message. End with the character '$'.
SOLO PERSONAL AUTORIZADO IEA$

4.8 Configuración Telnet

SW1IEA
SW1IEA>enable
Password:
SW1IEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1IEA(config)#vlan 99

%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

SW1IEA(config-vlan)#name Telnet
SW1IEA(config-vlan)#exit
SW1IEA(config)#interface vlan 99
SW1IEA(config-if)#ip address 192.168.11.1 255.255.255.252
SW1IEA(config-if)#no shut
SW1IEA(config-if)#interface fa0/24
SW1IEA(config-if)#switchport mode access
SW1IEA(config-if)#switchport access vlan 99

SW2IEA

```
SW2IEA>enable
Password:
SW2IEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW2IEA(config)#interface vlan 99
SW2IEA(config-if)#ip address 192.168.12.1 255.255.255.252
SW2IEA(config-if)#no shut
SW2IEA(config-if)#interface fa0/24
SW2IEA(config-if)#switchport mode access
SW2IEA(config-if)#switchport access vlan 99
```

SW3IEA

```
SW3IEA>enable
Password:
SW3IEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW3IEA(config)#interface vlan 99
SW3IEA(config-if)#ip address 192.168.13.1 255.255.255.252
SW3IEA(config-if)#no shut
SW3IEA(config-if)#interface fa0/24
SW3IEA(config-if)#switchport mode access
SW3IEA(config-if)#switchport access vlan 99
```

SW4IEA

```
SW4IEA>enable
Password:
SW4IEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW4IEA(config)#interface vlan 99
SW4IEA(config-if)#ip address 192.168.14.1 255.255.255.252
SW4IEA(config-if)#no shut
SW4IEA(config-if)#interface fa0/24
SW4IEA(config-if)#switchport mode access
SW4IEA(config-if)#switchport access vlan 99
```

ANEXO 5

CONFIGURACIÓN DEL ROUTER

5.1 Configuración DHCP

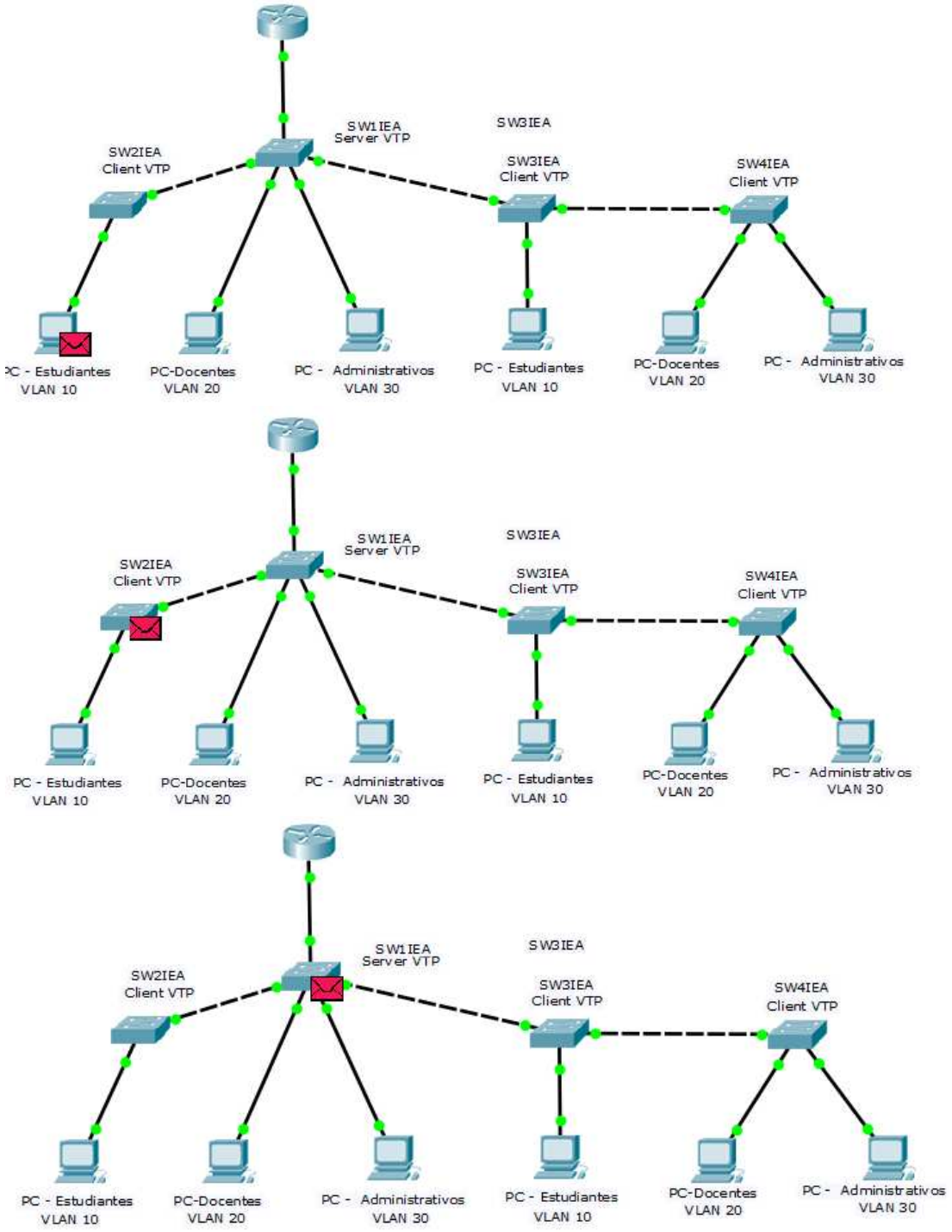
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname RouterIEA
RouterIEA(config)#ip dhcp pool Estudiantes
RouterIEA(dhcp-config)#network 192.168.1.0 255.255.255.192
RouterIEA(dhcp-config)#default-router 192.168.1.1
RouterIEA(dhcp-config)#ip dhcp pool Docentes
RouterIEA(dhcp-config)#network 192.168.1.64 255.255.255.224
RouterIEA(dhcp-config)#default-router 192.168.1.65
RouterIEA(dhcp-config)#ip dhcp pool Administrativos
RouterIEA(dhcp-config)#network 192.168.1.96 255.255.255.224
RouterIEA(dhcp-config)#default-router 192.168.1.97
```

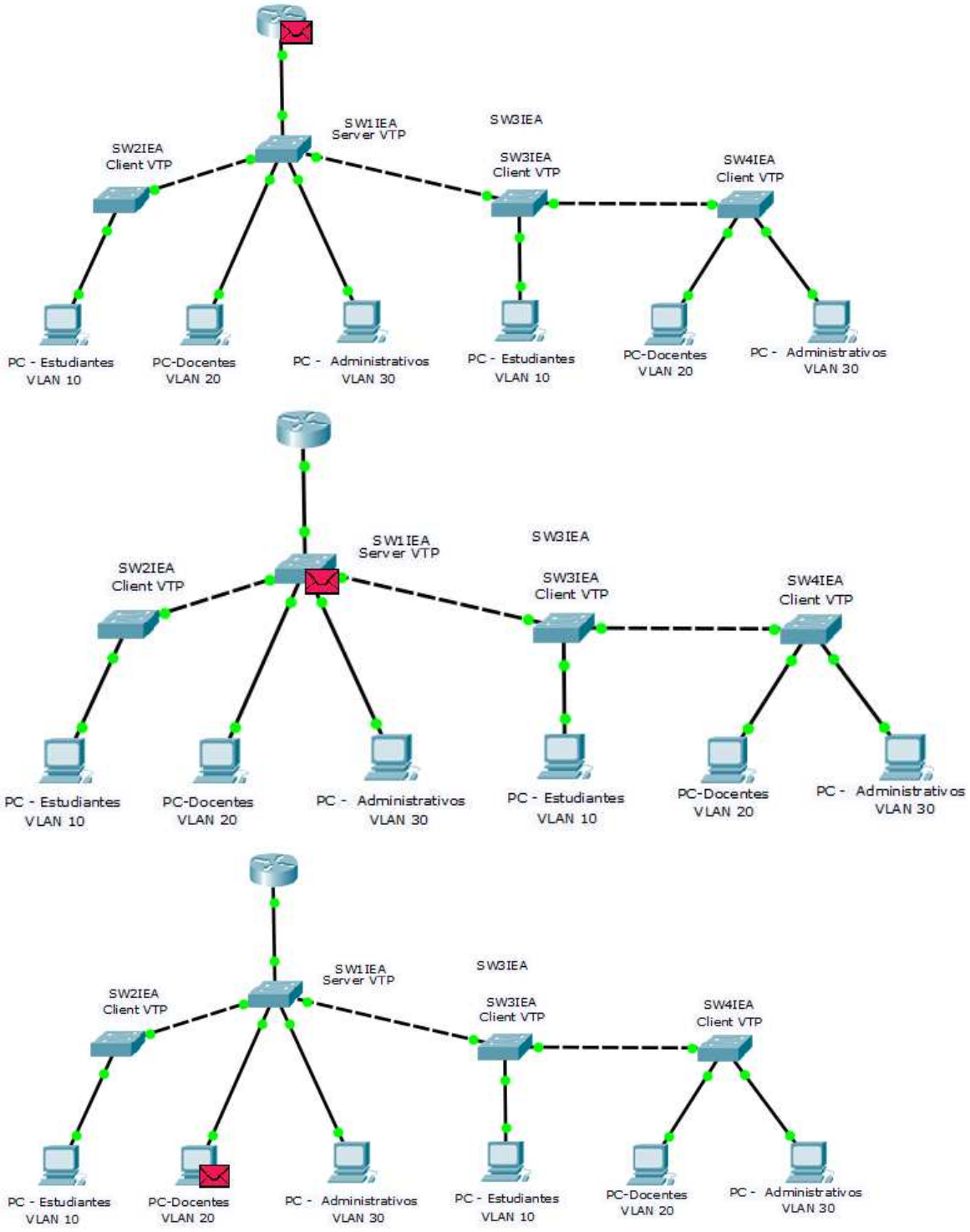
5.2 Configuracion de subinterfaces

