UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO

FACULTAD DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA, INFORMÁTICA Y MECÁNICA

ESCUELA PROFESIONAL DE INGENIERIA ELECTRONICA

ANÁLISIS Y MEJORA DE LA RED DE DATOS DE LA UNSAAC SOBRE LA PLATAFORMA IP-MPLS EN UN BANCO DE PRUEBAS

TESIS FINANCIADA POR LA UNSAAC

Tesis para optar el Título Profesional de Ingeniero Electrónico

Bach: EDISON YUVER MORENO CARDENAS T003_45848264_T

Bach: JOEL LENIN QUISPE VILCA T003_47343721_T

Asesor: ING. FERNANDO TAGLE CARBAJAL

CUSCO – 2017

AGRADECIMIENTO

Dios, tu amor y tu bondad me permiten sonreír antes todos mis logros que son resultado de tu voluntad que es buena, agradable y perfecta.

El amor recibido, la dedicación y la paciencia con la que cada día nuestras familias trabajaron cada avance y desarrollo de esta tesis cual ayuda idónea. A nuestros padres por su motivación constante, a nuestras madres por sus consejos y valores; y a nuestras hermanas, por su comprensión y aliento en momentos difíciles. Cada cual siendo la mejor expresión del amor de familia que se ve reflejado en la vida de un hijo agradecido con Dios.

A mis Pastores, Wilfredo y Jessica que son el instrumento idóneo utilizado por Dios para hacer de mi un verdadero Hombre de Bien y cada nuevo día la mejor versión de mí mismo.

Para llegar a cumplir nuestras metas y acercarse al éxito se requiere estar en el momento adecuado; lugar adecuado: nuestra Universidad, San Antonio Abad del Cusco, nuestra Escuela Profesional: Ingeniería Electrónica; y con las personas adecuadas: cada uno de nuestros docentes, arquetipos de nuestro perfil profesional; nuestros compañeros y mejores amigos.

INTRODUCCIÓN.

En la evolución hacia una red de servicios múltiples se busca optimizar la red conjunta y organizar el tráfico de la mejor forma posible para responder a la congestión y los cambios en el modelo de tráfico. Para ello se hace uso de la ingeniería de tráfico que ha llegado a ser una función indispensable en grandes sistemas basados en IP. Las claves de las prestaciones asociadas a la ingeniería de tráfico son tanto a la orientación del tráfico como la orientación de los recursos. Los objetivos de las prestaciones orientadas al tráfico incluyen aspectos que aumentan la calidad de servicio y el caudal de tráfico.

El crecimiento de internet y la flexibilidad de las redes de conmutación de paquetes contribuyen de forma importante para la convergencia de las redes tradicionales conmutación de circuitos hacia un nuevo concepto de red, con una arquitectura basada en la tecnología IP.

MPLS (Multi Protocol Label Switching) surge como una estrategia significativa para proporcionar ingeniería de tráfico debido a su capacidad de emular la orientación a conexión provista por la tecnología ATM (Modo de transferencia Asíncrona), además de ofrecer escalabilidad, bajo coste y la posibilidad de automatización de varios aspectos de la función de ingeniería de tráfico, como el control de la asignación de calidad de servicio y reserva de ancho de banda en la gestión de alto nivel.

Para alcanzar los objetivos se realizaran una combinación de soluciones de protocolos en enrutamiento dinámico BGP (Border Gateway Protocol), QoS (Calidad de Servicio), simulaciones e implementación de laboratorio en tiempo real para adquirir y demostrar pruebas reales y buscar la mejor alternativa.

RESUMEN

La presente tesis propone el diseño e integración de una red IP-MPLS para la Universidad Nacional San Antonio Abad del Cusco, que atenderá las necesidades requeridas y mejoras en el servicio a los usuarios.
Previo a un estudio, actualmente la UNSAAC posee una red de datos deficiente y brinda una baja calidad en sus servicios, esto debido a la antigüedad del equipamiento, no diferenciar los tráficos o servicios en la red actual y una arquitectura de red que no soporta un escalamiento físico y lógico; el diagnóstico y panorama que se tiene de la red de datos de la UNSAAC nos llevó a proponer un análisis y mejora en la red actual.

Mediante el análisis de la situación actual de los servicios en la UNSAAC y la proyección de la demanda de los mismos, se aplicaron los conocimientos de planificación de redes de telecomunicaciones y comunicaciones ethernet-ópticas para desarrollar la ingeniería del proyecto y mejorar las deficiencias de lentitud y crecimiento de la red, seleccionando la tecnología IP-MPLS y sus diferentes atributos y consideraciones que lo contemplan para la red de transporte, y la propuesta del equipamiento que esta tecnología requiere para implementarse e integrarse a la actual red de datos de la UNSAAC.

Durante el desarrollo de esta tesis se realiza la simulación global de toda la arquitectura de red propuesta en el software GNS3 y una pequeña muestra de simulación con equipos reales; se definen escenarios de redes IP; a los cuales serán sometidos a diversos tráficos; se evaluaran los comportamientos resultantes de la interacción con estos tráficos y se comprobará el funcionamiento de esta alternativa tecnológica para proporcionar QoS, Ingeniería de Tráfico, transmisión óptima de información, uso de recursos de red, entre otras características que son de interés.

Finalmente se realizó el análisis de costo beneficio que permitió determinar el precio de implementar la red propuesta de la presente tesis.

ABSTRACT

This thesis proposes the design and integration of an IP-MPLS network for the National University of San Antonio Abad of Cusco, which will meet the needs and improvements in the service to the users.

Prior to a study, UNSAAC currently has a poor data network and offers a low quality of services, due to the age of the equipment, not to differentiate the traffic or services in the current network and a network architecture that does not support physical and logical scaling; The diagnosis and overview of the UNSAAC data network led us to propose an analysis and improvement in the current network.

Through the analysis of the current situation of the services in the UNSAAC and the projection of the demand of the same ones, the knowledge of planning of networks of telecommunications and ethernet-optical communications was applied to develop the engineering of the project and to improve the deficiencies of slowness And network growth, selecting the IP-MPLS technology and its different attributes and considerations for the transport network, and the proposal of the equipment that this technology requires to be implemented and integrated into the current UNSAAC data network.

During the development of this thesis the global simulation of the entire network architecture proposed in the GNS3 software and a small sample of simulation with real equipment are performed; Define IP network scenarios; To which they will be subjected to various traffic; The behaviors resulting from the interaction with these traffic will be evaluated and the operation of this technological alternative will be verified to provide QoS, Traffic Engineering, optimum transmission of information, use of network resources, among other characteristics that are of interest.

Finally, the cost-benefit analysis was carried out to determine the price of implementing the proposed network of the present thesis.

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

GLOSARIO Y ACRONIMOS

AS: Autonomous System, áreas que en su conjunto modelan a una red y dentro de las cuales las rutas son determinadas por el ruteo intradominio.
ASBRs: Autonomous System Border Routers, Routers fronterizos del AS
ATM: Asynchronous Transfer Mode, Modo de Transferencia Asíncrona.
BACKBONE: Arteria principal o red principal que refiere a las redes de transporte de tráfico.
BGP: Border Gateway Protocol, protocolo de ruteo interdominio.
CEF: Cisco Express Forwarding, Para abordar los problemas asociados al almacenamiento en memoria inmediata de la demanda.
CoS: Class of Service, Clase de Servicio
CPE: Equipo de perímetro del cliente.
DLCI: Data Link Connection Identificator, ejemplo de etiqueta o encabezado que pueden utilizarse como etiqueta de MPLS.
DHCP: Dynamic Host Configuration Protocol, protocolo de configuración dinámica de host.
DiffServ: Differenciated Services, Servicios diferenciados
DNS: Domain Name System, Sistema de Nombre de Dominio
DSCP: DiffServ Code Point, Punto de Código de Servicios Diferenciados
E1: Sistema de transmisión digital de área amplia, utilizado predominantemente en Europa que transporta datos a una velocidad de 2.048 Mbps
EGP: Exterior Gateway Protocol, Protocolo de Pasarela Exterior, es un protocolo que emplea vecinos exteriores para difundir la información de accesibilidad a otros sistemas autónomos.
Frame relay: Frame-mode Bearer Service, técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual
GATEWAY: Puerta de Enlace
GNS3: **Graphical network simulator 3,** Simulador Gráfico de la Red 3.
FEC: Forwarding Equivalence Class, representación de un conjunto de paquetes que comparten los mismos requerimientos para su transporte en MPLS.
ICMP: Internet Control Message Protocol, protocolo de mensajes de control de internet.
IETF: Internet Engineering Task Force, grupo de trabajo dedicado en su mayoría al control del tráfico en lo que a la ingeniería de tráfico se refiere.
IGP: Interior Gateway Protocol, Protocolo de Pasarela Interno
IntServ: Integrated Services, Servicios Integrados
IP: Internet Protocol, Protocolo de Internet.
ISP: Internet Service Provider, proveedor de Servicios de Internet.
ISR G2: Integrate Service Router Generation 2, Router de servicios integrados de segunda generacion.
LAN: Local Area Network, Red de Área Local.
LDP: Label Distribution Protocol, protocolo responsable de que el LSP sea establecido para que sea funcional mediante el intercambio de etiquetas entre los nodos de la red.
LER: Label Edge Router, router encargado de la distribución de etiquetas.
LIB: Label Information Base, tabla de conectividad contra la cual es examinada y comparada la etiqueta MPLS al llegar del LER al LSR, determinando la acción a seguir.

LSE: Link State Algorithm
LSP: Label Switched Paths, ruta que sigue un paquete entre dos nodos de la red MPLS.
LSR: Lable Switch Router, router encargado de dirigir el tráfico dentro de la red MPLS.
MIB: Management Information Base, colección de información organizada jerárquicamente donde los objetos son accedidos usando SNMP y la cual reside en el elemento de red.
MPLS: Multi Protocol Label Switching, tecnología de ruteo y reenvío de paquetes en redes IP que se basa en la asignación e intercambio de etiquetas, que permiten el establecimiento de caminos a través de la red.
OSI: Open System Interconnection, interconexión de sistemas abiertos
OSPF: Open Shortest Path First, Es un protocolo de Encaminamiento jerárquico de pasarela interior o IGP.
PDU: Unidad de Datos de Protocolo de la capa de Red.
PE: Equipo de perímetro.
QoS: Quality of Service, distintos niveles de servicio que son ofrecidos al cliente en términos del ancho de banda o algún otro parámetro.
RFC: Request For Comments, solicitud de comentarios,
RPV: Red Privada virtual.
SDH: Synchronous Digital Hierarchy, Jerarquía Digital Síncrona**.**
SecureCRT 6.1: software que analiza el problema de brindar garantías de Calidad de Servicio (QoS) así como realizar Ingeniería de Tráfico sobre redes de datos.
SLA: Service Level Agreement, acuerdo sobre el nivel de servicio con el cliente donde se especifican parámetros como performance, confiabilidad y seguridad.
TCP/IP: Transmisión Control Protocol / Internet Protocol, Protocolo de Control de Transmision / Protocolo de Internet.
TCP: **Transmisión Control Protocol,** Protocolo de control de transmisión.
TE: Traffic Engineering, disciplina que procura la optimización de la performance de las redes operativas.
TED: Traffic Engineering Especialized Data Base, base de datos contenida en cada router, la cual mantiene atributos de los enlaces de la red e información de la topología.
UDP: User Datagram Protocol, protocolo de transporte que provee servicios de datagramas por encima de IP.
VLAN: Virtual Local Area Network, Área de Red Local Virtual, es una conexión lógica de un grupo de dispositivos que están ubicados en la misma subred, siendo posible la configuración de varias VLAN con un único Switch.
VoIP: Voice of IP, Voz sobre IP, es una tecnología sobre Red privada IP,
VPN: Virtual Private Network, Red Privada Virtual.
WAN: Wide Area Network, Wide Area Network

CAPITULO I

GENERALIDADES

En este capítulo se desarrolla los antecedentes y el planteamiento del problema que dan origen al estudio que se presenta en esta tesis. También se detallan la justificación, objetivos, hipótesis, alcances y limitaciones que soportan la realización del presente estudio.

(1.1.) Planteamiento del problema.

Se realizó en nuestro escenario Campus Perayoc – Ciudad Universitaria de la "UNIVERSIDAD NACIONAL SAN ANTONIO ABAD DEL CUSCO"; el diagnóstico siguiente:
La red de datos es deficiente y brinda una baja calidad de servicio; esto es debido a que la actual arquitectura de red de datos de la UNSAAC, adolece de congestión de tráfico de datos, perdida de flujos de información en la red, baja velocidad de transmisión de datos para los usuarios, repuestos inexistentes del data center de la UNSAAC en el mercado, entre otros, siendo los más resaltantes los mencionados líneas arriba; que están relacionados y se explican por la antigüedad de equipos y diseño actual de la red de datos. También que la actualidad de la red de datos de la UNSAAC es una red subneteada (red subdividida), que solo trabaja en capa 2 del modelo TCP/IP, además esta red tiene una configuración sin distinción de tráfico y fiabilidad de entrega de información.
Los cuales traen consecuencias como: una degradación e intermitencia en el servicio, duplicidad de IPs o conflicto de IPs esto ocurre cuando dos o más usuarios acceden al mismo tiempo a la red con la misma IP asignada manualmente, requerimiento en el cambio de todo el cableado estructurado a una categoría superior debido al ancho de banda actual que son 150 Mbps.

(1.1.1.) Justificación de la investigación.

El previo estudio y panorama que se tiene de la red de datos de la UNSAAC nos lleva a proponer un análisis y mejora en la red, donde se justifica el porqué:

- Al haber realizado el diagnóstico de la infraestructura de la red de datos de la UNSAAC se concluyó que esta red es deficiente y brinda una baja calidad de servicio razón por la cual se propone la red MPLS por sus diferentes características: Redes privadas virtuales, Ingeniería de tráfico, Soporte de Calidad de Servicio (QoS), Soporte multiprotocolo, Establecimiento de Clases de Servicio (CoS), mecanismos de protección frente a fallos, redundancia y más.
- La red IP-MPLS que proponemos permitirá brindar a los sistemas y usuarios una mejor calidad de servicio gracias a un transporte de tráfico óptimo.
- Actualmente se tiene configurado una red de datos LAN subneteada, esta red es básica frente a BGP que es el protocolo de enrutamiento dinámico más completo y óptimo para una red de la actualidad**.**
- Crecimiento del ancho de banda (BW), y el cambio de la red física de datos
- La antigüedad de equipos instalados en el Data Center, por ejemplo los componentes físicos del Core Alcatel ya no cuenta con reemplazo en el mercado.

- El conflicto de IPs genera problemas en el acceso a la red a los usuarios y problemas al administrador de la red.
- La red IP-MPLS que proponemos permitirá reducir algunos costos de operación.
- La red que proponemos utilizará tecnología disponible actual en el mercado y desarrollada lo suficiente para cumplir los objetivos.

(1.2.) Objetivos de la investigación

(1.2.1.) Objetivo general

Analizar y proponer la red IP-MPLS para mejorar la red de datos en la UNSAAC, que permita ofrecer diferentes niveles de servicio en un entorno de mayor fiabilidad y el transporte de un tráfico óptimo.

(1.2.2.) Objetivo específico

- Mejorar la arquitectura de la red en la UNSAAC, para que soporte un ancho de banda mínimo de 150 Mbps, y un crecimiento en el futuro en este BW (Ancho de Banda).
- Proponer el equipamiento necesario a nivel de las capas: físico, enlace de datos, red y transporte del modelo OSI.
- Realizar un laboratorio experimental de la simulación de la red IP-MPLS propuesta con routers y switches en tiempo real y obtener un banco de pruebas.
- Medir e interpretar los parámetros de configuración de MPLS, BGP, Ingeniería de tráfico, calidad de servicio (QoS), en los routers de prueba para la correcta distribución de los diferentes tipos de tráficos de la UNSAAC.
- Realizar un estudio de costo beneficio de la implementación de este proyecto.

(1.3.) Hipótesis

El transporte de cualquier tipo de información de una plataforma única, adecuada y convergente MPLS, nos permitirá transmitir voz, video, datos críticos, datos transaccionales y datos generales estableciendo niveles de Clases de Servicio (CoS) diferenciadas, asignándole la prioridad adecuada para aplicaciones de datos, voz y video con sus diferentes atributos y protocolos que la contienen enfocadas a la red de datos de la UNSAAC.

También una red IP-MPLS nos beneficiará con un envío rápido de información y fiabilidad de entrega: BGP que es un protocolo extremadamente complejo cuya función no es encontrar una red específica, sino proporcionar información que permita encontrar el AS (Sistema Autónomo) de dicha red, asegurando ninguna pérdida de paquetes y calidad de servicio para los usuarios.

(1.4.) Variables

Las variables relacionadas al desarrollo de la tesis son:

(1.4.1.) Variables dependientes.

Tasa de transmisión de las clases de servicio. (CoS1, CoS2 y CoS3)
Latencia en las clases de servicio.

(1.4.1.1.) Indicadores

Velocidad de transmisión.
Tiempo de respuesta.

(1.4.2.) Variables independientes

Ancho de banda de la UNSAAC.
Tipos de servicio.

(1.5.) Metodología

Esta metodología consiste en proponer una mejora en el manejo y transporte de a partir del análisis y diagnóstico de la red actual de datos de la UNSAAC y de cada componente involucrado.

Con el propósito de garantizar el confiable y óptimo transporte de los diferentes niveles de tráfico de la red de datos de la UNSAAC se pueden asumir los requerimientos, importancia y evolución de las variables de interés como son el ancho de banda congestión del tráfico, tiempo de transmisión, velocidad de transmisión, rendimiento, control de errores, eliminación de paquetes, cantidad usuarios entre otros que se predecirán en el desarrollo de la tesis y luego confrontar que los resultados obtenidos demuestren una mejora sobre la red actual de datos de la UNSAAC.

Para lograr estas especificaciones la primera etapa es el estudio de la arquitectura MPLS (Multi Protocol Label Switching) diferentes propuestas para hacer ingeniería de tráfico y el problema de la calidad de servicio en IP. Luego realizar es análisis de los protocolos y atributos del enrutamiento dinamico BGP y optar los más adecuados para la red de datos de la UNSAAC, también se tiene que simular usando varios software y proponer el más adecuado diseño de red de datos; sin embargo, es altamente costoso implementar y adquirir todos los equipos, entonces los resultados y banco de pruebas reales se obtendrán con la implementación y adquisición de dos a tres routers y simulación con el software GNS3 para complementar y así demostrar el funcionamiento de calidad de servicio referente a los diferentes tipos de tráfico así mismo utilizar el enrutamiento dinámico BGP (Border Gateway Protocol) con las ventajas y efectividad de los protocolos y atributos que posee.

(1.6.) Alcances y Delimitaciones.

Las delimitaciones que se presentan para el desarrollo de la tesis ANÁLISIS Y MEJORA DE LA RED DE DATOS DE LA UNSAAC SOBRE LA PLATAFORMA IP-MPLS EN UN BANCO DE PRUEBAS es que solo se realizara netamente en el Campus Perayoc de la UNSAAC. Es decir que el estudio se delimita a la sede principal, y dar un somero estudio y alcances de las sedes remotas para interconectar y dar el servicio del ancho de banda que contara la UNSAAC.

La tesis se realizara a nivel de simulación con GNS3, más no la implementación ni ejecución de la misma.

Para obtención de una base de datos a tiempo real se utilizara 5 Routers y se realizará un laboratorio.

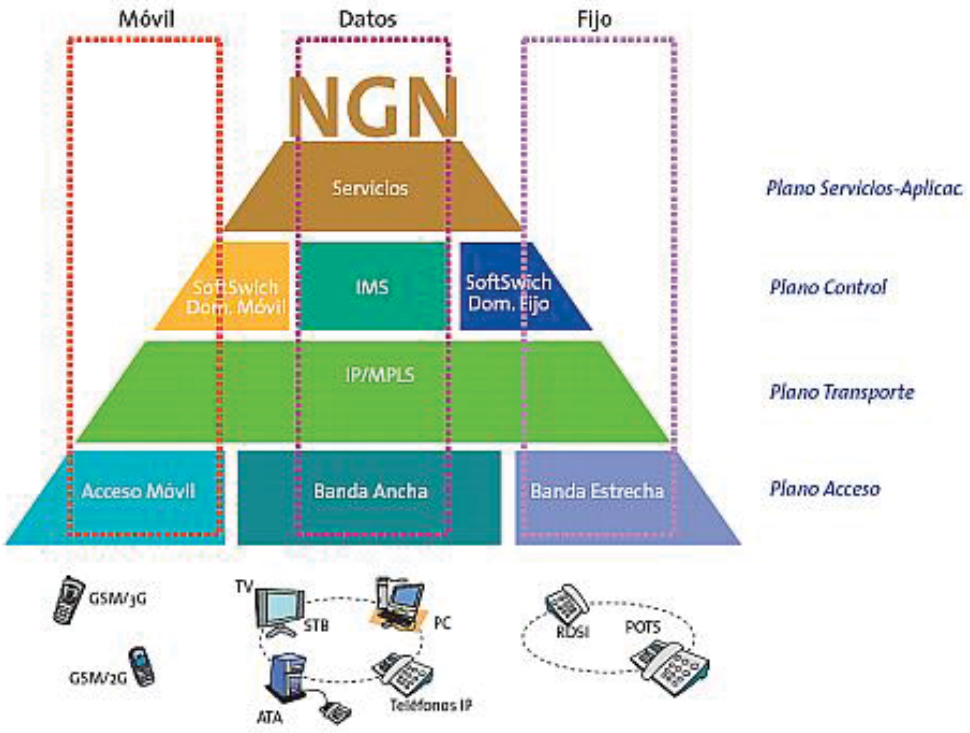
CAPITULO II

MARCO TEÓRICO

El marco teórico constituye el sustento teórico de este estudio y diseño. Como planteamientos teóricos, hemos seleccionado a los conceptos básicos relacionados a las redes de telecomunicaciones. Además, otro propósito es contribuir a la literatura existente conceptos en tecnología de redes de telecomunicaciones actuales.
Entre estos conceptos básicos, hemos seleccionado; y, priorizándolos, presentamos los siguientes

(2.1.) Redes de nueva generación

Es un amplio término que se refiere a la evolución de la actual infraestructura de redes de telecomunicación y acceso telefónico con el objetivo de lograr la convergencia tecnológica de los nuevos servicios multimedia (voz, datos, video). Es una red basada en la transmisión de paquetes capaz de proveer servicios integrados, incluyendo los tradicionales telefónicos, y capaz de explotar al máximo el ancho de banda del canal haciendo uso de las Tecnologías de Calidad del Servicio (QoS) de modo que el transporte sea totalmente independiente de la infraestructura de red utilizada. Las Redes de Siguiente Generación están basadas en



tecnologías Internet incluyendo el protocolo IP y el MPLS.[1]

Fig. 2.1. Red de la nueva generación.

[1] DIVISIÓN DE LA ITU-T PARA LAS REDES DE SIGUIENTE GENERACIÓN (FGNGN)

(2.2.) Internet.

Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.
Internet aporta o soporta una serie de instrumentos para que la gente difunda y acceda a documentos y a la información para que los individuos se relacionen a través de una serie de medios de comunicación (correo electrónico, webs, listas de distribución, videoconferencia, chats...) o más o menos viejos (como una conversación telefónica, poner un fax, etc.,)[2]

(2.3.) Intranet.

Es una red informática que utiliza la tecnología del Protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización. A veces, el término se refiere únicamente a la organización interna del sitio web, pero puede ser una parte más extensa de la infraestructura de tecnología de la información de la organización, y puede estar compuesta de varias redes de área local. El objetivo es organizar el escritorio de cada individuo con mínimo costo, tiempo y esfuerzo para ser más productivo, rentable, oportuno, seguro y competitivo.[3]

(2.3.1.) Tipos de intranet.

El parámetro utilizado para su clasificación desde una perspectiva tecnológica, es la capacidad que se le atribuye para ingresar, modificar y consultar datos dentro del sistema y se mencionan las siguientes:

(2.3.1.1.) Pasiva

Son interactivas pero no dinámicas, esto quiere decir, que no permiten el acceso a los datos de origen y sólo permiten desplegar información estática en la pantalla.

(2.3.1.2.) Activas

Son interactivas y dinámicas, ya que permiten acceso e interacción con los datos por parte del usuario o cliente, tienen herramientas de trabajo colaborativo y múltiples funcionalidades.

(2.3.2.) Requisitos para una intranet

Hardware: El equipamiento básico indispensable para instalar una intranet es: Servidor de Web, Conexión a red de datos, Equipos clientes.
Software: Éste debe definir: Sistema operativo de los servidores y de los clientes: es necesario distinguir dos tipos de sistemas operativos: el del sistema administrador de red y el del sistema cliente

---

[2] Internet: claves de redacción. Fundeu. Consultado el 30 de marzo de 2016.
[3] *Tesis.uson.mx/digital/tesis/docs/10025/Capitulo3.pdf*

(2.3.2.1.) Beneficiarios

A la institución o empresa porque optimiza sus recursos humanos y materiales al ahorrar tiempo y dinero en capacitación, soporte o apoyo técnico y adquisición periférica de software y hardware.

(2.4.) Extranet.

Una extranet es una red privada que utiliza protocolos de Internet, protocolos de comunicación y probablemente infraestructura pública de comunicación para compartir de forma segura parte de la información u operación propia de una organización con proveedores, compradores, socios clientes o cualquier otro negocio u organización.
Es una red que tiene acceso limitado y que está disponible únicamente a usuarios específicos, tales como clientes o proveedores.
Con el tiempo, las compañías se verán forzadas a usar Extranet con sus proveedores y clientes, ya que hoy en día, existen organizaciones que no hacen negociaciones con empresas que no tienen un servicio **seguro** de Extranet. [4]
Es muy importante aclarar que para que una empresa pueda aprovechar los beneficios que conlleva el uso de Extranet, es necesario que las empresas ya cuenten con un Intranet funcionando en su totalidad.

(2.4.1.) Diferencias entre internet intranet y extranet

Las diferencias de la extranet con Internet y la Intranet se dan principalmente en el tipo de información y en el acceso a ella. La extranet se dirige a usuarios tanto de la empresa como externos, pero la información que se encuentra en la extranet es restringida, solo tienen acceso a esta red aquellos que tengan permiso.[5] En cambio a la intranet solo acceden los empleados y las áreas internas de la empresa y permite el intercambio de información entre los trabajadores. Por último, a la Internet puede dirigirse cualquier usuario y tiene distintos usos, como recabar información de los productos, contactar con cualquier persona de la empresa, etc.

Fig. 2.2. Intranet, Extranet e Internet.[6]

[4] Castells, M.: La galaxia Internet – Reflexiones sobre Internet, empresa y sociedad. Barcelona (Plaza & Janés), 2001
[5] https://anagam87.wordpress.com/2009/12/30/diferencias-entre-internet-intranet-y-extranet/
[6] *https://sistemasinfojave.wikispaces.com/file/view/Contenido+8A-Intranet.ppt*

(2.5.) Enrutamiento.

Es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad. Dado que se trata de encontrar la mejor ruta posible, lo primero será definir qué se entiende por mejor ruta y en consecuencia cuál es la métrica que se debe utilizar para medirla.[7]

(2.5.1.) Métrica de la red.

Es un valor que toman los diferentes protocolos de enrutamiento para poder determinar cuál es la mejor ruta hacia una red de destino. No es difícil encontrarse con situaciones donde un router tenga más de un único camino hacia una red de destino y, por lo tanto, deberá emplear algún método para determinar cuál de esos caminos le conviene más. Esto va a depender de cual sea el protocolo de enrutamiento que se esté utilizando, ya que cada uno usa una métrica diferente.

(2.5.2.) Mejor ruta

El criterio más sencillo es elegir el camino más corto, es decir la ruta que pasa por el menor número de nodos. Una generalización de este criterio es el de "coste mínimo". En general, el concepto de distancia o coste de un canal es una medida de la calidad del enlace basado en la métrica que se haya definido.
Entendemos por mejor ruta aquella que cumple las siguientes condiciones: [8]

(2.5.3.) Clasificación de los métodos de encaminamiento.

Los algoritmos de encaminamiento pueden agruparse en:

(2.5.3.1.) Determinísticos o estáticos.

No tienen en cuenta el estado de la subred al tomar las decisiones de encaminamiento. Las tablas de encaminamiento de los nodos se configuran de forma manual y permanecen inalterables hasta que no se vuelve a actuar sobre ellas. Por tanto, la adaptación en tiempo real a los cambios de las condiciones de la red es nula. Estos algoritmos son rígidos, rápidos y de diseño simple, sin embargo son los que peores decisiones toman en general.

(2.5.3.2.) Adaptativos o dinámicos.

El encaminamiento dinámico o adaptativo pueden hacer más tolerantes a cambios en la subred tales como variaciones en el tráfico, incremento del retardo o fallas en la topología.

(2.5.4.) Encaminamiento adaptativo con algoritmos distribuidos.

---

[7] RFC0974-es - **Encaminamiento y el sistema de dominios**
[8] *http://es.wikipedia.org/wiki*

El encaminamiento mediante algoritmos distribuidos constituye el prototipo de modelo de encaminamiento adaptativo. Los algoritmos se ejecutan en los nodos de la red con los últimos datos que han recibido sobre su estado y convergen rápidamente optimizando sus nuevas rutas. [9]
Existen dos tipos principales de algoritmos de encaminamiento adaptativo distribuido.

(2.5.4.1.) Algoritmos por "vector de distancias".

Estos métodos utilizan el algoritmo de Bellman-Ford. Busca la ruta de menor coste por el método de búsqueda indirecta El vector de distancias asociado al nodo de una red, es un paquete de control que contiene la distancia a los nodos de la red conocidos hasta el momento. Ejemplos: RIP (versión 1 y 2), IGRP.

(2.5.4.2.) Algoritmos de "estado de enlace".

Se basa en que cada nodo llegue a conocer la topología de la red y los costes (retardos) asociados a los enlaces, para que a partir de estos datos, pueda obtener el árbol y la tabla de encaminamiento tras aplicar el algoritmo de coste mínimo (algoritmo de Dijkstra) algrafo de la red. Ejemplos: OSPF e IS-IS.[10]

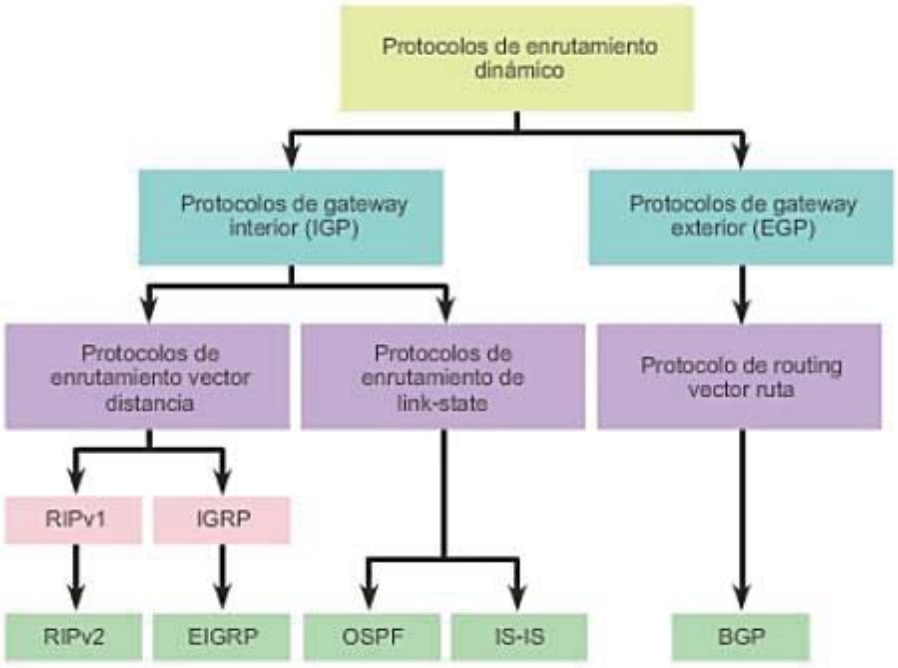


Fig. 2.3 Clasificación de los Protocolos de enrutamiento dinámico.[11]

[9] RFC 1753 The recommendation for the IP next generation protocol
[10] RFC 1583 OSPF Version 2
[11] RFC 904 Exterior Gateway Protocol Formal Specification

(2.5.5.) Protocolos de encaminamiento y sistemas autónomos.

Un sistema autónomo (AS) se trata de un conjunto de redes IP y routers que se encuentran bajo el control de una misma entidad (en ocasiones varias) y que poseen una política de encaminamiento similar a Internet.[12] Dependiendo de la relación de un router con un sistema autónomo (AS), encontramos diferentes clasificaciones de protocolos:

(2.5.5.1.) IGPs - Interior Gateway Protocols.

IGPs (Interior Gateway Protocols). Intercambian información de encaminamiento dentro de un único sistema autónomo. Los ejemplos más comunes son:[13]

- IGRP (Interior Gateway Routing Protocol). La diferencia con la RIP es la métrica de enrutamiento
- EIGRP (Enhanced Interior Gateway Routing Protocol). Es un protocolo de enrutamiento vector-distancia y estado de enlace
- OSPF (Open Shortest Path First). Enrutamiento jerárquico de pasarela interior
- RIPv2 (Routing Information Protocol). No soporta conceptos de sistemas autónomos
- IS-IS (Intermediate System to Intermediate System). Protocolo de intercambio enrutador de sistema intermedio a sistema intermedio

(2.5.5.2.) EGPs - Exterior Gateway Protocol.

EGPs - Exterior Gateway Protocol. Intercambian rutas entre diferentes sistemas autónomos. Encontramos:[14]

- EGP. Utilizado para conectar la red de backbones de la Antigua Internet.
- BGP (Border Gateway Protocol). La actual versión, BGPv4 data de 1995.

Fig. 2.4 Protocolo de Gateway Interior y Exterior.[15]

[12] RFC 6996 - Autonomous System (AS)
[13] RFC 3906 - CALCULATING INTERIOR GATEWAY PROTOCOL
[14] RFC 827 - EXTERIOR GATEWAY PROTOCOL (EGP)
[15] CCNA1 R&S v5.0 PDF.

(2.6.) OSPF.

OSPF son las siglas de Open Shortest Path First (El camino más corto primero), un protocolo que usa el algoritmo SmoothWall Dijkstra enlace-estado (LSE - Link State Algorithm) para calcular la ruta más idónea.
Su medida de métrica se denomina coste, y tiene en cuenta diversos parámetros tales como el ancho de banda y la congestión de los enlaces. OSPF construye además una base de datos enlace-estado (link-state database, LSDB) idéntica en todos los routers de la zona.

OSPF puede operar con seguridad usando MD5 (abreviatura de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) para autenticar sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado.
OSPF acepta VLSM y CIDR desde su inicio.
Una red OSPF se puede descomponer en regiones (áreas) más pequeñas. Hay un área especial llamada área backbone que forma la parte central de la red a la que se encuentran conectadas el resto de áreas de la misma. Las rutas entre las diferentes áreas circulan siempre por el backbone, por lo tanto todas las áreas deben conectar con el backbone. Si no es posible hacer una conexión directa con el backbone, se puede hacer un enlace virtual entre redes.[16]
Los routers en el mismo dominio de multidifusión o en el extremo de un enlace punto-a-punto forman enlaces cuando se descubren los unos a los otros. En un segmento de red Ethernet los routers eligen a un router designado (Designated Router, DR) y un router designado secundario o de copia (Backup Designated Router, BDR) que actúan como hubs para reducir el tráfico entre los diferentes routers. OSPF puede usar tanto multidifusiones como unidifusiones para enviar paquetes de bienvenida y actualizaciones de enlace-estado.

Tipo	Nombre del paquete	Descripción
1	Saludo	Descubre los vecinos y construye adyacencias entre ellos
2	Descripción de la base de datos (DBD)	Controla la sincronización de la base de datos entre routers
3	Solicitud de estado de enlace (LSR)	Solicita registros específicos de estado de enlace de router a router
4	Actualización de estado de enlace (LSU)	Envía los registros de estado de enlace específicamente solicitados
5	Acuse de recibo de estado de enlace (LSAck)	Reconoce los demás tipos de paquetes

Fig. 2.5 Tipos de paquetes OSPF.[17]

[16] RFC 1583 OSPF Version 2
[17] RFC 1245 OSPF Protocol Analysis

(2.6.1.) Tráfico de encaminamiento.

(2.6.1.1.) Diferencia administrativa.

La distancia administrativa (AD) es la confiabilidad (o preferencia) del origen de la ruta. OSPF tiene una distancia administrativa predeterminada de 110 como se muestra en la figura.

Origen de la ruta	Distancia administrativa
Conectado	0
Estático	1
Ruta de resumen de EIGRP	5
BGP externo	20
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externo	170
BGP interno	200

Fig. 2.6 Distancias administrativas predeterminadas. [18]

(2.6.1.2.) Autenticación

Esto garantiza que los routers sólo aceptarán información de enrutamiento de otros routers que estén configurados con la misma contraseña o información de autenticación. RIPv2, EIGRP, OSPF, ISIS y BGP pueden configurarse para encriptar y autenticar su información de enrutamiento.

(2.6.1.3.) Métrica del OSPF.

La métrica del OSPF se denomina costo. En RFC 2328: "Un costo se asocia con el resultado de cada interfaz de router. Dicho costo está configurado por el administrador del sistema. Cuanto más bajo sea el costo, más probabilidad hay de que la interfaz sea utilizada para enviar tráfico de datos."[19]

(2.6.2.) Encaminamiento, routers y áreas

OSPF organiza un sistema autónomo (AS) en áreas. Estas áreas son grupos lógicos de routers cuya información se puede resumir para el resto de la red. Un área es una unidad de encaminamiento, es decir, todos los routers de la misma área mantienen la misma información topológica en su base de datos de estado-enlace (Link State Database): de esta forma, los cambios en una parte de la red no tienen por qué afectar a toda ella, y buena parte del tráfico puede ser "parcelado" en su área.[20]

[18] RFC 1245 OSPF Protocol Analysis
[19] OSPF Version 2 (RFC 2328)
[20] RFC 1246 Experience with the OSPF Protocol

(2.7.) BGP

BGP (**B**order **G**ateway **P**rotocol) es un protocolo mediante el cual se intercambia información de encaminamiento o ruteo entre sistemas autónomos.
Entre los sistemas autónomos de los ISP se intercambian sus tablas de rutas a través del protocolo BGP. Este intercambio de información de encaminamiento se hace entre los routers externos de cada sistema autónomo, los cuales deben soportar BGP. Se trata del protocolo más utilizado para redes con intención de configurar un Exterior Gateway Protocol.
La forma de configurar y delimitar la información que contiene e intercambia el protocolo BGP es creando lo que se conoce como sistema autónomo. Cada sistema autónomo (AS) tendrá conexiones o, mejor dicho, sesiones internas (iBGP) y además sesiones externas (eBGP).
El protocolo de gateway fronterizo (BGP) es un ejemplo de protocolo de gateway exterior (EGP). BGP intercambia información de encaminamiento entre sistemas autónomos a la vez que garantiza una elección de rutas libres de bucles. Es el protocolo principal de publicación de rutas utilizado por las compañías más importantes de ISP en Internet. BGP toma decisiones de encaminamiento basándose en políticas de la red, o reglas que utilizan varios atributos de ruta BGP[21].

BGP realiza tres tipos de Ruteo:

- Ruteo Interautónomo
- Ruteo Intrautónomo
- Ruteo de pasc.

(2.7.1.) Relaciones entre AS.

Las relaciones que existen entre distintos sistemas autónomos son principalmente de peering y de tránsito. Las relaciones de peering consisten en un enlace para comunicar dos sistemas autónomos con el fin de reducir costes, latencia, pérdida de paquetes y obtener caminos redundantes.
Un escenario que se suele repetir es uno llamado "Multihoming". Este término hace referencia a un cliente que contrata a dos proveedores de tránsito, lo que implica que existen dos rutas de salida, de modo que se deberá decidir entre un camino u otro dependiendo de ciertas especificaciones, necesidades o simples políticas que se impongan en el sistema autónomo. Un ejemplo se puede ver en la figura prestando atención al Cliente A. Las especificaciones pueden ser para balancear el tráfico, para poner un enlace como preferido antes que otro (por ejemplo porque tenga más velocidad), por tolerancia a fallos, etc. El manejo de estas prioridades es lo que se llama ingeniería de tráfico y se consigue gracias a los atributos BGP que se definen en el protocolo.[22]

[21] RFC 1771 A border Gateway Protocol 4 (BGP–4
[22] RFC 1773 Experience with the BGP-4 Protocol

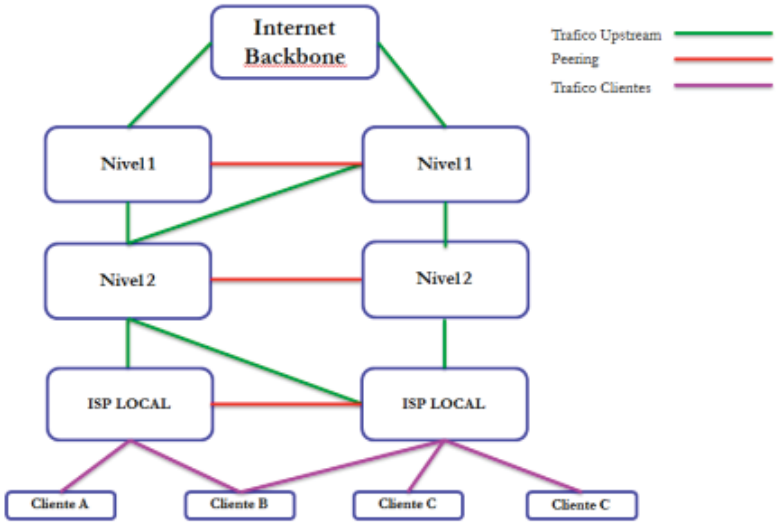


Fig. 2.7 Prestación de atención al Cliente A.[23]

(2.7.2.) Tipos de mensajes.

Existen cuatro tipos de mensajes BGP que son los siguientes:

OPEN: Se utiliza para el establecimiento de una sesión BGP una vez haya sido establecida la conexión TCP. Se suelen negociar ciertos parámetros que caractericen a esa sesión.
UPDATE: Es un mensaje de actualización, es un mensaje clave en las operaciones de BGP ya que contiene los anuncios de nuevos prefijos.
KEEPALIVE: Una vez que la sesión BGP está activa se envía periódicamente un mensaje KEEPALIVE para confirmar que el otro extremo sigue estando activo en la sesión BGP. Generalmente se acuerda un tiempo máximo de espera (hold time) durante el intercambio inicial de mensajes OPEN.
NOTIFICATION: Se envía al cerrar una sesión BGP y esto sucede cuando ocurre algún error que requiera el cierre de la misma. [24]

(2.8.) MPLS.

MPLS (Multiprotocol Label Switching) es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para **unificar el servicio de transporte de datos** para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.
MPLS está reemplazando rápidamente Frame Relay y ATM como la tecnología preferida para llevar datos de alta velocidad y voz digital en una sola conexión. MPLS no sólo proporciona una mayor fiabilidad y un mayor rendimiento, sino que a menudo puede reducir los costos generales mediante una mayor eficiencia de la red. Su capacidad para dar prioridad a los

[23] *www.cisco.com/cisco/web/support/LA/7/76/76167_bgp-toc.html*
[24] RFC 1772 Application of the Border Gateway Protocol in the Internet

paquetes que transportan tráfico de voz hace que sea la solución perfecta para llevar las llamadas VoIP.[25]

En resumen los objetivos establecidos por este grupo IETF en la elaboración del estándar eran:

- MPLS debía de funcionar sobre cualquier tecnología de transporte.
- MPLS debía de soportar el envío de paquetes tanto bajo demanda unidifusión (unicast) como multidifusión (multicast).
- MPLS debía de ser compatible con el modelo de servicios integrados de IETF, incluyendo protocolos RSVP
- MPLS debía permitir el crecimiento constante del internet.
- MPLS debía de ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

(2.8.1.) Conceptos básicos en la conmutación de etiquetas.

Antes de explicar cómo trabajo una red MPLS, deben ser aclarados varios conceptos básicos que aplican para cualquier tecnología de conmutación. A saber:

a) **Conmutación de etiqueta.** Describe la tecnología genérica que combina las tecnologías de capa 2 (capa de enlace de datos) y capa 3 (capa de red). La solución de conmutación de etiquetas puede caracterizarse por el uso de envío de paquetes con etiquetas intercambiadas combinada con los protocolos de control de IP y un mecanismo de distribución de etiqueta.
b) **Una etiqueta (label)** es un identificador relativamente corto, de longitud compuesta y no estructurado que puede ser usado en el proceso de envío. Las etiquetas están asociadas con un FEC a través de un proceso de ordenamiento (binding).
c) **Camino de etiqueta conmutada** (LSP – Label Switching Path) sobre el cual ocurre la transmisión de datos. Los RSS son una secuencia de etiquetas a lo largo de cada uno de los nodos en el camino de la fuente al destino. Los LSPs se establecen bien sea por prioridad en la trasmisión de datos (control de envío) o por detección de cierto flujo de datos (envío de datos).
d) **Dominio MPLS**. Es una porción de una red que contiene dispositivos que entienden MPLS.
e) **El enrutador de etiquetas de frontera** (LER – Label Edge Router). Es un dispositivo que opera en los límites de acceso de la red y dentro de un dominio MPLS. Y permite utilizar la información de enrutamiento para asignar etiquetas a datagramas y entonces enviarlos a un dominio MPLS.
f) **El enrutador de etiqueta conmutada** (LSR – Label Switching Router) es un dispositivo de alta velocidad que posee el componente de control IP y un componente de envío de etiquetas intercambiadas y que típicamente reside en el medio de una red y es capaz de enviar datagramas basados en etiquetas. Los LSRs de los extremos o límites de la red añaden o eliminan etiquetas.

[25] RFC 3031 Multiprotocol Label Switching Architecture

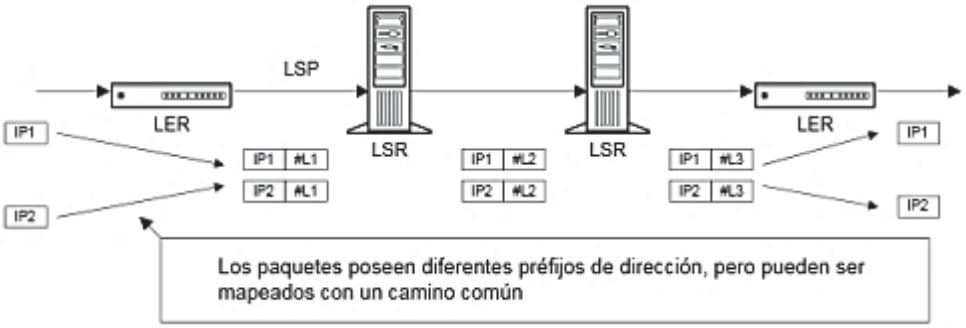


Fig. 2.8 Ilustración de funcionamiento de la clase de equivalencia de envío.[26]

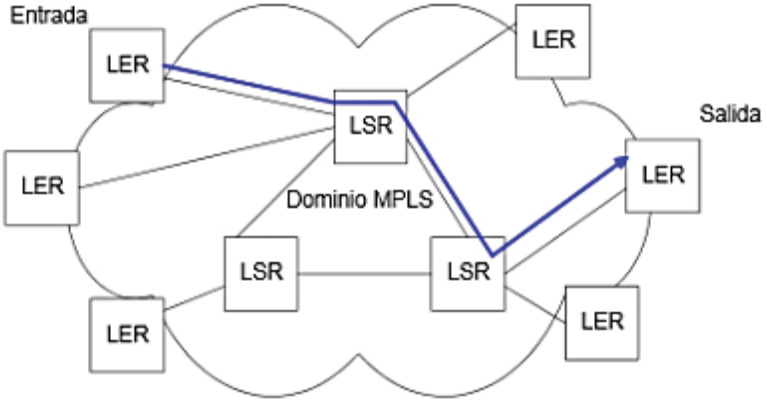


Fig. 2.9 Diferentes conceptos dentro de una red MPLS.[27]

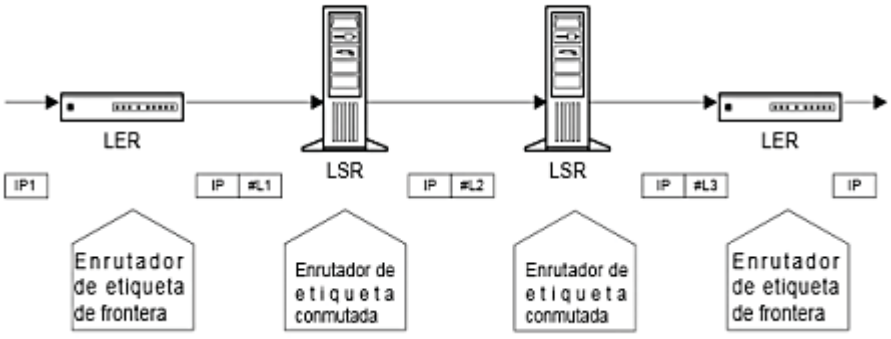


Fig. 2.10 Etiquetado en la frontera, intercambio en el medio.[28]

[26] RFC 3036 LDP Specification
[27] RFC 4206 - Label Switched Paths (LSP)
[28] JAVIER IGOR DOMÉNICO Y LUNA VICTORIA GARCÍA, Medición y Análisis de Tráfico En Redes MPLS, Tesis de Grado, 2007

(2.8.2.) Aplicaciones de MPLS.

Las principales aplicaciones que hoy en día tiene MPLS son:

- Ingeniería de trafico
- Diferenciación de niveles de servicio mediante clases (CoS)
- Servicio de redes privadas virtuales (VPN)

A continuación serán tratadas brevemente las características de estas aplicaciones y las ventajas que MPLS supone para ello frente a otras soluciones.[29]

(2.8.2.1.) Ingeniería de tráfico.

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. Esto es equilibrar de forma óptima la utilización de esos recursos, evitando que un subconjunto (enlaces, equipos, etc.) de la red se sature mientras otro subconjunto de la misma se encuentra infrautilizado, evitando así posibles cuellos de botella y mejorando el rendimiento de la red global.[30]

MPLS es una herramienta efectiva para esta aplicación en grandes redes, ya que:

- El administrador de red puede establecer rutas específicas por LSRs concretos, especificado el camino físico exacto de un LSP.
- Permite obtener estadísticas de uso de cada LSP en detalle, es decir, cuanto tráfico se cursa y de qué tipo. Con esta información, se puede replanificar la red de forma que ofrezca un uso más eficiente de los recursos, lo que resulta bastante útil en planes de expansión futura.
- Permite hacer Encaminamiento Restringido (CBR – Constrain-Based Routing), de modo que se puede seleccionar rutas específicas para transportar el tráfico de un tipo en concreto con unos requerimientos específicos.

La ventaja de la Ingeniería de Trafico MPLS es que se **puede aplicar** directamente sobre **una red IP**, independientemente de **la infraestructura que le de soporte**, con un mayor nivel de detalle y de forma más sencilla y eficiente que como se venía haciendo hasta el momento.[31]

[29] RFC 5921 - A Framework for MPLS in Transport Networks
[30] RFC 2702 - Requirements for Traffic Engineering Over MPLS
[31] *catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/capitulo2.pdf*

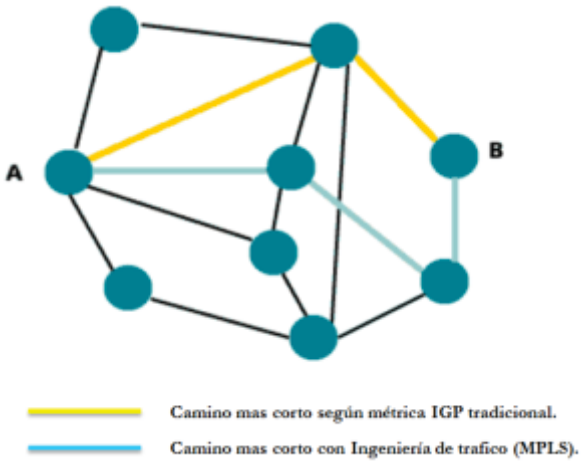


Fig. 2.11 Ingeniería de tráfico MPLS vs. IGP tradicional.[32]

(2.8.2.2.) Clases de servicio - CoS

La filosofía de una red orientada a ofrecer Calidad de Servicio (QoS) en la agrupación de los distintos Tipos de Trafico en un cierto número de Clases de Servicio, con diferentes prioridades. Los paquetes pertenecientes a una misma Clase de Servicio tienen en común los mismos requerimientos de tratamiento en cuanto a ancho de banda necesario, retardo, variación de retardo, jitter, y pérdidas de paquetes, es decir, Calidad de Servicio (QoS).[33]

(2.8.2.2.1.) Servicios integrados

IntServ (Integrated Services): apoyándose en RSVP, se reservan los recursos necesarios asociándose a LSPs concretos.[34]

(2.8.2.2.2.) Servicios diferenciados

DiffServ (Differenciated Services): orientado al tráfico IP, basa su funcionamiento en la clasificación del tráfico a la entrada de la red y en la asociación de prioridades a estos tipos de tráfico mediante el Campo de 8 bits DSCP (DiffServ Code Point), campo ToS (Type os Service) en IPv4 y Clase de Servicio de IPv6. Este modelo definió una variedad de mecanismos para poder clasificar el tráfico de un reducido número de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como WWW, el correo electrónico o la transferencia de ficheros, otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de video y voz interactiva. Para ello se emplea el campo ToS (Type of Service), rebautizado en DiffServ como el octeto DS. Esta es la técnica QoS de marcar los paquetes que se envían a la red.[35]

---

[32] RFC 4105 - Requirements for Inter-Area MPLS Traffic Engineering
[33] RFC 3270 - MPLS Support of Differentiated Services
[34] RFC 1633 - Integrated Services in the Internet Architecture
[35] RFC 2475 - An Architecture for Differentiated Services

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen en el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP. De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que:

- El tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP.
- Entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda.

(2.8.2.3.) Redes privadas virtuales - VPN.

Una red privada virtual (VPN – Virtual Private Network) está orientada a proporcionar conectividad a un cliente sobre una infraestructura compartida, con las funcionalidades de red y seguridad equivalente a las de una red privada, integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento y el término privada indica que el usuario cree que posee los enlaces. Las IP VPNs son soluciones de comunicación VPN basada en los protocolo de red IP de la internet. En esta sección se va a describir brevemente las ventajas que MPLS ofrece para este tipo de redes frente a otras soluciones tradicionales.[36]

Las principales características de una VPN son:

- **Escalabilidad:** Es capaz de asumir cambios de conectividad y capacidad de forma muy ágil. MPLS ofrece conectividad (todos-con-todos), lo que la convierte en una red realmente flexible con unos requerimientos de configuración mínimos a la hora de añadir de nuevo extremo a la VPN, pues solo hay que configurar de nuevo extremo, sin tener que tocar la configuración del resto de extremos.[37]

- **Seguridad**: Asegura que el tráfico de cada cliente es confidencial, ningún usuario ajeno a la VPN debe ser capaz de acceder a la información de viajar por esta.

- **QoS:** Asegura la priorización del tráfico critico o sensible de retardo sin despreciar tampoco el resto del tráfico gestionando el ancho de banda asignado a cada tipo de tráfico.

- **Gestión**: Tiene una gestión ágil y eficiente que resulta imprescindible para poder cumplir con los objetivos anteriores y alcanzar unos LSAs competitivos. La posibilidad de aplicar técnicas de Ingeniería de Trafico es la herramienta básica para la gestión en una red MPLS.

- **Fiabilidad:** Es indispensable para poder prever y garantizar una gran disponibilidad del servicio. La red MPLS "sabe" de la existencia de una VPN, ya que se trata de un modelo acoplado y no superpuesto.

---

[36] RFC 4364 - BGP/MPLS IP Virtual Private Networks (VPNs)

[37] PABLO BELZARENA, Ingeniería de Trafico en Línea en Redes MPLS Aplicando la Teoría de Grandes Desviaciones, Tesis Doctoral, 2003.

Las VPNs tradicionales se han venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada.
Además, la popularización de las aplicaciones TCP/IP, asi como la expansión de las redes de los ISPs, ha llevado a tratar de utilizar estas infraestructuras IP para el soporte de VPNs, tratando de conseguir una mayor flexibilidad en el diseño e implementación y unos menores costos de gestión y provisión de servicio. La forma de utilizar las infraestructuras IP para servicio VPN (IP VPN) ha sido la de construir túneles IP de diversos modos.[38]

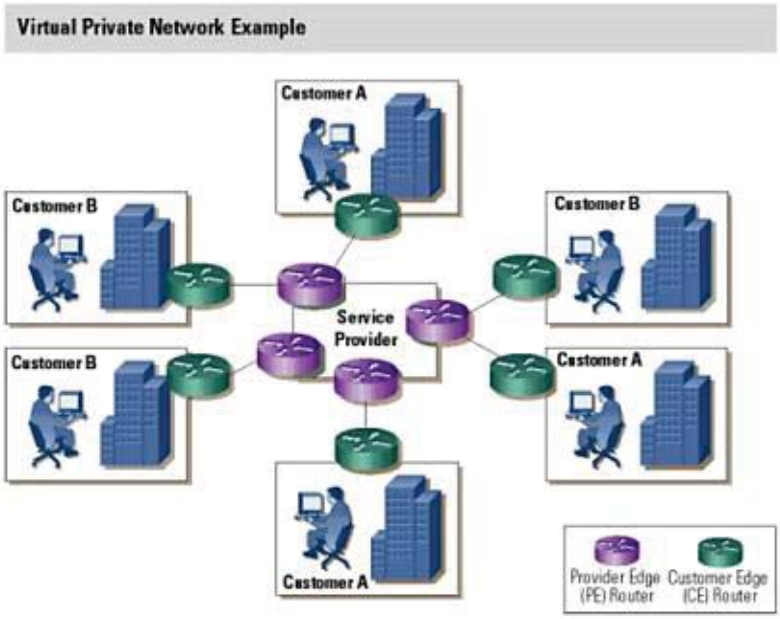


Fig. 2.12 Modelo de una Red Privada.[39]

Con una arquitectura MPLS se obvian inconvenientes ya que el modelo topológico no supone sino que se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos en una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mecanismo de intercambio de etiquetas MPLS. Los LSPs son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo. MPLS transporta esta información sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de routing IP

[38] RFC 2685 - Virtual Private Networks Identifier
[39] *https://books.google.com.pe/books?isbn=0471689971*

(2.9.) Aspectos complementarios a la red de datos IP-MPLS propuesta.

(2.9.1.) RPV - Red privada virtual

Es un servicio de transmisión de datos que sirve para interconectar 2 o más facultades o carreras profesionales a nivel local mediante enlaces privados, dedicados (1:1) y simétricos haciendo uso de la infraestructura de la propuesta de investigación de la red de datos de la UNSAAC en la plataforma IP/MPLS.[40]

Las características de la RPV propuesta en la red de datos de la unsaac son:

Se basa en tecnología MPLS.
Trabaja con clases de servicios (CoS), de 3 clases.
Trabaja con QoS sobre la N (tasa de transmisión) asignado para cada CoS y aplicado en la WAN (se define una política de encolamiento diferencial de paquete en función de la CoS en caso ocurra un incidente de congestión).
Trabaja con marcación de paquetes en la LAN.

(2.9.2.) Router CPE.

Equipo terminal instalado en el sitio de la facultad o carrera profesional, que permita conectar a la red de la facultad hacia el servicio.

(2.9.3.) Acceso a la red.

Elementos físicos y lógicos para conectar a la red de la facultad con la red de datos en la plataforma IP/MPLS.

(2.9.4.) Tasa de transmisión - N.

Es la velocidad que se asignara a cada facultad según el dimensionamiento de los tipos de servicio y es expresado en Kbps, Mbps o Gbps. [41]

$$N_{Acceso} = N_{CoS\ 1} + N_{CoS\ 2} + N_{CoS\ 3}$$

(2.9.5.) Clases de servicio.

Hace referencia al tipo de tráfico que la facultad pasara por el enlace asignado. Los tipos de servicios se muestran en la Fig. 1.13.

[40] 001_1 Presentacion Servicios Claro v1.pdf
[41] 001_1 Presentacion Servicios Claro - Parte II.pdf

Fig. 2.13. Clases de servicio en la propuesta de la red de datos de la UNSAAC.

(2.9.6.) Beneficios.

Los beneficios de la red IP-MPLS son:[42]

- Conectividad en malla.
- Administración de QoS
- Optimización de rutas
- Redundancia en el backbone
- Priorización de tráfico
- Convergencia IP voz/datos/video

Estos beneficios se muestran gráficamente en la Fig. 1.14.

[42] *mps.milwaukee.k12.wi.us/en/...at-MPS/Benefits-Summary.html*

Fig. 2.14. Beneficios de la red IP-MPLS.

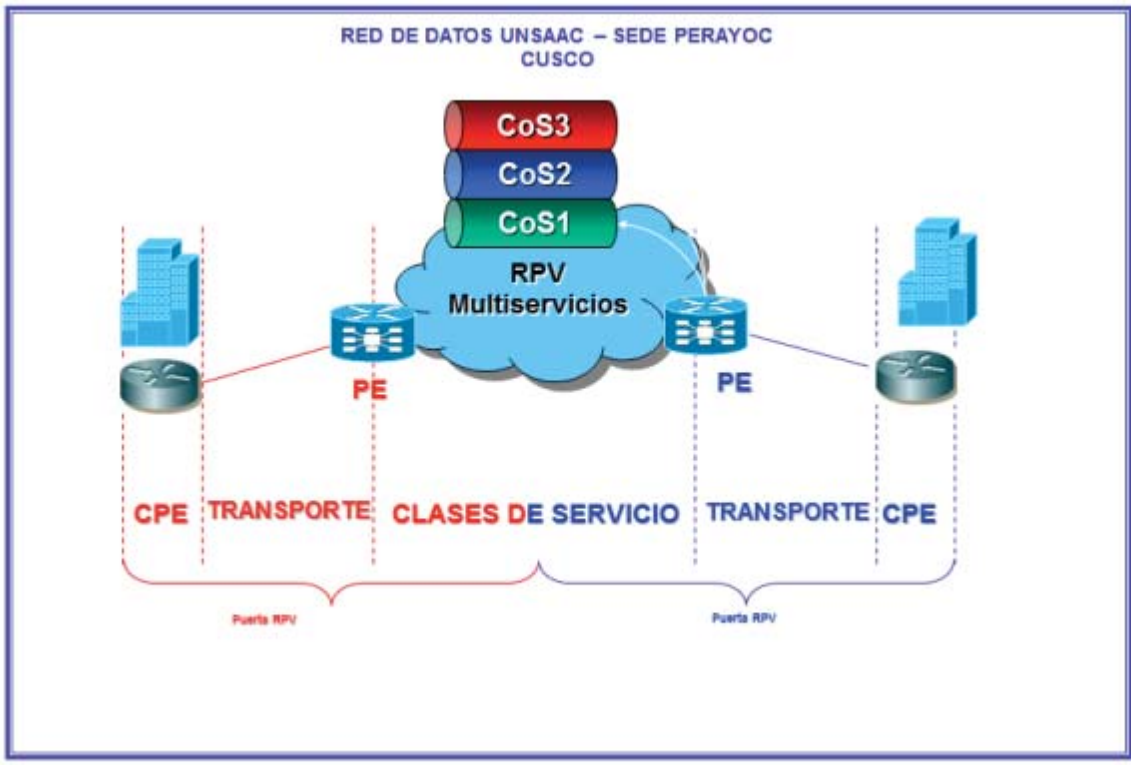


Fig. 2.15. Comunicación de CPE a CPE.

CAPITULO III

DESCRIPCION DE LA ARQUITECTURA DE RED DE DATOS ACTUAL DE LA UNSAAC.

(3.1.) Introducción.

En la actualidad las redes de área local (generalmente conocidas como LANs) y las tecnologías asociadas están evolucionando con una rapidez asombrosa. Esto se debe a que las necesidades de comunicación se han multiplicado en los últimos años llegando al entorno del usuario doméstico. Esta amplia gama de tecnologías ha llevado a una baja del precio de los equipos de red, pero ha hecho que la elección de un tipo de tecnología de red sea algo bastante difícil.

La red LAN física actual de la UNSAAC tiene una topología estrella, donde todos los switches convergen hacia un switch núcleo que es el equipo que fundamental de la red LAN física; mediante la creación de VLANs se puede distinguir a todas las carreras profesionales, la red inalámbrica, servicio de telefonía, servidores web y servidores de correo. El tipo de red LAN física de la UNSAAC es una red LAN subneteada, que solo trabaja en capa 2 del modelo TCP/IP, sin distinción de tráfico y fiabilidad de entrega de información.

La red de datos de la UNSAAC posee una infraestructura que en su mayor cantidad de equipamiento mantiene los mismos equipos operando desde su primera licitación de montaje; debido a la antigüedad de equipos, antigüedad de cableado vertical u horizontal en los diferentes pabellones, configuración de equipos, limitación de configuración de parámetros en los equipos existentes y entre otros factores relacionados que afectan a la red, conlleva a una degradación en el servicio hacia los usuarios, como lentitud de servicio, perdida de información, colisión de paquetes, uso inadecuado del ancho de banda, caída del servicio debido a no contar con repuestos en el mercado, limitación del crecimiento futuro en la red.

(3.2.) Descripción de la arquitectura de red actual de la UNSAAC.

(3.2.1.) Definición de la Infraestructura de red de la UNSAAC

Actualmente la Universidad Nacional de San Antonio Abad del Cusco cuenta con la siguiente infraestructura:

- Cableado del Campus.
- Cableado vertical (Backbone de Fibra Óptica)
- Cableado horizontal (Cableado estructurado en el Campus)
- Sistemas de protección eléctrica.
- Servidores
- Equipos activos.

(3.2.1.1.) Cableado del campus.

Es una solución basada en Cable no Blindado de Pares Trenzados (UTP) y Cable de Fibra Óptica. El sistema de cableado estructurado soporta sistemas LAN basados en cobre, en fibras o en la combinación de ambas. Soporta aplicaciones 10BaseTX, 100BaseTX, 100 BaseVG AnyLAN, 155 ATM, 622 ATM, Fast Ethernet (100 BASE TX) y Giga Ethernet (1000 BASE TX).
El sistema de cableado estructurado está basado en las especificaciones dadas por la Norma EIA/TIA 568B.3.1 que indica que las transmisiones serial en fibra multimodo de 50um son hasta 10 Gbps. Para la fibra monomodo debe obedecer al Estándar ITU G652.B que permite trabajar en la 2da ventana (1310nm) y 3ra ventana (1550nm) de longitud de onda y permitir velocidades de transmisión de hasta 10 Gbps a 300m lo que garantiza aplicaciones futuras. El sistema de cableado estructurado de datos para la UNSAAC soporta aplicaciones de alta velocidad tales como comunicaciones IP de voz y video convergente, videoconferencia o enseñanza a distancia y grandes operaciones de almacenamiento de datos.

(3.2.1.2.) Cableado vertical (backbone de fibra óptica).

Incluye 8 enlaces con fibra óptica multimodo (Tipo antiroedor y gel antihumedad - tipo toose tube) entre el nodo principal y nodos de distribución.
Para los enlaces entre los nodos de distribución y los switch de acceso se utilizó fibra óptica multimodo 50/125um (Tipo antiroedor y gel antihumedad - tipo loóse tube.)
La conexión realizada es de tipo fusión para lo cual se utilizaron pigtails y acopladores SC.
El tendido de la fibra es vía subterránea desde el nodo principal a los nodos de distribución, utilizando canalización subterránea para el backbone de fibra óptica en los tramos hasta llegar a la ubicación de los gabinetes terminales, mediante ductos de PVC SAP de 2" de diámetro y canaletas PVC decorativas de marca Bticino en las zonas interiores de los edificios.

(3.2.1.3.) Cableado horizontal (cableado estructurado en el campus).

Actualmente se cuenta con aproximadamente más de 2000 tomas de red 10/100/1000 Ethernet desde los switch de acceso hasta las áreas de trabajo; se cuenta con cableado estructurado hecho con cable UTP de 4 pares calibre 24 AWG categoría 5e y 6 (+250MHz).
En todos los nodos; principal y secundario, se instalaron como mínimo un gabinete metálico para la seguridad y soporte de los paneles de distribución y de fusión, así como de los equipos de datos. Para el caso de los switch de acceso (borde) se contempla el uso de gabinetes igual que para los demás nodos. La canalización Interna está realizada con canaleta PVC decorativa Marca Bticino y la canalización externa con tubos PVC SAP.
Esta estructura además de la transmisión de datos soporta telefonía sobre IP (VoIP), se utiliza el equipo de red switch Alcatel Omnivista 4760, el cual permite una solución común para la servicio de voz y datos.
El cableado estructurado permite brindar servicio de Internet a los centros de cómputo de las diferentes carreras profesionales que existen dentro de la sede principal de la UNSAAC, así mismo brinda servicio de telefonía IP a las coordinaciones y principales entes de administración de la UNSAAC, los puntos de acceso a la red, están distribuidos como sigue: En cada nodo, excepto en el nodo principal, se instalaron distribuidores secundarios (Gabinete de comunicaciones). Cada Gabinete de Comunicaciones puede ser de 24 RU o 18 RU que incluyen:

- Gabinete de pared, regleta eléctrica de 6 tomas, barra de tierra y kit de ventiladores.
- Paneles de parcheo de 24 puertos tipo 110IDC Categoría 6.
- Patch cords de 4 pies.
- Bandeja de fibra óptica con acopladores SC.

El distribuidor principal MTC consta de un gabinete de comunicaciones de 45 RU que incluye:

- Gabinete de pared, regleta eléctrica de 6 tomas, barra de tierra y kit de ventiladores.
- Paneles de parcheo de 24 puertos tipo 110IDC Categoría 6.
- Patch cords de 4 pies.
- Bandeja de fibra óptica con acopladores SC.
- Patch cord de fibra.
- Gabinete de fibra.
- Patch cord de cobre CAT 6 RJ45-RJ45.
- Switch core ALCATEL.
- Ordenador de cable horizontal de 1 RU.
- Patch panel De RJ45 Categoría 6.
- Switch de acceso ALCATEL.

(3.2.2.) Definición de la topología de la red LAN física actual

La figura 3.2 muestra el plano de la infraestructura de red de todo el campus universitario; actualmente la UNSAAC cuenta con una topología de red estrella con conexión directa hacia un switch núcleo Alcatel OmniSwitch 7800, de este núcleo salen con 6 enlaces de fibra óptica hacia diferentes pabellones como son el pabellón Ingeniería Eléctrica, Biblioteca, pabellón C, pabellón Administrativo, Ciencias Contables y pabellón de Ingeniería Informática, y 2 nuevos enlaces de fibra óptica multimodo desde un switch agregador del switch núcleo hacia las carreras de Economía e Ingeniería Electrónica, la figura 3.3 nos muestra que el núcleo Alcatel equipo posee una tarjeta con puertos 12 puertos 100/1000 Mbps RJ-45 y enlazar un switch agregador switch Alcatel Omnistack 6124 para los nuevos enlaces de fibra hacia otros pabellones, la red inalámbrica de la UNSAAC, central telefónica, servidores WEB y servidores de correo.

Para extender la red LAN física hacia las diferentes carreras profesionales se utiliza los switches 3com 5500 y switch Juniper EX_3200 como distribución de la red y los switches cisco WS-C2960S y switch Juniper EX_3200 como acceso a la red.

El principio de la configuración de la red LAN física de la UNSAAC son las VLAN para diferenciar a cada carrera profesional, la cual se crea en el Switch Core Alcatel y en los switches de distribución y acceso esta creado por puertos LAN y con la ayuda del equipo Exinda serie 4010, monitor de trafico en tiempo real, a su vez limita el canal para cada carrera de la red.

El cableado estructurado en los diferentes sectores del campus es una combinacion de la primera licitacion del 2004 con cable UTP Cat 5e y cable UTP Cat 6, estos instalados en el data center de RCU, gabinetes, patch panel, terminales desde roseta a los equipos.

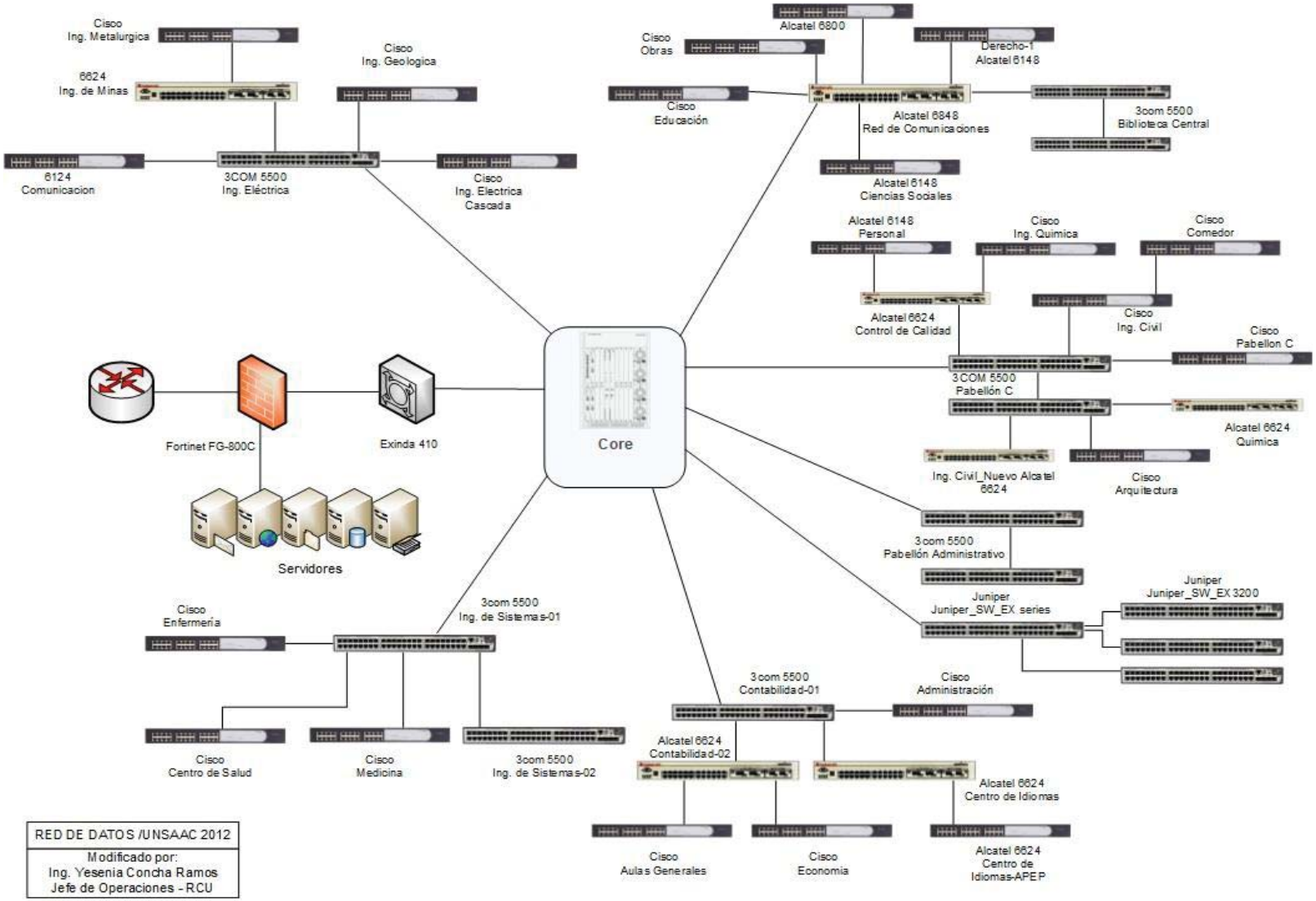


Fig. 3.1 Topología actual de la Red General de datos de la UNSAAC - 2013

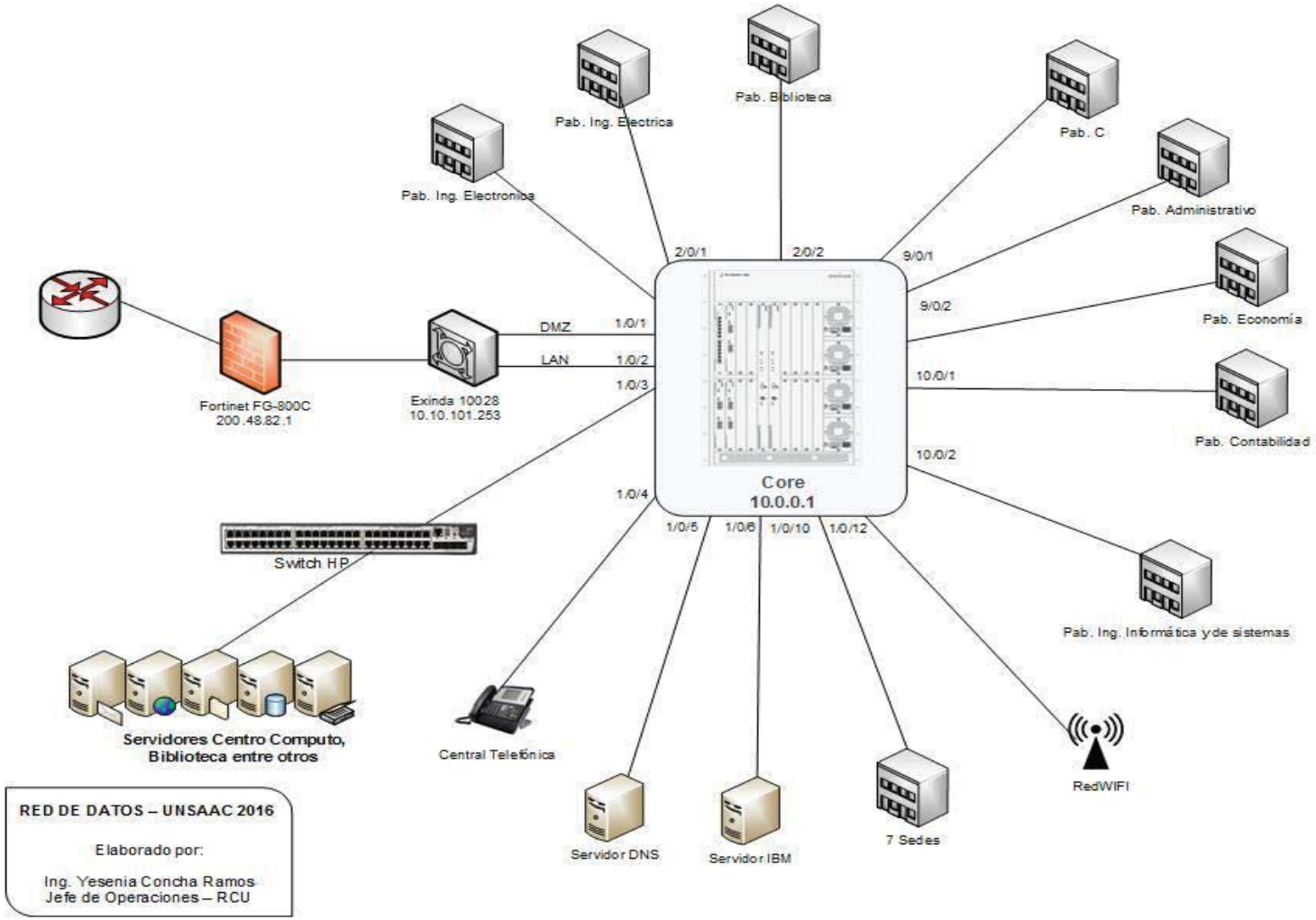


Fig. 3.2 Infraestructura de red actual de la UNSAAC - 2016

(3.2.3.) Definición de la topología de la red LAN WIRELESS actual.