```
RouterIEA(dhcp-config)#inter g0/0.1
RouterIEA(config-subif)#encapsulation dot1q 10
RouterIEA(config-subif)#ip address 192.168.1.1 255.255.255.192
RouterIEA(config-subif)#exit
RouterIEA(config)#inter g0/0.2
RouterIEA(config-subif)#encapsulation dot1q 20
RouterIEA(config-subif)#ip address 192.168.1.65 255.255.255.224
RouterIEA(config-subif)#inter g0/0.3
RouterIEA(config-subif)#encapsulation dot1q 30
RouterIEA(config-subif)#ip address 192.168.1.97 255.255.255.224
RouterIEA(config-subif)#exit
RouterIEA(config)#interface g0/0
RouterIEA(config-if)#no shutdown
RouterIEA(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.1, changed
state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0.2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.2, changed
state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0.3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.3, changed
state to up
```

5.3 Configuración de Access Control List (ACL).

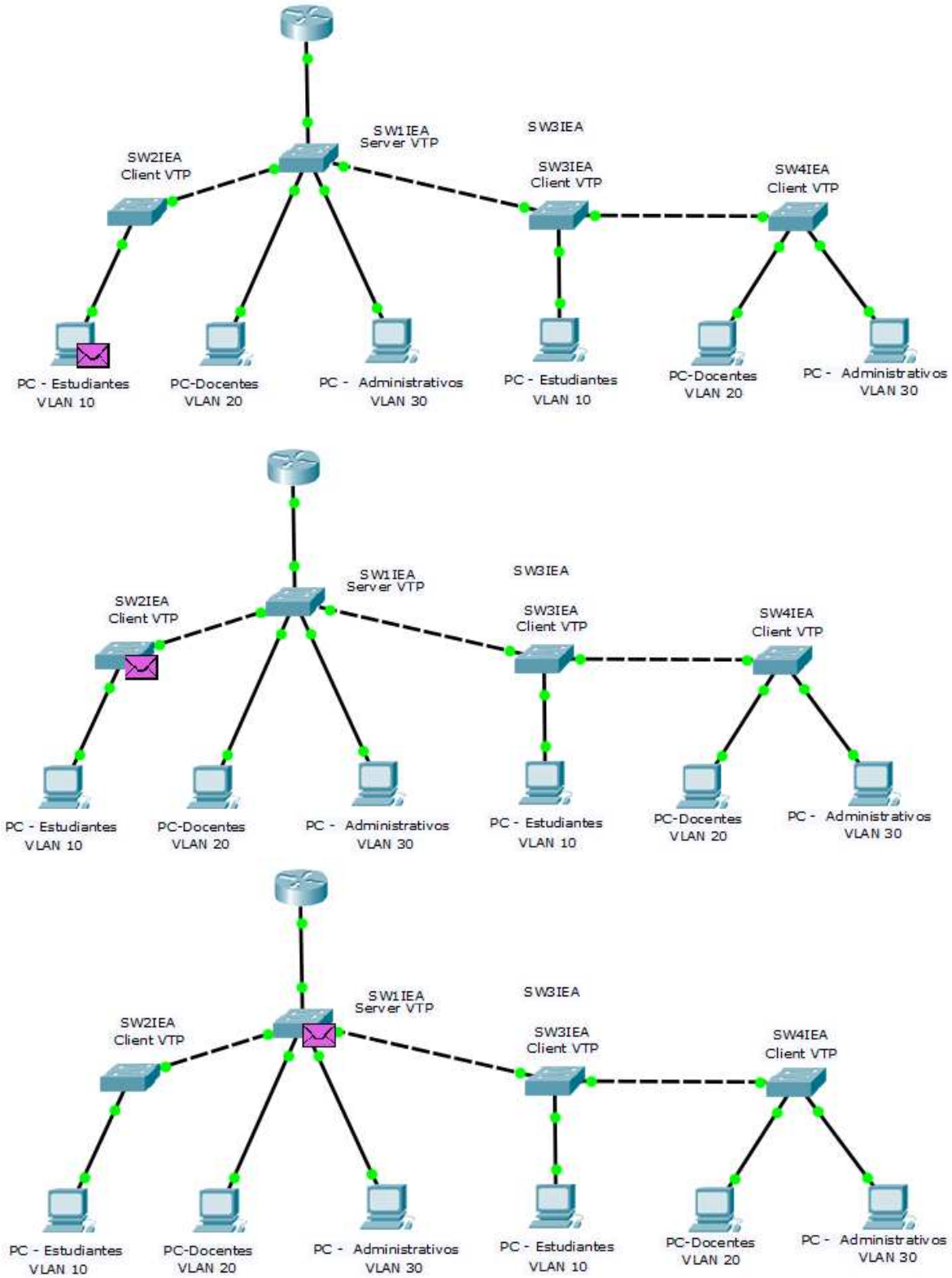
5.4 Antes del ACL Estudiantes a Docentes

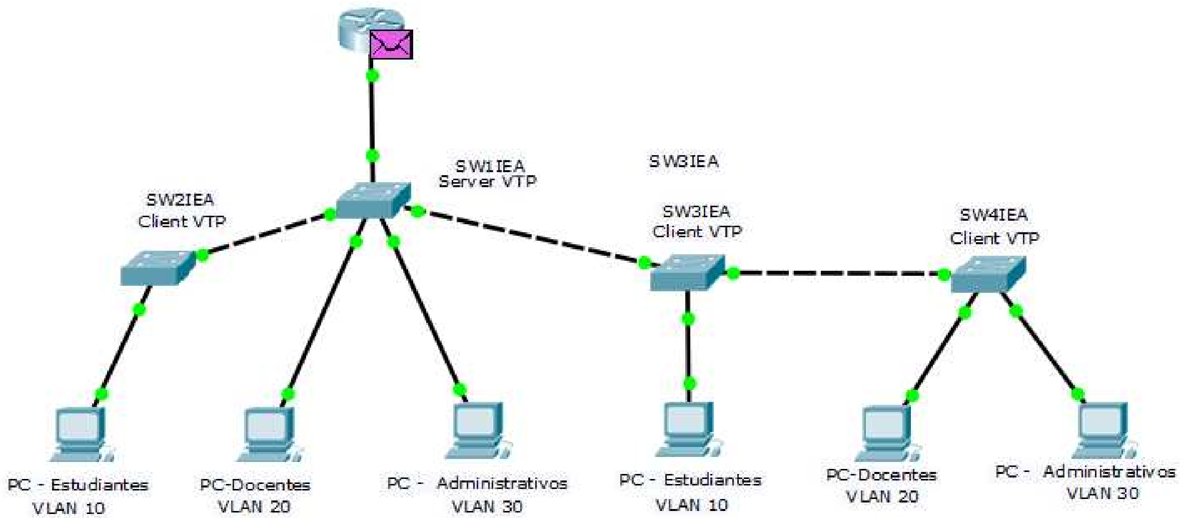


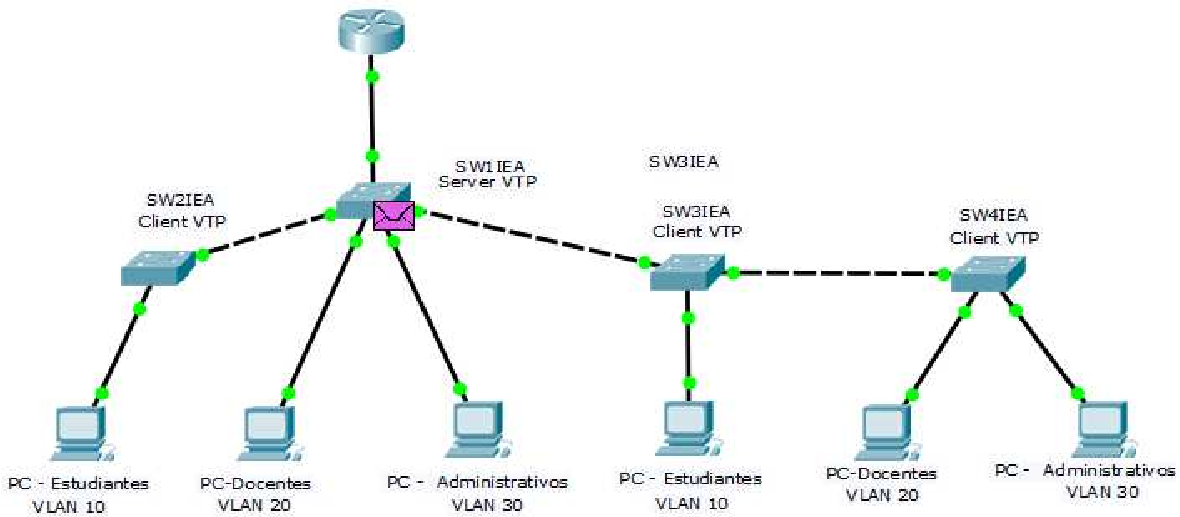


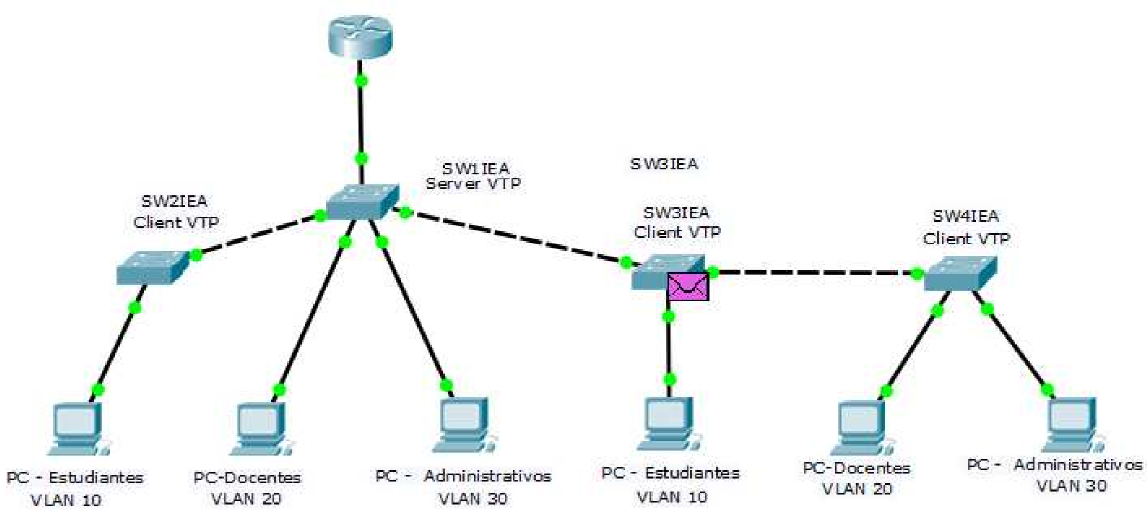
Comunicación exitosa entre Estudiantes y Docentes.

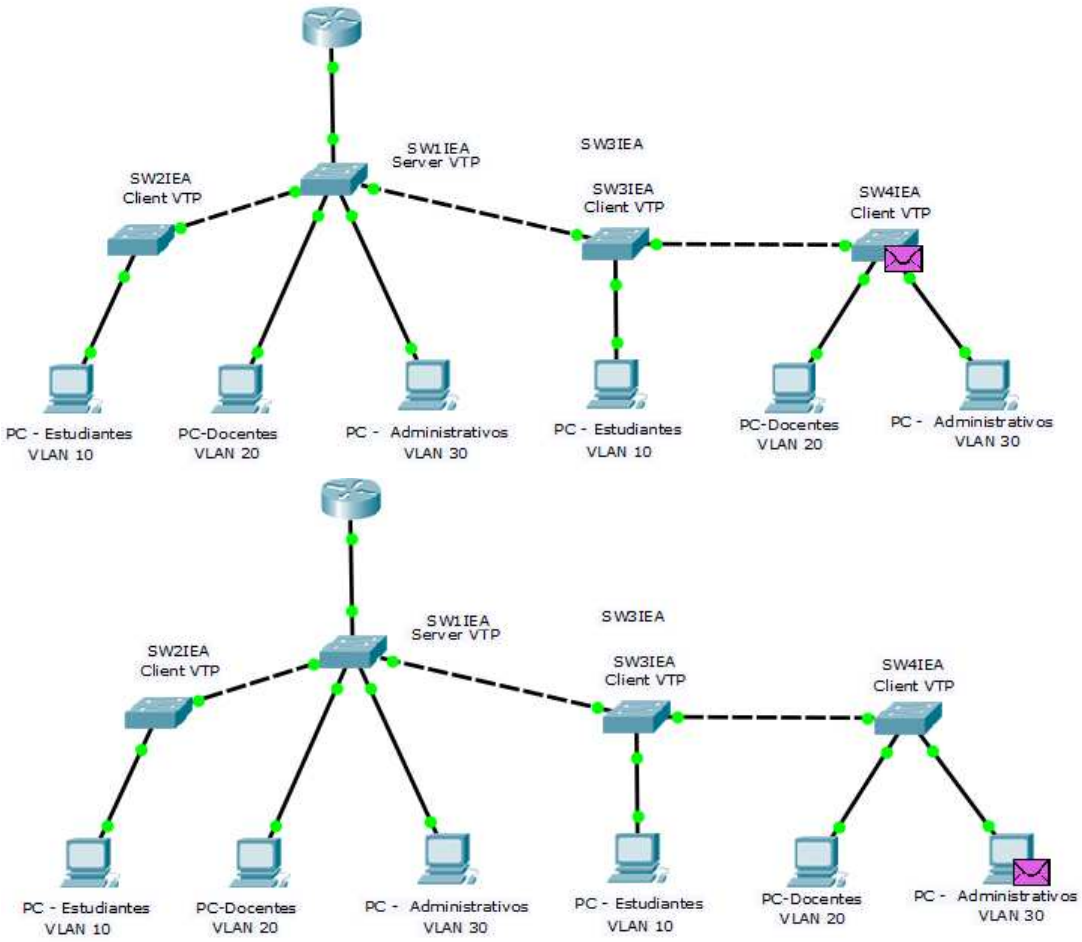
5.5 Antes del ACL Estudiantes y Administrativos