La red inalámbrica de la UNSAAC está basada en un Cisco Wireless LAN Controller 5508. Es decir se trata de la arquitectura de red Cisco Unified Wireless Network.
Con esta arquitectura los Access Point se registran en el Controller. La configuración de los SSID y esquemas de seguridad correspondientes se configuran en el Controller de manera centralizada.
En el caso de los AP Outdoor se instalaron en postes y adosados a pared, para lo cual se utilizaron estructuras metálicas con tubos de 2" para el montaje de los AP.
El equipos Wireless LAN Controller AIR-CT5508-K9 está ubicado en el data center del RCU y luego tiene una conexión directa hacia el switch Cisco Catalyst 2960 instalado con la nueva red.
En la figura 3.3 se muestra plano de ubicación de todos los access point en la red de wireless en la UNSAAC.

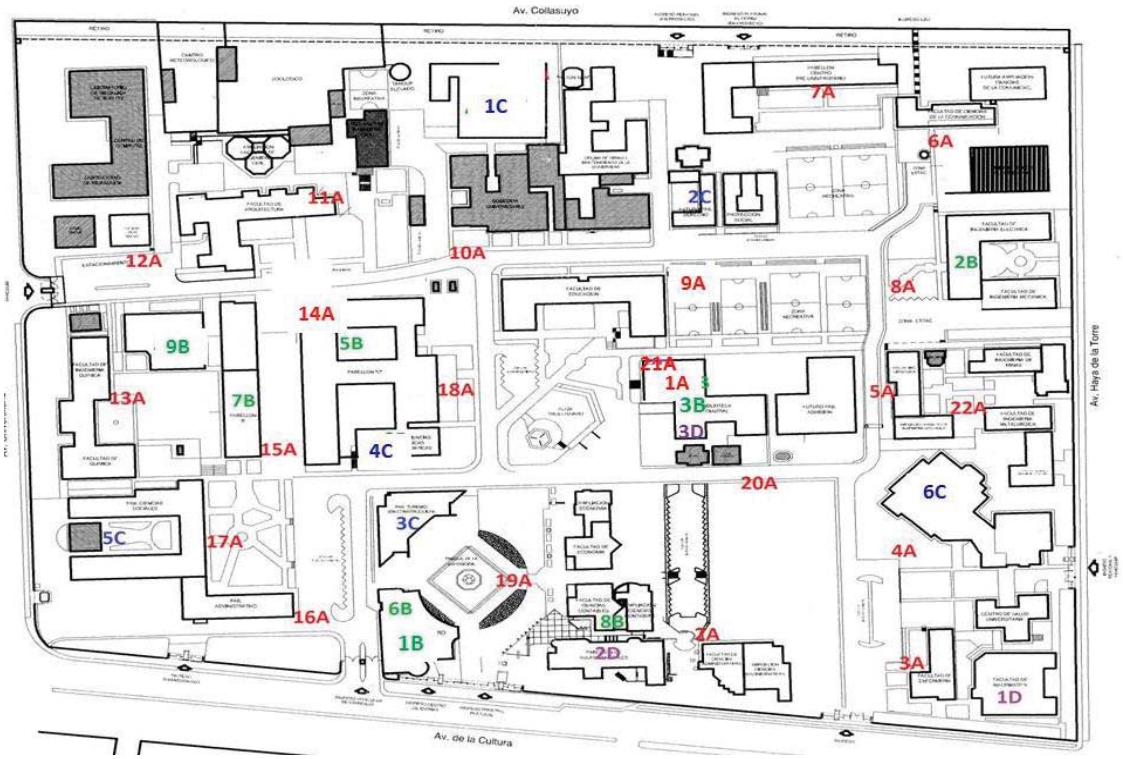


Fig. 3.3. Red inalámbrica actual de la UNSAAC

(3.3.) Primera licitación pública de la arquitectura de datos de la UNSAAC

Uno de los logros más importantes de la Universidad Nacional de San Antonio Abad, fue la realización del proyecto Red Integral de Conectividad en la UNSAAC, donde la Red de Comunicaciones tuvo gran participación. Este proyecto fue realizado el 2004 culminando la instalación de toda la infraestructura a fines del mismo año. (Licitación Pública Internacional N° 001-2004-UNSAAC, Adquisición de bienes e Integración de la Red de Conectividad de la UNSAAC)

La Red de Datos de la Universidad fue implementada con equipos que toda RED LAN posee:

- Switches de núcleo.
- Switches de distribución.
- Switches de acceso.
- Firewall.
- Enrutadores.
- Servidores.
- Backbone de fibra en todo el campus universitario.

Más de mil puntos instalados en todo el campus universitario con equipamiento Alcatel y cableado cat 5e., contemplando oficinas de administración, ambientes de docentes, estudiantes y la sede de Kayra.
La Red de Comunicaciones UNSAAC se encarga de la administración, control y soporte de la infraestructura de Datos, brindando servicios como: Internet, Intranet, Correo, Web, Base de Datos, etc.

(3.4.) Primer inventario de equipos de red instalados.

Haciendo mención a la primera licitación de instalación y puesta en marcha de la primera red de datos de la UNSAAC se instalaron los siguientes equipos y a su vez cabe resaltar que varios de ellos siguen trabajando hoy en día.
Todos los equipos se detallan en el ANEXO A.

(3.5.) Descripción y estado actual de los componentes y recursos de la red de datos de la UNSAAC.

Actualmente la red de datos de la UNSAAC cuenta con una gran cantidad de sistemas y usuarios con mención de algunos: servidores de correo, Exinda, firewall, telefonía IP, cámaras de seguridad, red inalámbrica, alumnos, administrativos y docentes entre otros, los cuales necesitan de un correcto funcionamiento de la red y prestación de servicio. Debido a la infraestructura de red existente con equipamiento y cableado antiguo, diseño de la topologia física y lógica de la red conlleva a congestión de tráfico, pérdida de paquetes, lentitud en petición y envío de data generando retraso y malestar en los usuarios, y actualmente esta altamente expuesto a una caida total del funcionamiento de la red de datos UNSAAC.

En estos últimos años la red de la UNSAAC viene presentando deficiencia de la infraestructura y servicios de red y en cuestiones de comunicación de datos e internet.

De acuerdo al diagnóstico y alcance de información del administrador de red de la UNSAAC un factor importante en la deficiencia de servicios es la antigüedad de los equipos ya que vienen trabajando desde el año 2004 y los requerimientos en procesamiento y capacidad de información se siguen incrementando, el funcionamiento del núcleo Alcatel tiene mucha relevancia porque en él convergen todos los servicios y según análisis de red

existen caídas de conectividad en algunos escenarios como son horas pico con acceso de todos los usuarios, cuando el administrador de red quita la restricción de Youtube y páginas de video, también cuando el centro de cómputo necesita hacer uso del servicio de internet caen otras conexiones.

Otro factor importante es el conflicto de IPs que genera colisiones en la red; para conectarse en red y poseer servicio hay que hacerlo de manera manual e ingresar una IP a nuestra tarjeta de red de la red inalámbrica, alumnos, red física de las facultades, etc.

Fisicamente cualquier red debería ser segura y tener un respaldo para dar el mantenimiento correctivo y mantenimiento preventivo correspondiente en caso de una avería, en la actualidad estos equipos ya no se encuentran en el mercado asi es que la red corre un riesgo alto.

(3.6.) Cambios de equipos en inventario actual de los equipos de red.

Con el proyecto de la implementación de la red inalámbrica en la ciudad universitaria de Perayoc, se llego a cambiar todos los swtiches de acceso de 3Com a Switches Cisco dejando la instalación con la misma configuración Vlan por puerto LAN para todos los equipos Switch.

(3.7.) Inventario actual de equipos de red instalados.

Según la licitación del año 2004 e implementación de la primera red LAN física ver (ANEXO A) la mayor parte de los equipos instalados se mantiene en operación como es el switch núcleo Alcatel, switches de distribución, servidores web, servidores de correo, firewall, etc.
En este inventario se adjunta el equipamiento de la red inalámbrico y el reemplazo de todos los switches de acceso de la marca 3Com a Cisco, ver (ANEXO B).

Tabla 3.1. Inventario actual de equipos de la red de datos de la UNSAAC.

(3.8.) Diagrama de arquitectura de la red de datos de la UNSAAC - 2016.

En la figura se muestra el diagrama actual de la red de datos de la UNSAAC en la cual se agrega los nuevos enlaces como son el Pabellon A y el pabellon de Ingeniería Electrónica.

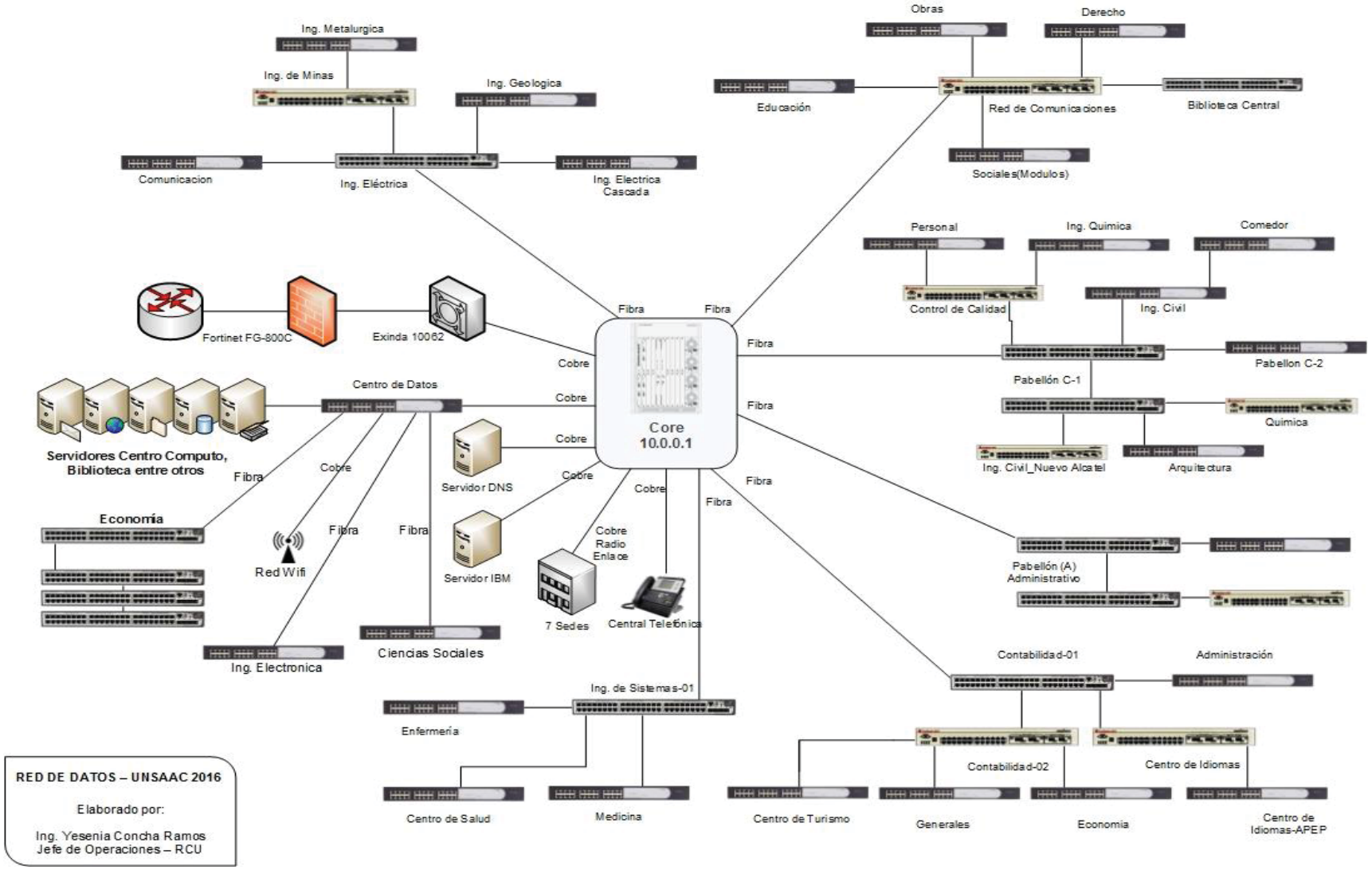


Fig. 3.4. Topología actual de la Red General de datos de la UNSAAC - 2016

(3.9.) Estado actual de las configuraciones de los componentes de red de datos.

De acuerdo al diagnóstico y la información obtenida por la red de datos de la UNSAAC la configuración del switch núcleo se adjunta en el **ANEXO A,** y con respecto a la configuración de los swiches de distribución y acceso están configurados VLAN por puertos.

(3.10.) Velocidad del internet contratada por la UNSAAC.

Actualmente la universidad contrata 150Mbps de velocidad de internet simétrico (carrier class) al proveedor Telefónica del Perú S.A. para satisfacer del servicio a todo el campus universitario de Perayoc y sus 7 sedes que se encuentran en Cusco.

La universidad entre los años 2013 y 2015 contrataba 100 Mbps de velocidad de internet simétrico (carrier class), en el cual se obtuvo información y mayor referencia de la degradación de servicios.

A inicios del año 2016 se realizó la ampliación de internet (upgrade) a 150 Mbps de velocidad de internet carrier class.

(3.11.) Diagnóstico del estudio de tráfico en la red de datos de la UNSAAC.

Según el análisis obtenido del estudio a la red de datos de la UNSAAC y sus servicios, la configuración de los equipos, no diferencia tipos de tráfico, ni calidad de servicio a los paquetes según sea el requerimiento.
La red de datos de la UNSAAC es una red LAN subneteada, la cual todas las consultas las hacen por la extranet, donde se crea congestión de tráfico por el uso de internet debido a que no se puede limitar filtros o velocidad en la nube.

(3.12.) Estudios previos

Para el estudio y análisis de tráfico de la red de datos de la UNSAAC se recolectó información de 4 a 5 meses del año 2016 de los equipos de red de monitoreo Exinda y Fortinet que nos proporcionó la red de comunicación de la UNSAAC, dicha información privilegiada y muy difícil de obtener por los derechos reservados de la dirección de la red de comunicaciones de la UNSAAC, se analizó la demanda de tráfico y horas pico de saturación del consumo de internet. En base a la información se muestra el siguiente estudio:

(3.12.1.) Descripción del tráfico de entrada y salida de la red de datos de la UNSAAC.

La descripción del estudio de carga se realizó en base al historial del consumo, tabla de graficas en tiempo real y el tráfico cursado en promedio de un día común sin contar los días feriados, caídas de servicio, reservas de comedor o días atípicos que nos muestra el equipo Firewall Fortinet y Exinda del Data Center:

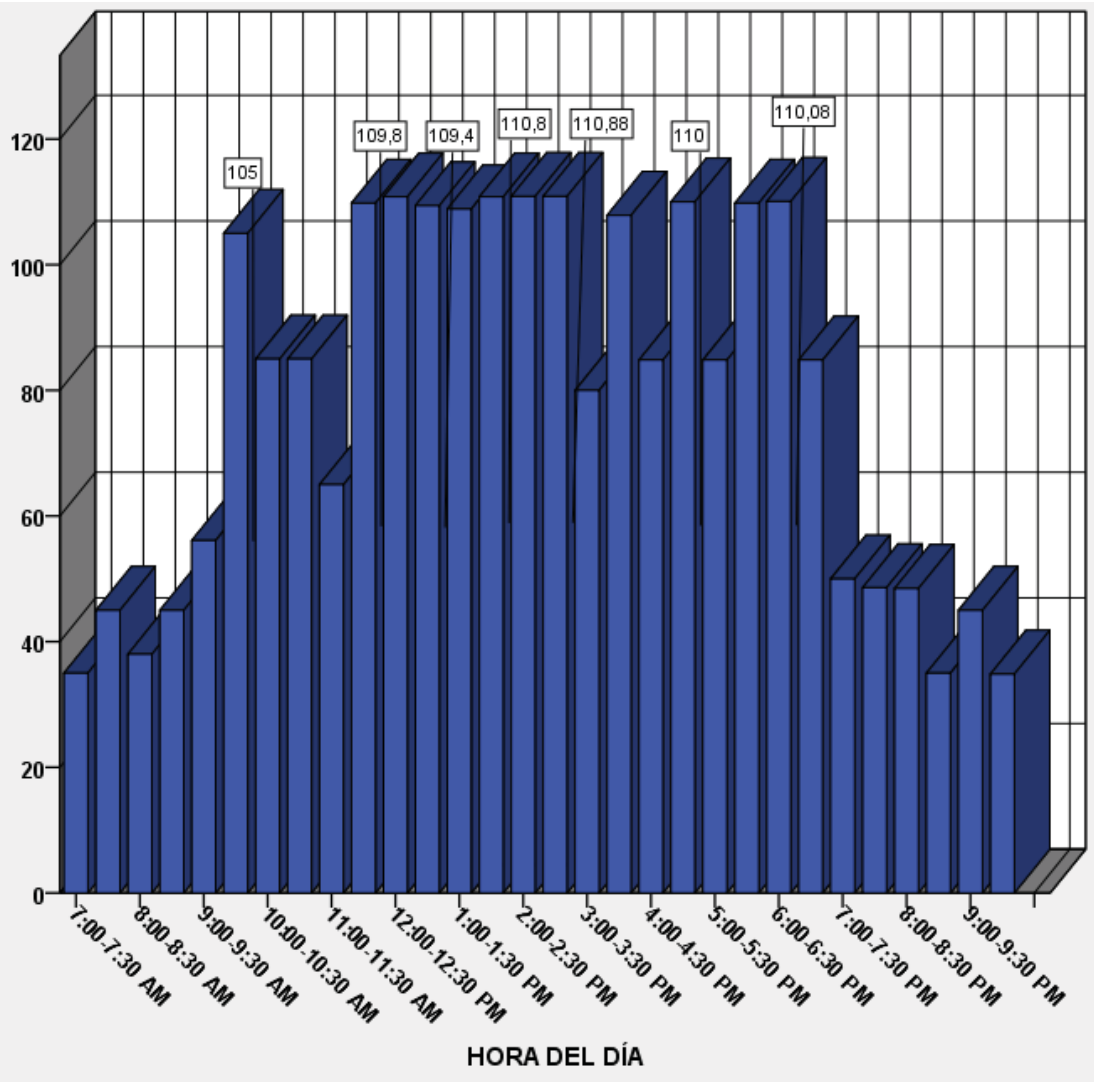


Fig. 3.5. Promedio de los cinco meses analizados del tráfico de entrada (traffic in) en Mbps de la red de datos de la UNSAAC

FUENTE: Base de datos del trabajo de investigación.

Viendo el gráfico N° 3.5 observamos que durante los meses de Enero – Mayo el tráfico de salida, en promedio, excede los 100 Mbps entre las 9:30 am y la 10:00 am, también entre las 11:30 am a 3:00 pm, 3:30 pm a 4:00 pm, 4:30 pm a 5:00 pm y finalmente entre las 5:30 y 6:30 pm. La media del consumo más alto registrado en los cinco meses fue de 112 Mbps, mientras que el más bajo fue de 35 Mbps.

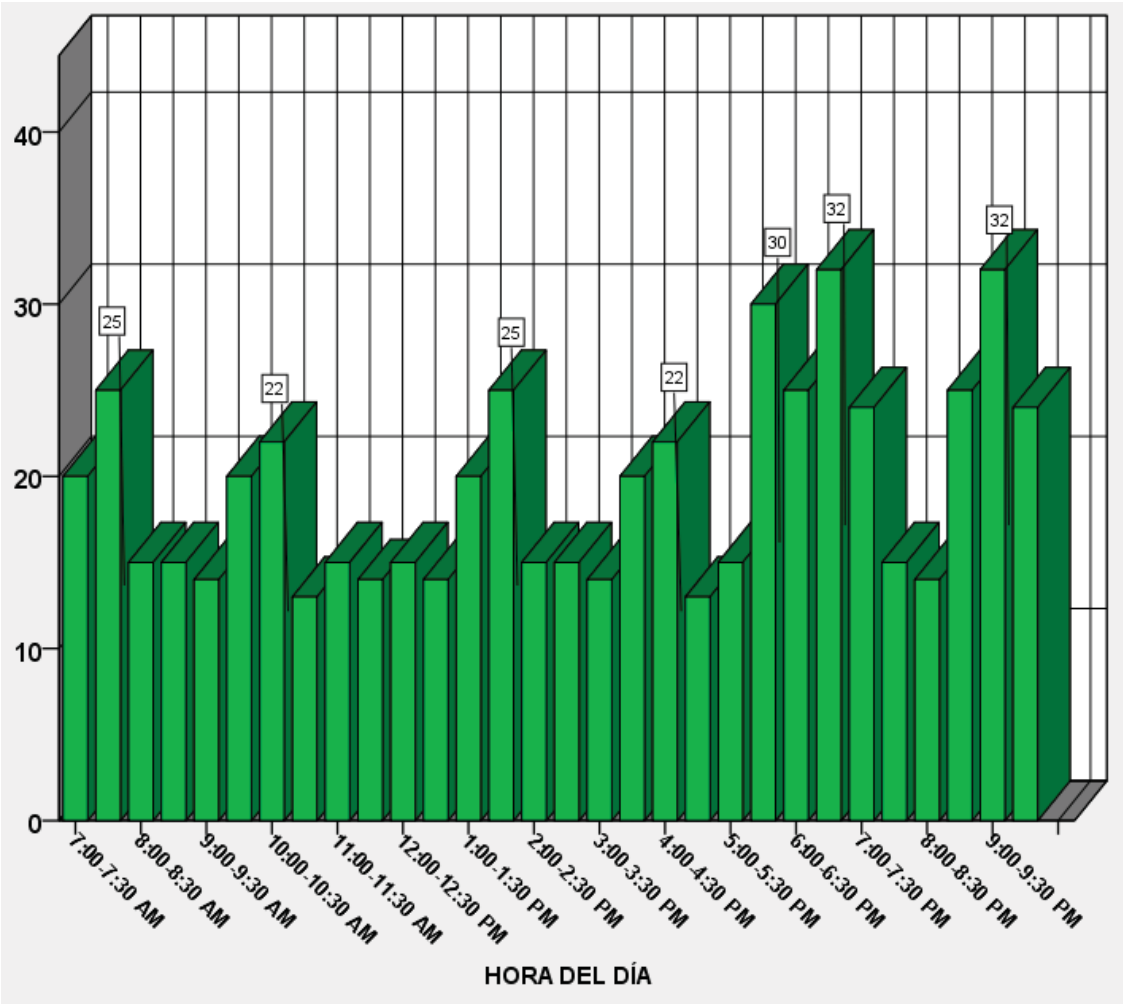


Fig. 3.6. Promedio de los cinco meses analizados del tráfico de salida (traffic out) en Mps de la red de datos de la UNSAAC

FUENTE: Base de datos del trabajo de investigación.

Viendo el gráfico N° 3.6 apreciamos que durante los meses de Enero - Mayo el tráfico de salida, en promedio, alcanza los 32 Mbps entre las 6:30 pm y 9:00 pm. La media de los consumos más bajos registrados en estos cinco meses alcanza los 14 Mbps durante varias horas del día.

CAPITULO IV

DISEÑO DE LA ARQUITECTURA DE LA RED DE DATOS DE LA UNSAAC EN LA PLATAFORMA IP-MPLS

(4.1.) El universo de la investigación.

El universo de la investigación viene a ser la red de datos de la UNSAAC sobre la plataforma IP-MPLS propuesta, la cual comprende varios puntos en lo físico y lógico.

(4.2.) Diseño de la red de datos IP-MPLS.

(4.2.1.) Función de los equipos de red

Los equipos de red se suelen dimensionar de acuerdo a la función que van a cumplir en la red.
En este caso se van a definir 3 tipos de equipos de red.

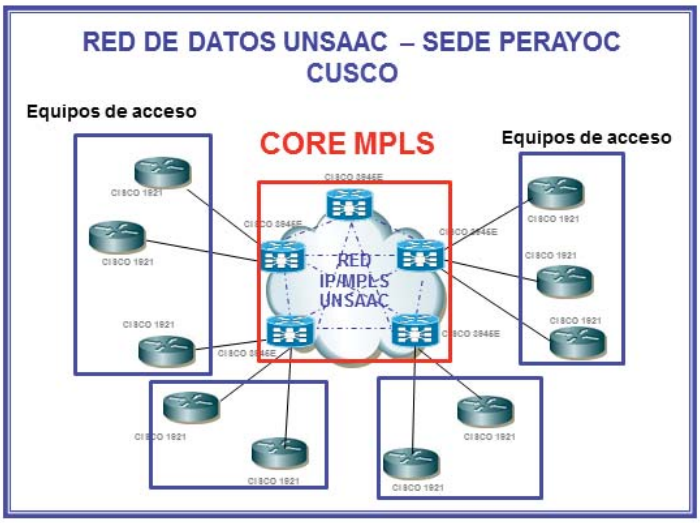


Fig. 4.1. Función de los equipos de red.

Equipos de red troncal: son aquellos equipos que estarán ubicados en el núcleo o en el Backbone MPLS de la red. Son equipos cuyas características son: Interfaces de gran velocidad y ancho de banda. En este caso estarán conformados y denominados por los equipos PE_1, PE_2, PE_3, PE_4 y PE_5.

Equipos de red acceso: son aquellos equipos que estarán ubicados en cada facultad, en este caso son enrutadores de acceso, switches de distribución y acceso, dentro de la nomenclatura del diseño de la red MPLS se le conoce como equipos de acceso.

Son equipos cuyas características son: interfaces de mediana velocidad, tarjetas de múltiples enlaces y ancho de banda).

Equipos de red gestión: son los equipos dedicados para acceso remoto mediante la utilización de un cable de consola que conecta directamente a los equipos PE, CPE y switches, permitiendo el acceso a éstos por la red de gestión (VPN dedicada para gestión de equipos en banda o por la propia red).

(4.3.) Planteamiento del MPLS sobre OSPF e inclusión del BGP.

La tecnología MPLS de Cisco Systems, a través del software Cisco IOS, hace a las redes VPN más fáciles de desplegar gracias a la utilización de una plataforma que combina la inteligencia de encaminamiento con el rendimiento de la conmutación. Esta red MPLS permiten comunicaciones privadas a través de una infraestructura de red compartida, ofrecen mayor escalabilidad para atender a las necesidades de miles de usuarios, y son lo bastante flexibles para dar cabida a métodos o esquemas de tráfico del tipo de cualquiera-a-cualquiera, para aceptar rápidamente nuevas instalaciones. Además, ofrecen un rendimiento predecible y fiable a través de diferentes clases de servicio, permiten a los usuarios conectarse a través de diferentes medios y cumplen con los requerimientos de transporte y ancho de banda de nuevas aplicaciones intranet.
Cabe destacar que la tecnología MPLS de Cisco posibilita optimizar el ancho de banda de red, aplicando selectivamente clases de servicio basadas en etiquetas o "labels" MPLS. Las redes MPLS escalan fácilmente al aumentar la cantidad de rutas y usuarios, y ofrecen el mismo nivel de privacidad que las tecnologías de conmutación. Además, los usuarios pueden utilizar direcciones IP privadas sin necesidad de conversión y puede alcanzarse la máxima privacidad y seguridad sin necesidad de túneles ni encriptación. La tecnología MPLS de Cisco es ampliamente aceptada por el mercado actual.[43]

(4.4.1.) Consideraciones del protocolo OSPF.

La función del OSPF permite al administrador de red realizar configuraciones avanzadas del MPLS entre dispositivos PEs en una conmutación de etiquetas multiprotocolo (MPLS) de red privada virtual (VPN). Esta característica aumenta la flexibilidad al cambio de los dispositivos de información de enrutamiento entre los sitios porque un identificador de enrutador por separado para cada interfaz o subinterfaz se configura en un dispositivo PE unido PEs dentro de una VPN. Una VPN MPLS consiste en un conjunto de sitios que están interconectados por medio de un enlace a la red central MPLS.

(4.4.2.) Consideraciones de Ingeniería de Tráfico.

La consideración de ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de los recursos, de manera de evitar que un subconjunto (enlaces y equipos) de la red se sature mientras otro subconjunto de la misma se encuentra infrautilizado, mejorando el rendimiento de la red global.

[43] http://www.networkworld.es/archive/mpls-ventajas-para-las-empresas

(4.4.2.1.) Marcación de paquetes

Para admitir el entorno de QoS, los extremos se configuran para marcar el tráfico IP que lleva el tráfico IP de audio y vídeo en tiempo real, según las clases establecidas de servicios diseñados para proteger el tráfico de comunicación en tiempo real de otro tráfico asincrónico en la red IP, incluida la mensajería instantánea, datos de las aplicaciones compartidas y descargas de archivos. Estas marcas se pueden cambiar para asignar a diferentes clases de servicios según se desee en la red de datos.
Una red habilitada para los Servicios diferenciados (DiffServ) proporciona un establecimiento de prioridades de nivel de clase basándose en el marcado de Punto de código de servicios diferenciados (DSCP) de los paquetes IP. Cada valor DSCP se corresponde con un tipo de servicio para la transferencia de paquetes desde el remitente o enrutador intermedio al siguiente enrutador o receptor en la red.
El marcado QoS se aplica a todos los puertos de medios, independientemente de si el tráfico es de audio/vídeo/datos.[44]

(4.4.2.2.) Políticas de calidad de servicio.

El tráfico de datos y voz tienen diferentes requisitos en lo que respecta al tratamiento de los paquetes de la red. La voz en una aplicación en tiempo real y, como tal, para garantizar la calidad de servicio requerida para la aplicación de mecanismos de QoS en la red para permitir este tipo de priorización de tráfico para transmitir inmediatamente.
La calidad de servicio de la red IP-MPLS de transporte se implementa mediante la definición de diferentes clases de servicio (CoS).

Por lo tanto, el tráfico asociado a cada clase es tratado de manera diferente en la red.

(4.4.2.3.) Priorización de clases de servicio.

Para utilizar la calidad de servicio, debe analizar el tráfico de la red para determinar los grandes grupos en los que se puede dividir el tráfico. Después, debe organizar los grupos en clases de servicio con características y prioridades individuales. Estas clases forman las categorías básicas en las que se basa la directiva QoS de la organización. Las clases de servicio representan los grupos de tráfico que se desea controlar.

(4.4.3.) Consideraciones del protocolo BGP.

Las consideraciones del BGP son implementación de políticas de enrutamiento que sean: Escalable, Estable y Simple.
BGP nos permite implementar políticas, cada prefijo maneja una serie de características llamadas atributos. Permite manejar las miles de rutas. Utiliza enlaces reduciendo cuellos de botella y congestión. En este caso se necesitan decisiones de routing basadas en política basadas en el enlace

[44] https://technet.microsoft.com/es-es/library/gg405407(v=ocs.14).aspx

(4.4.3.1.) Definición de las clases de servicios[45]

Las clases de servicio son un parámetro utilizado en datos y voz, protocolos para diferenciar los tipos de cargas útiles contenidos en el paquete que se transmite. El objetivo de esta diferenciación se asocia generalmente con la asignación de prioridades a los niveles de carga útil de datos o el acceso a la llamada telefónica.

(4.4.3.1.1.) Red de telefonía

Esta clase de servicio no se adapta fácilmente a variaciones de retardos y rendimientos de una red, son tolerantes a perdidas pero no a retardos.

- Tráfico en tiempo real video, voz y audio.

Las aplicaciones en tiempo real normalmente no reducen su demanda para enfrentarse a la congestión

Esta red va relacionada con los sistemas de telefonía existentes como: transmisión de voz. La red de telefonía agrupa a todos los teléfonos analógicos y teléfonos IP que se encuentra en nuestro campus Perayoc, además definimos a la red de telefonía que tendrá la máxima prioridad por sus características.

Nota: Consideramos a la red de cámaras de la facultad de Economía dentro de esta red.

[45] http://www.spw.cl/08oct06_ra/doc/REDES%20WAN%20IP-ATM/CalidaddeservicioenredesIP.pdf

(4.4.3.1.2.) Red de servidores.

Esta clase de servicio se adapta fácilmente a variaciones de retardos y rendimientos de una red, sin embargo la información que transcurra por él es crítica ya que es de suma importancia la actualización de información que se debe manejar en la universidad y evitar problemas.

Esta red va relacionada con el banco de servidores existentes en el data center y las subredes de servidores que proponemos en la nueva topología, donde la información que se manejará son: datos transaccionales, tráfico web en servidores de la INTRANET, tráfico web en servidores de la EXTRANET, correo electrónico profesional, monitorización de la red, gestión de tráfico de la red, y definimos a esta red de servidores que tendrá una moderada prioridad por sus características.

(4.4.3.1.3.) Red de internet y correo electrónico.

Esta clase de servicio se puede ajustar a los cambios de retardos y rendimientos de una red, sin dejar de satisfacer las necesidades de sus aplicaciones.

Esta red va relacionada con los servicios existentes como: correo electrónico personal, transferencia de archivos, conexión remota, acceso web (internet), FTP, telnet, y definimos a esta red que tendrá baja prioridad por sus características.

(4.4.) Cálculos

Para realizar los cálculos se toma en cuenta la descripción de la red actual y tráfico cursado. La UNSAAC cuenta con la red de datos y telefonía que funcionan sobre una LAN subneteada, es decir que no tiene configuraciones dedicadas a cada clase de servicio.

Para el cálculo, primero se busca independizar las tres clases de servicios, que son datos en tiempo real **(máxima prioridad)**, datos críticos como son SERVIDORES, SIAF **(moderada prioridad)**, y por ultimo datos no críticos como internet y correos electrónicos **(mínima prioridad)**.

Para cada clase de servicio se realiza el dimensionamiento correspondiente que se muestra a continuación.

(4.5.1.) Demanda de tráfico por clase de servicio.

En las tres clases de servicios que se da en la propuesta de la red de datos, la demanda de tráfico es diferente según la necesidad de cada uno de ellas.

Actualmente la clase de servicio de internet es la que tiene mayor demanda por la cual es un punto clave que da inicio al dimensionamiento, es decir que esta clase de servicio de internet, tendrá mayor demanda o alta tasa de transmisión de datos, seguido del servicio de los SERVIDORES en aplicaciones como el software SIAF, Página de la UNSAAC, descarga de información académica de Servidores por carrera, las cuales tienen una demanda moderada y por último el servicio de la telefonía que tiene una demanda baja.

La demanda de tráfico por clase de servicio que estimamos sería de la siguiente manera.

CoS3 demanda de tráfico bajo
CoS2 demanda de tráfico moderado.
CoS1 demanda de tráfico alto.

(4.5.2.) Dimensionamiento de las velocidades de las clases de servicio.

Teniendo información del consumo de tasa de transmisión en la universidad revisado en los estudios previos, cual solo se ve únicamente el consumo del servicio de internet (CoS1), entonces dimensionamos tasa de transmisión para la red de servidores (CoS2) y la red de telefonía (CoS3).

(4.5.2.1.) Dimensionamiento de la red de telefonía - CoS3.

Para el caso del servicio de telefonía:

El dimensionamiento de la red de Telefonía 1 es en base:

- N definimos la tasa de transmisión global por subred de telefonía.
- Cantidad de teléfonos IP por carrera profesional realizando llamadas simultaneas.
- Tasa de transmisión del teléfono IP.
- Cantidad de carreras profesionales por facultad.

Calculo del N:

La respuesta tiene cálculos matemáticos que se pueden utilizar en una ecuación.

De acuerdo a la agenda telefónica [46]de la UNSAAC se posee una información completa de la cantidad de teléfonos por carrera profesional, la cantidad total de carreras profesional por área geográfica y la tasa de transmisión teórica que tiene cada teléfono. Esta es la fórmula a utilizar:[47]

$$N (CoS3) = G * X$$

Dónde:

N (CoS3) = Tasa de transmisión de la red de telefonía
X = Cantidad de teléfonos IP por carrera profesional.
G = Tasa de transmisión del teléfono. Este valor está definido teóricamente y es igual a 16Kbps~64Kbps por una llamada.

[46] http://www.unsaac.edu.pe/directorio/index.php
[47] http://blog.acostasite.com/2010/01/como-determinarcalcular-el-ancho-de.html

Con respecto al valor de la tasa de transmisión para una llamada nos basamos en la teoría de Muestreo de Nyquist-Shannon[48] y teorema de cuantización [49]y para el dimensionamiento consideramos el máximo valor que es de 64Kbps.

Se realiza el análisis para la primera facultad que comprende el equipo CPE_1, el cual comprende las carreras profesionales de Ing. Eléctrica, Geológica, Metalurgia, Minas y Mecánica, de acuerdo a la agenda telefónica obtenida de la UNSAAC se posee 13 anexos activos

X = 13 (teléfonos IP por carrera)
G = 64 Kbps (tasa de transmisión "garantizado" por teléfono IP)[50]

N (CoS3) = X* G
N (CoS3) = 13 * 64 Kbps = 832 Kbps ~1 Mbps(valor entero próximo)

A este valor se agrega 1024 Kbps con una proyección de un crecimiento del 100% a futuro. Este factor de crecimiento se realiza a un crecimiento de números de teléfonos en los próximos 5 años, donde se toma de referencia las consideraciones de diseño de Telefonía Analógica.

Entonces la tasa de transmisión del tráfico de la red de Telefonía 1 en el CPE_1 es:

N (CoS3) total = 1024 Kbps + 1024 Kbps = 2048 Kbps = **2 Mbps**

En el dimensionamiento no se considera los factores de compresión y se trabaja con la máxima tasa de velocidad según teorías de voz y video, sin embargo se debe mencionar teoría de voz sobre IP [51] debido a que los Codec ayudan a reducir el consumo de tasa de transferencia y garantizan la comunicación.

Según los factores de compresión:
Factor de compresión recomendado es: **G.711 del ITU-T[52]**
Otros factores de compresión: **G.723 del ITU-T, G.729 del ITU-T[53],**

Nota: Se aplica el mismo procedimiento para los demás equipos CPE, tomando en cuentas las mismas consideraciones que se aplicó para dimensionar la N de la red de Telefonía 1 en el equipo CPE_1.

[48] http://www.dicis.ugto.mx/profesores/ljavier/documentos/Lec01%20-%20Teorema%20de%20Muestreo.pdf
[49]http://serbal.pntic.mec.es/srug0007/archivos/radiocomunicaciones/3%20SE%D1ALES%20DIGITALES/Muestreo%20digital.pdf
[50] http://www.voipforo.com/codec/nuevos-codecs-g7111-g7291.php
[51]https://eciencia.urjc.es/bitstream/handle/10115/5939/Voz%20sobre%20IP.pdf;jsessionid=7EEEA4A82BF7DE46F8B47069C6BC8A14?sequence=1
[52] http://www.itu.int/rec/T-REC-G.711/es
[53] www.itu.int/rec/T-REC-G.729/es

Para la única red de cámaras que existe en la facultad de Economía podemos dimensionar de acuerdo a la resolución de video y tomando de referencia la página web de tasa de transmisión mínimas considerables.[54]

Se toma como máxima tasa de transmisión de 256 Kbps por cámara IP y de acuerdo a las cuatro cámaras que se posee en dicha facultad resulta 1024 Kbps.