SW1IEA
Server VTP
SW3IEA
SW2IEA
Client VTP
SW3IEA
Client VTP
SW4IEA
Client VTP
PC - Estudiantes
VLAN 10
PC-Docentes
VLAN 20
PC - Administrativos
VLAN 30
PC - Estudiantes
VLAN 10
PC-Docentes
VLAN 20
PC - Administrativos
VLAN 30


SW1IEA
Server VTP
SW3IEA
SW2IEA
Client VTP
SW3IEA
Client VTP
SW4IEA
Client VTP
PC - Estudiantes
VLAN 10
PC-Docentes
VLAN 20
PC - Administrativos
VLAN 30
PC - Estudiantes
VLAN 10
PC-Docentes
VLAN 20
PC - Administrativos
VLAN 30


SW1IEA
Server VTP
SW3IEA
SW2IEA
Client VTP
SW3IEA
Client VTP
SW4IEA
Client VTP
PC - Estudiantes
VLAN 10
PC-Docentes
VLAN 20
PC - Administrativos
VLAN 30
PC - Estudiantes
VLAN 10
PC-Docentes
VLAN 20
PC - Administrativos
VLAN 30

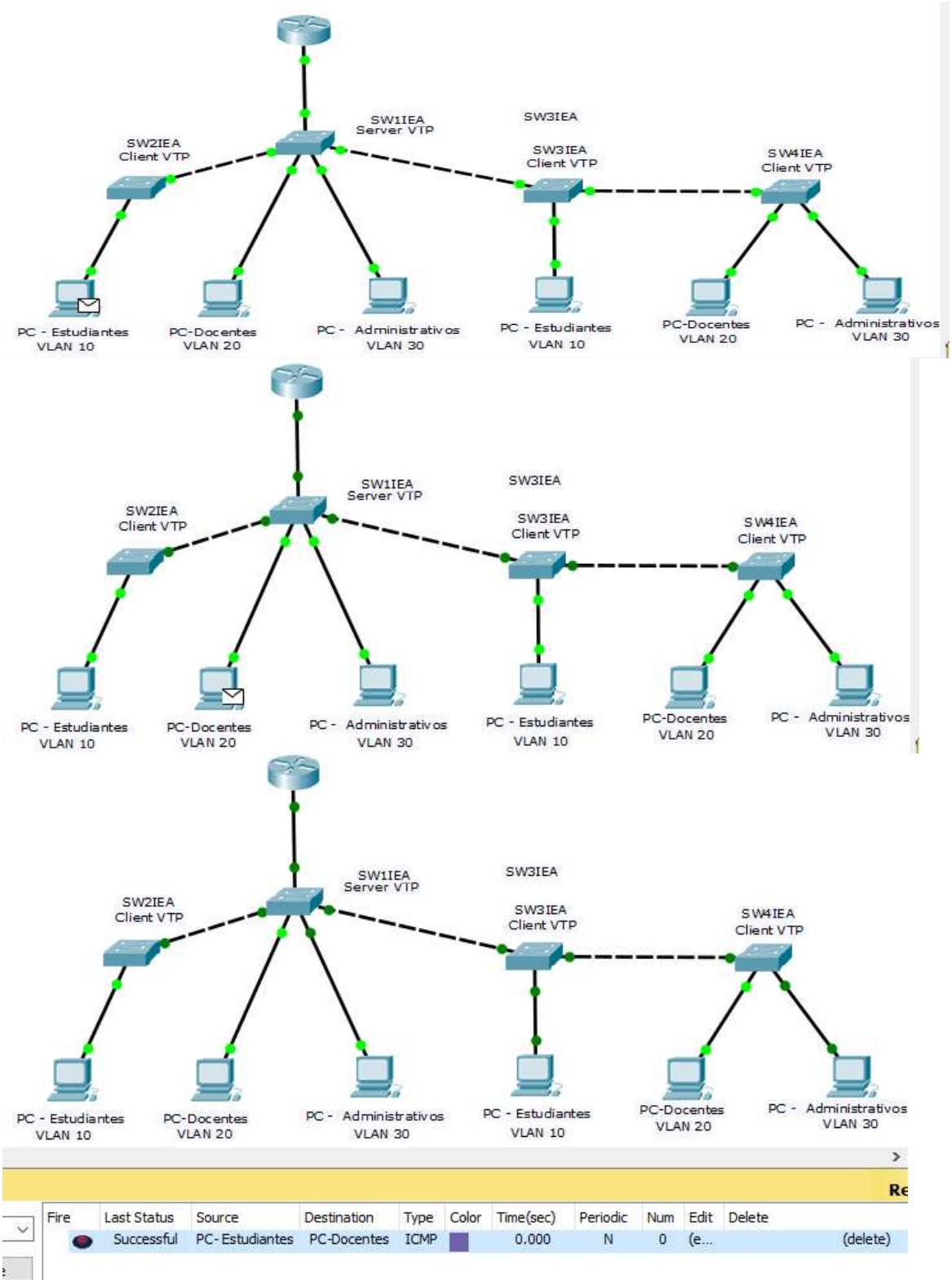


Comunicación exitosa entre Estudiantes y Administrativos

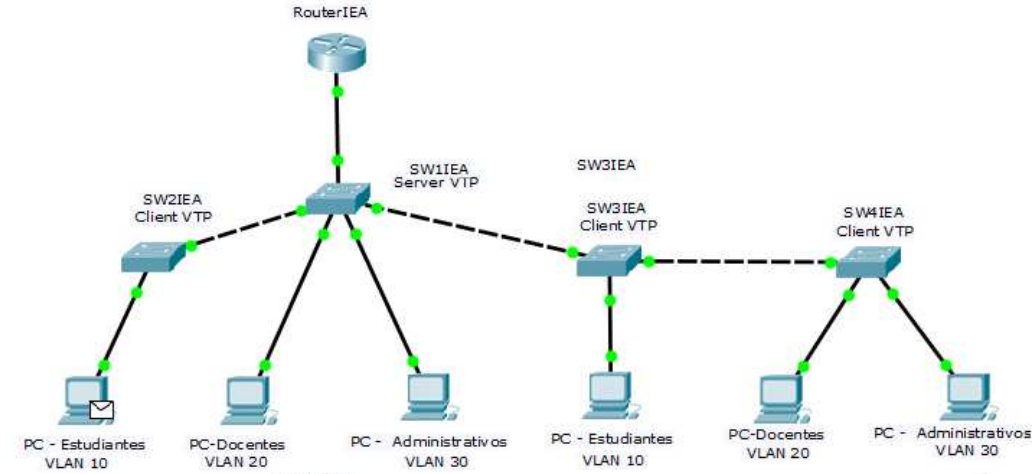
5.6 Configuración del ACL

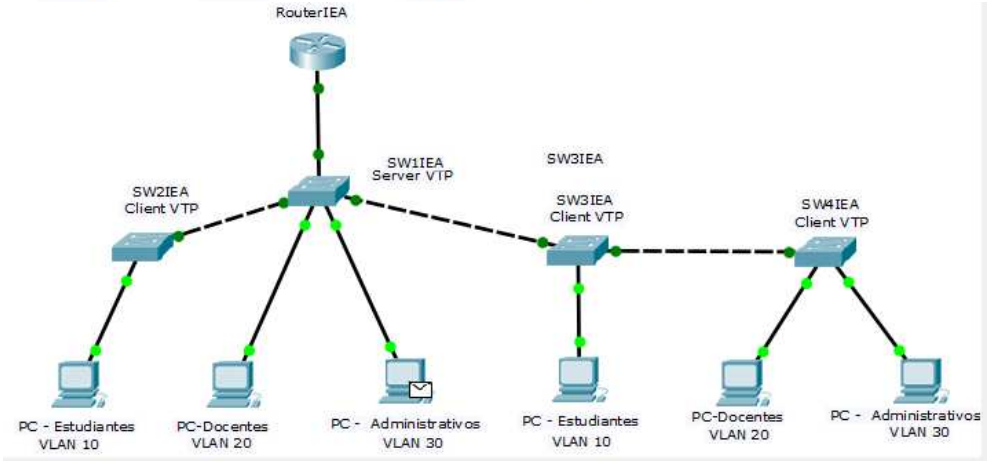
```
RouterIEA>enable
RouterIEA#configure terminal
RouterIEA(config)#access-list 10 deny 192.168.1.96 0.0.0.31
RouterIEA(config)#access-list 10 permit ip any
RouterIEA(config)#inter g0/0.1
RouterIEA(config-subif)#ip access-group 10 out
%SYS-5-CONFIG_I: Configured from console by console
```

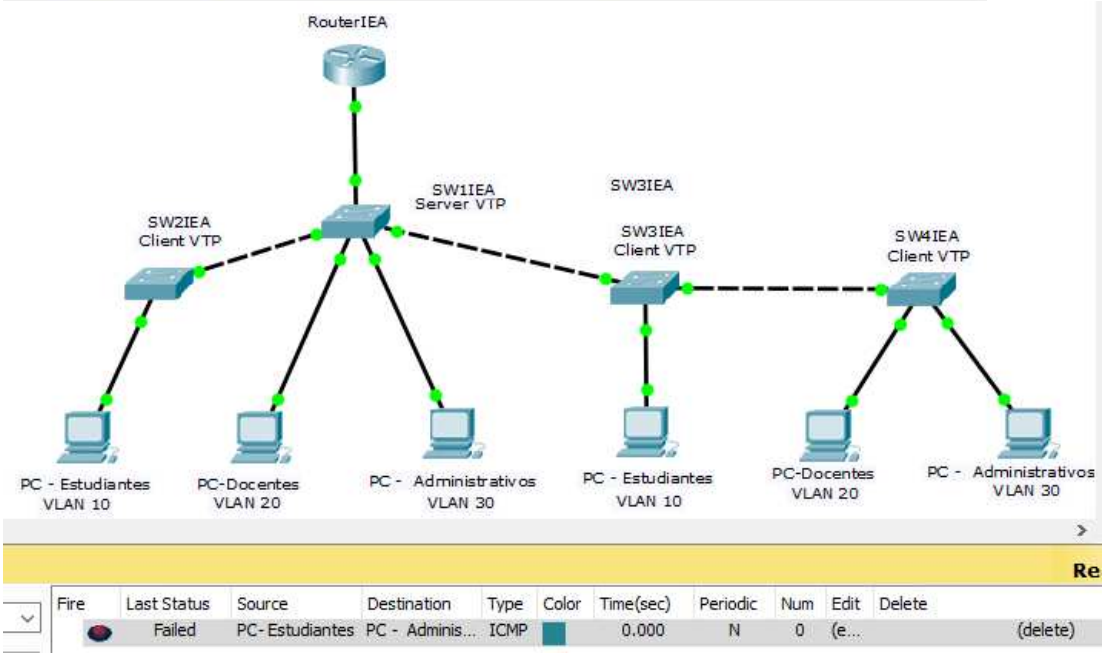
5.7 Despúes del ACL Estudiantes y Adminisitrativos