Luego de realizar los cálculos, se tiene la siguiente tabla del dimensionamiento.

N - CoS 3				
VLAN	**NOMBRE**	**Cantidad de teléfonos actual**	**CoS 3 (Mbps)**	**CPE**
60	TELEFONIA 1	13	2	1
61	TELEFONIA 2	14	2	2
62	TELEFONIA 3	9	1.5	3
63	TELEFONIA 4	4	0.512	4
64	TELEFONIA 5	24	3	5
65	TELEFONIA 6	13	1.5	6
66	TELEFONIA 8	16	2	8
67	TELEFONIA 9	13	2	9
68	TELEFONIA 10	26	3.5	10
70	CAMARAS	4	1	4
TOTAL DE TASA DE TRANSMISION			**19**	

Tabla 4.1. Dimensionamiento de la clase de servicio de Telefonía (CoS3)

(4.5.2.2.) Dimensionamiento de la red de servidores - CoS2.

Para el caso del servicio de red de Servidores:

El dimensionamiento de la red de Servidores 1 es en base:

- N definimos la tasa de transmisión global por cada subred de servidores.
- Cantidad de usuarios realizando descarga de archivos simultaneas de servidores remotos por carrera profesional.
- Tasa de transmisión de la descarga por usuario.
- Cantidad de carreras profesionales por facultad.

Calculo del N:

Suponemos una cantidad de usuarios realizando una descarga por carrera profesional, la cantidad total de carrera profesional por facultad y una tasa de transmisión tiene cada usuario al descargar. Para dimensionar la tasa de transmisión esta es la fórmula a utilizar:

N (CoS2) = G * X* C

[54] https://technet.microsoft.com/es-es/library/jj688118(v=ocs.15).aspx

Dónde:

N (CoS2) = Tasa de transmisión de la red de Servidores 1.
X = Cantidad de usuarios realizando una descarga por carrera profesional (no se limita)
G = Ancho de banda por usuario al descargar. Este valor varía dependiendo a la demanda de descargas. Al realizar una descargar consume un ancho de banda de 64Kbps, pero este consumo incrementa al disminuir el número de descargas, es decir que mientras menos usuarios descargan, aumenta la tasa de transmisión por usuario llegando a 512 o 1024 Kbps, esto se debe a que el tráfico que se genere desborda al BW que no se utilice por las otras carreras.[55]
C = Cantidad de carrera profesional por CPE.

En fin, se realiza el análisis para la primera facultad que comprende el equipo CPE_1, el cual comprende las carreras profesionales de Ing. Eléctrica, Geológica, Metalurgia, Minas y Mecánica:

X = 16 (usuarios por carrera)
G = 64 Kbps (ancho de banda por usuario, valor que puede incrementar)
C = 5 carrera profesional (Estimamos que las 5 carreras profesionales estarán realizando una descarga simultáneamente)

N (CoS2) = C * N* G
N (CoS2) = 5 * 16 * 64 Kbps = 5120 Kbps

A este valor se agrega 1024 Kbps con el propósito de reserva de canal, para cursar tráfico de gestión de equipos y cambios de configuración en remoto de la red, además del monitoreo de red avanzado en la prioridad Cos2.

Entonces el BW del tráfico de la red de Servidores 1 en el CPE_1 es:

N (CoS2) total = 5120 Kbps + 1024 Kbps = 6144 Kbps = **6 Mbps.**

En resumen la tasa de transmisión adecuada por un usuario depende del tamaño de la página web y tamaño de información que desea descargar, actualmente todas las sesiones que se tiene hacia los servidores de la universidad son de consulta de la páginas web UNSAAC tales como ingreso y consulta de Notas, matrículas, correo corporativo universitario, etc.

Según datos teóricos sobre el tamaño de la información una página web estandarizada [56]y accesible pesa entre 10 KByte y 100 Kbyte considerando los parámetros de compresión y tiempo de respuesta hacia el usuario, otro dato a tomar en cuenta es el promedio de una sesión de un usuario hacia servidores que es entre 32 Kbps~64 Kbps de consumo.[57]

[55] http://blog.acostasite.com/2010/01/como-determinarcalcular-el-ancho-de.html
[56] http://www.paginaswebempresariales.com/blog/como_se_mide_el_ancho_de_banda.php
[57] http://www.usabilidad.tv/usabilidad_web/peso_de_pagina.asp

Tomando como referencia estos valores predeterminados asumimos la mayor tasa de transmisión que es de 64 Kbps y haciendo cálculos en tiempo de respuesta con el mayor peso de una página que es de 100 KB nos da:

64 Kbps≈8 Kbyte por segundo

Entonces resulta un tiempo de 100 KB/8 KB=12.5 segundos.

Es el tiempo máximo y considerable que un usuario debe esperar para visualizar todas las aplicaciones de la página considerando que toda la red está saturada.

Verificación de tiempos de descarga de archivos.

Como ejemplo, ponemos el peso promedio máximo de información de un archivo de 2 MB de datos comprimido en formato pdf.

Archivo a descargar = 2 MB = 2000 KB
Ancho de banda de descarga por usuario = 64 Kbps = 8KBs **(TESIS)**[58]

Tiempo de descarga =T

Tenemos:

T = 2000 KB/8KBs = 250 segundos = 4.16 minutos.

Este tiempo varía dependiendo al número de usuarios que realicen una descarga.
Es decir que a menor cantidad de usuario que realice una descarga, mayor ancho de banda para el que realice una descarga, estimando cantidades de usuarios realizando una descarga ponemos la tabla de tabulaciones:

[58] JUAN CARLOS FERNANDEZ ZARPAN, Diseño de una Red de Voz sobre IP para una Empresa que Desarrolla Proyectos de Ingeniería de Comunicaciones, Tesis Grado, 2008.

Tiempos de descargas			
Cant. Usuario por CPE	**Ancho de banda por descarga (Kbps)**	**Tamaño de archivo (KB)**	**Tiempo de descarga por usuario (minutos)**
80	64	4 000	4.16
40	128	4 000	2.08
20	256	4 000	1.04
10	512	4 000	0.52
5	1024	4 000	0.26

Tabla 4.2. Tiempo de descarga para cada usuario en (CoS2)

Nota: Se aplica el mismo procedimiento para los demás equipos CPE, tomando en cuentas las mismas consideraciones que se aplicó para dimensionar la tasa de transmisión de la red de Servidores 1 en el equipo CPE_1.

Luego de realizar los cálculos, se tiene la siguiente tabla del dimensionamiento.

N – CoS 2			
VLAN	**NOMBRE**	**CoS 2 (Mbps)**	**CPE**
50	SERVIDORES 1	6	1
51	SERVIDORES 2	6	2
52	SERVIDORES 3	3	3
53	SERVIDORES 4	1	4
54	SERVIDORES 5	8	5
55	SERVIDORES 6	2	6
56	SERVIDORES 8	4	8
57	SERVIDORES 9	4	9
58	SERVIDORES 10	2	10
TOTAL DE TASA DE TRANSMISION		**36**	

Tabla 4.3. Dimensionamiento de la clase de servicio de Servidores (CoS2)

(4.5.2.3.) Dimensionamiento de la red de internet - Cos1.

El dimensionamiento de la red de internet **(Cos1)** es en base a los datos proporcionados y brindados de la RCU como se muestra a continuación:

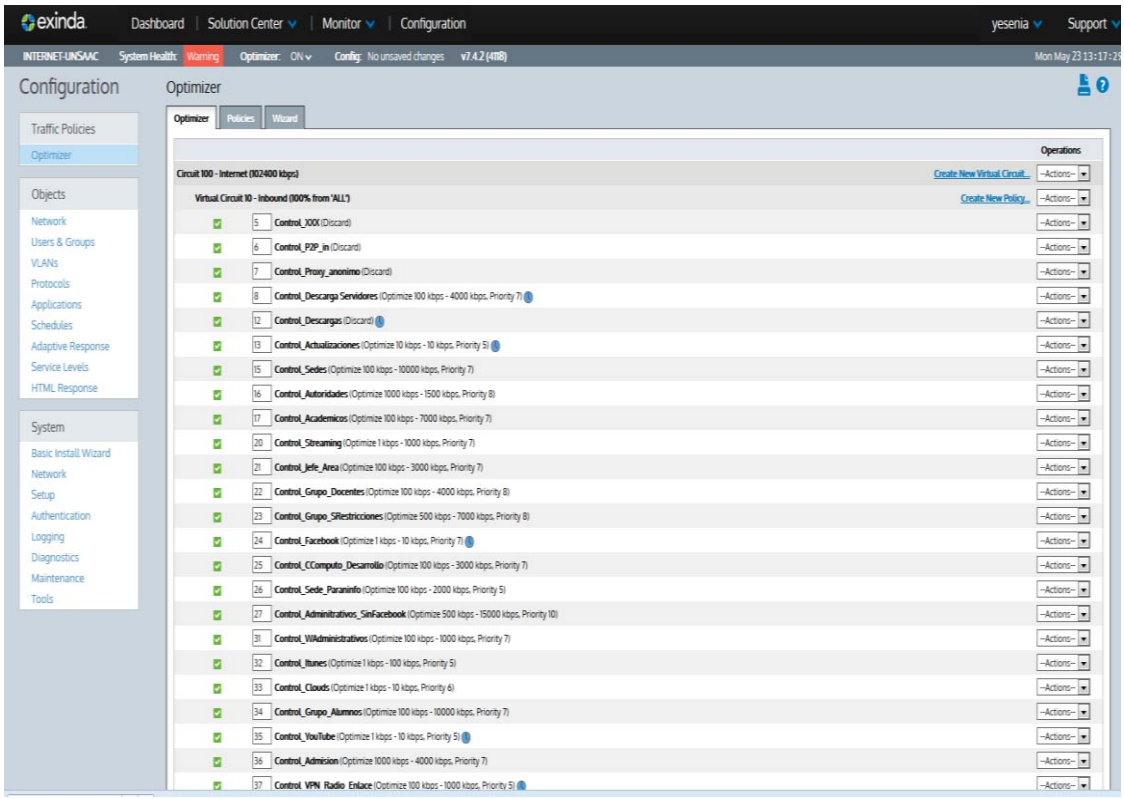


Fig. 4.2. Vista general de la tasa de transmisión en el EXINDA - RCU 05/05/16.

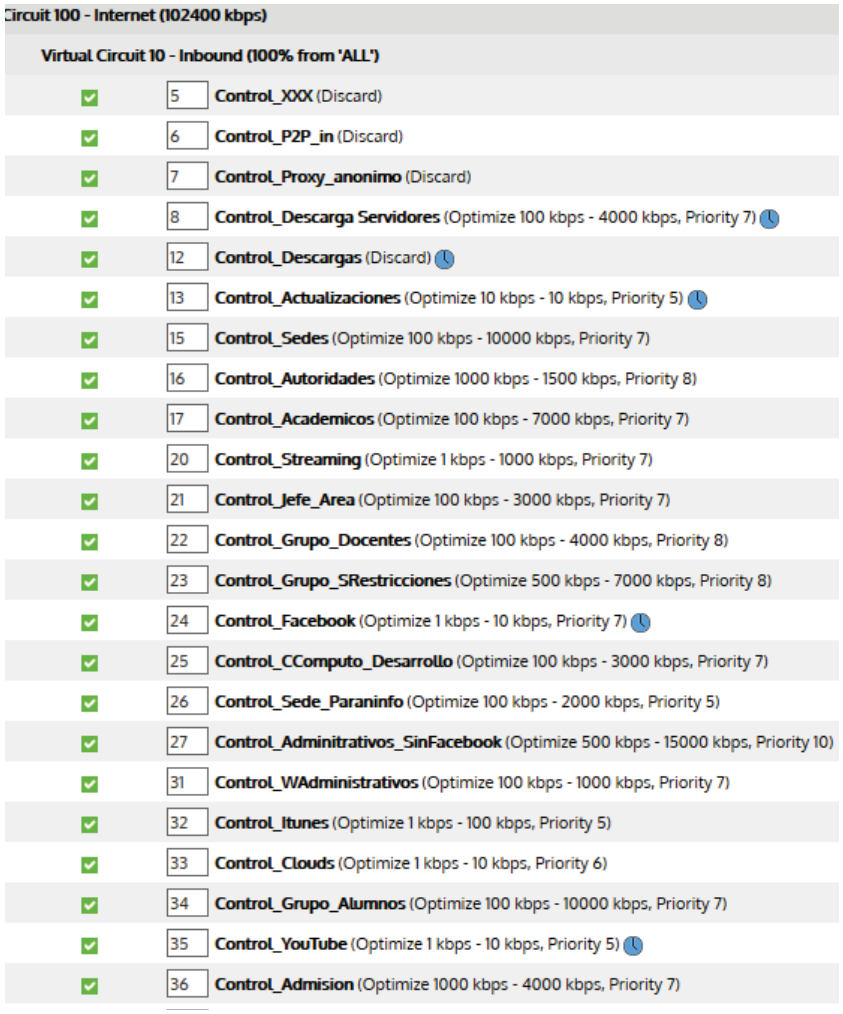


Fig. 4.3. Vista de la tasa de transmisión de las carreras profesionales - EXINDA – 1.

De la Fig. 4.13 Cabe resaltar las asignación de 10 Mbps para las sedes de la universidad que están fuera del campus Perayoc y con respecto a la red inalámbrica de la UNSAAC mencionar que para el Grupo_Docente se asigna 4 Mbps, al Grupo_Alumnos se asigna 10 Mbps y por ultimo al Grupo_Administrativos se asigna 15 Mbps que en total suman 29 Mbps para Wireless.

Estas tasas de transmisión de 10 Mbps Grupo_Sedes y 29 Mbps Grupo_Wireless debemos restar para la asignación de velocidades en la topología física.

Fig. 4.4. Vista de la tasa de transmisión de las carreras profesionales - EXINDA - 2.

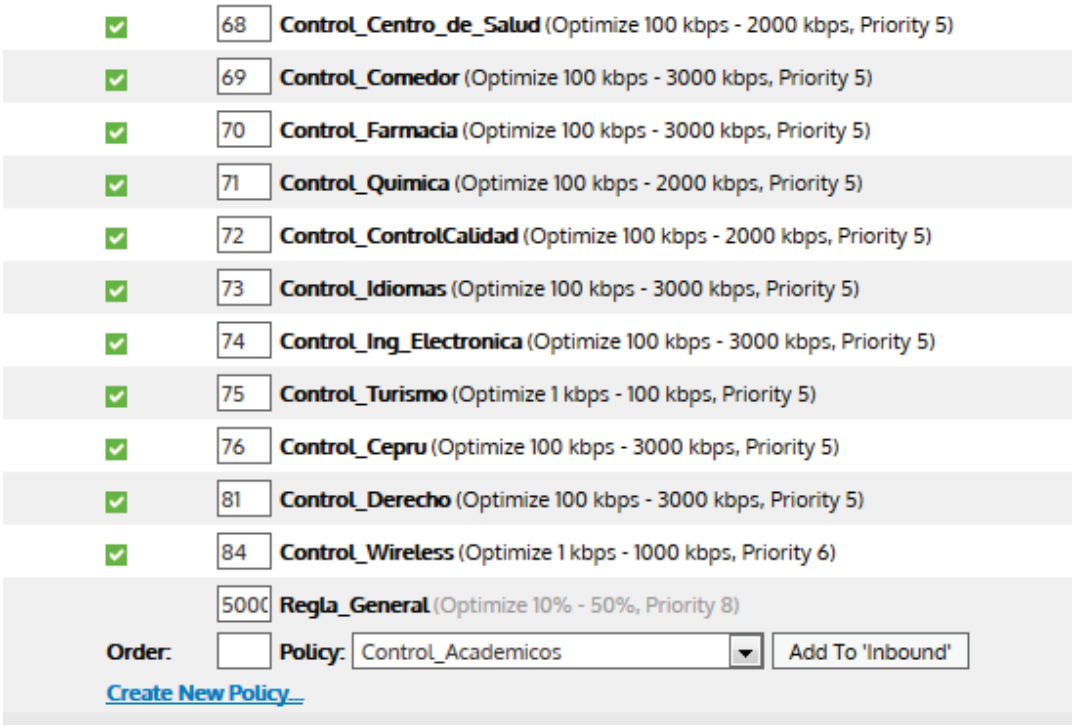


Fig. 4.5. Vista de la tasa de transmisión de las carreras profesionales - EXINDA - 3.

Con los datos de la Fig. 4.13, Fig. 4.14 y Fig. 4.15 realizamos un cuadro por carrera y subredes específicas que detallamos en el diagrama de red (ver Fig. 4.21) que proponemos, para las VLANs de Ing. Mecánica, Red de Comunicaciones y Personal no se asignó velocidades puesto que en comparación a otras carreras asumimos un tasa de transmisión promedio.

N - CoS 1				
VLAN	**NOMBRE**	**N (Mbps)**	**N TOTAL (Mbps)**	**CPE**
2	ING ELECTRICA	3	12	1
3	ING GEOLOGICA	2		
4	ING METALURGICA	1		
5	ING DE MINAS	3		
6	ING MECANICA	3		
8	EDUCACION	3	17	2
9	OBRAS	3		
10	DERECHO	3		
11	BIBLIOTECA CENTRAL	5		
12	RED DE COMUNICACIONES	3		
13	CEPRU	3	9	3
14	ING ELECTRONICA	3		
15	COMUNICACIÓN	3		
17	CONTROL DE CALIDAD	2	24.5	5
18	PERSONAL	3		
19	ING QUIMICA	1.5		
20	COMEDOR	3		
21	ARQUITECTURA	3		
22	ING CIVIL	3		
23	QUIMICA	2		
24	INST SISTEMAS	4		
25	CENTRO DE COMPUTO	3		
26	PABELLON C	5	6	6
27	TURISMO	1		
29	RED WIRELESS	29	29	7
32	ADMINISTRACION	3	12	8
33	CENTRO DE IDIOMAS	3		
34	CONTABILIDAD	3		
35	AULAS GENERALES	3		
36	ENFERMERIA	3	12	9
37	ING DE SISTEMAS	4		
38	MEDICINA	3		
39	CENTRO DE SALUD	2		
40	PABELLON ADMINISTRATIVO	5	8	10
41	CIENCIAS SOCIALES	3		
42	ECONOMIA	3	3	4
TASA DE TRANSMISION TOTAL		**132.5**	**132.5**	

Tabla 4.4. Dimensionamiento de la clase de servicio de datos o internet (CoS1)

La suma total según la Tabla 4.5 resulta 132.5 Mbps y los 10 Mbps del consumo de las sedes resulta 142.5 Mbps quedando 7.5 Mbps libres que según datos de la RCU son usados en otros circuitos virtuales específicos como el de autoridades, actualización software, control VPN radio enlace, jefe de área, etc, que el administrador de red ve por conveniente asignar.

Haciendo un análisis de cálculos de descarga promedio por usuario tenemos:

Por ejemplo a la carrera de Ing. Eléctrica se le asigna 3 Mbps y revisando el subnumeral (4.5.2.2) las consultas de páginas web tienen un tamaño máximo de 100 KB y una tasa de transmisión adecuada sería de 64 Kbps sin considerar descargas de archivos multimedia, video, archivos pesados.

Dónde:
B velocidad de transmisión global de acceso a internet
U definimos la cantidad de usuarios.
V tasa de transmisión adecuada

U= B/V = 3Mbps/64Kbps = 48 usuarios con acceso normal.

Esta ecuación podemos aplicar a todas las carreras y tener un promedio de usuarios.

(4.5.3.) Verificación del dimensionamiento de cada enlace.

La verificación del dimensionamiento de las tres clases de servicio se sustenta en las pruebas realizadas en el laboratorio, visto en el **CAPÍTULO VII** con equipos reales obteniendo así un banco de pruebas. En estas pruebas no solo se muestra los BW de cada clase de servicio, sino que la capacidad de cada equipo CPE, ya que por medio de estos equipos estarán cursando tráficos de CoS1, CoS2 y CoS3. Las capacidades de estos equipos se muestran en las características técnicas en el **ANEXO H**.

(4.5.) Descripción de la red IP-MPLS propuesta.

(4.6.1.) Descripción de la red IP-MPLS

El estudio de la presente tesis titulada ANÁLISIS Y MEJORA DE LA RED DE DATOS DE LA UNSAAC SOBRE LA PLATAFORMA IP-MPLS EN UN BANCO DE PRUEBAS, plantea dotar al campus Perayoc de la Universidad Nacional San Antonio Abad del Cusco, de una red de datos en la plataforma IP-MPLS para dar soporte a los programas aplicativos, unificar el servicio de transporte de datos para las redes basadas en circuitos y en paquetes de administrativos y académicos. La red IP-MPLS dará soporte a la ampliación de servicios a la comunidad universitaria con zonas de internet inalámbrico WIFI, redes privadas virtuales, ingeniería de tráfico, soporte de calidad de servicio (QoS), soporte multiprotocolo, establecimiento de clases de servicio (CoS), mecanismos de protección frente a fallos, redundancia, telefonía IP, transferencia de datos críticos, sistemas de vigilancia, seguridad con cámaras IP, asignación de IPs automáticas para evitar conflictos y congestión en la red.

Para el logro de las metas propuesta se desarrollaran por etapas, es vital que la red IP-MPLS se encuentre al 100% incluyendo el tendido de cable de fibra óptica, en las condiciones actuales se tiene una serie de limitaciones principalmente por la falta de equipamiento que no permite que se implemente esta tecnología MPLS, esto constituye la primera etapa del proyecto de la red IP-MPLS.

(4.6.2.) Descripción de la Red IP-MPLS y tendido de la fibra óptica.

(4.6.2.1.) Sala de máquinas – nodo principal edificio biblioteca central.

Actualmente el nodo principal de la red IP-MPLS tiene su acometida principal en el edificio de la Biblioteca Central, en lo que llamaremos la sala de máquinas (cuarto de telecomunicaciones), hasta este punto la empresa proveedora de servicios de internet ISP, Telefónica del Perú instalo un enrutador utilizando como medio de transmisión fibra óptica del tipo mono modo del fabricante Cisco modelo 2901. Se conecta mediante cable UTP Cat 6 hasta el enrutador Cisco modelo 3941E en lo que llamaremos equipo PE, a partir de este primer equipo PE_1 se conectan 4 equipos PE (PE_2, PE_3, PE_4, PE_5) en malla creando así la red IP/MPLS, a partir de los equipos PEs mediante cables UTP Cat 5e se distribuye a los convertidores de medio de cobre a fibra óptica del fabricante Raisecom está su vez se conecta con un enrutador Cisco modelo (1921) a las diferentes facultades en lo que llamaremos equipos CPE (CPE_1, CPE_2, CPE_3, CPE_,4 CPE_5, CPE_6, CPE_7, CPE_8, CPE_9, CPE_10), como lo detallamos en la siguiente Fig. 5.16.

Debemos indicar que los equipos en la instalación no cuentan con: Gabinetes o bastidores rackeables de piso disponibles para el cuidado adecuado de los equipos a instalar en la sala de máquinas.

No se cuenta con equipos PE administrables con los que deberían de contar la Red IP-MPLS en una instalación para el campus universitario Perayoc, tampoco en las facultades se tiene los equipos CPE, que deben de estar ubicados en el cuarto de telecomunicaciones para cada facultad. Cada facultad debe tener bastidor de telecomunicaciones, donde deben ir alojados los equipos CPE, switches de distribución y switches de acceso.

Todos estos detalles hace que el servicio sea interrumpido, debemos mencionar además que con la instalación de Plataformas de Enseñanza Virtual (e-learning) en todas las carreras de la UNSAAC en un periodo de plazo se debe de considerar la creación de centros de datos en cada facultad, en la cual se alojaran servidores educativos y sus correspondientes base de datos de información de libros de especialidad.

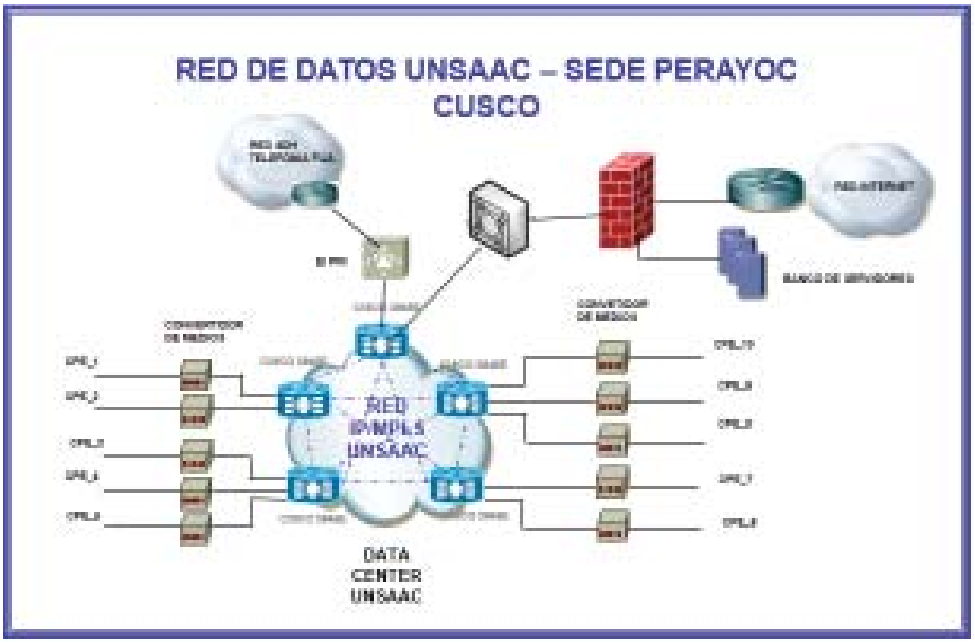


Fig. 4.6. Instalaciones cuarto de máquinas, Red IP-MPLS – Edificio Biblioteca Central

(4.6.2.2.) Nodos de distribución de la Red IP-MPLS en las facultades.

La Red IP-MPLS se tiende por medio de fibra óptica (reutilizando el tendido de FO existente de la UNSAAC) que llega a las facultades de tipo monomodo que ofrece mejores prestaciones para las futuras ampliaciones de la Red IP-MPLS, la fibra se despliega a través de ductos debajo de la tierra, protegidos con tubo PVC, distribuidos por todo el campus universitario Perayoc y brindando unificar los diferentes tipos de servicio y acceso a internet a las facultades como se muestra en el esquema.

La toma de fibra llega al convertidor de medios Raisecom y posteriormente al enrutador Cisco 1921, luego se conecta a un switch de cada facultad para su distribución. Por medio del equipo PE_1 que se configura para el NAT (Traducción de Direcciones de Red) y tener más direcciones IP a partir de un grupo de direcciones publicas asignados por el Proveedor de Internet ISP para la red IP-MPLS. Todas las instalaciones no cuentan ningún bastidor adecuado para la protección de los equipos. El segmento de la red IP-MPLS se detalla en la siguiente figura, que es para todas las facultades.
La figura anterior muestra la topología malla que se está empleando para la distribuir la conexión de RPV e Internet en cada facultad, la línea de fibra óptica llega al convertidor de medios, el convertidor de medios convierte la señal óptica a señal eléctrica que viaja en cable UTP de cobre. Seguidamente pasa al enrutador Cisco 1921, que se encarga de cambiar las direcciones IP de los diferentes segmentos de red, luego pasa al switch de distribución, de ahí a los switches de acceso de cada carrera profesional ubicado en cada facultad y distribuirse entre las computadoras que tienen laboratorios de cómputo, oficinas administrativas; la misma configuración se tiene para:

Facultad CPE_2, Facultad CPE_3, Facultad CPE_4, Facultad CPE_5, Facultad CPE_6, Facultad CPE_7, Facultad CPE_8, Facultad CPE_9, Facultad CPE_10

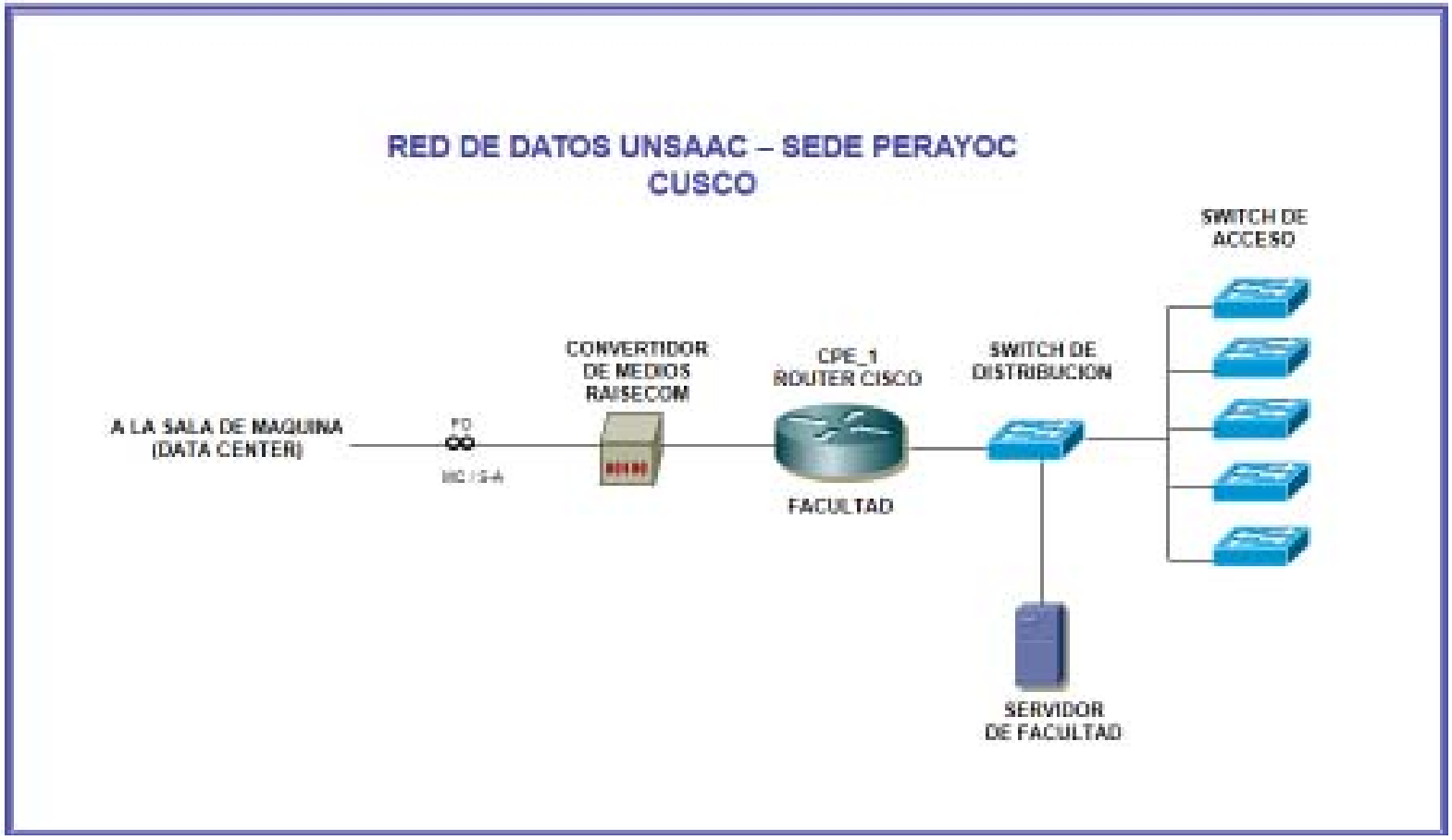


Fig. 4.7. Instalaciones de la red IP-MPLS en cada Facultad.

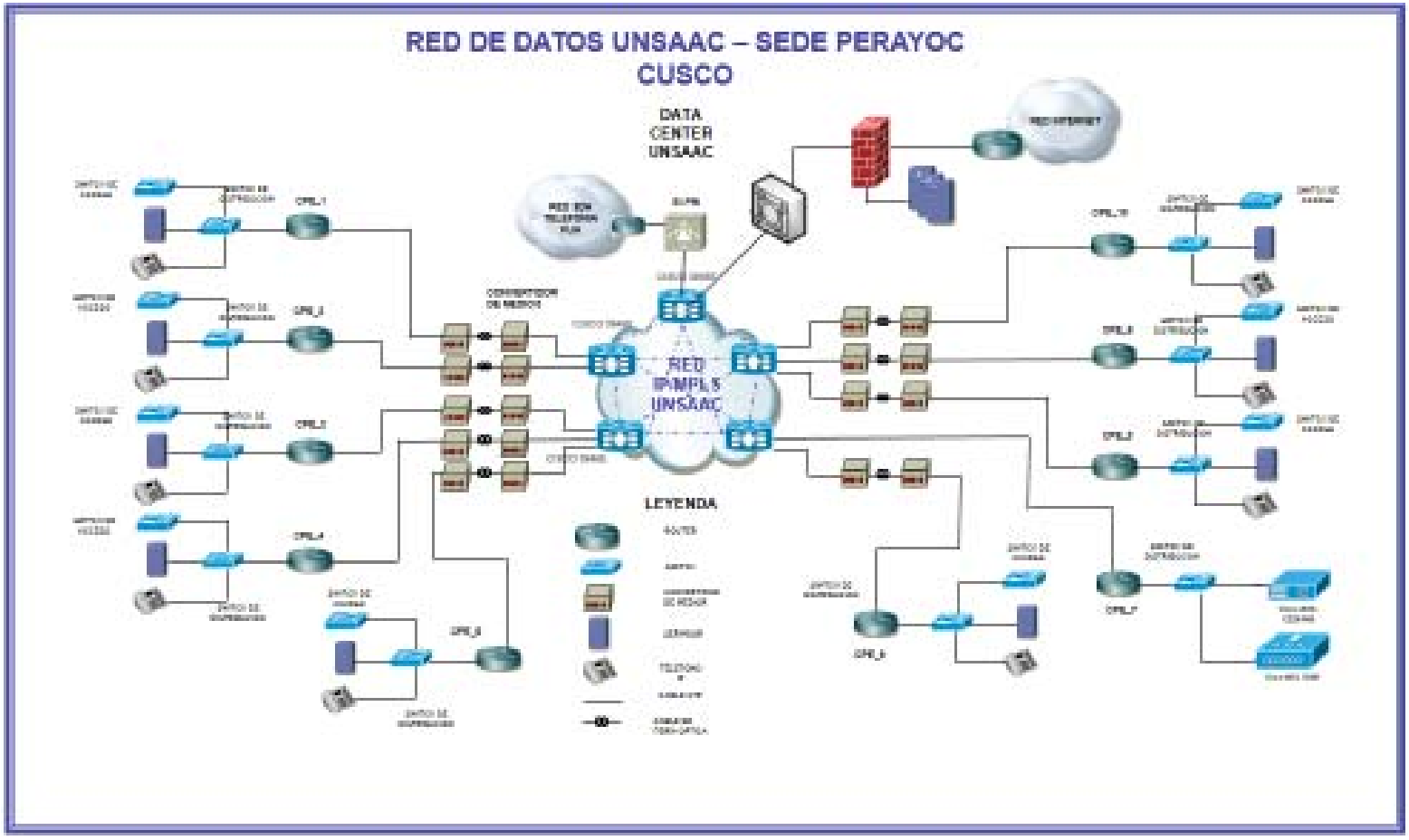


Fig. 4.8. Topología física de la Red IP-MPLS de la Universidad Nacional San Antonio Abad del Cusco.

(4.6.) Ampliación de la Red IP-MPLS.

(4.7.1.) Descripción de la ampliación Red IP-MPLS y tendido de la fibra óptica.

Para la ampliación de la red de datos en la plataforma IP-MPLS, es importante el equipamiento y el funcionamiento de estos, los cuales se explican a continuación.

(4.7.1.1.) Equipamiento para la distribución de la Red IP-MPLS

La red de datos de la Universidad Nacional San Antonio Abad del Cusco, necesita del equipamiento para su correcta distribución en todo el campus para ello se debe de emplear equipos que soporten el alto tráfico que se concentrara en la sala de máquinas, también debe de soportar los servicios que posteriormente se instalaran como: Telefonía Local sobre VoIP, Datos Críticos, Zonas de internet Inalámbrico para estudiantes, y sistemas de seguridad de cámaras además de los servidores de educación virtual que se implementaran paulatinamente en el futuro, en el siguiente grafico Fig. 4.21 se detalla la topología lógica de la Red General de datos en la plataforma IP/MPLS de la UNSAAC de alta velocidad que proveerá de estos servicios a la Universidad.

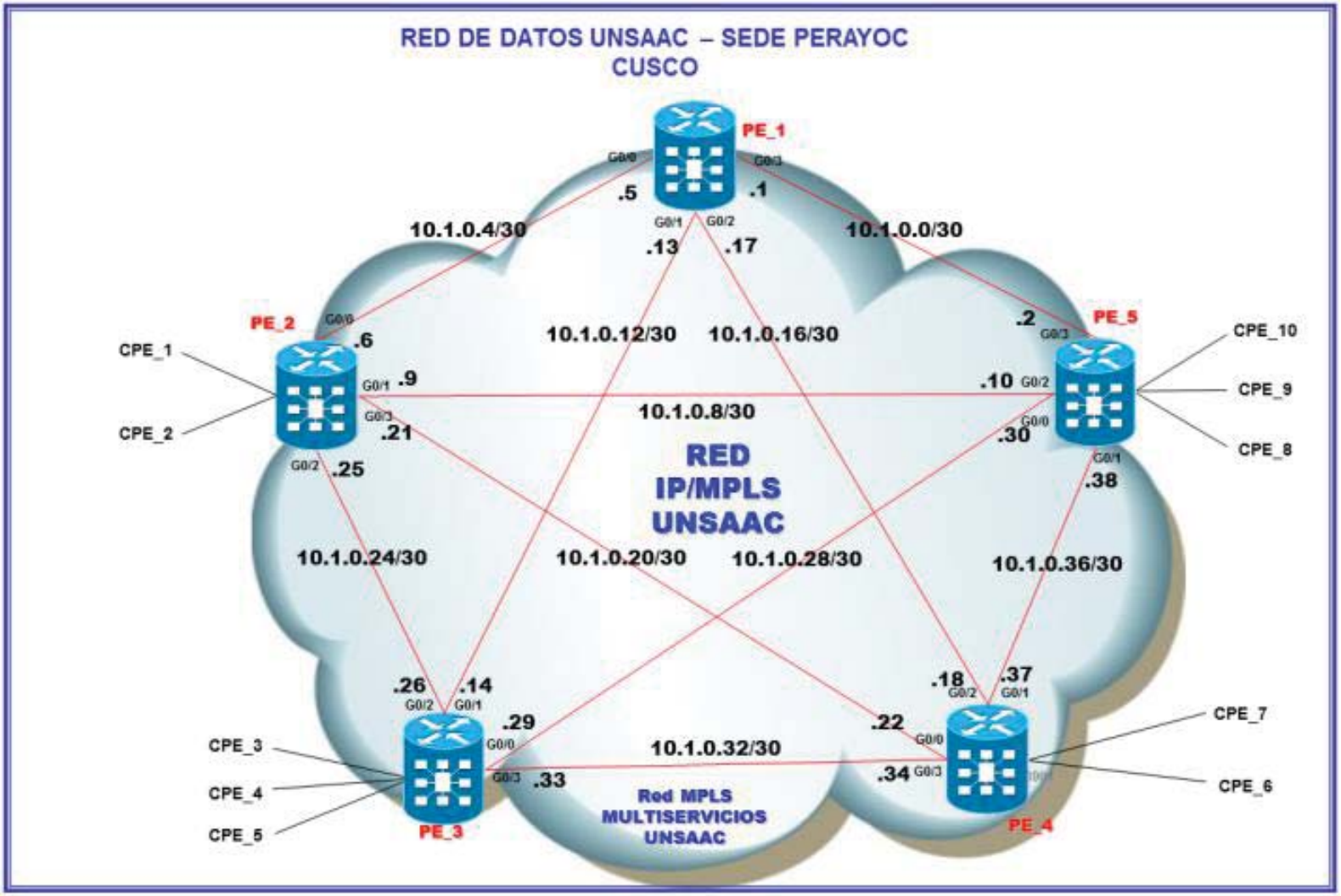


Fig. 4.9. La topología lógica de la Red IP-MPLS de la UNSAAC.