Comunicación exitosa entre Estudiantes y Docentes.



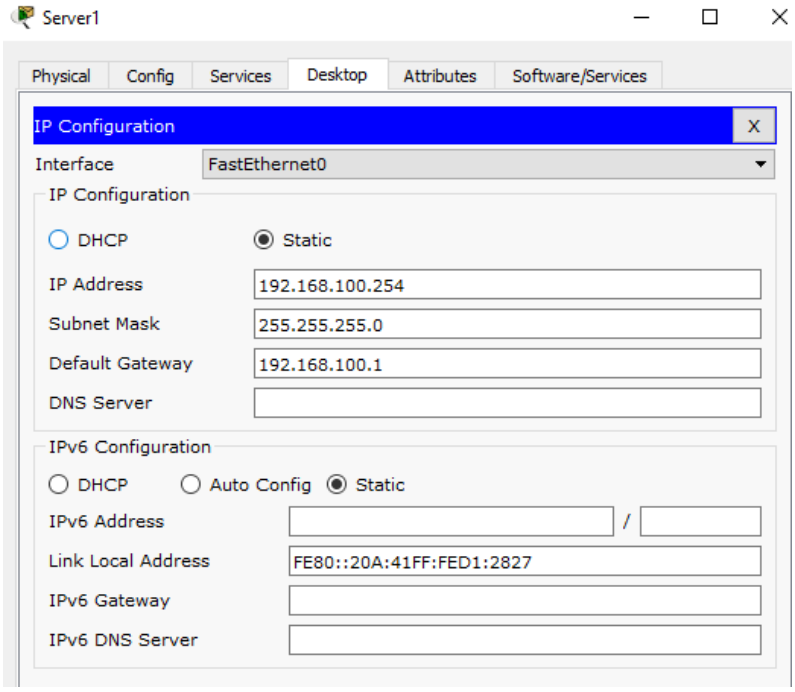




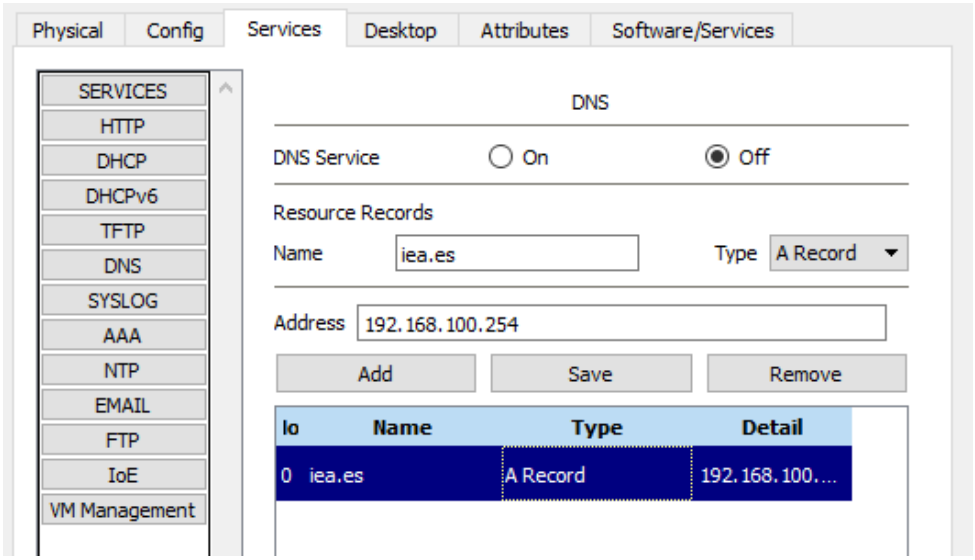
La comunicación entre Estudiantes y Administrativos no es posible debido al ACL.

5.8 Configuración Firewall

Asignación de dirección IP al servidor.



Asignación de dirección IP server 1



Añadir servicio DNS server 1

5.9 Asignar el DNS al DHCP

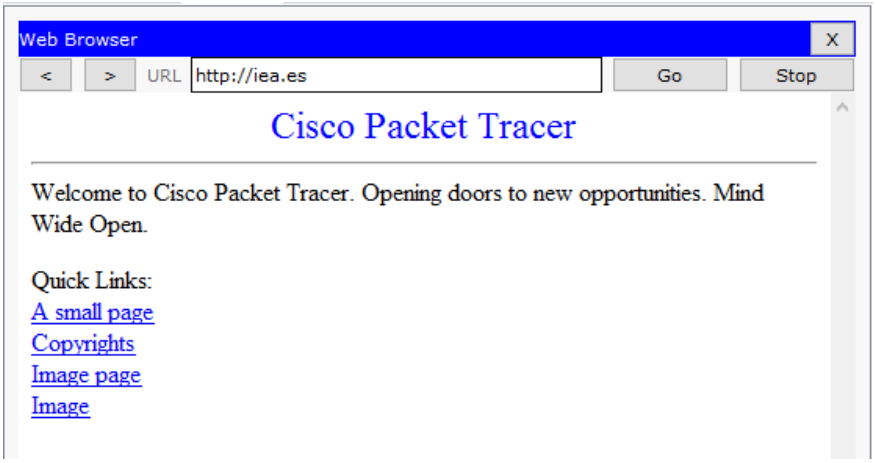
```
RouterIEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterIEA(config)#ip dhcp pool Estudiantes
RouterIEA(dhcp-config)#dns-server 192.168.100.10
RouterIEA(dhcp-config)#exit
RouterIEA(config)#ip dhcp pool Docentes
RouterIEA(dhcp-config)#dns-server 192.168.100.10
RouterIEA(dhcp-config)#exit
RouterIEA(config)#ip dhcp pool Administrativos
RouterIEA(dhcp-config)#dns-server 192.168.100.10
RouterIEA(dhcp-config)#exit
```

Ping desde PC de: Estudiantes, Docentes y Administrativos, a el servidor

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.10

Pinging 192.168.100.10 with 32 bytes of data:

Reply from 192.168.100.10: bytes=32 time<1ms TTL=127
Reply from 192.168.100.10: bytes=32 time<1ms TTL=127
Reply from 192.168.100.10: bytes=32 time=1ms TTL=127
Reply from 192.168.100.10: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.100.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Se tiene ping desde todas las PCs.

Acceso al servicio DNS por HTTP



Se tiene acceso por HTTP al servidor.

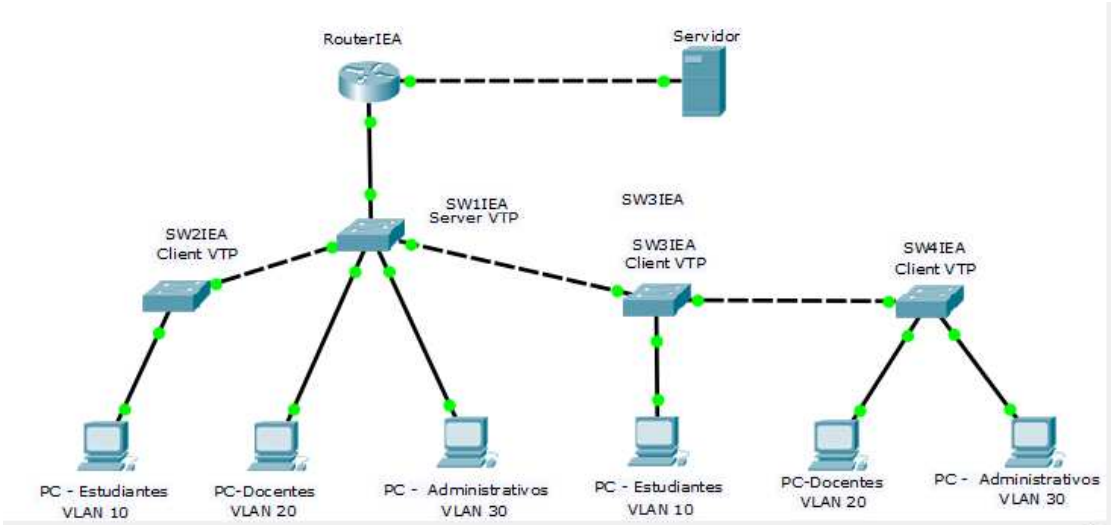
5.10 Configuración Firewall

RouterIEA>enable
RouterIEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterIEA(config)#access-list 101 deny icmp any any host-unreachable
RouterIEA(config)#access-list 101 permit tcp any any eq www
RouterIEA(config)#interface g0/1
RouterIEA(config-if)#ip access-group 101 out
RouterIEA(config-if)#exit

Se realiza un ping desde cualquier PC (Estudiantes, Docentes o Administrativos).

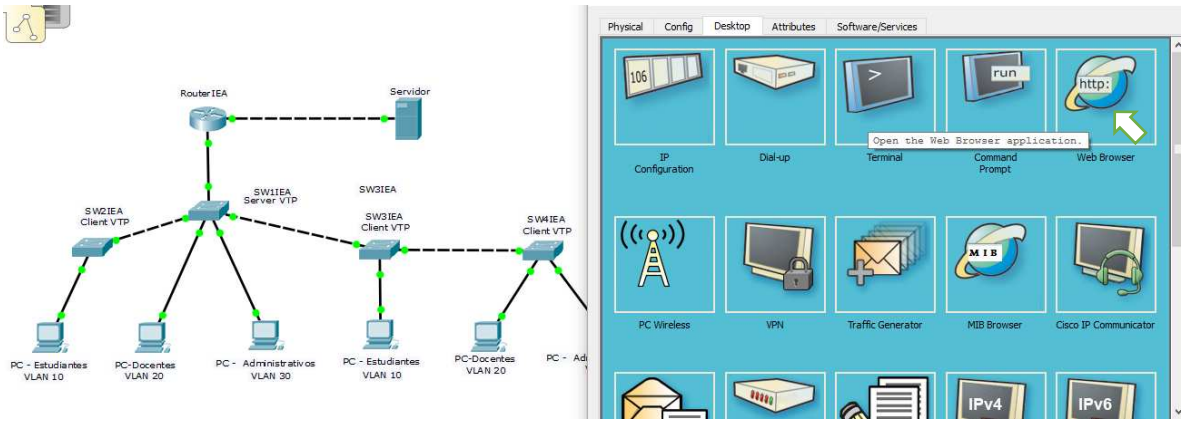
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.10

Pinging 192.168.100.10 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.100.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ya no se tiene ping desde ninguna PC hacia el servidor debido al firewall configurado, ya que los paquetes enviados por el ping son ICMP.



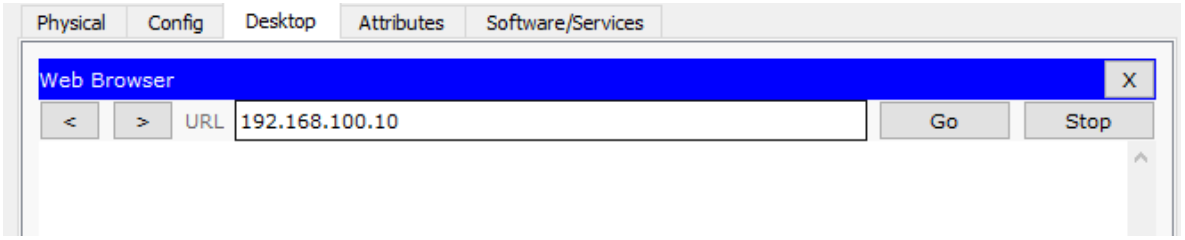
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC-Estudiantes	ServerIEA	ICMP		0.000	N	0	(e...	(delete)
	Failed	PC-Docentes	ServerIEA	ICMP		0.000	N	1	(e...	(delete)
	Failed	PC - Administrativos	ServerIEA	ICMP		0.000	N	2	(e...	(delete)