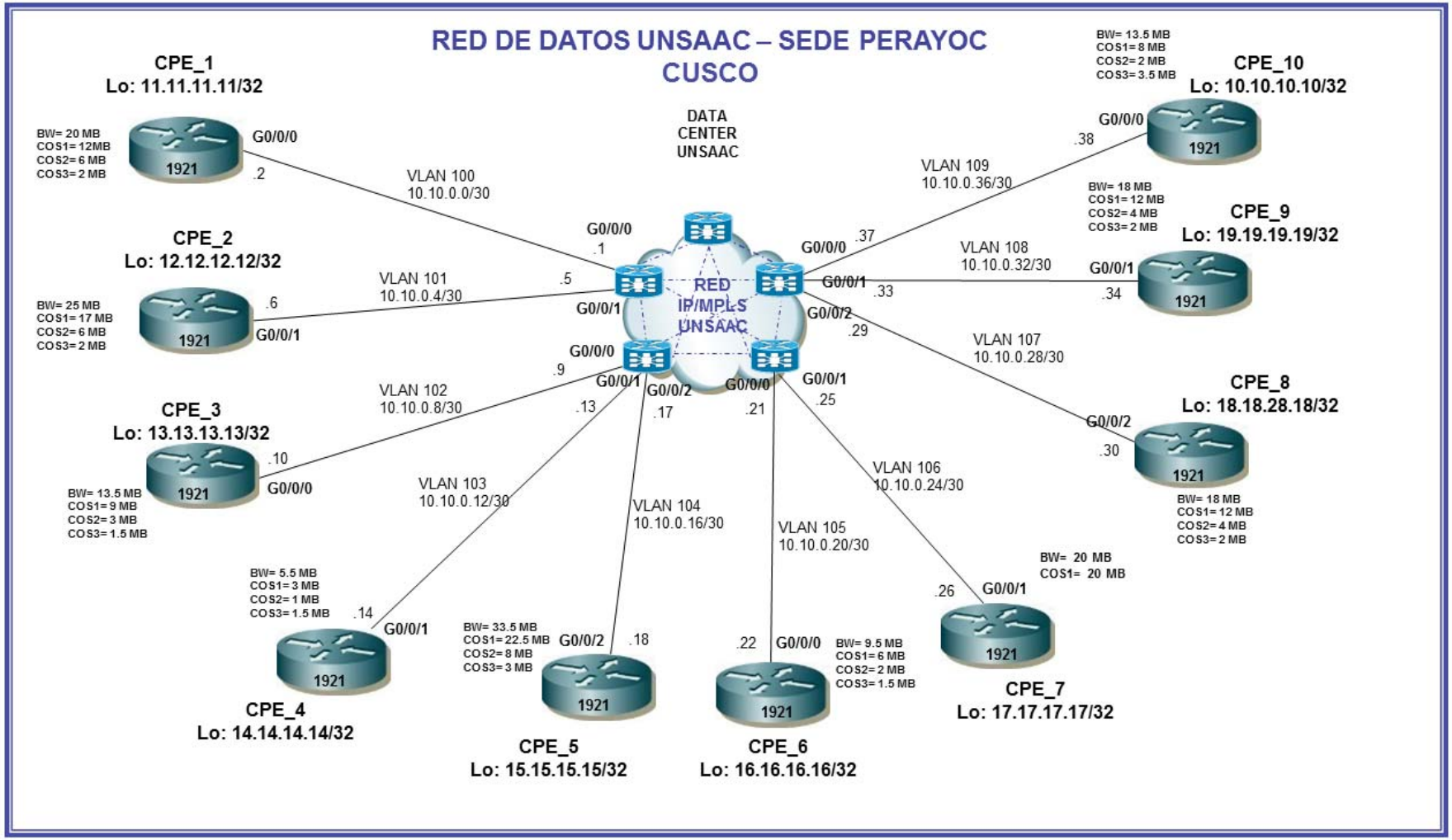


Fig. 4.10. La topología lógica de la Red IP-MPLS hacia las Facultades.

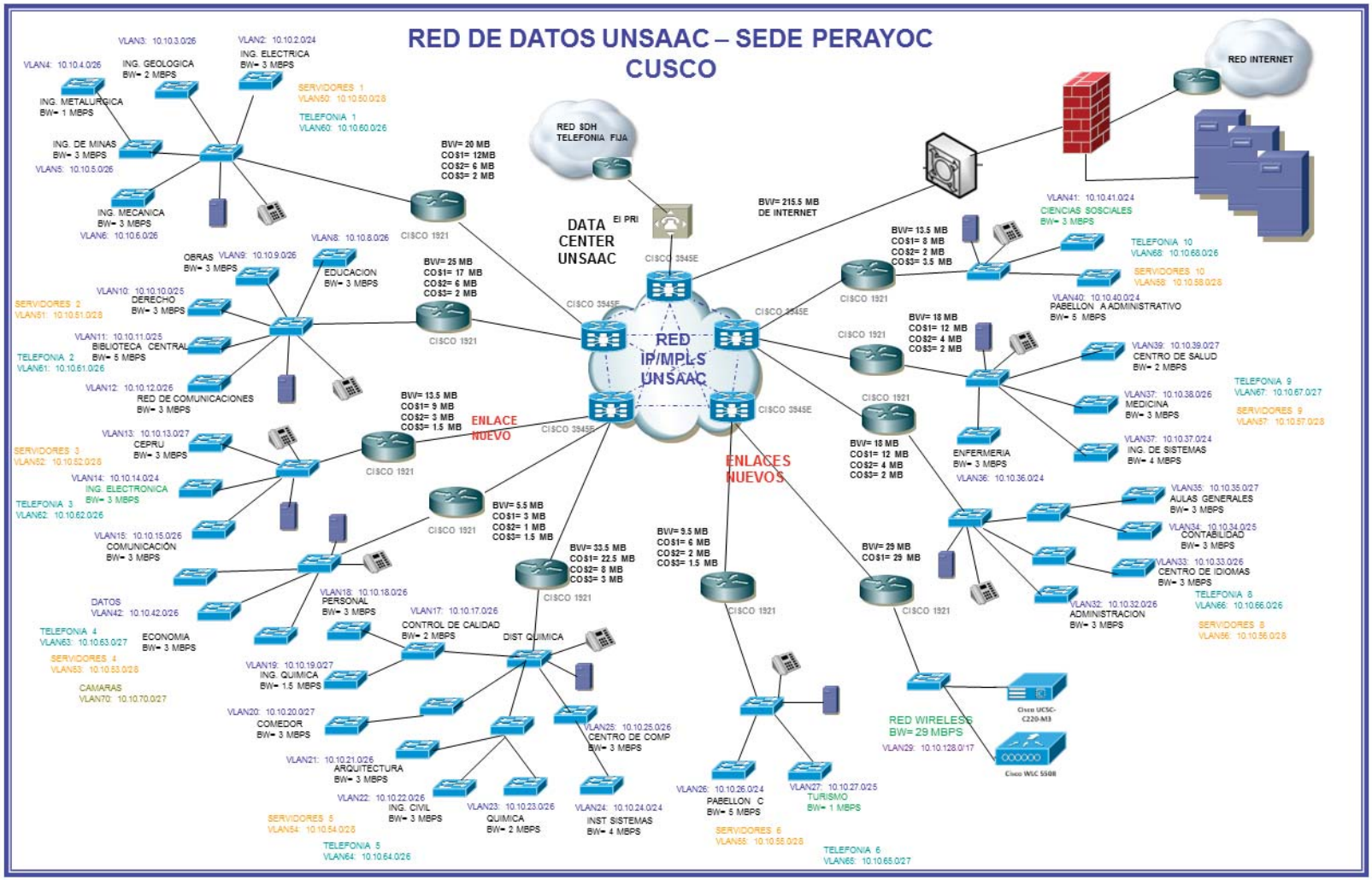


Fig. 4.11. La topología lógica de la Red General de datos en la plataforma IP-MPLS de la UNSAAC.

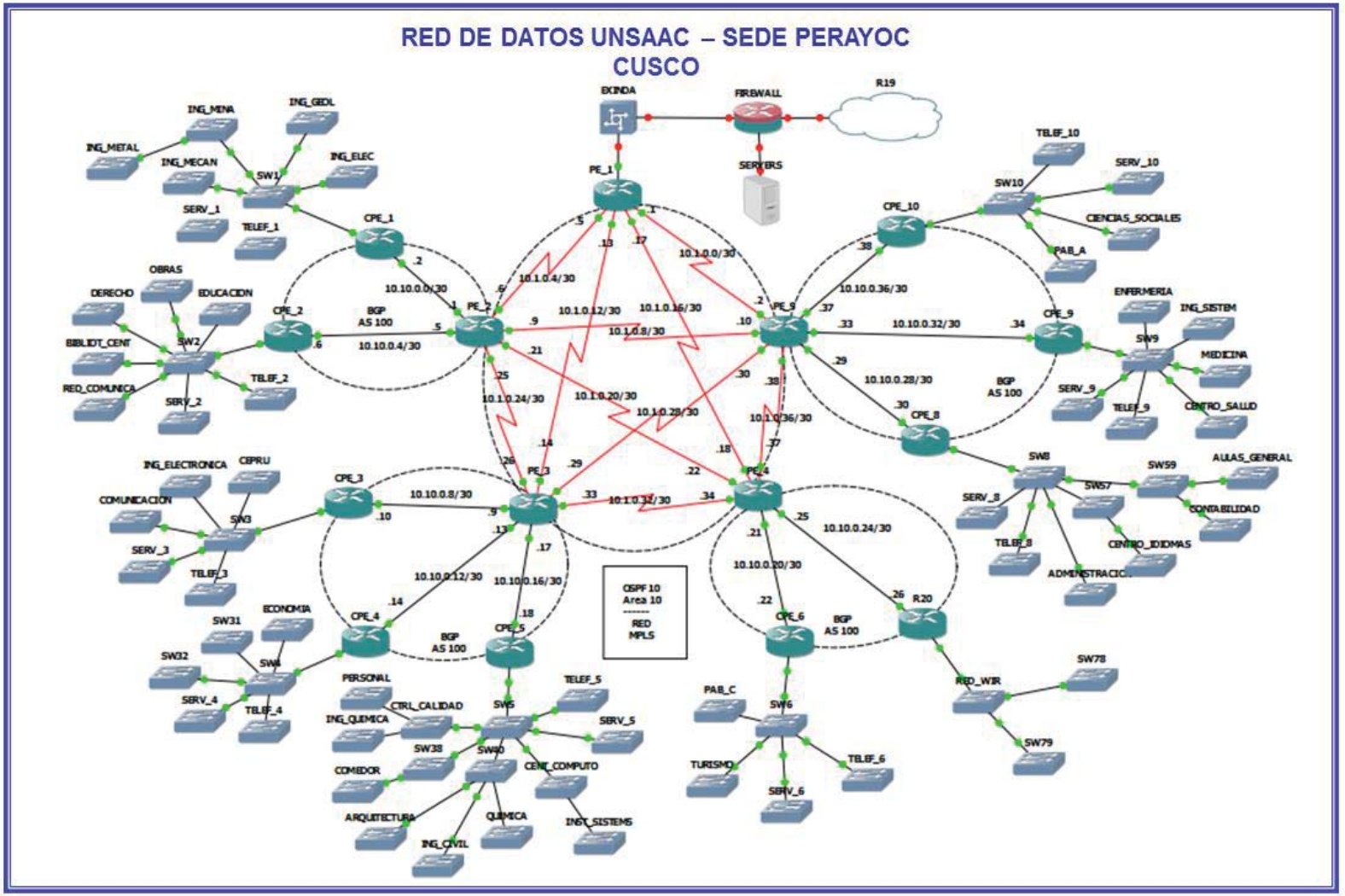


Fig. 4.12. Red MPLS propuesta para la UNSAAC – visto en software GNS3.

(4.7.1.2.) Tramos de ampliación de la Red IP-MPLS

La ampliación en la instalación de la Red de Datos de la Universidad interconecta directamente a todas las facultades dentro de los cuales agrupa un número específico de carreras profesionales.

Estas facultades están organizadas por los equipos CPE, y su agrupación de carrera es como sigue:

FACULTAD	CARRERA PROFESIONAL
FACULTAD CPE_1	ING ELECTRICA
	ING GEOLOGICA
	ING METALURGICA
	ING DE MINAS
	ING MECANICA
FACULTAD CPE_2	EDUCACION
	OBRAS
	DERECHO
	BIBLIOTECA CENTRAL
	RED DE COMUNICACIONES
FACULTAD CPE_3	CEPRU
	ING ELECTRONICA
	COMUNICACIÓN
FACULTAD CPE_4	ECONOMIA
FACULTAD CPE_5	CONTROL DE CALIDAD
	PERSONAL
	ING QUIMICA
	COMEDOR
	ARQUITECTURA
	ING CIVIL
	QUIMICA
	INST SISTEMAS
	CENTRO DE COMPUTO
FACULTAD CPE_6	PABELLON C
	TURISMO
FACULTAD CPE_7	RED WIRELESS
FACULTAD CPE_8	ADMINISTRACION
	CENTRO DE IDIOMAS
	CONTABILIDAD
	AULAS GENERALES
FACULTAD CPE_9	ENFERMERIA
	ING DE SISTEMAS
	MEDICINA
	CENTRO DE SALUD
FACULTAD CPE_10	PABELLON ADMINISTRATIVO
	CIENCIAS SOCIALES

Tabla 4.5. Organización de facultades y carreras profesionales.

La finalidad de la ampliación es reducir el tráfico y tener mayor independencia en el manejo de los equipos de red. De esta manera la eficiencia en la red de datos que funciona sobre la Red IP-MPLS de la universidad será mejorada.

Entre los accesorios también se necesita módulos de media converter, chasis de media converter para la fibra óptica y patch panel de UTP cat 5e o cat 6, en los bastidores de piso en l sala de máquinas y en los bastidores de pared en las facultades y carreras profesionales donde ha de llegar la fibra óptica.

a) Resumen de Equipos de la Red IP/MPLS.

En la siguiente tabla se enumeran los equipos necesarios para la ampliación de la Red IP-MPLS del campus universitario.

FACULTAD	EQUIPO	CANTIDAD
SALA DE MAQUINAS EDIFICIO DE LA BIBLIOTECA CENTRA	CISCO 3941E ROUTER	5
FACULTAD CPE_1	CISCO 1921 ROUTER	1
	CISCO 2960 SWITCH	6
FACULTAD CPE_2	CISCO 1921 ROUTER	1
	CISCO 2960 SWITCH	6
FACULTAD CPE_3	CISCO 1921 ROUTER	1
	CISCO 2960 SWITCH	4
FACULTAD CPE_4	CISCO 1921 ROUTER	1
	CISCO 2960 SWITCH	4
FACULTAD CPE_5	CISCO 1921 ROUTER	1
	CISCO 2960 SWITCH	12
FACULTAD CPE_6	CISCO 1921 ROUTER	1
	CISCO 2960 SWITCH	3
FACULTAD CPE_7	CISCO 1921 ROUTER	1
	CISCO 2960 SWITCH	1
FACULTAD CPE_8	CISCO 1921 ROUTER	1
	CISCO 2960 SWITCH	7
FACULTAD CPE_9	CISCO 1921 ROUTER	1
	CISCO 2960 SWITCH	5
FACULTAD CPE_10	CISCO 1921 ROUTER	1
	CISCO 2960 SWITCH	3

Tabla 4.6. Resumen de equipos de telecomunicaciones para la red de datos sobre la plataforma IP/MPLS.

Para su instalación se necesitarán bastidores de piso y bastidores de pared, así como el equipamiento eléctrico, suministro y protección. Los bastidores son recintos de protección de los equipos de telecomunicaciones. Se necesitara módulos y chasis convertidores de cobre a fibra, que deben de ser instalados en la sala de máquinas, y en cada facultad.

(4.7.2.) Técnicas, instrumentos e informantes o fuentes.

Una fuente de información es la red de la Operadora CLARO, la técnica del análisis de la red propuesta es comparativo a la red de una de las operadoras del país que viene a ser Claro, la red de esta operadora esta implementada en la plataforma IP/MPLS sobre el cual está el funcionamiento el servicio RPV (Red Privada Virtual) donde funciona el QoS (calidad de servicio), esta red es solo comparativa a la red de datos propuesta.

La propuesta de la red de datos de la UNSSAC en la plataforma IP/MPLS es en particular la más adecuada a la creciente demanda de BW y necesidad de velocidad, además de unificar las diferentes clases de servicios, RPV está orientado a dar solución a esta necesidad.
No puede ser incluido documentos, gráficas, diseños, entre otros de la infraestructura de red de la Operadora CLARO por derechos de privacidad.
Para la investigación de campo es necesario tomas de muestras de la conexión de CPE a CPE.

(4.7.3.) Poblaciones de informantes y muestra(s).

La red de datos actual de la UNSAAC, es como se muestra:

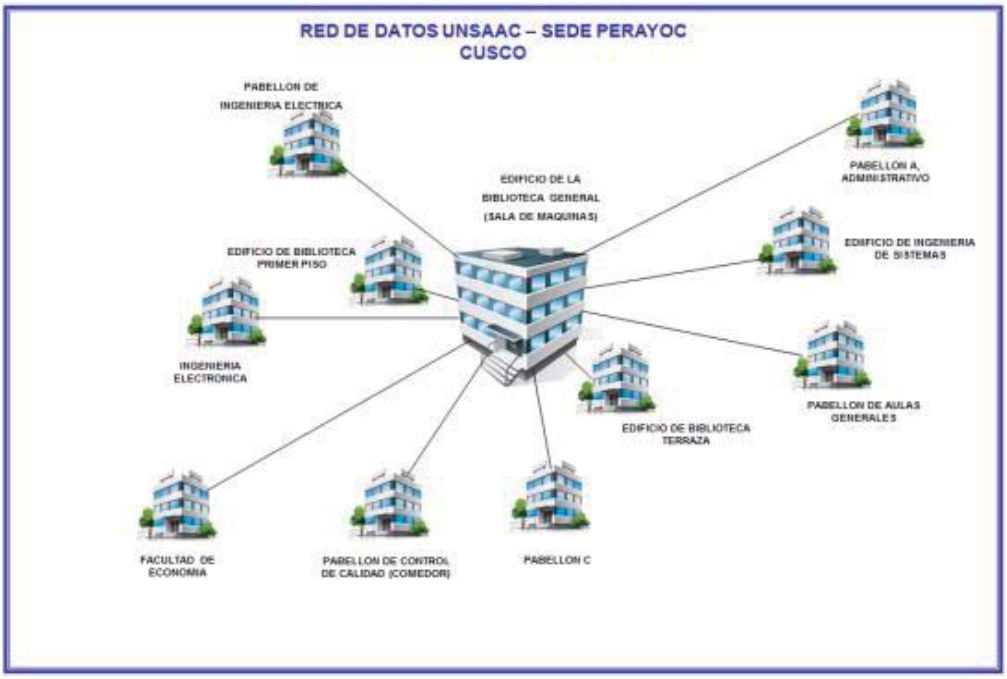


Fig. 4.13. Instalación Actual de la Red de Datos en el Campus de la UNSAAC

(4.7.) Determinación tramos de la Red IP-MPLS.

(4.8.1.) Planta externa

Comprende todos los equipos y materiales que están dentro del data center esto inicia desde la parte interna de los ODF principal y secundarios, jumpers de fibra óptica, conversores de fibra a Ethernet, enrutadores, switches, patch panel RJ-45, patch panel ópticos, reflejos RJ-45 y ópticos.

También comprende el cableado vertical entre pisos que se poseen todos los pabellones hacia los switches de acceso a la red, y el cableado horizontal para los diferentes puntos de red.

CAPITULO V

ESPECIFICACIONES Y REQUERIMIENTOS TECNICOS PARA LA RED DE DATOS PROPUESTA

Para la propuesta de la red de datos de la UNSAAC en la plataforma IP-MPLS, son necesarios ciertos requerimientos, equipamiento y especificaciones técnicos para el óptimo funcionamiento.

(5.1.) Equipamiento para la distribución de la Red IP-MPLS.

Los equipos a utilizarse para la instalación de la Red IP-MPLS propuesta se detallan a continuación en la siguiente tabla, se especifica el fabricante, su ubicación, el número de equipos.

Ítem	EQUIPO	FABRICANTE	CANT.	UBICACION
1	Router Cisco Modelo 3945E	CISCO	5	Sala de Maquinas
2	Módulo de Convertidor de Medio RC002-16 chasis	RAISECOM	1	Sala de Maquinas
3	Conversor de medios RC512-FE-S-SS15	RAISECOM	1	Sala de Maquinas
4	Router Cisco Modelo 1921/k9	CISCO	1	Facultad CPE_1
5	Conversor de medios RC512-FE-S-SS13	RAISECOM	1	Facultad CPE_1
6	Stand Alone RC001-1M chassis	RAISECOM	1	Facultad CPE_1
7	Router Cisco Modelo 1921/k9	CISCO	1	Facultad CPE_2
8	Conversor de medios RC512-FE-S-SS13	RAISECOM	1	Facultad CPE_2
9	Stand Alone RC001-1M chassis	RAISECOM	1	Facultad CPE_2
10	Router Cisco Modelo 1921/k9	CISCO	1	Facultad CPE_3
11	Conversor de medios RC512-FE-S-SS13	RAISECOM	1	Facultad CPE_3
12	Stand Alone RC001-1M chassis	RAISECOM	1	Facultad CPE_3
13	Router Cisco Modelo 1921/k9	CISCO	1	Facultad CPE_4
14	Conversor de medios RC512-FE-S-SS13	RAISECOM	1	Facultad CPE_4
15	Stand Alone RC001-1M chassis	RAISECOM	1	Facultad CPE_4
16	Router Cisco Modelo 1921/k9	CISCO	1	Facultad CPE_5
17	Conversor de medios RC512-FE-S-SS13	RAISECOM	1	Facultad CPE_5
18	Stand Alone RC001-1M chassis	RAISECOM	1	Facultad CPE_5
19	Router Cisco Modelo 1921/k9	CISCO	1	Facultad CPE_6
20	Conversor de medios RC512-FE-S-SS13	RAISECOM	1	Facultad CPE_6
21	Stand Alone RC001-1M chassis	RAISECOM	1	Facultad CPE_6
22	Router Cisco Modelo 1921/k9	CISCO	1	Facultad CPE_7
23	Conversor de medios RC512-FE-S-SS13	RAISECOM	1	Facultad CPE_7
24	Stand Alone RC001-1M chassis	RAISECOM	1	Facultad CPE_7
25	Router Cisco Modelo 1921/k9	CISCO	1	Facultad CPE_8
26	Conversor de medios RC512-FE-S-SS13	RAISECOM	1	Facultad CPE_8
27	Stand Alone RC001-1M chassis	RAISECOM	1	Facultad CPE_8
28	Router Cisco Modelo 1921/k9	CISCO	1	Facultad CPE_9
29	Conversor de medios RC512-FE-S-SS13	RAISECOM	1	Facultad CPE_9
30	Stand Alone RC001-1M chassis	RAISECOM	1	Facultad CPE_9

31	Router Cisco Modelo 1921/k9	CISCO	1	Facultad CPE_10
32	Conversor de medios RC512-FE-S-SS13	RAISECOM	1	Facultad CPE_10
33	Stand Alone RC001-1M chassis	RAISECOM	1	Facultad CPE_10

Tabla 5.1. Equipamiento utilizado en la Red IP-MPLS.

(5.1.1.) Equipamiento en sala de máquinas

SERVIDOR DE SEGURIDAD. La red IP-MPLS debe contar con un Centro de Datos para la administración y gestión del tráfico que genera la red, para ello necesitamos Servidor de administración que nos permitan proteger las configuraciones de los equipos de redes como enrutadores, switches y los servidores almacenamiento de archivo académico que se ubicarían en el campus universitario para el aprendizaje virtual que se tiene implementado; para ello se necesita servidores como el Firewall que tienen muchas aplicaciones para la seguridad de redes IP.[59]

El centro de cómputo de la universidad posee la base de datos de la formación académica de todos los alumnos de la universidad, esta información se encuentra digitalizada en un banco de servidores que está ubicada en el sótano de la Biblioteca Central – Data Center RCU, este banco de información necesita ser protegida y para ello se necesitan servidores que limiten el acceso, sólo modo usuario en la red de la universidad, motivo por el que necesitamos un Servidor de seguridad de redes.

El servidor de seguridad nos permitirá administrar y configurar la red internamente, filtrar la información que ve nuestros estudiantes, personalizar el perfil de acceso de los usuarios de la red y gestionar los equipos como enrutadores, switches, o los puntos de acceso inalámbrico, equipos que deben de ser monitoreados periódicamente, debe de contar con tarjetas de red que soporten velocidades de 1Gbps/10Gbps y ser rackeables para ser montados en el bastidor de comunicaciones.

ROUTER CISCO 3941E (EQUIPO PE).
Debe de contar con los equipos enrutador Cisco 3941E debido a sus características de estos equipos se diseña y configura una topología malla la Red IP-MPLS, que es el núcleo de la Red de datos del campus universitario. Esta topología malla de la Red IP-MPLS soporta todo el tráfico de la red y permite el máximo aprovechamiento de la fibra óptica instalada en todas las facultades, como característica principal de estos equipos soportan velocidades de 1Gbps/10Gbps, la posibilidad de adicionar módulos de interfaces de cobre de 10/100/1000Mbps.[60]
En estos equipos se configuran: el protocolo de enrutamiento dinámico OSPF sobre el cual funcionara la Red IP-MPLS, La Red Privada de Virtual (RPV), redundancia de rutas, ruta para la salida al Internet, la interacción de los protocolos de enrutamiento dinámico BGP y OSPF para su óptimo funcionamiento.

[59] *www.monografias.com*
[60] CISCO 3900 SERIES INTEGRATED SERVICES ROUTERS DATA SHEET

Fig. 5.1. Router cisco 3041E.

MÓDULO RC002-16 CHASIS Y CONVERSOR DE MEDIOS RC512-FE-S-SS15. Son módulos donde se insertaran las tarjetas media converter de señal Eléctrica a señal óptica, la conexión proveniente será de los enrutadores Cisco 3941E (Equipos PE) hacia los Chasis de media converter de señal Eléctrica a señal óptica de un slot y de esta a los enrutadores 881 o 1921 (Equipo CPE).[61]

Fig. 5.2. Módulo RC002-16 chasis y conversor de medios RC512-FE-S-SS15.

FIREWALL DE SEGURIDAD. Un firewall restringe el acceso externo y acceso interno. Externamente protege a la red de alguna hacker que pueda ingresar a la red vía internet, también protege la intranet del acceso a servidores de seguridad, servidores de base de

[61] *www.davantel.com/user/image/rc002-16-rev-e.pdf*

datos y servidores web, que debe tener todo Data Center. Los firewalls cumplen el papel de dirigir las políticas de acceso a la red, denegar y permitir acceso en las capa 1, capa 2 y capa 3 del modelo OSI.[62]

BASTIDORES DE PISO. Los bastidores de piso son los recintos metálicos donde se instalaran los enrutadores, switches, firewall, módulo de media converter de Fibra Óptica marca Raisecom, paneles de conexión de Cables UTP Cat 6, estabilizadores, UPS, y sistemas de ventilación que deben de incluir los bastidores.[63]

EQUIPAMIENTO ELECTRICO. El equipamiento eléctrico debe de brindar alimentación de tensión alterna 220 VAC, además de contar con supresores de picos, estabilizadores y sistemas de alimentación ininterrumpida UPS, los mismo que protegerán a los equipos ante cualquier fluctuación de la tensión alterna necesaria para el buen funcionamiento de os equipos de la sala de máquinas.

Nota. Las especificaciones de las capacidades de los equipos propuestos están en el **ANEXO H** donde se detalla para el tipo de servicio que llegue brindar.

(5.1.2.) Equipamiento en Facultades

Las facultades cuentan con varias carreras y estas a su vez cuentan con laboratorios de computo que deben de ser interconectados a la red IP/MPLS e internet, para ello se tienen que instalar equipos CPE y switches de distribución y acceso que garanticen la marcación de paquetes, las políticas de Calidad de Servicio, funcionamiento del protocolo de enrutamiento dinámico BGP, y el trafico generados por las diferentes Clases de Servicios (número de máquinas, servidores y teléfonos IP) de cada facultad en cuanto a ello se toma en consideración el número de centros de cómputos, el número de máquinas y a partir de allí determinar el modelo de enrutador y switch que se necesitara además de poder controlar el tráfico generado.
Los estándares de equipamiento recomiendan que se emplee enrutadores (Equipo CPE), switches de distribución, switches de acceso, por lo tanto tendríamos que emplear enrutadores y switches que se ajusten a estos requerimientos.

STAND ALONE RC001-1M CHASSIS Y CONVERSOR DE MEDIOS RC512-FE-S-SS13. Son chasis donde se insertaran los convertidores de medios RC512-FE-S-SS13 de señal eléctrica a señal óptica, la conexión proveniente será de la tarjeta insertada en el chasis media converter ubicadas en la salas de comunicaciones hacia los enrutadores 881 o 1921 (Equipo CPE).

[62] *www.segu-info.com.ar/firewall/firewall.htm*
[63] *www.jsl-online.net/Imgs/content/page_270/folheto_bastidores_castellano.pdf*

Fig. 5.3. Stand Alone RC001-1M chassis y conversor de medios RC512-FE-S-SS13.

ROUTER CISCO 1921 - EQUIPO CPE. Debe de contar con los equipos enrutador Cisco 1921 en cada facultad, porque en estos equipos se configuran: el protocolo de enrutamiento dinámico BGP, La Red Privada de Virtual (RPV), las políticas de calidad de servicio (QoS), marcación de paquetes, súper redes, para su óptimo funcionamiento. [64]

Fig. 5.4. Router cisco 1921.[65]

TARJETAS EHWIC CISCO. es un tipo de tarjeta de interfaz de red especializada (NIC) realizado por Cisco que permite a un dispositivo de red, como un enrutador para conectar y transmitir datos a través de una red de área extensa . Un WIC tiene una unidad de datos de servicio de canal integrado (CSU / DSU interfaz) para conectarse a un circuito digital y proporcionar la corrección de errores y la supervisión de la línea.[66]

[64] www.cisco1900router.com/cisco-1900-datasheet

[66] www.myriadsupply.com/product/cisco-ehwic-4esg/

Fig. 5.5. Tarjeta EHWIC Cisco.[67]

SWITCH DE DISTRIBUCIÓN. Los switches de distribución, son equipos encargados de realizas la distribución en las facultades a las diferentes carreras profesionales, deben estar conectado directamente al enrutador (Equipo CPE) de cada facultad, debe de trabajar a las velocidades de 1Gbps, además de realizar tareas de administración.[68]

SWITCH DE ACCESO. Finalmente los switches de Acceso, estos equipos deben de ubicarse en cada carrera profesional donde cada una de ellas tiene laboratorios, son equipos que trabajan en capa 2, deben de soportar velocidades de transmisión de 10/100/1000Mbps, con la capacidad de realizar RPV y control de acceso por MAC.[69]

(5.2.) Medios de transmisión utilizados.

Los medios de transmisión que se emplearan son fibra óptica multimodo (a fin de reutilizar el tendido de **Fibra Optica OM4**[70] existente actualmente en la UNSAAC, cuyas características se ve en la Fig. 5.6), cable UTP Cat 5e y UTP Cat 6, dependiendo del segmento de red en que se encuentre se emplea un determinado tipo de cable; para la sala de máquinas los cables de fibra que se usarían son fibra monomodo ya que en este ambiente se congestionará todo el tráfico de la red y por sus características este tipo de fibra lo soportaría, también se encuentran el cable de cobre UTP Cat 6 que realiza transmisiones de 10/100/1000/10000 Mbps que interconecta del enrutador Proveedor a la Red IP/MPLS, y la interconexión entre los equipos PEs en la topología malla.

Ya en las facultades se puede encontrar cables de tipo UTP Cat 5e y UTP Cat 6, con estos cables pueden alcanzar velocidades de 10/100/1000Mbps y 100/1000/10000Mbps, siempre debemos recordar que las tarjetas de red deben de soportar esta velocidad de 1000Mbps para que se aproveche al máximo, sino se tuviera estas tarjetas de red no se podría realizar una transmisión de datos a estas velocidades.

---

[67] www.myriadsupply.com/product/cisco-ehwic-4esg/
[68] *www.cisco.com/c/es_mx/products/switches/*
[69] *www.cisco.com/web/ES/products/switches_lan.html*
[70] *www.radio-enlace.com/tipos-de-fibra-om1-om2-om3-om4-om5-os1-os2*

Categoría	Ancho de banda modal mínimo	100 Mb Ethernet 100BASE-FX	1 GB (1000 Mb) Ethernet 1000BASE-SX	10 GB Ethernet 10GBASE-SR	40 GB Ethernet	100 GB Ethernet
OM1 (62.5/125)	200 / 500 MHz·km	Hasta 2000 metros (FX)	275 metros (SX)	33 metros (SR)(	No soportado	No soportado
OM2 (50/125)	500 / - MHz·km	Hasta 2000 metros (FX)	550 metros (SX)	82 metros (SR)(	No soportado	No soportado
OM3 (50/125) **Laser Optimized**	1500 / 2000 MHz·km	Hasta 2000 metros (FX)	550 metros (SX)	300 metros (SR)(	100 metros 330 metros QSFP+ eSR4	100 metros
OM4 (50/125) **Laser Optimized**	3500 / 4700 MHz·km	Hasta 2000 metros (FX)	1000 metros (SX)	400 metros (SR)(	150 metros 550 metros QSFP+ eSR4	150 metros

Fig. 5.6. Características de la Fibra Óptica OM4.[71]

(5.3.) Normas y reglamentos

Como se ha referido anteriormente, para la selección de los diferentes equipos del sistema se han aplicado los requisitos mínimos de seguridad prescrito en el reglamento nacional de construcción, los estándares internacionales de equipamiento electrónico para la compatibilidad entre equipos de distintos fabricantes. Se considera también sus normas técnicas de cableado estructurado, en la instalación y montaje de los equipamientos propuesto, y que son las siguientes.

Norma IEEE 802.11a, para las redes inalámbricas.[72]
Norma ANSI/TIA/EIA-568-A, norma para la construcción comercial de cableado de telecomunicaciones.[73]
Norma ANSI/TIA/EIA-569, norma de construcción comercial para vías y espacio de telecomunicaciones.
Norma ANSI/TIA/EIA-606, norma de administración para la infraestructura de telecomunicaciones en edificios comerciales.[74]
Índice de protección IP para las cámaras de IP67, IP66 e IP56.[75]
Índice de protección NEMA 4X

[71] *www.radio-enlace.com/tipos-de-fibra-om1-om2-om3-om4-om5-os1-os2*
[72] *ieeestandards.galeon.com/aficiones1573579.html*
[73] *unitel-tc.com/normas-sobre-cableado-estructurado/*
[74] *informaticcbtis263.blogspot.com/2012/03/tiaeia-606-2-1.html*
[75] *www.reinmedical.com/es/conocimientos-tecnologia/clases-de-proteccion-ip.html*

(5.4.) Software para la administración de la red general.

La administración de la red con respecto al monitoreo de red avanzado, trafico cursado, subida o bajada seguirá pasando por el Exinda cuya función específica es monitoreo de red.
Con respecto al troubleshooting a nivel trasporte y protocolos de red, cambios en las red, ampliación o disminución de anchos de banda, estará bajo las interfaces gráficas del software SecureCRT[76] versión actualizada o software HyperTerminal Private Edition[77], Putty con el cual el administrador a cargo de la red IP-MPLS, podrá controlar de manera directa y remota de cada equipo.
La seguridad de equipos enrutadores se da en la configuración de cada equipo enrutador con los comandos tacas AAA que podría ser administrado desde una PC o server-host (administrador de red).
Según la información de la Red de Datos de la UNSAAC es posible gestionar todos los swtiches de distribución y acceso de la red por lo cual también podrían acoplarse a la administración desde un server-host.

(5.5.) Consideraciones de la propuesta de equipos CISCO.

(5.5.1.) Equipos de red CISCO.

Las consideraciones de la propuesta de la red de datos en base a los equipos de red CISCO, son las siguientes.

Cisco proporciona una red segura y fiable que puede manejar todos los tipos de tráfico, a lo largo de toda la red, más de prácticamente cualquier medio, mientras que proporciona la prestación de servicios consistente para todos los usuarios.
Cisco ha sido el centro de muchos cambios históricos en la tecnología y su uso. Ahora, cuando la industria de la tecnología está atravesando un período de cambios dramáticos, Cisco sigue siendo el líder del mercado en múltiples áreas, tales como routing y switching, comunicaciones unificadas, movilidad y seguridad. La compañía ayudó a catalizar el movimiento de la industria hacia IP, y, ahora que está en pleno desarrollo, Cisco está en el centro de los cambios fundamentales en la forma en que el mundo se comunica. [78]

Cisco y su sistema de red. El éxito de una empresa depende de sus sistemas de red. Como una empresa cuyo éxito depende de la propia sus sistemas de red, Cisco entiende perfectamente esta relación.
La necesidad de sistemas de alta disponibilidad, sensibles y seguros de red no es nueva. Sin embargo, en el entorno actual de las fusiones, adquisiciones y expansión global, las empresas ahora requieren sistemas de red que permiten a los servicios de innovación tecnológica y críticos para el negocio, no sólo en la sede, sino a través de campus corporativos geográficamente dispares, a lo largo de las ramas, y hacia fuera a los trabajadores remotos. Cisco puede proporcionar una red de extremo a extremo, compuesto por sistemas específicamente diseñados para hacer frente a las necesidades

[76] *https://www.vandyke.com/products/securecrt/*
[77] *www.hilgraeve.com/hyperterminal/*
[78] *www.cisco.com/c/es_pe/index.html*

únicas de cada lugar en la red, conectados por una infraestructura común y un sistema operativo común y manejable desde una ubicación central como una entidad única, cohesiva.

Sistemas de red para lugares en la Red. En la mayoría de los casos, la red de una empresa u organización no es una sola isla. Es probable que se compone de múltiples redes, incluyendo uno o más campus, algunas número de sucursales, teletrabajadores remotos, y uno o más centros de datos, todos conectados a través de una WAN o MAN. Estas empresas y organizaciones requieren soluciones que funcionan a través de toda la red, a través de todos los "lugares en la red."
Cisco entiende y responde a las necesidades únicas de cada lugar en la red:
- **Campus:** Cisco proporciona una plataforma diseñada para la colaboración con el Campus de la Comunicación de la red, que permite el dominio de aplicación, las comunicaciones multimedia seguras, mejorar la productividad y la innovación, continuidad de negocio y operaciones eficientes a través de una infraestructura flexible.
- **Sucursal / WAN:** Cisco ofrece a los usuarios de llegada, un pie de igualdad con el Poder Empowered, que integra la mayor cantidad de servicios y aplicaciones al mismo tiempo que optimiza su interoperabilidad y rendimiento para una experiencia consistente. En la cabecera de red WAN, Cisco ofrece soluciones de servicios de agregación que combinan la integración de servicios virtualizados, la optimización del ancho de banda, y la inteligencia de aplicaciones para proporcionar enrutamiento segura e inteligente de aplicaciones a través de la WAN de la empresa.
- **Centro de datos:** Las soluciones de los centros de datos de Cisco se basan en los principios de consolidación, virtualización y automatización para proporcionar la seguridad, disponibilidad, capacidad de gestión y distribución de aplicaciones que permiten optimizar el rendimiento de prestación de servicios y la aplicación superior.