Como se observa en la simulación ninguna PC puede llegar al servidor por ICMP. Acceso por TCP desde HTTP.



Ingresamos a cualquier PC (Estudiantes, Docentes o Administrativos) y seleccionamos el Web Browser.

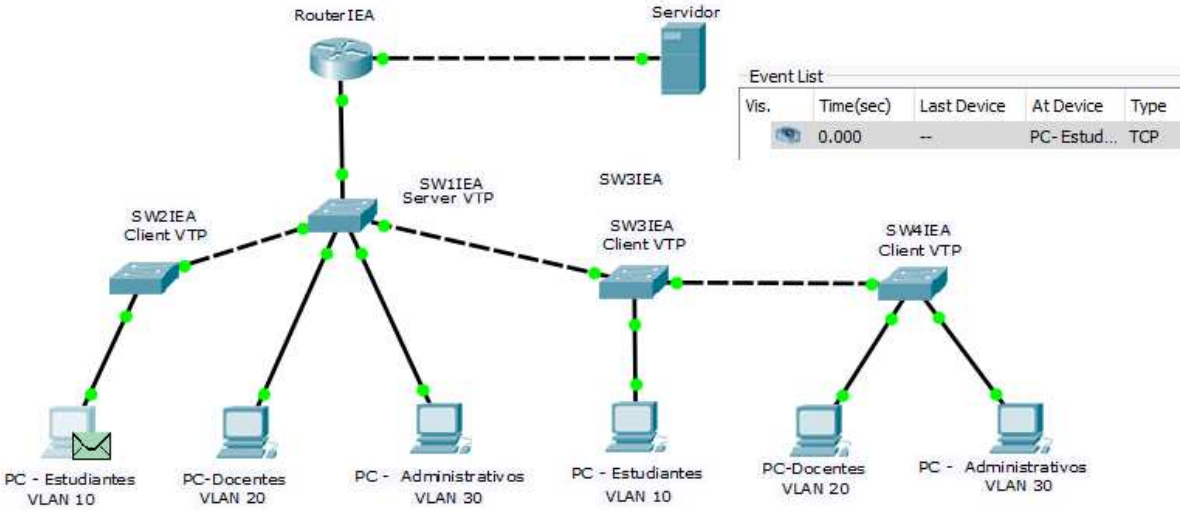
Ingresar la dirección IP del servidor 192.168.100.10

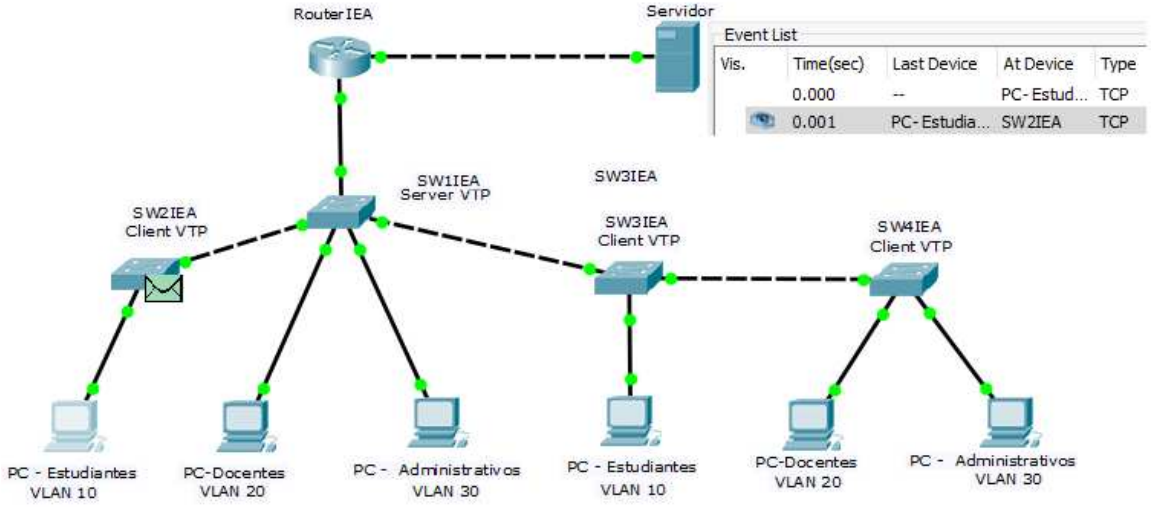


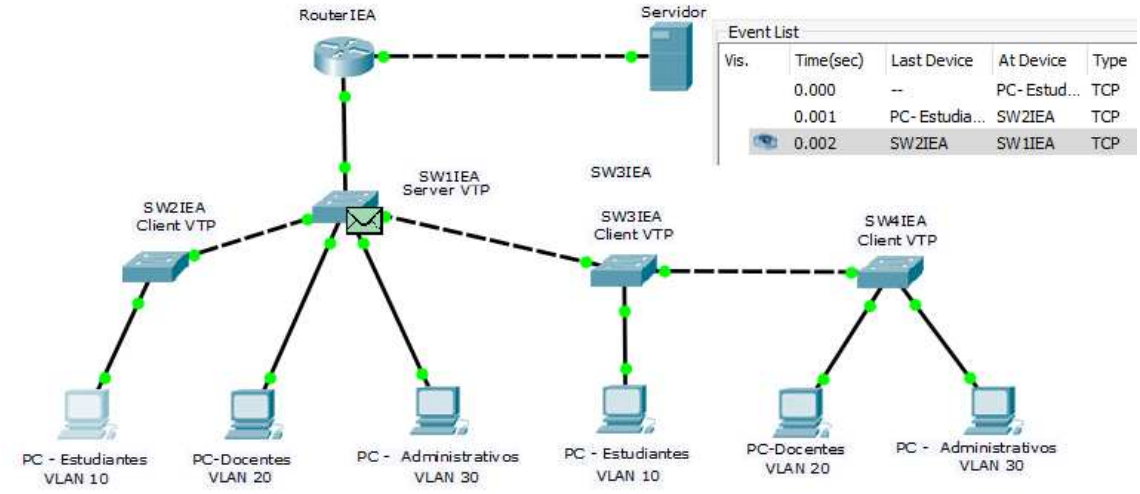
Hacer clic en “Go” o presionar Enter.

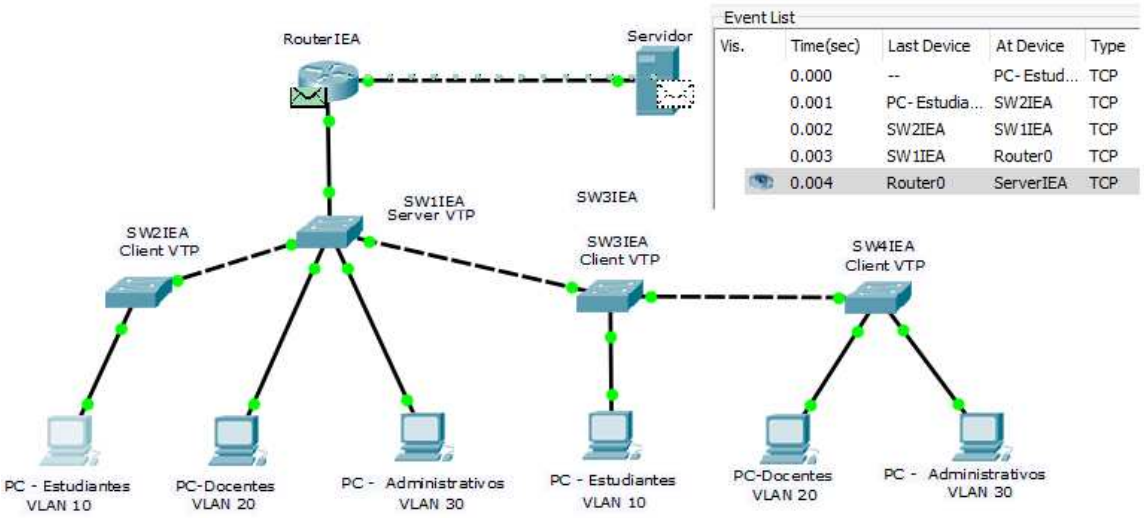
Mediante el browser podemos ingresar al servidor, debido a que se permite el protocolo TCP.

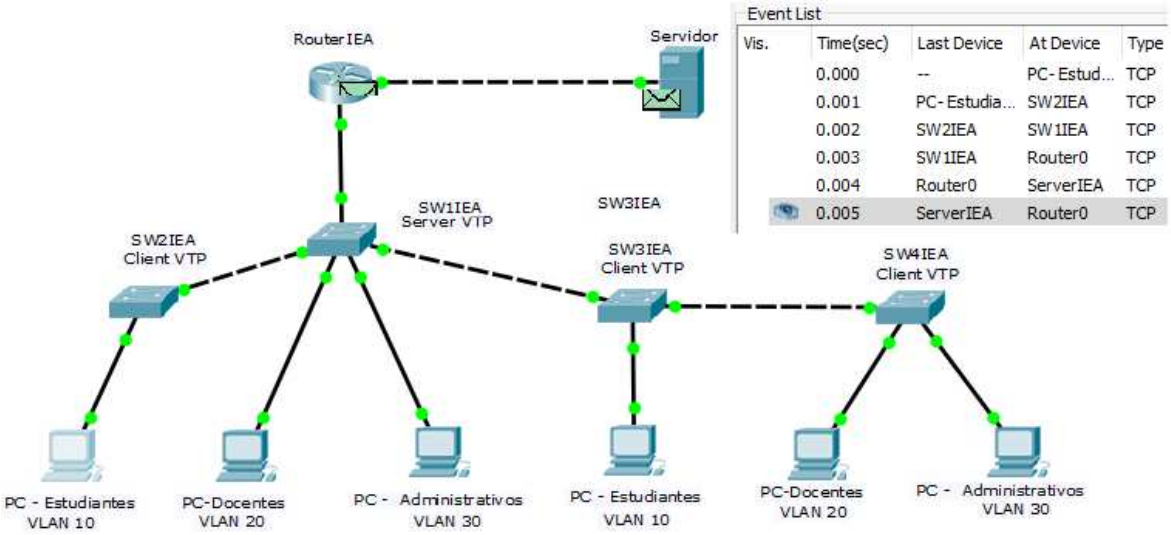
5.11 Simulación del protocolo TCP

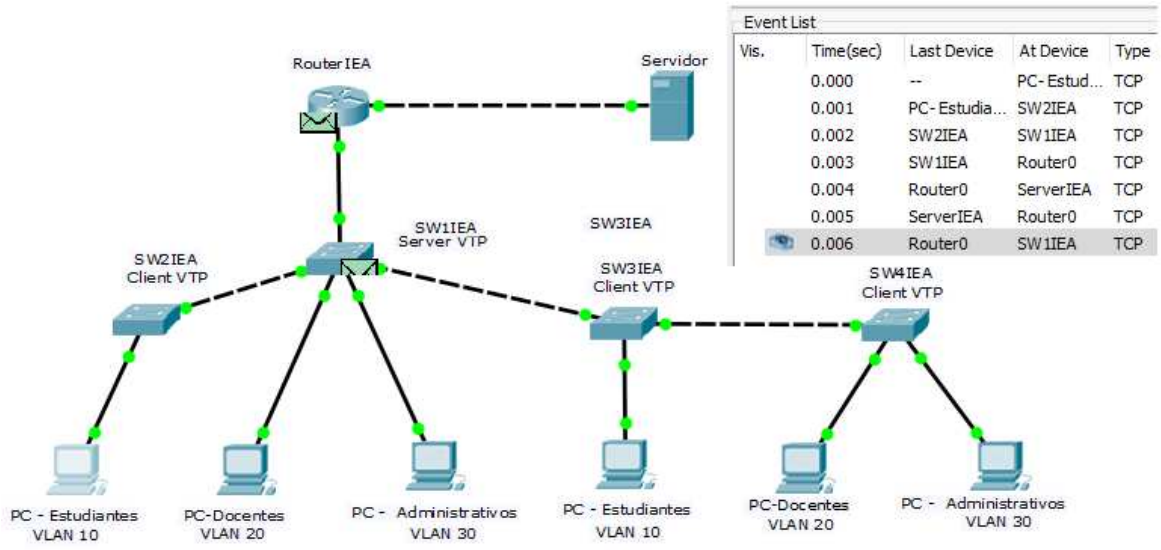


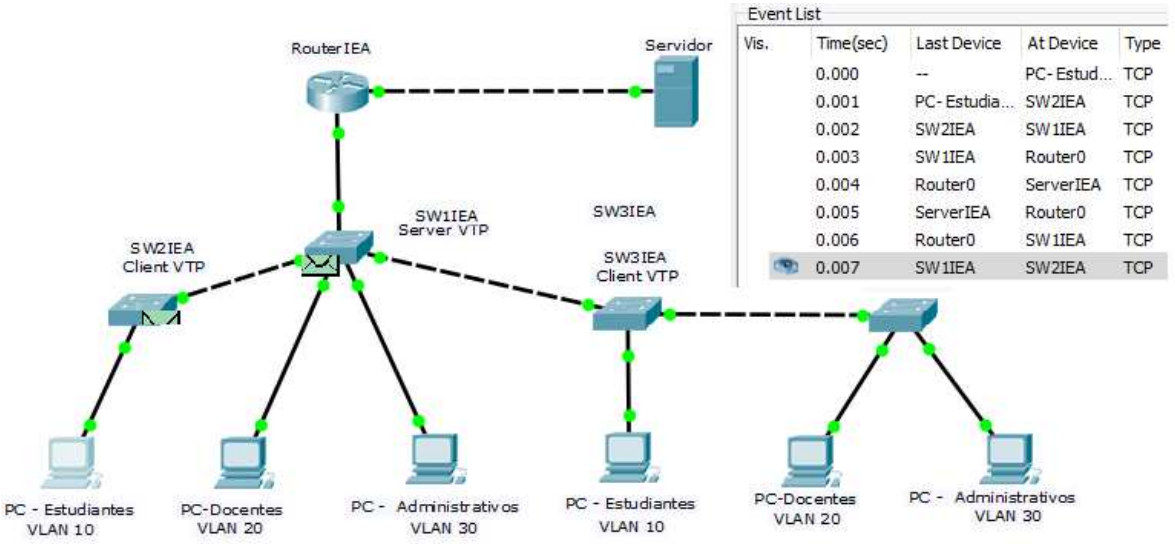


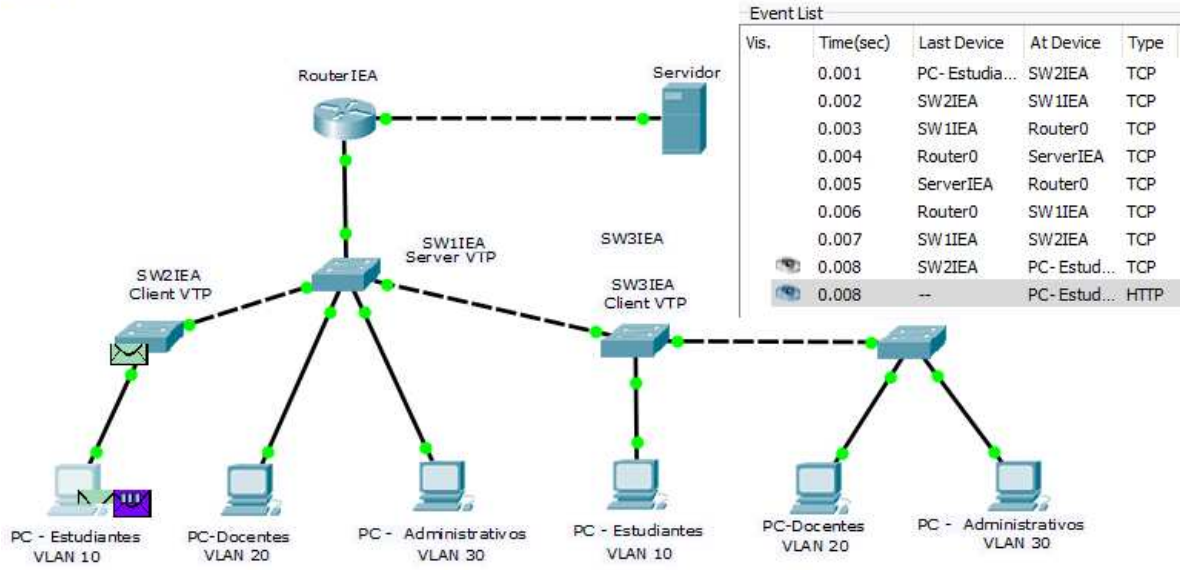



Event List
Vis. Time(sec) Last Device At Device Type
0.000 -- PC- Estud... TCP
0.001 PC- Estudia... SW2IEA TCP
0.002 SW2IEA SW1IEA TCP
0.003 SW1IEA Router0 TCP
0.004 Router0 ServerIEA TCP
RouterIEA
Servidor
SW1IEA
Server VTP
SW3IEA
SW2IEA
Client VTP
SW3IEA
Client VTP
SW4IEA
Client VTP
PC - Estudiantes
VLAN 10
PC-Docentes
VLAN 20
PC - Administrativos
VLAN 30
PC - Estudiantes
VLAN 10
PC-Docentes
VLAN 20
PC - Administrativos
VLAN 30


Event List
Vis. Time(sec) Last Device At Device Type
0.000 -- PC- Estud... TCP