Enrutamiento. Los enrutadores Cisco permiten a las organizaciones crear una base para una red inteligente, auto-defensa, que ofrece servicios de seguridad mejor en su clase y las tecnologías de enrutamiento para un coste total de propiedad bajo y un alto retorno de la inversión. Estos enrutadores ofrecen:
• Líder en el sector servicios, las densidades de ancho de banda, la disponibilidad y opciones de rendimiento para máxima flexibilidad de configuración y escalabilidad de los entornos de red más exigentes
• El rendimiento de servicios de calidad y protección de la inversión
• Un enfoque de sistemas integrados a los servicios integrados que acelera el despliegue de aplicaciones y reduce los costos operativos y la complejidad
Para ayudar a garantizar la seguridad de la red, estos enrutadores incluyen soporte para cifrado de seguridad IP (IPsec), unos cortafuegos de estado integrado, y soporte para control de acceso basado en la identidad.

(5.5.2.) Otras marcas de equipos de red frente CISCO.

La propuesta de equipos CISCO frente a marcas como JUNIPER, 3COM y otro; se basa en referencia a esta información.

Cisco vs / Juniper / 3Com / otros.

Sólo Juniper ha dado a Cisco un verdadero desafío.

Cisco todavía lleva a cabo la mayor parte del mercado de enrutadores proveedor de empresa y servicios, con una base de clientes que en su mayoría leales a su presencia predominante. Pero es Cisco y Juniper que tratan de superar a sí tecnológicamente en el núcleo proveedor de servicios y el borde. En este momento, la carrera de núcleo multi-chasis enfrenta Carrier Routing System de Cisco en contra de la serie T de Juniper para decenas - incluso cientos - de la supremacía terabits.[79]

Juniper está teniendo mejor suerte contra Cisco en el mercado de proveedores de servicio que Cabletron, Bahía, IBM y 3Com tenían en la empresa. La compañía robó un tercio de la cuota de mercado de enrutadores proveedor de servicios global de Cisco y sigue siendo un competidor viable y alternativa a Cisco en ese mercado. Juniper también está tratando de ampliar este éxito en el mercado de la empresa, donde adquirió VPN y tecnologías de firewall líder NetScreen.
Ambas compañías están rodeados de socios de alto perfil para ayudar a empujar sus visiones opuestas: Cisco con EMC y VMware, y Juniper con IBM.

Bay. Se formó a partir de la necesidad de la fusión de dos rivales más pequeños - Cisco sinópticos en los centros empresariales y conmutadores, y Wellfleet en la empresa enrutadores. Pero incluso la combinación de dos jugadores importantes en sus respectivos mercados no pudo frenar al gigante Cisco.

Cabletron, por su parte, se comprometió a paso en falso competitivos por tener su licencia de software del enrutador Cisco IOS revocado después de un evento de dobles.
Cabletron había desaparecido unos años más tarde, después de haber dividido en cuatro empresas en 1999.

[79] http://www.networkworld.com/article/2287422/lan-wan/cisco-vs--bay-3com-cabletron-juniper.html

	COMPARACIONES		
	CISCO	JUNIPER	ALCATEL
RED SIN FRONTERA	Una red sin frontera para mediante ayuda a garantizar que la red proporcione una experiencia de video de alta calidad y este lista para responder a los cambios en las demandas de ancho de banda	integracion incompleta de servicios en comparacion con las de los routers ISR G2 y ASR 1000 de Cisco. No ofrece aceleracion de WAN ni voz en los gateways de servicios de la serie SRX para sucursales. Los routers de extremo universal de juniper no incorpora VPN IPSec. control de limites de sesiones y firewall con funciones incompletas.	La .solución de enrutamiento IP de Alcatel-Lucent, ofrece un conjunto completo de herramientas para implantar redes "MPLS de extremo a extremo"
CENTRO DE DATOS Y VIRTUALIZACION	Cisco ofrece una solucion completa de centro de datos con computacion, redes, switching de almacenamiento, seguridad y servicios de capa 4-7. Cisco proporciona funciones de mayor escala para los centros de datos de gran magnitud.	No ofrece ninguna soluciones de computacion. No ofrece soluciones de optimizacion de aplicaciones ni equilibrio de carga para centros de datos. No ofrecen ninguna solucion de switching de almacenamiento.	Dificultad de despliegue, sus comunicaciones puede integrar problemas con los actuales centrales privados de un cliente (PBX) y correo de voz de sistemas, lo que no les permite reemplazar los componentes de acuerdo con su propia calendario y el presupuesto
COLABORACION	Comunicaciones unificadas empresariales a traves de soluciones VoIP, de conferencia, mensajeria instantanea y colaboracion.	Juniper no tiene una solucion completa de colaboracion.	trampas y estrategias de réplica de Cisco. Alcatel no ofrece un conmutador LAN viable para comunicaciones IP y así no intentarán vender OmniSwitches. Aplicación de etiquetado 802.1p / Q de Alcatel no lo hace prever cualquier integración directa con un conmutador de capa 2
VIDEO	Cisco ofrece una solucion completa desde el punto terminal hasta el nucleo, que comprende Cisco TelePrecence, decodificadores y transporte optimizado para video, a fin de que los proveedores ofrezcan servicios de alta calidad.	no ofrece transporte optimizado para video; los niveles de QoS son deficientes, no ofrece supervision de video en linea, la tecnologia multicast es fragil.	Aunque Alcatel indica que puede habilitar un sistema PCX con la adición de tarjetas de INT-IP, la construcción de un sistema fiable requiere el despliegue de servidores de llamadas externas. La implementación de la nueva de correo de voz 4645 requiere un servidor dedicado o CPU llamada externa. La función de respaldo de enlace de señalización requiere el nuevo "común" pasarelas de medios. Para hacer uso del teléfono basado en software o cualesquiera otras nuevas características, servidores dedicados deben estar desplegados
IP REDES DE SIGUIENTE GENERACION	Cisco ofrece amplias soluciones IP y opticas para brindar maxima flexibilidad en operaciones arquitectonicas y minimizar los costos.	no ofrece ninguna solucion optica.	La señalización de Alcatel de copia de seguridad del enlace instalación no es comparable a SRST. En la solución de Alcatel, la pasarela de medios a distancia se reinicia cuando se pierde el contacto con el servidor de llamadas y los teléfonos pierden toda la conectividad.
ASISTENCIA TECNICA	Cisco ha implementado 50 millones de dispositivos y mantiene 6 millones de interacciones anuales con clientes. El 80% de los casos se resuelven por internet.	ha implementado menos dispositivos, ha resuelto menos problemas mediante interacciones con los clientes, y sus arquitecturas de referencia son insuficientes.	Servicios de integración, equipo internacional de consultores con más de 2.500 sistemas IP y TDM, aplicando conocimientos acreditados y las mejores prácticas en tareas de gestión de proyectos.
SERVICIOS PROFESIONALES	Cisco cuenta con una gama completa de servicios profesionales, entre ellos los Smart (inteligencia de red proactiva)	las ofertas de juniper son mucho mas reducidas y n abarcan el ciclo de vida util de la red. Servicios especificos de arquitectura muy limitada.	Alcatel no cuenta con servicios profesionales Smart en su portafolio.
ALCANCE MUNDIAL	Cisco cuenta con mas de 900 centros logisticos en todo el mundo.	Juniper cuenta con pocos depositos de repuestos y centros de reparacion, por lo cual se producen demoras importantes a la hora de cambiar hardware defectuoso.	Cuenta con pocos depositos de repuestos en todo el mundo.
TIEMPO DE RESPUESTA	El tiempo de respuesta inicial de los servicios de Cisco es de entre 4 veces y 15 veces superior al de Juniper.	procesos de resolucion mas prolongados en el tiempo. Mas interrupciones de servicios. Mayores costos a causa de las posibles interrupciones mas prolongadas.	Mas interrupciones de servicio.

Tabla 5.2. Tabla comparativa de características de marcas en el mercado.[80] [81]

[80] http://es.slideshare.net/ciscolatinoamerica/por-qu-cisco-y-no-juniper

[81] http://www.cisco.com/web/partners/downloads/sell/technology/storage/unifiedcomm/Cisco_vs_Alcatel_IP_Communications_for_the_BDM.pdf

CAPITULO VI

ANALISIS DE LA MUESTRA DE LA RED IP-MPLS

(6.1.) Escenario básico

En esta parte de la tesis se va a explicar cómo se configura los distintos enrutadores y equipos para poder realizar pruebas. Además del significado de los comandos.

El escenario está compuesto por tres enrutadores Cisco 1921 como equipos PEs que configuran dos tramos MPLS, un enrutador Cisco 1921 y un enrutador Cisco 881 como equipos CPEs en las salidas de los equipos PE hacia las facultades, un switch en la entradas de las redes LANs de cada equipos CPE y un host de origen y destino en los extremos de la red. En los host que viene a ser laptops se analizaran los paquetes y marcación por medio del Wireshark. La siguiente fig. 6.1 ilustra el escenario implementado.

(6.2.) Topología lógica y física de la simulación.

En el escenario es necesaria la topología física o los recursos físicos y la topología lógica que comprende el direccionamiento, interfaces, AS, áreas, anchos de banda, VLANs, protocolos de enrutamiento dinámico como OSPF, BGP y MPLS, las cuales se ve a continuación.

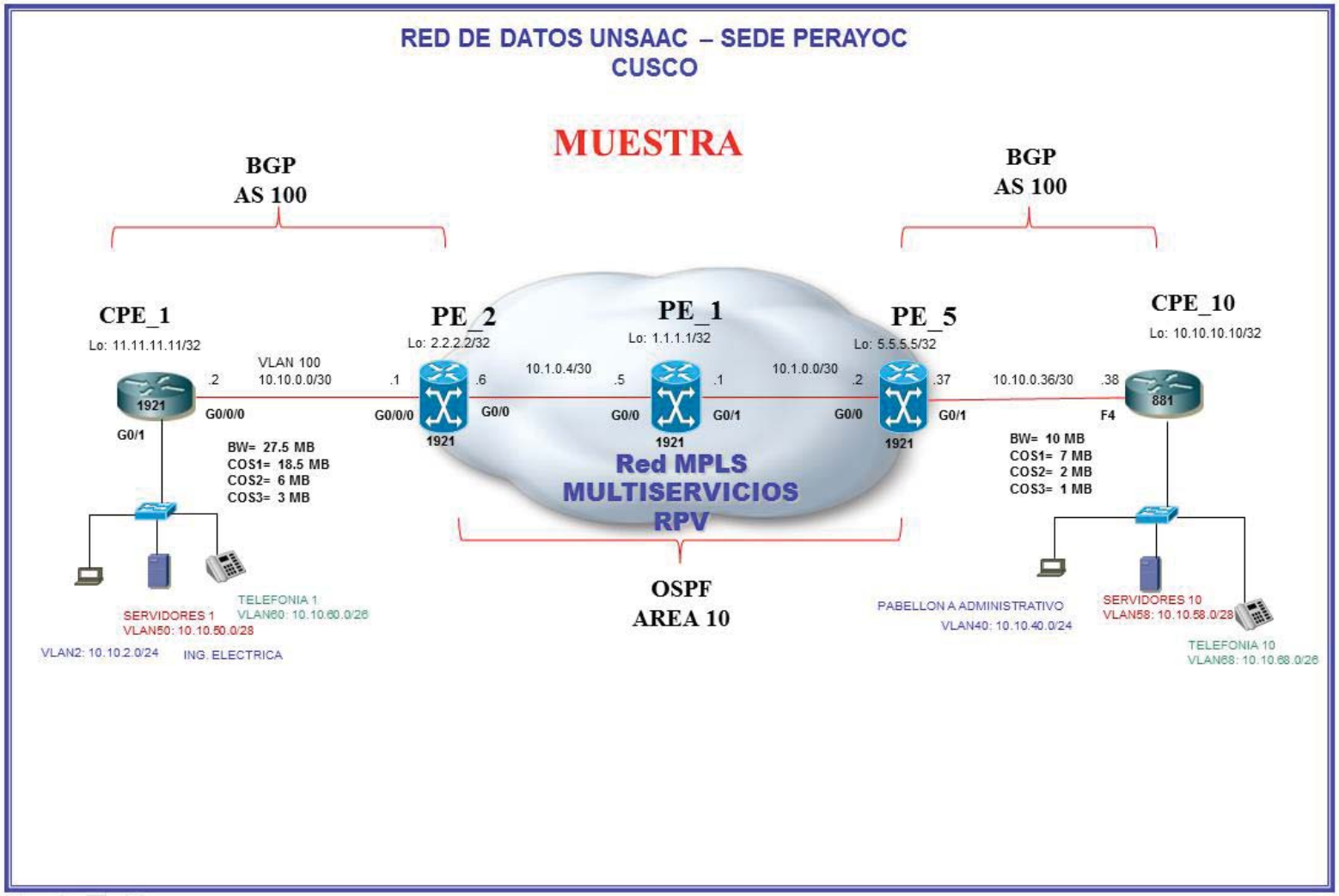


Fig. 6.1 Muestra en equipos reales cisco, para el análisis.

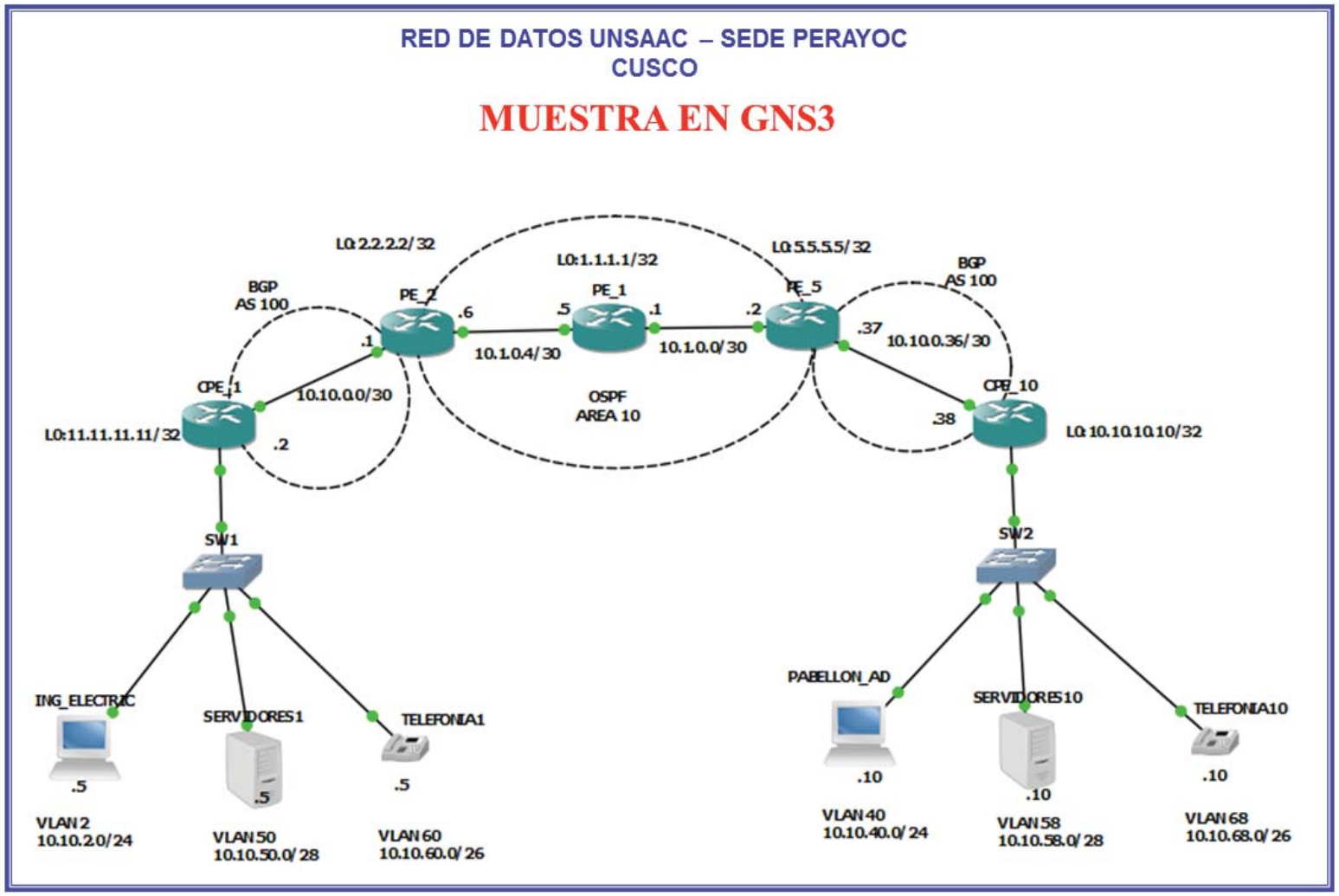


Fig. 6.2. Muestra de equipos en GNS3, para el análisis complementario.

(6.3.) Consideraciones de las configuraciones de los equipos.

La razón por lo que se ha elegido este escenario es porque es el mínimo equipamiento para poder observar correctamente la conectividad extremo-extremo de la red IP-MPLS.

Según el análisis teórico, en una red MPLS, para poder realizar la parte experimental de la red MPLS se debe tener en cuenta que el penúltimo enrutador de la red MPLS es el que quita la etiqueta MPLS (Penultimate Hop Popping). Si solo tuviéramos 2 enrutadores MPLS en la red, el enrutador de entrada seria a su vez el penúltimo y de salida. Al ser este el que añadiría (push) y quitaría (pop) la etiqueta, no podríamos observar su comportamiento. Por lo tanto el número mínimo de enrutadores es de 3 para que se implemente una red MPLS.

Se han escogido 2 enrutadores como equipos CPE, para las conexiones a cada facultad para configurar políticas de calidad de servicio (QoS), marcación de paquetes y ver las interacciones de los protocolos OSPF, BGP y MPLS.
También se han escogido dos hosts en cada extremo para visualizar funcionamiento del BGP, OSPF y MPLS, QoS, velocidades, saturamiento de BW, publicación de las redes.

Nuestro objetivo es establecer un enlace MPLS que esté capacitado para ofrecer Ingeniería de Trafico, por eso vamos a orientar la configuración para que soporte la implementación de DiffServ (servicios diferenciados), además del funcionamiento de BGP y OSPF simultáneamente y por último la aplicación de las políticas de QoS en una Red Privada Virtual (RPV).

Para trabajar con una red MPLS con Ingeniería de Trafico debemos comprobar que la red tiene habilitada una serie de protocolos:

- La red tiene que tener habilitado el protocolo CEF (Cisco Express Forwarding)
- Un protocolo de routing, en nuestro caso OSPF, para el funcionamiento del MPLS.
- Un protocolo de routing, BGP.
- Una interfaz de Loopback para poder ser usada como enrutador ID (RID).

Configuración de políticas de QoS

En la configuración del escenario, los paquetes se marcan en el campo DSCP en la red LAN de cada CPE, antes de entrar en la red MPLS. Esto nos permitirá definir distintos comportamientos y calidades para el tráfico que pasa a través de la red.
Para asignar QoS en MPLS se tienen que seguir 3 pasos:

- Definir las clases de tráfico (CoS).
- Definir las políticas de QoS.
- Asignar a qué interfaces se aplican las políticas.

RED DE DATOS UNSAAC – SEDE PERAYOC CUSCO

ITEM	CoS3	CoS2	CoS1
Tipo de Datos	Voz y Video	Datos Críticos	Datos No críticos
Prioridad	Máxima	Media	Normal
Precedencia / IP DSCP	P5 / IP DSCP 40	P2 / IP DSCP 16	P1 / IP DSCP 8
Ancho de Banda del Acceso	Sumatoria de los anchos de banda de cada una de las sedes		
Política aplicable al trafico excedente	Se descarta	Se Remarca como P1	No aplica
Aplicaciones	Aplicaciones en Tiempo Real como VoIP, Video conferencia	Aplicaciones de Datos sensibles al retardo y criticas para el negocio como: FTP, SMTP.	Aplicaciones tradicionales como: E-mail, HTTP.

Clase de servicio	Tráfico	IP Precedence	IP DSCP
CoS 3	Voz/Video	5	40
CoS 2	Datos Críticos	2	16
CoS 1	Datos no Críticos	1	8

Fig. 6.3. Muestra de marcación de paquete y prioridad de cada clase de servicio.

(6.4.) Configuraciones de los equipos

Primero se deben configurar las tareas básicas en un enrutador Cisco, los cuales son:

- Reseteo de la configuración inicial de los enrutadores
- Asignar un nombre al dispositivo
- Proteger el acceso administrativo
- Configurar un mensaje para proporcionar notificaciones legales de acceso no autorizado.
- Configuración de las interfaces de un enrutador
- Configuraciones avanzadas como: OSPF, MPLS, BGP, marcación de paquetes, políticas de calidad de servicio.

(6.4.1.) Reseteo de la configuración de los enrutadores.

El primer paso que realizamos fue eliminar cualquier configuración de usos anteriores.

Para ellos realizamos los siguientes pasos:

Eliminamos cualquier tipo de configuración que tiene.

CPE_1 # erase NVRAM
CPE_1 # reload

El equipo se reinicia y vuelve a encender, una vez ya en el modo usuario entramos a la configuración global de cada enrutador y copiamos las configuraciones de cada equipo detallados en las plantillas de configuración, al finalizar guardamos las configuraciones con los comandos:

CPE_1 # wr
CPE_1 #

(6.4.2.) Asignación de un nombre a cada equipo

La asignación de un nombre al dispositivo es para distinguirlo de otros dispositivos.

La configuración de la asignación de nombre en el equipo CPE_1 se muestra a continuación. La plantilla completa de cada dispositivo está en el **ANEXO G.**

Router1#configure terminal **(Encripta los passwords)**
Router1 (config)#hostname CPE_1 **(Asignacion de nombre CPE_1)**
CPE_1(config)#clock timezone GMT -5 **(Define la zona horaria)**
CPE_1(config)#service password-encryption **(Encripta los Passwords)**
CPE_1(config)#exit
CPE_1#wr **(Guarda los cambios realizados)**

(6.4.3.) Protección del acceso administrativo.

La configuración de acceso administrativo es para proteger el acceso a EXEC privilegiado, a EXEC de usuario y el acceso por Telnet, y cifrar las contraseñas con el máximo nivel.

La configuración es en tres partes del enrutador las cuales son:

Para proteger el acceso a EXEC privilegiado:
CPE_1(config)#
CPE_1(config)#enable secret cisco **(Password Enable= cisco)**
CPE_1(config)#

Para proteger el acceso a EXEC de usuario:
CPE_1(config)#
CPE_1(config)#line con 0 **(configuración en la línea de consola)**
CPE_1(config-line)# exec-timeout 0 0
CPE_1(config-line)# privilege level 15
CPE_1(config-line)# password 7 13061E010803 **(Password Enable= cisco)**
CPE_1(config-line)# logging synchronous **(Activación del password)**
CPE_1(config-line)#exit
CPE_1(config)#

Para proteger el acceso por Telnet:

```
CPE_1(config)#
CPE_1(config)#line vty 0 4                    (Configuración en la línea  vty - telnet)
CPE_1(config-line)# password 7 070C285F4D06   (Password Enable= cisco )
CPE_1(config-line)# login                     (Activación del password)
CPE_1(config-line)#exi
CPE_1(config)#
CPE_1#
```

Nota: Siempre es necesario configurar un mensaje para proporcionar notificaciones legales de acceso no autorizado. Esta configuración del mensaje se realiza como se muestra a continuación para la presente tesis.

```
CPE_1(config)#                                (En modo configuración global)
CPE_1(config)#banner motd ^CCCC               (para poner el mensaje de advertencia)
Enter TEXT message.  End with the character '^'.

&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&
&                                                                    &
&                                                                    &
&      Tesis: ANALISIS Y MEJORA DE LA RED                            &
&      DE DATOS DE LA UNSAAC SOBRE LA PLATAFORMA                     &
&      IP-MPLS EN UN BANCO DE PRUEBAS                                &
&                                                                    &
&      Tesistas:                                                     &
&      EDISON YUVER MORENO CARDENAS                                  &
&      JOEL LENIN QUISPE VILCA                                       &
&      > FACULTAD DE INGENIERIA ELECTRONICA                          &
&                                                                    &
&      ADVERTENCIA: Se prohíbe copiar la tesis                       &
&      de investigación. Derechos Reservados.                        &
&                                                                    &
&                                                                    &
&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&

^C
CPE_1(config)#
CPE_1(config)#
```

Las configuraciones mostradas hasta este punto son lo mismo para los demás equipos, ya que cada uno necesita seguridad en el acceso, nombre del dispositivo como identificador y mensajes de advertencia al personal no autorizado de realizar cambios.

(6.4.4.) Configuración de las interfaces de los enrutadores.

La configuración de las interfaces en el equipo CPE_1 es como sigue:

En la interfaz WAN enlace hacia equipo PE_2.

CPE_1#conf t
CPE_1(config)#interface GigabitEthernet0/0 **(En interfaz WAN enlace a PE_2)**
CPE_1(config-subif)# description ENLACE PE_2 **(Descripción del enlace a PE_2)**
CPE_1(config-if)# ip address 10.10.0.2 255.255.255.252 **(RED asignada según el diseño para la red IP- MPLS 10.10.0.0/30 donde la IP del equipo de red (PE) es la IMPAR 10.10.0.1)**
CPE_1(config-if)# duplex auto **(Velocidad de enlace respecto el equipo de acceso - automático)**
CPE_1(config-if)# speed auto **(Modo de trabajo de la interfaz depende del equipo de acceso – automático)**
CPE_1(config-if)# no shutdown **(modo lógico activo de la interfaz)**
CPE_1(config-if)#exi
CPE_1(config)#

En la interfaz LAN enlace hacia las carreras dentro de la facultad.

CPE_1(config)#interface GigabitEthernet0/1
CPE_1(config-subif)# description ENLACE LAN FACTULTAD
CPE_1(config-if)# no ip address
CPE_1(config-if)# duplex auto
CPE_1(config-if)# speed auto
CPE_1(config-if)# no shutdown **(modo lógico activo de la interfaz)**
CPE_1(config-if)#exi
CPE_1(config)#

Creación de subinterfaces para las redes de las vlans 2, 50 y 60 que son de la carrera profesional de Ing. Eléctrica, servidores 1 y telefonía 1, correspondientemente

CPE_1(config)#interface GigabitEthernet0/1.10 **(Subinterfaz asociada a la VLAN 2, Trafico de datos no críticos de la red Ing. Electrica)**
CPE_1(config-subif)# description LAN_ELECTRICA **(Descripción de la subinterfz)**
CPE_1(config-subif)# encapsulation dot1Q 2 **(encapsulación de la vlan2 de Ing Electrica)**
CPE_1(config-subif)# ip address 10.10.2.1 255.255.255.0 **(RED asignada según el diseño para la red IP- MPLS 10.10.2.0/24 donde la IP es 10.10.2.1 que es el default Gateway para la vlan2)**
CPE_1(config-subif)#exit
CPE_1(config)#

CPE_1(config)#
CPE_1(config)#interface GigabitEthernet0/1.20 **(Subinterfaz asociada a la VLAN 50, Tráfico de datos criticos de la red servidores 1)**
CPE_1(config-subif)# description SERVIDORES_1 **(Descripción de la subinterfz)**
CPE_1(config-subif)# encapsulation dot1Q 50 **(encapsulación de la vlan50 de servidores 1)**
CPE_1(config-subif)# ip address 10.10.50.1 255.255.255.240 **(RED asignada según el diseño para la red IP- MPLS 10.10.50.0/28 donde la IP es 10.10.50.1 que es el default Gateway para la vlan50)**
CPE_1(config-subif)#exit
CPE_1(config)#

CPE_1(config)#
CPE_1(config)#interface GigabitEthernet0/1.30 **(Subinterfaz asociada a la VLAN 60, Trafico de Voz de la red Telefonia 1)**
CPE_1(config-subif)# description TELEFONIA_1
CPE_1(config-subif)# encapsulation dot1Q 60 **(encapsulación de la vlan60 de Telefonia 1)**
CPE_1(config-subif)# ip address 10.10.60.1 255.255.255.192 **(RED asignada según el diseño para la red IP- MPLS 10.10.60.0/26 donde la IP es 10.10.60.1 que es el default Gateway para la vlan60)**
CPE_1(config-subif)#exit
CPE_1(config)#

(6.4.5.) Configuración de la interface Loopback para la gestión remota.

La configuración de una dirección lógica es con el propósito de la gestión de cada equipo remotamente.

CPE_1(config)#
CPE_1(config)# interface Loopback0 **(Interfaz Loopback logica)**
CPE_1(config-subif)#description GESTION **(Descriptcion de la Interfaz Loopback)**
CPE_1(config-subif)#ip address 11.11.11.11 255.255.255.255 **(IP asignada según el diseño de la red IP- MPLS para la gestión MASK /32)**
CPE_1(config-subif)#exit
CPE_1(config)#

(6.5.) Configuraciones avanzadas en los equipos.

Las configuraciones para la implementación del protocolo MPLS tiene un requisito importante la cual es que trabaja sobre el protocolo de enrutamiento dinámico OSPF, por lo cual es necesario primero configurar OSPF en los equipos PEs, para la muestra se analizara la plantilla de configuración del equipo PE_2, ya que en este equipo trabaja los tres protocolos que son: OSPF, MPLS y por ultimo BGP simultáneamente.

(6.5.1.) Configuraciones de OSPF y MPLS

La configuración del protocolo de enrutamiento dinámico OSPF, se muestra a continuación en el equipo PE_2:

Una vez realizada la asignación de nombre y configuración de acceso al equipo como se vio anteriormente, se procede a la configuración del OSPF.

PE_2(config)#
PE_2(config)#ip cef **(Habilitacion del protocolo CEF en el router)**
PE_2(config)#mpls label protocol ldp **(Protocolo LDP como protocolo para la distribución de las etiquetas)**
PE_2(config)#mpls ip **(Habilitacion MPLS a nivel global)**
PE_2(config)#
PE_2(config)#router ospf 10 **(Enrutamiento interno con OSPF con el identificador 10)**
PE_2(config-router)# mpls traffic-eng router-id Loopback0 **(Usamos la interfaz de Loopback como identificador del router para Traffic Engineering)**
PE_2(config-router)# mpls traffic-eng area 10 **(Configuracion el area 10 como la area en la que habiltamos el traffic engineering)**
PE_2(config-router)# router-id 2.2.2.2 **(Identificador del router en OSPF)**
PE_2(config-router)# redistribute bgp 100 subnets **(redistribucion de OSPF y BGP de las subredes para el óptimo funcionamiento de estos protocolos)**
PE_2(config-router)# network 2.2.2.2 0.0.0.0 area 10 **(Habilitacion del interfaz de Loopback para usar OSPF y lo asignamos al area 10)**
PE_2(config-router)# network 10.1.0.4 0.0.0.3 area 10 **(Habilitacion la subred 10.1.0.4/30 para usar OSPF y lo asignamos al area 10)**
PE_2(config-router)# network 10.10.0.0 0.0.0.3 area 10 **(Habilitacion la subred 10.10.0.0/30 para usar OSPF y lo asignamos al area 10)**
PE_2(config-router)# default-information originate **(Optimizacion del trafico descartable)**
PE_2(config-router)#exi
PE_2(config)#

La configuración también se realiza en las interfaces donde estará asociada este protocolo MPLS que va conectado hacia otros equipos PE_1 y PE_5, en este caso hacia el equipo PE_1.

PE_2(config)#
PE_2(config)#interface GigabitEthernet0/0
PE_2(config-if)# ip address 10.1.0.6 255.255.255.252 **(RED asignada según el diseño para la red IP- MPLS 10.1.0.4/30 donde la IP es 10.10.0.6 es asignada a esta interfaz)**
PE_2(config-if)# mpls ip **(Habilitacion MPLS en el interfaz)**
PE_2(config-if)#exi
PE_2(config)#

En este caso solo es en la interfaz GigaEthernet0/0 ya que por medio de eta interfaz se conecta hacia PE_1 quien a su vez también trabaja en el protocolo MPLS.

(6.5.2.) Configuración de BGP

La configuración del protocolo de enrutamiento dinámico BGP está en los equipos CPEs en las distintas facultades y PE de borde de la nube MPLS, esta configuración va después de haber configurado OSPF y MPLS, es el complemento para que la red de datos general en la plataforma IP-MPLS funcione de manera óptima, haciendo uso de toda la capacidad de los recursos físicos.

La configuración de BGP lo vemos en el equipo PE_2 y CPE_1, a continuación se muestra como se configuro el equipo PE_2:

PE_2#conf t
PE_2(config)#router bgp 100 **(Sistema Autónomo AS BGP Local 100)**
PE_2(config-router)# bgp router-id 2.2.2.2 **(Identificador de la sesión BGP = Loopback de Gestión)**
PE_2(config-router)# bgp log-neighbor-changes
PE_2(config-router)# neighbor WAN_CPE_1 peer-group **(Se crea el Peer BGP)**
PE_2(config-router)# neighbor WAN_CPE_1 remote-as 100 **(Neighbord con el Sistema Autónomo de la red CPE_1)**
PE_2(config-router)# neighbor WAN_CPE_1 password unsaac **(Authentication Password asignado en el diseño de la red IP-MPLS)**
PE_2(config-router)# neighbor WAN_CPE_1 timers 10 30
PE_2(config-router)# neighbor 10.10.0.2 peer-group WAN_CPE_1 **(Peer (IP CPE_1) contra quien se levantara session BGP)**
PE_2(config-router)# neighbor 10.10.0.2 description ENLACE CPE_1
PE_2(config-router)# !
PE_2(config-router)# address-family ipv4
PE_2(config-router-af)# redistribute ospf 10 match internal external 1 external 2 **(redistribución del OSPF y BGP para enrutamiento interno y esterno)**
PE_2(config-router-af)# neighbor WAN_CPE_1 soft-reconfiguration inbound
PE_2(config-router-af)# neighbor 10.10.0.2 activate
PE_2(config-router-af)# no auto-summary
PE_2(config-router-af)# bgp redistribute-internal **(redistribución BGP interno)**
PE_2(config-router-af)# network 2.2.2.2 mask 255.255.255.255 **(Anuncia la IP Gestión)**
PE_2(config-router-af)# network 10.1.0.4 mask 255.255.255.252 **(Anuncia Redes Locales)**
PE_2(config-router-af)# network 10.10.0.0 mask 255.255.255.252 **(Anuncia Redes Locales)**
PE_2(config-router-af)# exit-address-family
PE_2(config-router)#exi
PE_2(config)#
PE_2(config)#

Las plantillas de configuración de todos los equipos esta al final de esta tesis en la parte del **ANEXO G**.

(6.5.3.) Configuración de marcación de paquetes.

Las configuraciones de la marcación de paquetes se realizan en los equipos CPEs, ya que estos equipos realizan la selección de las clases de servicio y los etiqueta para luego darles una prioridad dependiendo de la clase de servicio.

Las configuraciones de la marcación de paquetes se hacen en los equipos CPE_1 y CPE_10. Ahora configuramos en el equipo CPE_1.

(6.5.3.1.) Marcación de paquetes - aplicado a la LAN

```
CPE_1#conf t
CPE_1(config)#class-map match-any P2
CPE_1(config-cmap)# match ip dscp cs2
CPE_1(config-cmap)# match access-group name qos2
CPE_1(config-cmap)#class-map match-any P5
CPE_1(config-cmap)# match ip dscp cs5
CPE_1(config-cmap)# match access-group name qos5
CPE_1(config-cmap)#exi
CPE_1(config)#
```

Clasificación de trafico

```
CPE_1(config)#policy-map SetDscpLan (Marcación de paquetes: CS5, CS2 y CS1)
CPE_1(config-pmap)# class P5
CPE_1(config-pmap-c)#  set ip dscp cs5      (Marco paquetes como CS5)
CPE_1(config-pmap-c)# class P2
CPE_1(config-pmap-c)#  set ip dscp cs2      (Marco paquetes como CS2)
CPE_1(config-pmap-c)# class class-default
CPE_1(config-pmap-c)#  set ip dscp cs1      (Marco paquetes como CS1)
CPE_1(config-pmap-c)#exi
CPE_1(config-pmap)#exi
CPE_1(config)#
```

(6.5.3.2.) Aplicación de la marcación para el tráfico entrante en la interface LAN

```
CPE_1(config)#
CPE_1(config)#interface GigabitEthernet0/1.10
CPE_1(config-subif)# description LAN_ELECTRICA
CPE_1(config-subif)# encapsulation dot1Q 2
CPE_1(config-subif)# ip address 10.10.2.1 255.255.255.0
CPE_1(config-subif)# service-policy input SetDscpLan (Aplicando Marcación para el tráfico
entrante en la interfaz LAN, en la subinterfaz para la red de Ing Electrica)
CPE_1(config-subif)#exit
CPE_1(config)#
CPE_1(config-subif)#interface GigabitEthernet0/1.20
CPE_1(config-subif)# description SERVIDORES_1
CPE_1(config-subif)# encapsulation dot1Q 50
CPE_1(config-subif)# ip address 10.10.50.1 255.255.255.240
CPE_1(config-subif)# service-policy input SetDscpLan (Aplicando Marcación para el tráfico
entrante en la interfaz LAN, en la subinterfaz para la vlan50 de Servidores1)
CPE_1(config-subif)#exit
CPE_1(config)#
CPE_1(config-subif)#interface GigabitEthernet0/1.30
CPE_1(config-subif)# description TELEFONIA_1
CPE_1(config-subif)# encapsulation dot1Q 60
```

CPE_1(config-subif)# ip address 10.10.60.1 255.255.255.192
CPE_1(config-subif)# service-policy input SetDscpLan **(Aplicando Marcación para el tráfico entrante en la interfaz LAN, en la subinterfaz para la vlan60 de Telefonía1)**
CPE_1(config-subif)#exit
CPE_1(config)#

(6.5.3.3.) Configuración de las listas de acceso de para la marcación de paquetes y selección de tráfico.

CPE_1(config)#
CPE_1(config-ext-nacl)#ip access-list extended qos5 **(Clasificando trafico Multimedia)**
CPE_1(config-ext-nacl)# permit ip 10.10.60.0 0.0.0.63 any **(Dirección origen - Dirección destino)**
CPE_1(config-ext-nacl)#exi
CPE_1(config)#
CPE_1(config)#ip access-list extended qos2 **(Clasificando tráfico de Servidores (Critico o Aplicaciones) o hacia servidores)**
CPE_1(config-ext-nacl)# permit ip 10.10.50.0 0.0.0.15 any **(Dirección origen -- Dirección destino)**
CPE_1(config-ext-nacl)# permit ip any 10.10.58.0 0.0.0.15 **(Dirección origen -- Dirección destino)**
CPE_1(config-ext-nacl)#exit
CPE_1(config)#

(6.5.4.) Configuración de las políticas de calidad de servicio - QoS

Las configuraciones de las políticas de calidad de servicio (QoS) se realizan también en los equipos CPEs, ya que una vez seleccionada los paquetes y etiquetado estos, se les asigna su respectiva prioridad, dependiendo si es trafico multimedia, tendrá máxima prioridad, si es tráfico de datos críticos su prioridad será moderado, y el resto de tráfico que es datos no críticos como internet su prioridad es baja.
Todo esto se toma en cuenta en las políticas de (QoS) en la interfaz WAN del enrutador CPE_1
Las configuraciones de las políticas de calidad de servicio (QoS) se hacen en los equipos CPE_1 y CPE_10.

Ahora configuramos en el equipo CPE_1.