0.001 PC- Estudia... SW2IEA TCP
0.002 SW2IEA SW1IEA TCP
0.003 SW1IEA Router0 TCP
0.004 Router0 ServerIEA TCP
0.005 ServerIEA Router0 TCP
RouterIEA
Servidor
SW1IEA
Server VTP
SW3IEA
SW2IEA
Client VTP
SW3IEA
Client VTP
SW4IEA
Client VTP
PC - Estudiantes
VLAN 10
PC-Docentes
VLAN 20
PC - Administrativos
VLAN 30
PC - Estudiantes
VLAN 10
PC-Docentes
VLAN 20
PC - Administrativos
VLAN 30


Event List
Vis. Time(sec) Last Device At Device Type
0.000 -- PC- Estud... TCP
0.001 PC- Estudia... SW2IEA TCP
0.002 SW2IEA SW1IEA TCP
0.003 SW1IEA Router0 TCP
0.004 Router0 ServerIEA TCP
0.005 ServerIEA Router0 TCP
0.006 Router0 SW1IEA TCP
RouterIEA
Servidor
SW1IEA
Server VTP
SW3IEA
SW2IEA
Client VTP
SW3IEA
Client VTP
SW4IEA
Client VTP
PC - Estudiantes
VLAN 10
PC-Docentes
VLAN 20
PC - Administrativos
VLAN 30
PC - Estudiantes
VLAN 10
PC-Docentes
VLAN 20
PC - Administrativos
VLAN 30





5.12 Configuracion Password modo privilegiado, consola y banner de alerta

RouterIEA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterIEA(config)#enable password IEA
RouterIEA(config)#enable secret UMSA
RouterIEA(config)#line console 0
RouterIEA(config-line)#password IEA
RouterIEA(config-line)#exit
RouterIEA(config)#Banner motd $!!!!!!!!!ALERTA!!!!!!!!!
SOLO PERSONAL AUTORIZADO IEA$

5.13 Guardar configuración.

```
SW1IEA>enable
Password:
SW1IEA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

SW2IEA>enable
Password:
SW2IEA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

SW3IEA>enable
Password:
SW3IEA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

SW4IEA>enable
Password:
SW4IEA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

RouterIEA>enable
Password:
RouterIEA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

ANEXO 6

Calculo de capacidad

6.1 Estimación de la demanda de tráfico por cada usuario.

REQUERIMIENTO DE ANCHO DE BANDA ACTUAL POR CADA USUARIO	CAPACIDAD REQUERIDA
Navegación	0.20 Mbps
Actualizaciones en línea de sistemas operativos	0.20 Mbps
Actualizaciones en línea de sistemas de seguridad	0.20 Mbps
Accesos a aplicaciones	6.00 Mbps
Transferencia de archivos entre terminales	50.00 Mbps
Descarga de contenido institucional	5.00 Mbps
REQUERIMIENTO DE ANCHO DE BANDA FUTURO POR CADA USUARIO	CAPACIDAD REQUERIDA
Presentaciones, video, mensajería, audio	5.00 Mbps
Video llamadas	1.00 Mbps
Video conferencias	1.00 Mbps
Aplicaciones Futuras (streaming de video, multimedia, etc.)	100.00 Mbps
Total, de ancho de banda	168.60 Mbps

Del análisis se determina que el ancho de banda requerido por cada usuario es de 61,6 Mbps. En el futuro se requerirá tener mayores anchos de banda para incluir nuevas funciones y aplicaciones que se desarrollen en el IEA, y se estima que puede alcanzar los 168.6 Mbps, como indica la tabla anterior.

6.2 Definición de la velocidad de los puertos para los usuarios

Para evitar posibles encolamientos y saturación en los puertos de red estos deberían tener mínimo el doble de la capacidad calculada (168.6 Mbps * 2 = 336.4 Mbps). Por tal motivo los puertos de red de los Switches deben ser de 1Gbps, al ser el inmediato superior a la velocidad requerida.

6.3 Velocidad y tipo de puertos de enlace de Up-link para conexión al Backbone

Para calcular la velocidad del puerto de enlace al backbone (up-link), se utilizó dos métodos:

- Método de la fórmula de distribución de Poisson.
- Métodos de las mejores prácticas de diseño de Cisco.

6.4 Método de la fórmula de distribución de Poisson.

Utilizando la fórmula de distribución de Poisson, se calcula la probabilidad de los arribos al puerto de up-link, en función de la siguiente ecuación:

$$Probabilidad\ de\ arribos(r) = P(r) = \frac{e^{-\lambda}(\lambda)^r}{r!}$$

P(r) es la probabilidad de los arribos al puerto de up-link.
r es el número de arribos al puerto up-link
λ es la velocidad promedio de arribos al puerto up-link

Para el caso de un switch de 24 puertos, el número de arribos simultaneos r es 24, la velocidad promedio de arribo es 24 arribos por unidad de tiempo y la probabilidad de arribo al puerto de up-link utilizando la ecuación será:

$$P(24) = \frac{e^{-24}(24)^{24}}{24!} = 0.0811$$

El resultado anterior se utiliza para calcular la velocidad de enlace de up-link del Switch, mediante la ecuación propuesta:

$$vel.de\ puerto\ up-link \geq (\#\ de\ puertos\ del\ switch) * (v.de\ los\ puertos) * P(r)$$

$$vel.de\ puerto\ up-link \geq (24) * (1\ Gbps) * 0.0811 = 1.95\ Gbps$$

De los resultados anteriores, se determina que la velocidad del puerto de up-link utilizando la fórmula de Poisson debe ser mayor a 1.95 Gbps.

6.5 Método de las mejores prácticas de diseño de Cisco.

La mejor práctica de diseño de Cisco para los switches de acceso se basa en los niveles de sobresuscripción de los equipos, que es la cantidad de puertos de usuario final. los valores de sobresuscripción se podrían clasificar de la siguiente manera:

De 1:1 a 20:1, para las redes con un nivel de tráfico bajo.
De 10:1 a 20:1, para redes con un nivel de tráfico medio-bajo, que utilizan la mayor parte del tiempo aplicaciones típicas.
De 4:1 a 12:1, para las redes empresariales, con un nivel de tráfico medio utilizan aplicaciones típicas todo el tiempo y también aplicaciones especiales que requieren de alto ancho de banda
De 5:1 a 10:1, para las redes empresariales con tráfico de servidores virtuales
De 1:1 a 4:1, para las redes de data centers, con nivel de tráfico alto, que utilizan aplicaciones especiales todo el tiempo que requieren de un alto ancho de banda.

En este caso concreto considerando que la red en cuestión es una red empresarial con tráfico medio-bajo para redes con un nivel de tráfico medio-bajo, que utilizan la mayor parte del tiempo aplicaciones típicas necesitaríamos que nuestro nivel de sobresuscripción quedara encuadrado

entre 10:1 y 20:1. Esto conlleva por lo tanto que nuestro enlace de up-link requiere una capacidad de:

$$10 \leq \frac{Número\ total\ de\ puertos\ de\ usuario\ del\ Switch\ de\ acceso * Velocidad\ de\ los\ puertos}{Velocidad\ del\ puerto\ de\ up-link} \leq 20$$

Para un switch de acceso de 24 puertos ethernet de 1 Gbps, considerando que todos sus puertos transmiten a su máxima velocidad de manera simultánea se requiere transmitir a través del puerto up-link un enlace de 48 Gbps.

$$10 \leq \frac{24\ Puertos * 2\ Gbps}{Velocidad\ del\ puerto\ de\ up-link} \leq 20$$

$$10 \leq \frac{48\ Gbps}{Velocidad\ del\ puerto\ de\ up-link} \leq 20$$

$$\frac{48\ Gbps}{20} \leq Velocidad\ del\ puerto\ de\ up-link \leq \frac{48}{10}$$

$$2.4\ Gbps \leq Velocidad\ del\ puerto\ de\ up-link \leq 4.8\ Gbps$$

Para tener un mejor desempeño y capacidad de crecimiento del switch se deben utilizar puerto de enlace Ethernet de 10 Gbps.

- Una interface para la conexión al backbone de 10 Gbps
- Interfaces de conexión entre switches de 10 Gbps