(6.5.4.1.) Políticas de calidad de Servicio QoS - aplicado a la interfaz WAN

CPE_1#conf t
CPE_1(config)#class-map match-any qos5
CPE_1(config-cmap)# match ip dscp cs6
CPE_1(config-cmap)# match ip dscp cs5
CPE_1(config-cmap)#class-map match-any qos2
CPE_1(config-cmap)# match ip dscp cs2
CPE_1(config-cmap)#class-map match-any qos1
CPE_1(config-cmap)# match ip dscp cs1
CPE_1(config-cmap)#exi

Clasificación de trafico

CPE_1(config)#policy-map wan **(Asignación de BW por Clase de Servicio)**
CPE_1(config-pmap)# class qos5 **(Trafico Multimedia: CoS3)**
CPE_1(config-pmap-c)# priority 3072 **(BW asignado para CoS3 (máxima prioridad))**
CPE_1(config-pmap-c)# police 3072000 576000 1152000 conform-action transmit exceed-action drop violate-action drop **(No desborda, trafico excedente lo descarta)**
CPE_1(config-pmap-c-police)# class qos2 **(Trafico Servidores o Aplicaciones críticas: CoS2)**
CPE_1(config-pmap-c)# bandwidth 6144 **(BW asignado para CoS2)**
CPE_1(config-pmap-c)# police 6144000 1152000 2304000 conform-action transmit exceed-action set-dscp-transmit cs1 violate-action set-dscp-transmit cs1 **(desborda, trafico excedente remarca CoS1)**
CPE_1(config-pmap-c-police)# class qos1 **(Tráfico no crítico: CoS1)**
CPE_1(config-pmap-c)# bandwidth 18944 **(BW asignado para CoS1)**
CPE_1(config-pmap-c)# class class-default **(Trafico default)**
CPE_1(config-pmap-c)# fair-queue
CPE_1(config-pmap-c)#policy-map Shape28160
CPE_1(config-pmap)# class class-default
CPE_1(config-pmap-c)# shape average 28161000 **(BW asignado total: CoS1+ CoS2 + CoS3)**
CPE_1(config-pmap-c)# service-policy wan **(Políticas de Calidad que reserva un ancho de banda por cada Clase)**
CPE_1(config-pmap-c)#exi
CPE_1(config-pmap)#exi
CPE_1(config)#

(6.5.4.2.) Aplicación de las políticas de QoS para el tráfico saliente en la interface WAN

CPE_1#conf t
CPE_1(config)#interface GigabitEthernet0/0/0
CPE_1(config)# description ENLACE A PE_2
CPE_1(config-if)# switchport access vlan 100 **(encapsulación de la vlan100 de la red para el funcionamiento del CPE_1 y PE_2)**
CPE_1(config-if)# duplex full **(Velocidad de enlace respecto el equipo de acceso - duplex full)**
CPE_1(config-if)# speed 100 **(Modo de trabajo de la interfaz depende del equipo de acceso – speed 100)**
CPE_1(config-if)#exi
CPE_1(config)#

CPE_1(config)# interface Vlan100 **(configuración de la vlan 100)**
CPE_1(config)# description ENLACE A PE_2 **(Descripción del enlace a PE_2)**
CPE_1(config-if)# ip address 10.10.0.2 255.255.255.252 **(RED asignada según el diseño para la red IP- MPLS 10.10.0.0/30 donde la IP del equipo de red (PE) es la IMPAR 10.10.0.1)**
CPE_1(config-if)# service-policy output Shape28160 **(Aplicando QoS para el tráfico salida en la interface WAN, en la interfaz G0/0/0 para la vlan100 y el funcionamiento del BGP)**

CAPITULO VII

RESULTADOS.

En este capítulo se muestra y analiza los resultados del estudio y diseño de la red de datos de la UNSAAC en la plataforma IP-MPLS. Los resultados que se muestran van desde la arquitectura de la red de datos, hasta las configuraciones avanzadas y comportamiento de los equipos de red.

(7.1.) Implementación de pruebas

Para la realización de las pruebas se tomó el escenario básico de la muestra de la red de datos IP-MPLS propuesta en la tesis, con su topología física y lógica mostradas en la Fig. 6.1, debido a que no se cuenta con los equipos completos.

(7.2.) Resultados de la arquitectura de la red datos propuesto.

La arquitectura de red vista en la Fig. 5.21. "La topología lógica de la Red General de datos en la plataforma IP/MPLS de la UNSAAC" muestra las diferencias de la red datos de la UNSAAC en la plataforma IP-MPLS propuesta, frente a la actual topología de la Red de datos de la UNSAAC que es una arquitectura árbol con switches de capa 3, el cual posee un switch núcleo que alimenta a 6 switches de distribución por medio de fibra óptica multimodo para que los switches de acceso puedan estar conectados según la zona geográfica.

La nueva topología de red que se propone es una arquitectura de red Malla o Full Mesh; una red flexible, que se refiere a interactuar en operabilidad con la red ya existente con equipos y protocolos de capa 3 y capa 4.

Nota: Para la generación de tráfico de cada clase de servicio se utilizó el software **tfgen** (traffic generator – generador de tráfico); el cual realiza la generación de tráfico de cualquier tipo de servicio en tiempo real.

(7.3.) Resultados de pruebas de conectividad.

Una vez que se tiene configurado todo el escenario, se comprobó que funciona la conexión extremo-extremo en ambos sentidos.
Se entiende como conexión extremo-extremo dentro de una red IP-MPLS, en donde un paquete va desde el Host "Fuente" al Host "Destino" pasando a través de los 3 enrutadores MPLS, 2 enrutadores de acceso con protocolo de enrutamiento BGP y último el paso por los switches de distribución y acceso.
Para ello enviaremos una serie de paquetes ICMP (Internet Control Message Protocol), o sea, pings a través de la red, en las tres redes asociadas a cada VLAN diferente de cada CPE.
Nos conectamos al Host "Fuente" (10.10.2.5) y enviamos paquetes al Host "Destino" (10.10.40.10)

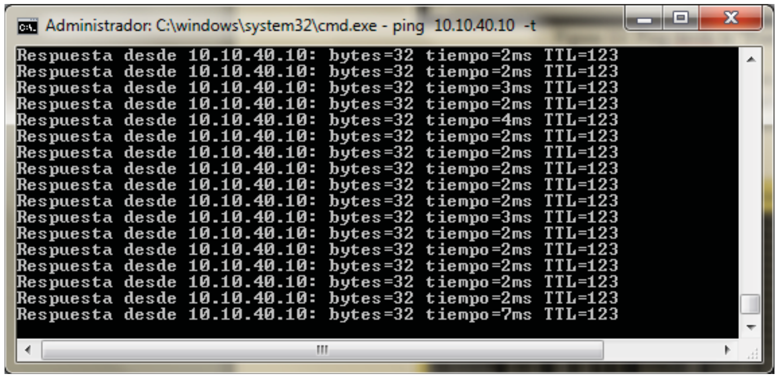


Fig. 7.1 Ping desde la "Fuente" hacia el "Destino"

El resultado se observa cómo se han recibido los 4 paquetes y ninguno se ha perdido, por lo tanto podemos confirmar que hay conectividad extremo-extremo.
Finalmente vamos a realizar la misma prueba pero en sentido contrario, del Host “Destino” al Host “Fuente”

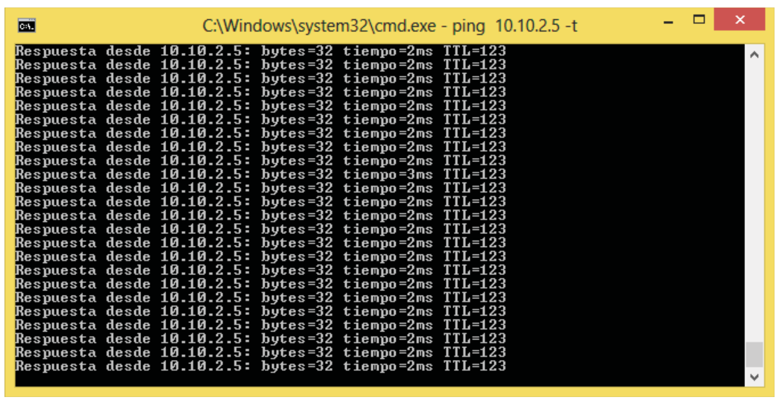


Fig. 7.2 Ping desde el "Destino" hacia la "Fuente"

Igual que en el caso anterior la prueba de conexión ha sido un éxito.

(7.4.) Resultados de OSPF.

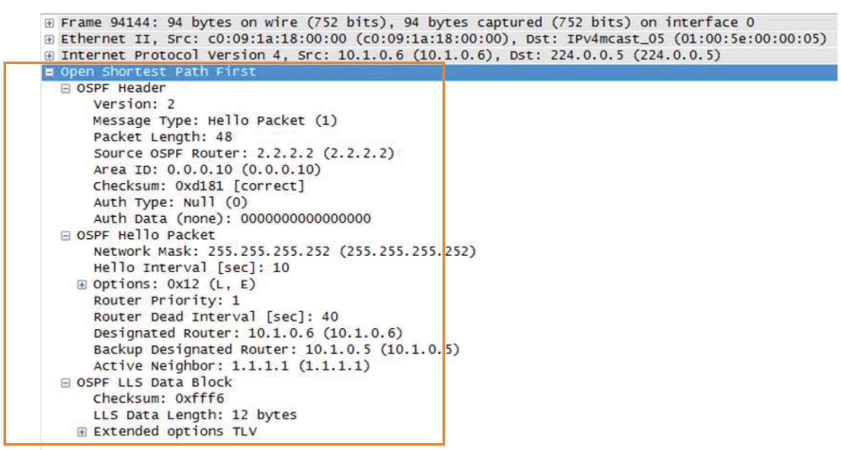


Fig. 7.3. Vista del funcionamiento del OSPF en Wireshark.

En el resultado se observa cómo que el protocolo OSPF ha levantado su sesión avisando a su vecino la tabla que obtuvo mediante el protocolo HELLO, que a su vez se muestra encapsulada en la cabecera OSPF.
Se aprecia el intervalo de 10 segundos para reconocer el estado activo de OSPF y las IP del siguiente salto e IP loopback de gestión contra quien esta enlazado.

(7.5.) Resultados de MPLS.

Los resultados de las pruebas del funcionamiento del MPLS, son capturas de imágenes a través del software de administración de red SecurCRT 6.1, el dual da datos estadísticos detallado para su a análisis correspondiente, además de usar el software Wireshark para analizar a fondo los paquetes enviados por las tres clases de servicio.

De las pruebas realizadas, los resultados se muestran en los siguientes sub numerales.

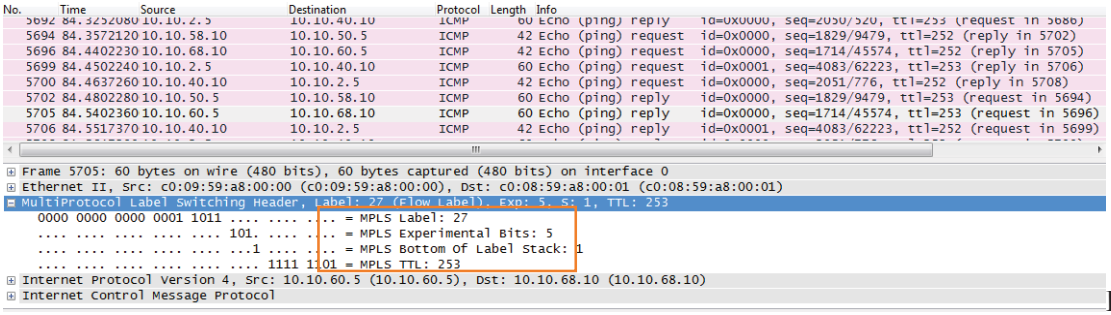


Fig. 7.4. Vista general del MPLS en un escenario saturado - Wireshark.

En el resultado se observa como el enrutador PE2 agrega un encabezado MPLS al paquete con dicha etiqueta label 27. Este es el proceso mencionado como MPLS Label.

(7.5.1.) Resultados del funcionamiento del MPLS.

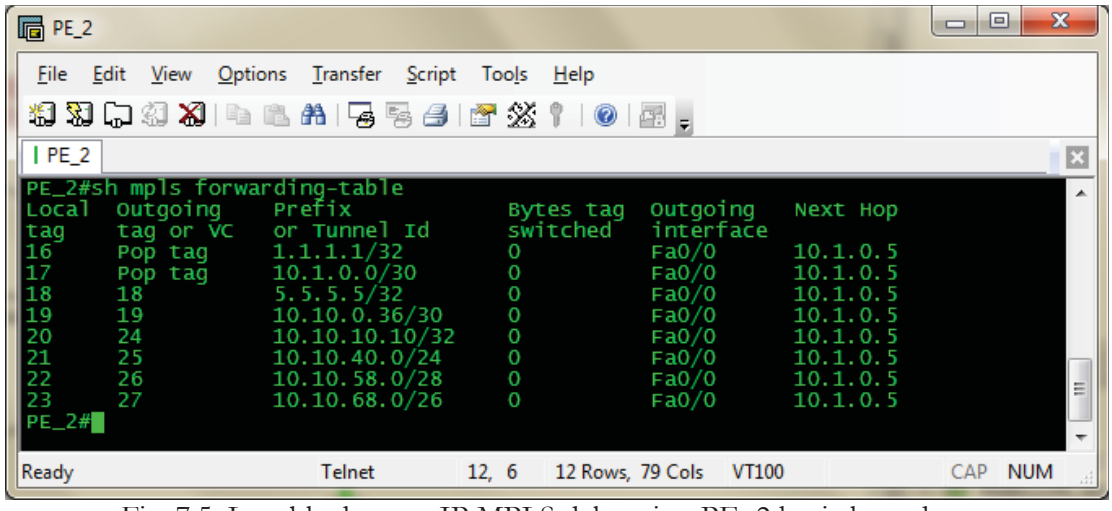


Fig. 7.5. La tabla de rutas IP MPLS del equipo PE_2 hacia las redes remotas.

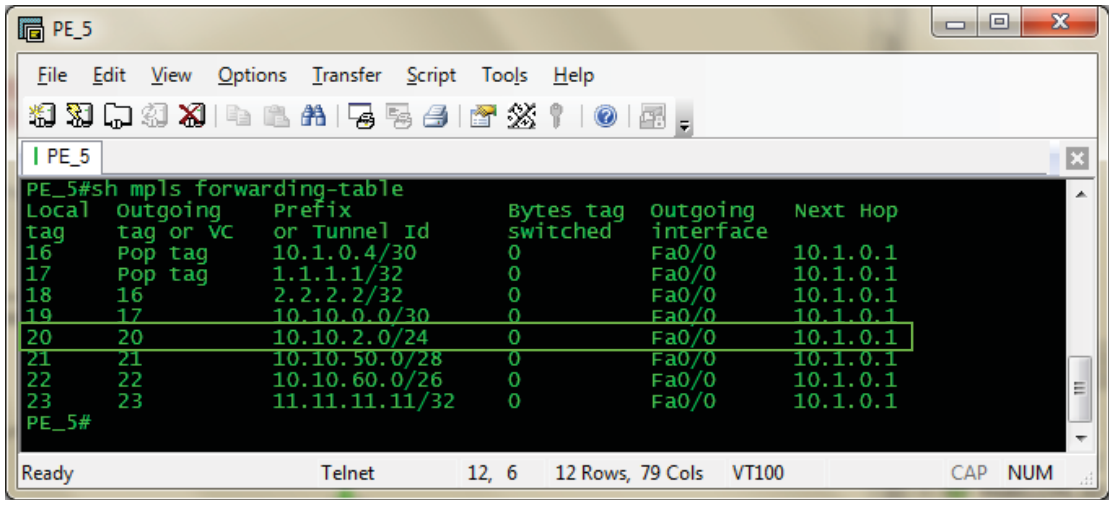


Fig. 7.6. La tabla de rutas IP MPLS del equipo PE_5 hacia las redes remotas.

La Fig. 7.6 "La tabla de rutas IP MPLS del equipo PE_5 hacia las redes remotas" muestra cómo llegar hacia las redes remotas aprendidas por medio del protocolo MPLS, como por ejemplo: vemos que para llegar a la red 10.10.2.0/24 lo hare por su siguiente salto que es 10.1.0.1.

Analizando una ruta de la figura 7.6:

20 20 10.10.2.0/30 0 F0/0 10.1.0.1

- 20: identifica la etiqueta local
- 20: identifica la etiqueta local de salida
- 10.10.2.0/30: identifica la red destino
- 0:
- F0/0: identifica la interfaz de salida
- 10.1.0.1: identifica la dirección IP del siguiente salto para llegar a la red remota

Pruebas complementarias obtenidas en el simulador GNS3, de la muestra en el GNS3.

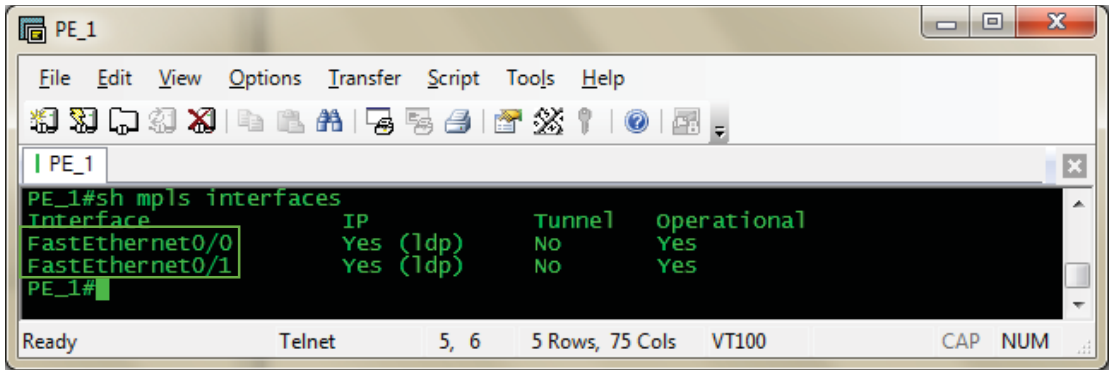


Fig. 7.7. Interfaces que están aplicando MPLS en el equipo PE_1.

El resultado muestra que interfaces del enrutador se está aplicando MPLS. En este caso se aplica en las interfaces FastEthernet0/0 y FastEthernet0/0.

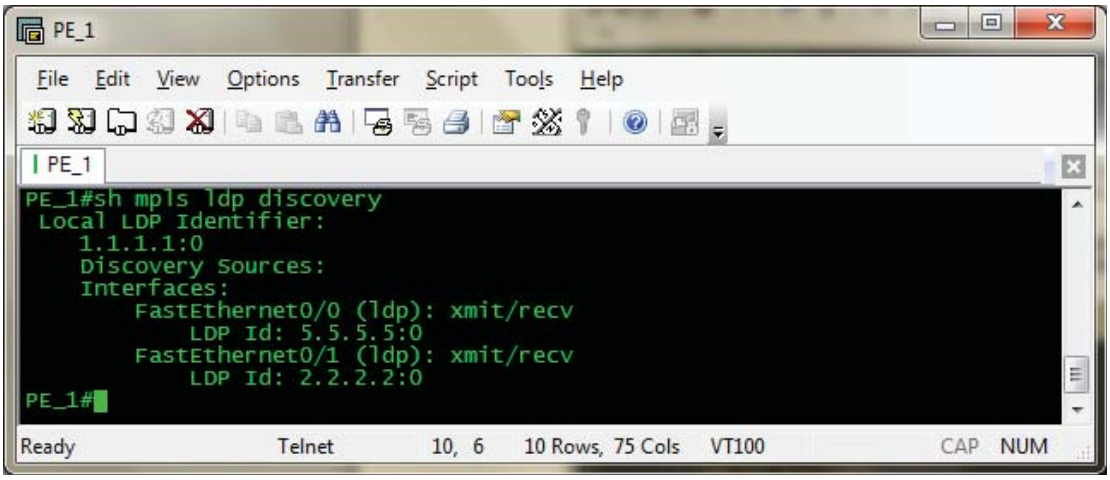


Fig. 7.8. Descubrimiento del Router ID que aplican MPLS.

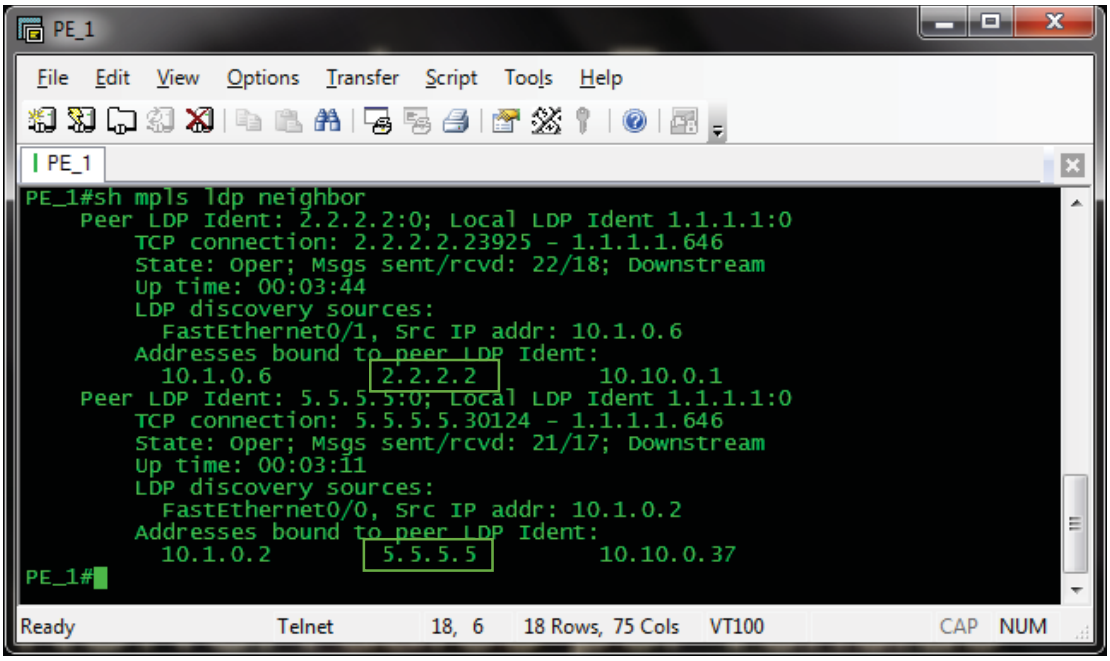


Fig. 7.9. Descubrimiento de los Routers vecinos que aplican el MPLS

Esta gráfica, muestra por medio de que interfaces descubre los enrutadores ID (identificador de enrutador) vecinos que también están aplicando MPLS.
En este caso su enrutador ID local es 1.1.1.1 que viene a ser el mismo enrutador. La identificación de los enrutadores ID vecinos son: **5.5.5.5** y **2.2.2.2** que son identificados por medio de sus interfaces: FastEthernet0/0 y FastEthernet0/1.

Los resultados de la implementación del MPLS muestra mejoras a la red de dato actual de la UNSAAC ver Fig. 3.24. "Topología actual de la Red General de datos de la UNSAAC – 2016"; ya que diferencia tipo de tráfico, aprovecha la INTRANET propuesto, todas las peticiones no necesitan salir a internet, cuenta con el respaldo de un banco de servidores necesarios. La red IP-MPLS se basa en el etiquetado de los paquetes en base a criterios de prioridad y/o calidad (QoS), la idea de MPLS es realizar la conmutación de los paquetes o datagramas en función de

las etiquetas añadidas en capa 2 y etiquetar dichos paquetes según la clasificación establecida por la QoS.

Los resultados de las capturas y tablas de rutas encontradas en la simulación con el software GNS3 y el escenario en tiempo real muestran el correcto funcionamiento de la deferencia de tráficos; como los enrutadores marcan el paquete dependiendo de la lista de prioridad en que la hemos definido, para luego pasar por la red MPLS y nuevamente convertirlos en protocolo IP y llegar a su destino.

Estos resultados resaltan el concepto de ingeniería de tráfico porque mejora en la comunicación dentro de la INTRANET, hace uso de la EXTRANET cuando sea necesario y optimiza la red.

(7.5.2.) Resultados de etiquetas de los paquetes por medio del Wireshark.

(7.5.2.1.) Resultados complementarios en el software GNS3 de etiquetas de los paquetes del MPLS en las tres clases de servicios.

Telefonía

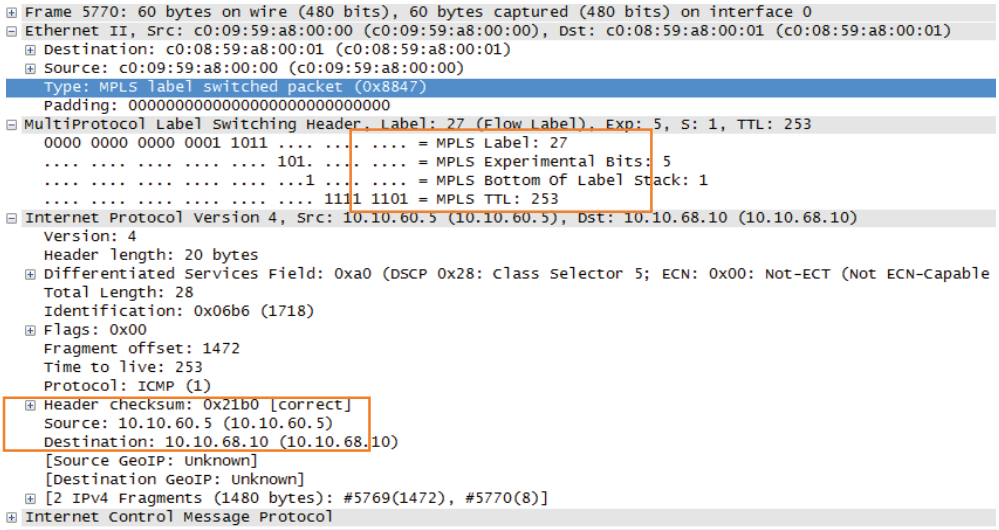


Fig. 7.10. Detalle de un paquete MPLS en la clase de servicio de telefonía.

En el resultado se observa la comunicación entre 2 host PC fuente 10.10.60.5 y PC destino 10.10.68.5, la cual estas IPs están asignadas en la topología de Muestra; y vemos también que el enrutador PE2 agrega un encabezado MPLS al paquete con dicha etiqueta label 27.

Label 27 = etiqueta 27

Servidores

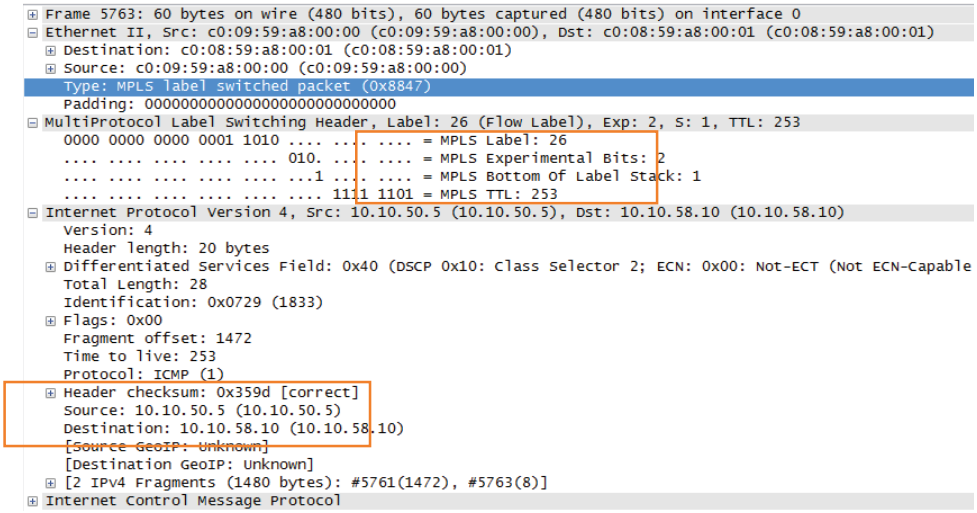


Fig. 7.11. Detalle de un paquete MPLS en la clase de servicio de servidores.

En el resultado se observa la comunicación entre 2 host PC fuente 10.10.50.5 y PC destino 10.10.58.5, la cual estas IPs están asignadas en la topología de Muestra; y vemos también que el enrutador PE2 agrega un encabezado MPLS al paquete con dicha etiqueta label 26.

Label 26 = etiqueta 26

Internet

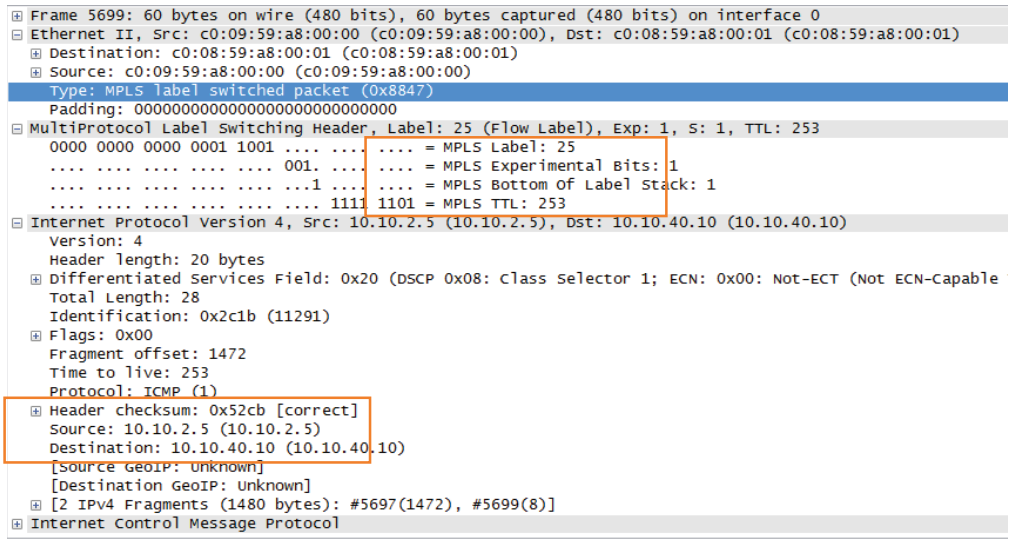


Fig. 7.12. Detalle de un paquete MPLS en la clase de servicio de Internet.

En el resultado se observa la comunicación entre 2 host PC fuente 10.10.2.5 y PC destino 10.10.40.5, la cual estas IPs están asignadas en la topología de Muestra; y vemos también que el enrutador PE2 agrega un encabezado MPLS al paquete con dicha etiqueta label 26.

Label 25 = etiqueta 25

(7.6.) Resultados de BGP.

Los resultados de protocolo de enrutamiento dinámico BGP, está en detallado en tres partes, debido a que por medio de este protocolo se realizan la convergencia con el protocolo de enrutamiento OSPF y MPLS, publicación y recepción de las VLANs, Loopback.

(7.6.1.) Resultados del funcionamiento del BPG.

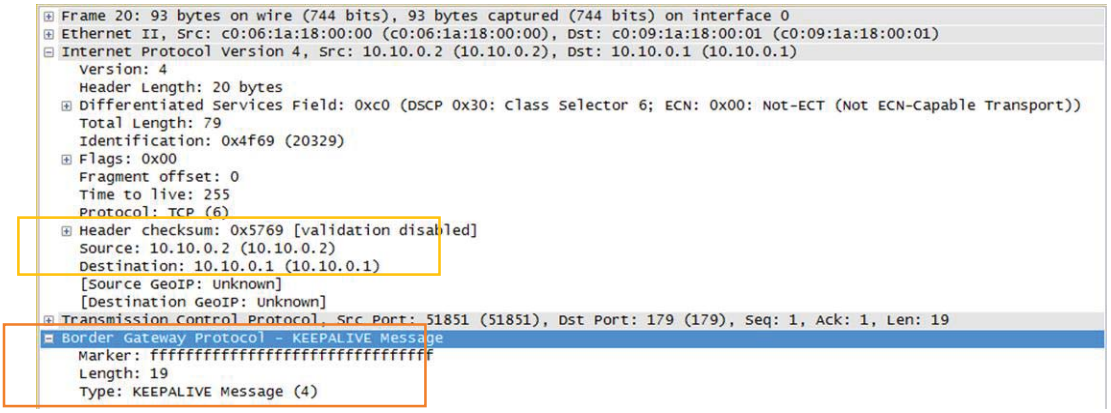


Fig. 7.13. Vista del funcionamiento del BGP en Wireshark.

En el resultado vemos la sesión activa del BGP entre los routers CPE1 - PE2, donde podemos apreciar sus direcciones IPs fuente y destino. Además la imagen muestra los protocolos de conexión, encapsulados en la cabecera BGP.

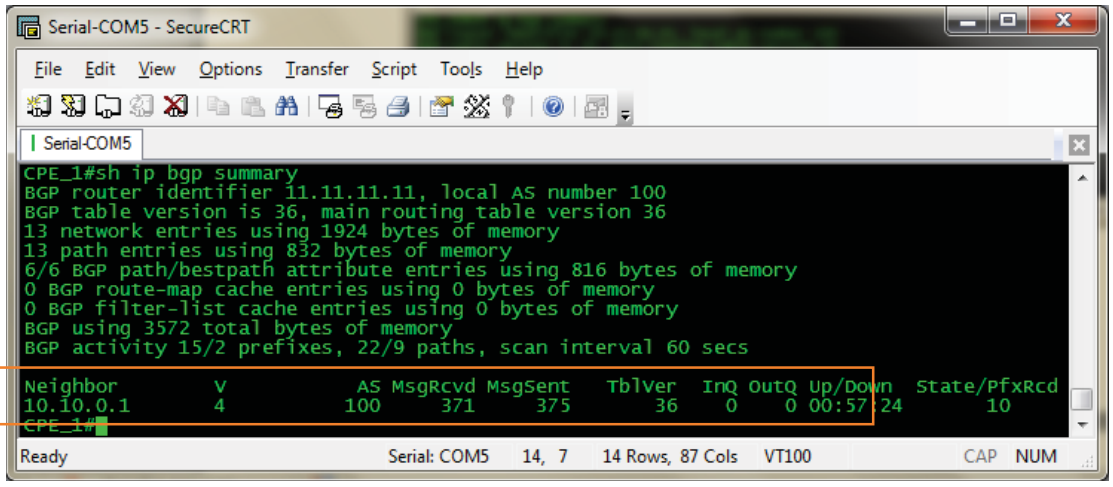


Fig. 7.14. Tiempo transcurrido del funcionamiento del BGP.

La Fig. 7.4 muestra el tiempo desde el inicio del funcionamiento del BGP junto al equipo conectado al otro extremo del medio de comunicación, en la captura de imagen es 57 minutos y 24 segundos. El enrutamiento BGP (Protocolo de Gateway de Frontera) implementado es completo debido a sus atributos que logra mejorar la entrega de los paquetes, su mision de este protocolo es encontrar el camino más eficiente entre los nodos para propiciar una correcta circulación de la información en la INTRANET.

Los resultados en la simulación y pruebas en tiempo real se nota las características del BGP, se contrasta el funcionamiento desde el momento en que levanta la sesión como son las subredes que anuncia detrás del enrutador y como pide y recibe todas las subredes con las que podrá comunicarse de los vecinos adyacentes. Estos análisis vienen de la Fig. 7.14.

Tiempo transcurrido del funcionamiento del BGP es **57 minutos y 24 segundos**.

(7.6.2.) Resultados de las publicaciones de redes.

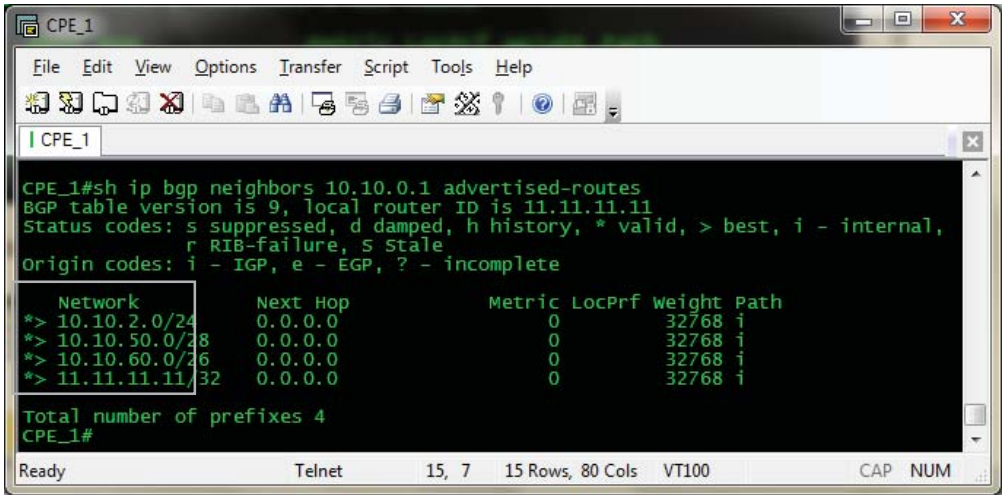


Fig. 7.15. Publicación de redes del CPE_1 hacia la WAN.

Los resultados según la Fig. 7.15, **en el recuadro verde** vemos las redes que el enrutador CPE_1 está publicando hacia el enrutador vecino PE_2, anuncia las redes detrás del enrutador CPE_1 hacia al enrutador PE_2 vecino.

En este caso las redes que está publicando por medio del BGP son: 10.10.2.0/24, 10.10.50.0/28, 10.10.60.0/26 y 11.11.11.11/32 que vienen a ser la red de datos VLAN2 de Ing. Eléctrica, la red de SERVIDORES 2, por último la red de TELEFONIA 1 y la LOOPBACK DE GESTION del enrutador CPE_1.

(7.6.3.) Resultados de la recepción de redes

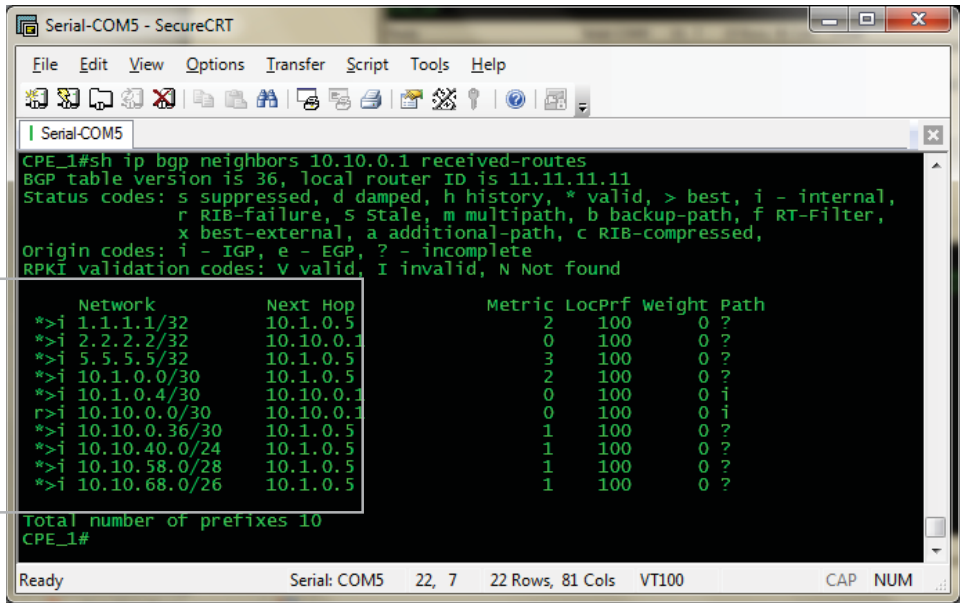


Fig. 7.16. Redes que recibe el CPE_1 de la WAN.

Los resultados según la Fig. 7.16 en el **recuadro verde** vemos las redes que el enrutador CPE_1 está recibiendo de su enrutador vecino PE_2. En este caso las redes que está recibiendo por medio del BGP son: 1.1.1.1/32 (Loopback de enrutador PE_1), 2.2.2.2/32 (Loopback de enrutador PE_2), 5.5.5.5/32 (Loopback de enrutador PE_5), 10.1.0.0/30 (red de enlace), 10.1.0.4/30 (red de enlace), 10.10.0.0/30 (red de enlace), 10.10.0.36/30 (red de enlace), 10.10.40.0/24 (red VLAN2 de Ing. Eléctrica), 10.10.58.0/28 (red de SERVIDORES 2) y 10.10.68.0/26 (red de TEEFONIA 1).

Se tiene mejor entendimiento sobre el trayecto que realiza un paquete desde el origen hacia su destino, las tablas de enrutamiento nos ayudan a identificar el trayecto, así mismo poder actualizar los eventos y recibir información sobre una posible falla en la red y en comparación a la red actual no se puede obtener esta información.

(7.7.) Resultados de Ingeniería de tráfico.

Los resultados en esta parte de la tesis, es para verificar que se cumplen los objetivos propuestos con respecto a todo lo concerniente de Ingeniería de tráfico, para lo cual detallamos por partes que con lleva esta implementación en la red de datos IP-MPLS de la UNSAAC.

(7.7.1.) Resultados de la Marcación para el tráfico entrante en la interfaz LAN.

Los resultados de la marcación de paquetes es individualmente para cada clase de servicio, en la prueba realizada es en un escenario con las tres clases de servicio funcionando simultáneamente, y los resultados y análisis es para cada clase de servicio como se ve a continuación.

(7.7.1.1.) Resultados de la marcación de paquetes tráfico telefonía 1 - CoS3 - VLAN60

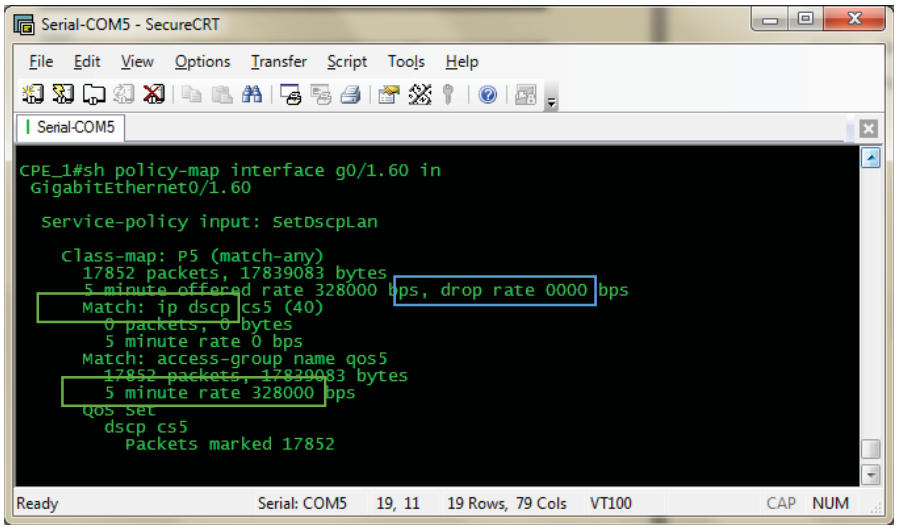


Fig. 7.17. Marcación de paquetes del tráfico telefonía COS3.

El resultado muestra la marcación de paquetes de la clase de servicio de COS3, en la parte de Class-map: P5, con la marcación de **dscp cs5**.
Además se aprecia la velocidad en la marcación de paquetes P5 de **328000 bps** que es igual a **328Kbps** y drop rate **de 0000 bps** el cual indica que no hay perdida de paquetes.

Drop rate **de 0000 bps** es equivalente a **0% perdida de paquetes.**

La marcación de paquetes se realiza en la LAN del enrutadores, en donde se genera la selección del tipo de tráfico, y posteriormente lo marca los paquetes.

(7.7.1.2.) Resultados de la marcación de paquetes tráfico de servidores 1 CoS2 - VLAN50

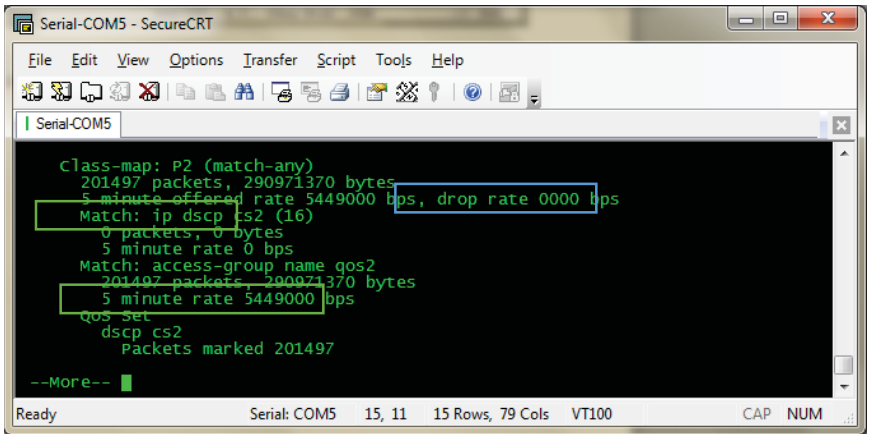


Fig. 7.18. Marcación de paquetes del tráfico de servidores COS2.

El resultado muestra la marcación de paquetes de la clase de servicio de COS2, en la parte de Class-map: P2, con la marcación de **dscp cs2**.
Además se aprecia la velocidad en la marcación de paquetes P2 de **5449000 bps** que es igual a **5.44Mbps** y drop rate de **0000** bps el cual indica que no hay perdida de paquetes.

Drop rate **de 0000 bps** es equivalente a **0% perdida de paquetes.**

(7.7.1.3.) Resultados de la marcación de paquetes tráfico de internet - CoS1 - VLAN2

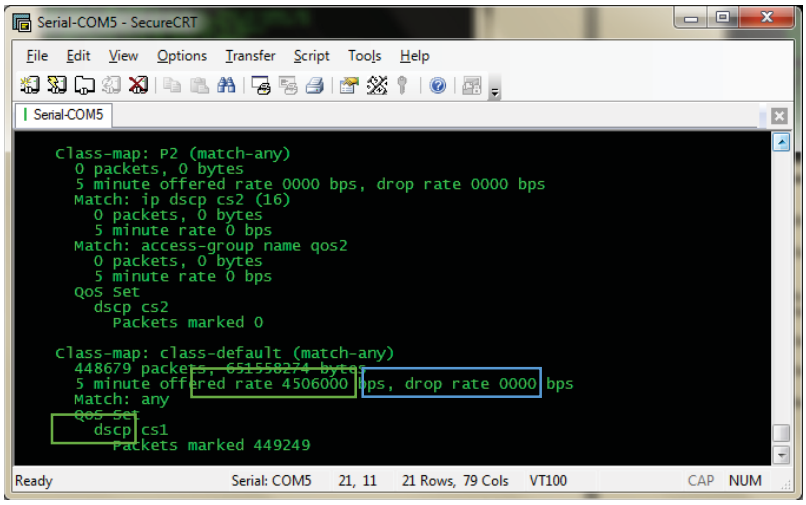


Fig. 7.19. Marcación de paquetes del tráfico de internet COS1.

El resultado muestra la marcación de paquetes de la clase de servicio de COS1, en la parte de Class-map: **class-default**, con la marcación por defecto de **dscp cs1**.
Además se aprecia la velocidad en la marcación de paquetes class-default de **4506000 bps** que es igual a **4Mbps** y drop rate de 0000 bps el cual indica que no hay perdida de paquetes.

Drop rate **de 0000 bps** es equivalente a **0% perdida de paquetes.**

Los resultados obtenidos en las Fig. 7.17, 7.18 y 7.19 notamos cómo los enrutadores clasifican los paquetes antes de ser enviados a su destino, esto se puede ver en las interfaces LAN de los enrutadores; según la configuración asignada para los enrutadores se crea 3 tipos de clases:

- P5.- Clasifica el tráfico en tiempo real (voz y video), en nuestro escenario la red de telefonía.
- P2.- Clasifica el tráfico crítico, comunicación hacia la red de servidores.
- P1 (CLASS-DEFAULT).- Clasifica el tráfico no crítico, es el tráfico no priorizado correo, FTP, HTTPS, etc.

(7.7.2.) Resultados de las Políticas de calidad de Servicio - QoS para el tráfico salida en la interface WAN.

Los resultados de las políticas de QoS es individual para cada clase de servicio, ya que estas políticas van asociado al dimensionamiento del BW de cada Equipo CPE y este a su vez del tráfico que genera la facultad a cual hace referencia.
Los resultados de las políticas de QoS se detallan para cada clase de servicio a continuación:

(7.7.2.1.) Resultados de políticas QoS para el tráfico de salida CoS3 - máxima prioridad

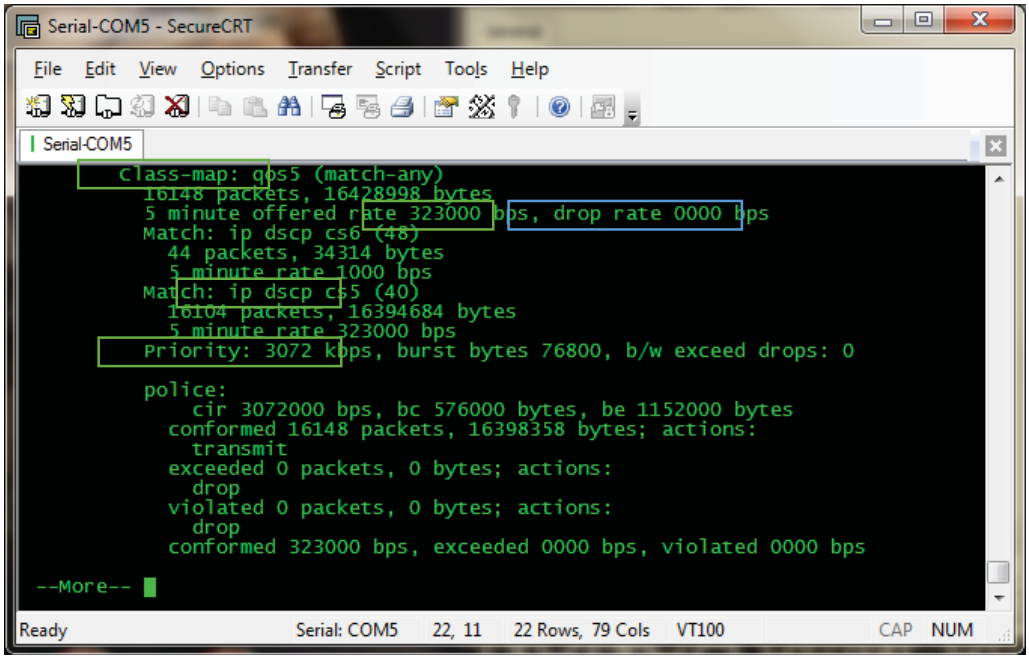


Fig. 7.20. Calidad de servicio, asignación de clase con qos5 del tráfico COS3.

El resultado muestra las políticas de calidad de servicio, asignación de clase con **qos5** del tráfico de telefonía COS3, Class-map: **qos5**, con la marcación de **dscp cs5**.
Además la velocidad de transmisión de clase qos5 de **323000 bps** que es igual a **3.23 Kbps** y drop rate de **0000** bps el cual indica que no hay perdida de paquetes. **0%** perdida de paquetes.
La tasa de transmisión máxima de esta clase de servicio **qos5** es de **3 Mbps**, esto se ve en la parte de **priority: 3072 Kbps**, el enlace está generando una tasa de **323000 bps** por lo cual no hay perdida de paquetes.

Las políticas de calidad de servicio se aplican en la interfaz WAN, para garantizar los tiempos de envío y su respectiva prioridad.

(7.7.2.2.) Resultados de políticas QoS para el tráfico de salida CoS2 - moderada prioridad

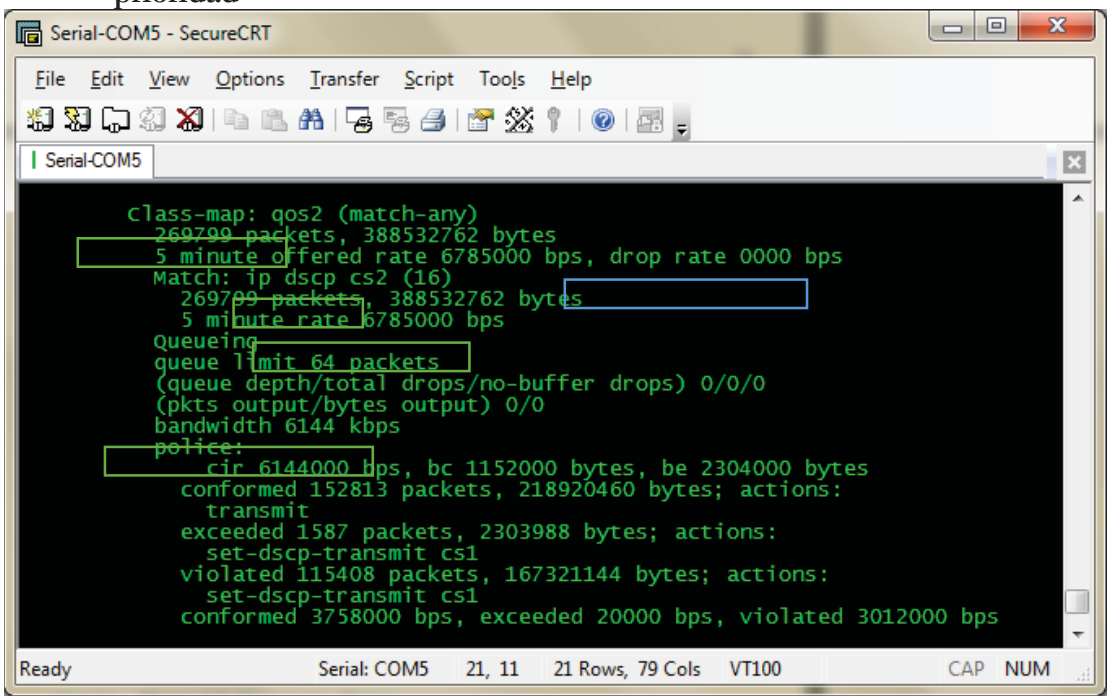


Fig. 7.21. Calidad de servicio, asignación de clase con qos2 del trafico COS2.

El resultado muestra las políticas de calidad de servicio, asignación de clase con **qos2** del tráfico de telefonía COS3, Class-map: **qos2**, con la marcación de **dscp cs2**.
Además la velocidad de transmisión de clase qos2 de **6785000 bps** que es igual a **6.78Mbps** y drop rate de **0000** bps el cual indica que no hay perdida de paquetes. **0%** perdida de paquetes.
La tasa de transmisión de esta clase de servicio **qos2** es de **6 Mbps** se ve en la parte **bandwidth: 6144 Kbps** y la tasa de transmisión máxima puede llegar a **24 Mbps** porque desborda las tasas de transmisión de los otros dos clases de servicio CoS3 y CoS1 si estos no generan tráfico, el enlace está generando una tasa de **6785000 bps** con **drop rate** de **0000** bps = **0%** perdida de paquetes.

(7.7.2.3.) Resultados de la asignación del BW para CoS1 - mínima prioridad

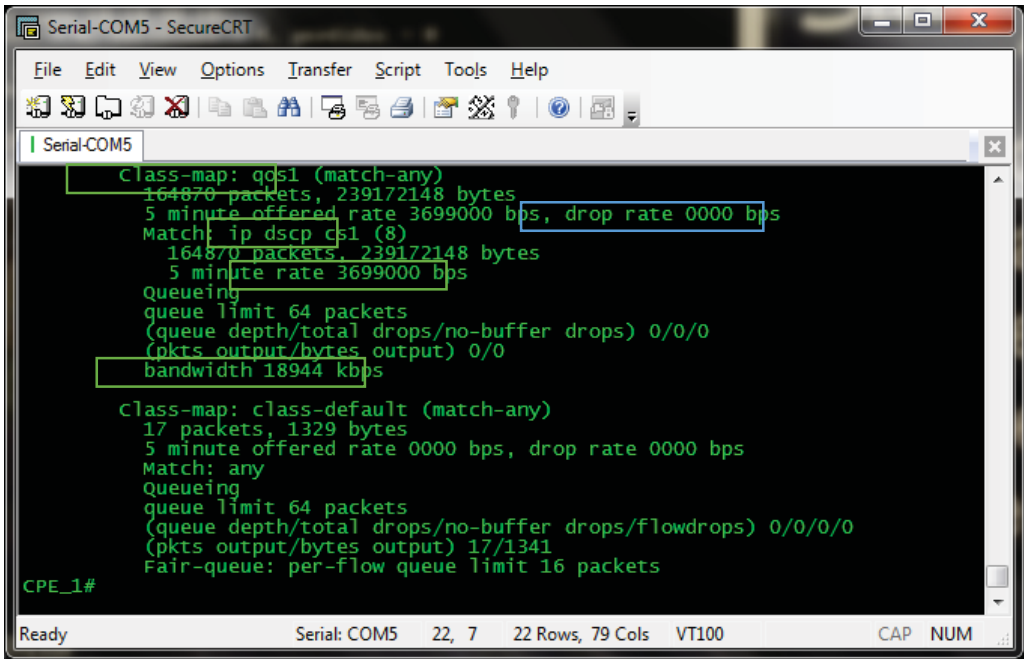


Fig. 7.22. Calidad de servicio, asignación de clase con qos1 del trafico COS1.

El resultado muestra las políticas de calidad de servicio, asignación de clase con **qos1** del tráfico de servidores COS1, Class-map: **qos1**, con la marcación de **dscp cs1**.
Además la velocidad de transmisión de clase qos2 de **3699000 bps** que es igual a **3.699Mbps** y drop rate de **0000** bps el cual indica que no hay perdida de paquetes. **0%** perdida de paquetes.
La tasa de transmisión de esta clase de servicio **qos1** es de **18.5 Mbps** se ve en la parte **bandwidth: 18944 Kbps** y la tasa de transmisión máxima puede llegar a **24 Mbps** porque desborda las tasas de transmisión de los otros dos clases de servicio CoS3 y CoS2 si estos no generan tráfico, el enlace está generando una tasa de **3699000 bps** con **drop rate** de **0000** bps = **0%** perdida de paquetes.

Los resultados obtenidos en las Fig. 7.20, 7.21 y 7.22, notamos que luego de clasificar los paquetes ingresados en la interface LAN de todos los enrutadores, pasan a la etapa de marcación de paquetes en las interface WAN de todos los enrutadores; según la configuración asignada para los enrutadores se crea 3 tipos de marcados:

- Qos5.- Marca la clase P5 con el término **dscp cs5** y asocia el ancho de banda asignado en el canal (solo usa dicho ancho de banda).
- Qos2.- Marca la clase P2 con el término **dscp cs2** y asocia el ancho de banda asignado en el canal. En este caso el ancho de banda puede desbordar hacia sus vecinos, puede aprovechar el ancho de banda de qos5 siempre y cuando no este cursando tráfico sobre ese canal, y puede desbordar y priorizar su tráfico sobre el qos1 ya que tiene la prioridad más alta.
- Qos1.- Marca la clase CLASS-DEFAULT con el término **dscp cs1** y asocia el ancho de banda asignado en el canal, para este caso puede desbordar a los otros dos vecinos siempre y cuando no estén cursando trafico sobre esos canales.

(7.7.3.) Resultados del comportamiento de la convergencia IP de voz - CoS3, Servidores - CoS2 e Internet CoS1.

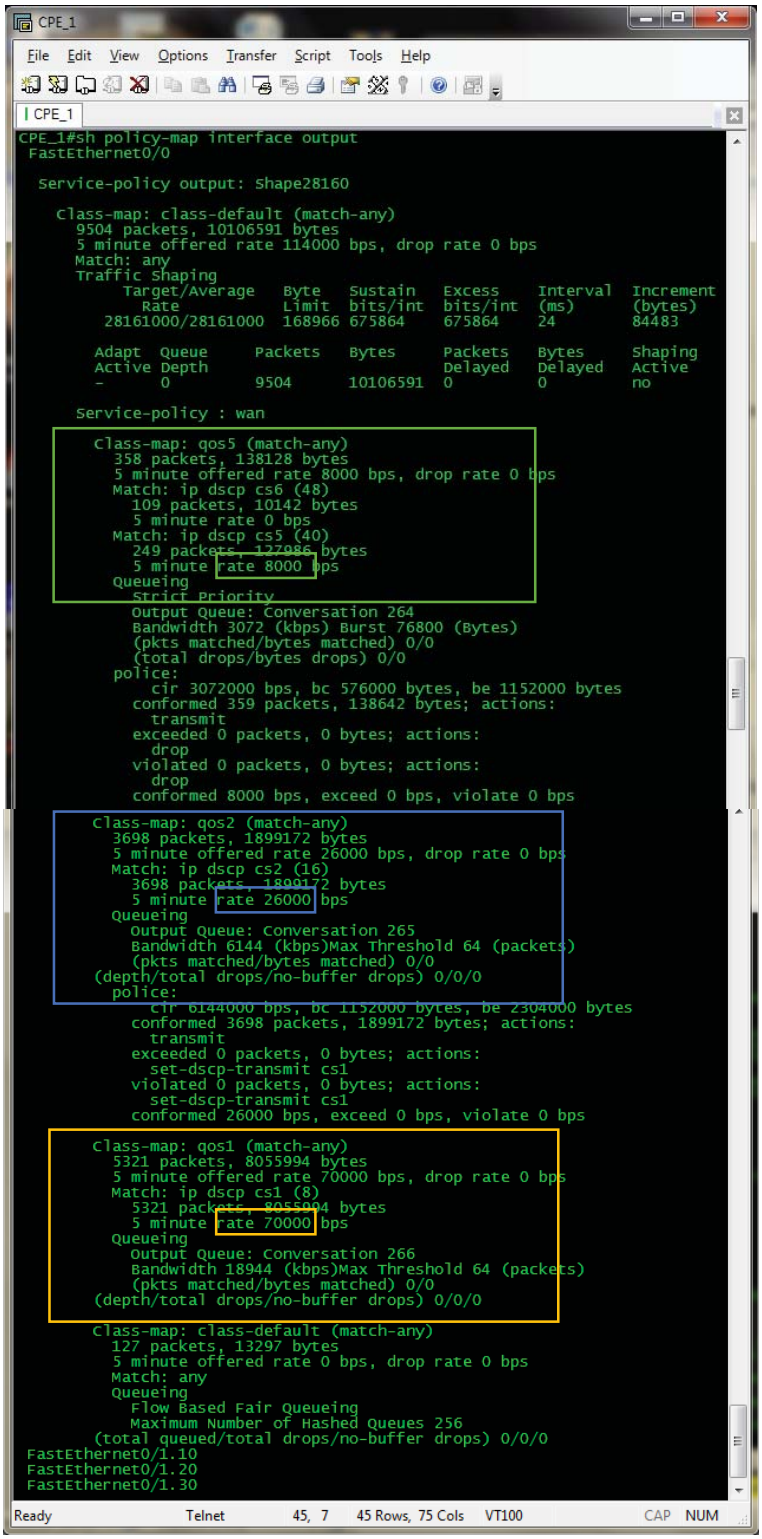


Fig. 7.23. Tráfico de los tres servicios Cos1, CoS2 y Cos3 funcionando simultáneamente.

El resultado muestra el funcionamiento simultáneo de las tres clases de servicio, cada uno a una tasa de transmisión:

CoS3: 8 000 bps = **8 Kbps** drop: 0 es decir **0% perdida de paquetes**.

CoS2: 26 000 bps = **26 Kbps** drop: 0 es decir **0% perdida de paquetes**.

CoS1: 70 000 bps = **70 Kbps** drop: 0 es decir **0% perdida de paquetes**.

La tasa de transmisión que genera la interfaz WAN del CPE_1 es la suma de las tres:

Tasa de transmisión de la interfaz WAN = 8 Kbps + 26 Kbps + 70 Kbps
Tasa de transmisión de la interfaz WAN = **104 Kbps.**

La tasa de transmisión máxima de la interfaz WAN es 24.5 Mbps = **24500 Kbps.** Por esta razón es que **no hay pérdida de paquetes**.

(7.7.4.) Resultados de los tiempos de envío para CoS3, CoS2 y CoS1 funcionando simultáneamente.

El análisis de los resultados de los tiempos es por medio del Wireshark para cada clase de servicio: Telefonía, Servidores e Internet.

(7.7.4.1.) En un escenario normal, tiempos de envío.

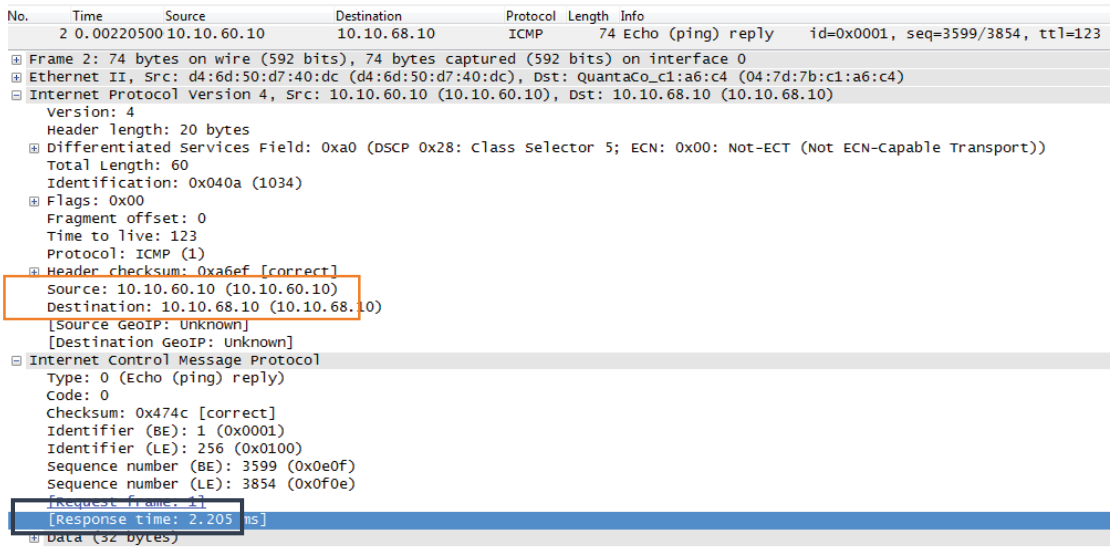


Fig. 7.24. Ping de host fuente a host destino del trafico COS3 en un escenario normal.

Esta gráfica, muestra un envío de ping en el servicio Telefonía CoS3:

Host fuente 10.10.60.10 de la red de Telefonía 1 – VLAN 60 – CoS3
Host destino 10.10.68.10 de la red de Telefonía 10 – VLAN 68 – CoS3

El tiempo de host a host es **2.205 ms**

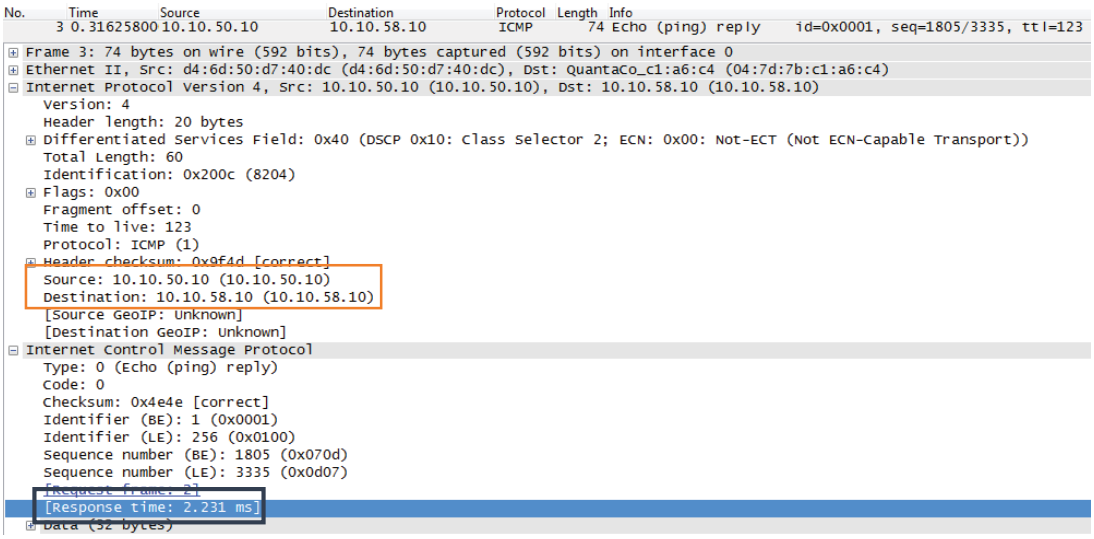


Fig. 7.25. Ping de host fuente a host destino del trafico COS2 en un escenario normal.

Esta gráfica, muestra un envío de ping en el servicio Servidores CoS2:

Host fuente 10.10.50.10 de la red de Servidores 1 – VLAN 50 – CoS2
Host destino 10.10.58.10 de la red de Servidores 10 – VLAN 58 – CoS2

El tiempo de host a host es **2.231 ms**

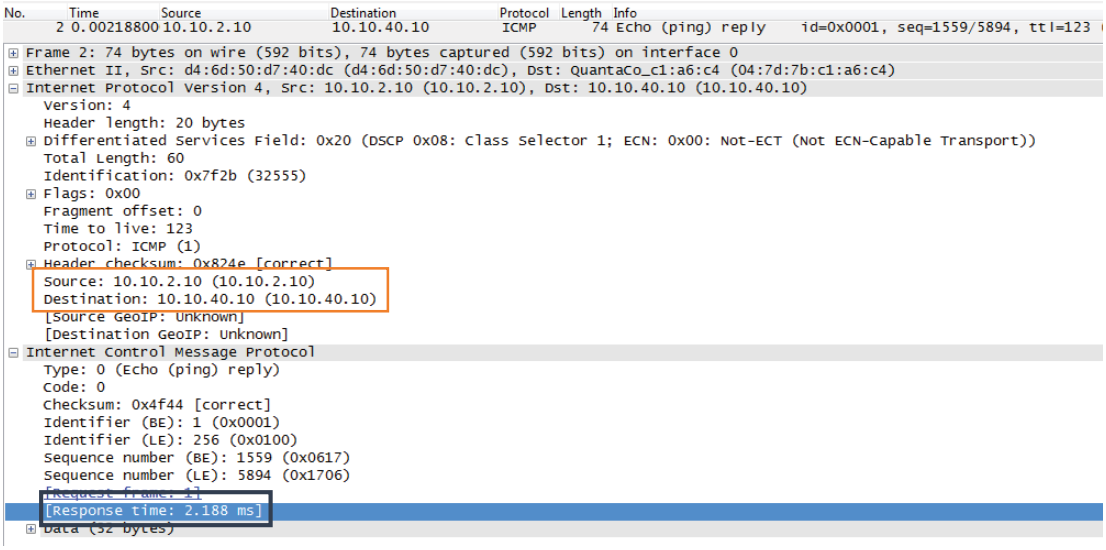


Fig. 7.26. Ping de host fuente a host destino del trafico COS1 en un escenario normal.

Esta gráfica, muestra un envío de ping en el servicio Internet CoS1:

Host fuente 10.10.2.10 de la red de Ing. Eléctrica – VLAN 2 – CoS1
Host destino 10.10.40.10 de la red de Ciencias Sociales – VLAN 40 – CoS1

El tiempo de host a host es **2.188 ms**

(7.7.4.2.) En un escenario saturado, tiempos de envío.

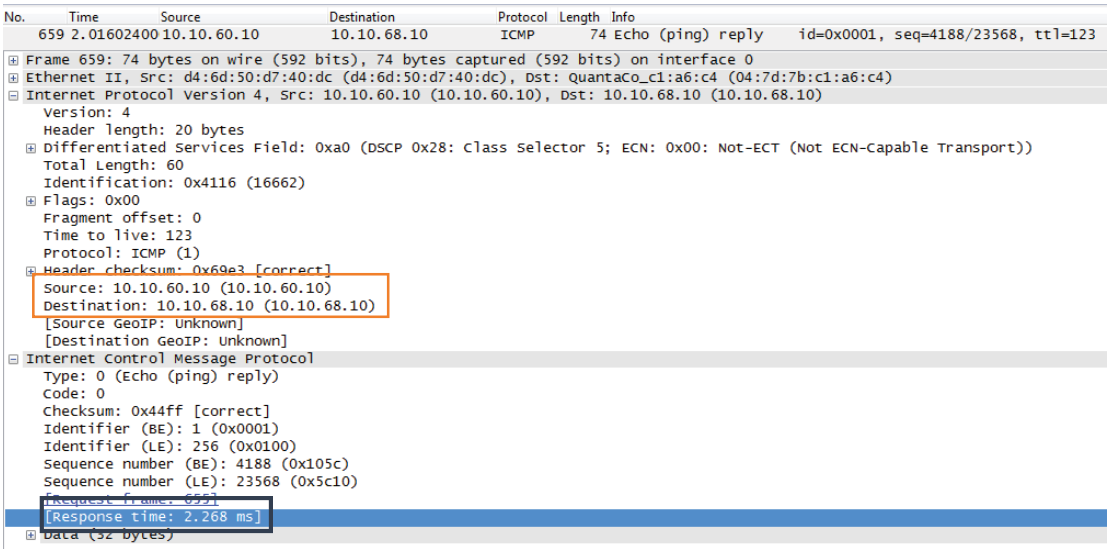


Fig. 7.27. Ping de host fuente a host destino del trafico COS3 en un escenario saturado.

Esta gráfica, muestra un envío de ping en el servicio Telefonía CoS3 en un escenario saturado:

Host fuente 10.10.60.10 de la red de Telefonía 1 – VLAN 60 – CoS3
Host destino 10.10.68.10 de la red de Telefonía 10 – VLAN 68 – CoS3

El tiempo de host a host es **2.268 ms**

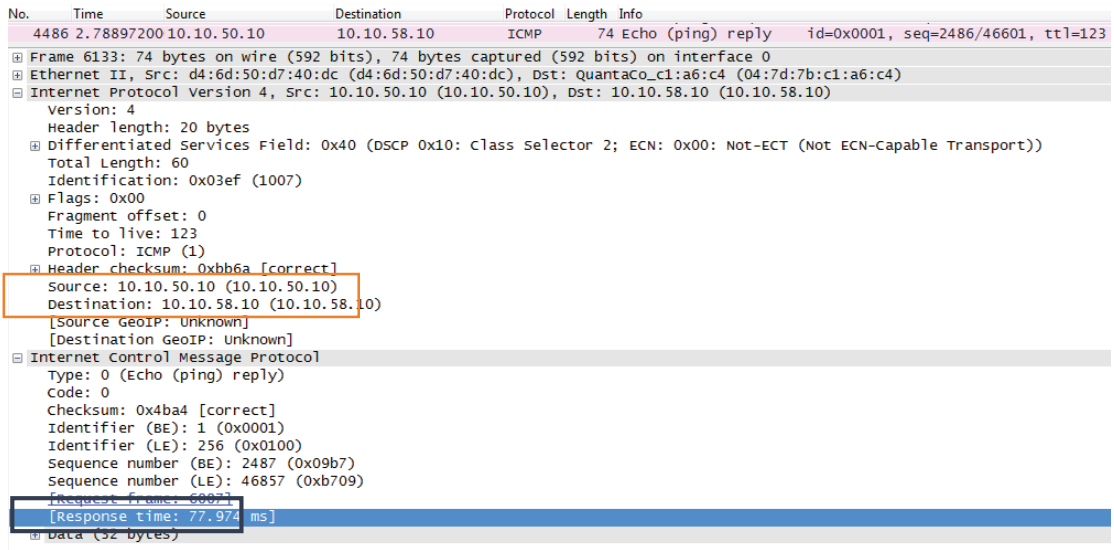


Fig. 7.28. Ping de host fuente a host destino del trafico COS2 en un escenario saturado.

Esta gráfica, muestra un envío de ping en el servicio Servidores CoS2 en un escenario saturado:

Host fuente 10.10.50.10 de la red de Servidores 1 – VLAN 50 – CoS2
Host destino 10.10.58.10 de la red de Servidores 10 – VLAN 58 – CoS2

El tiempo de host a host es **77.974 ms**

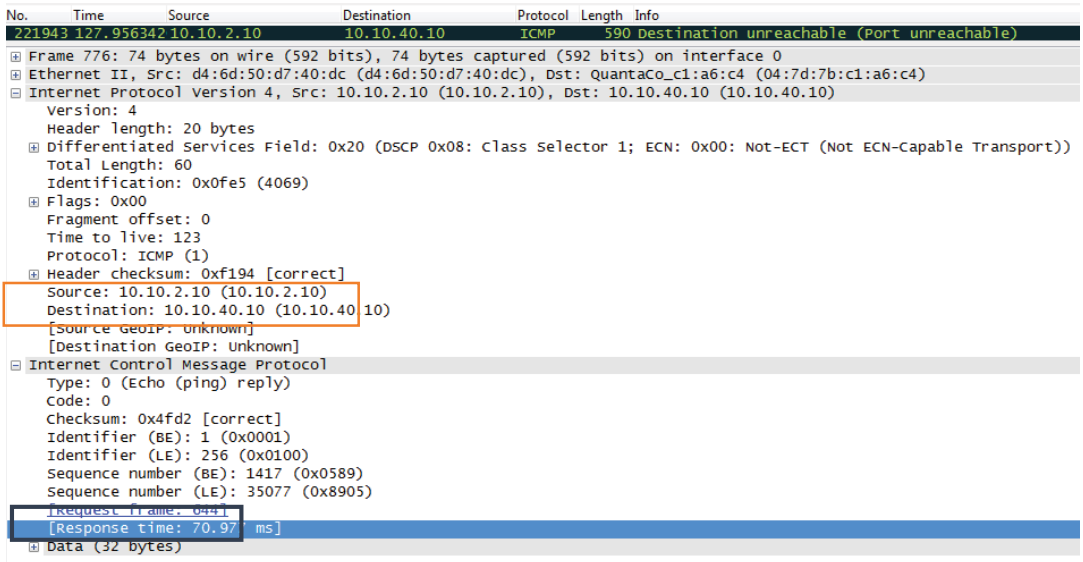


Fig. 7.29. Ping de host fuente a host destino del trafico COS1 en un escenario saturado.

Esta gráfica, muestra un envío de ping en el servicio Internet CoS1 en una escenario saturado:

Host fuente 10.10.2.10 de la red de Ing. Eléctrica – VLAN 2 – CoS1
Host destino 10.10.40.10 de la red de Ciencias Sociales – VLAN 40 – CoS1

El tiempo de host a host es **70.977 ms**

Comparación de tiempos

TIEMPO (ms)			
	ESCENARIO		
CLASE DE SERVICIO	NORMAL	SATURADO	DIFERENCIA
TELEFONIA - COS3	2.205	2.268	0.063
SERVIDORES - COS2	2.231	77.974	75.743
INTERNET - COS1	2.188	70.977	68.789

Tabla 7.1. Comparación de tiempos.

En la tabla muestra la diferencia en tiempos de envío, en la clase del servicio de telefonía la diferencia es poco, pero en los servicios de servidores e internet la diferencia de tiempos es mayor, esto depende a la demanda del servicio.
Actualmente el servicio de internet es el que tiene mayor demanda.
La diferencia de tiempos no causa caídas del servicio, solo una ligera demora.

(7.8.) Resultados de tablas de rutas generales a redes remotas

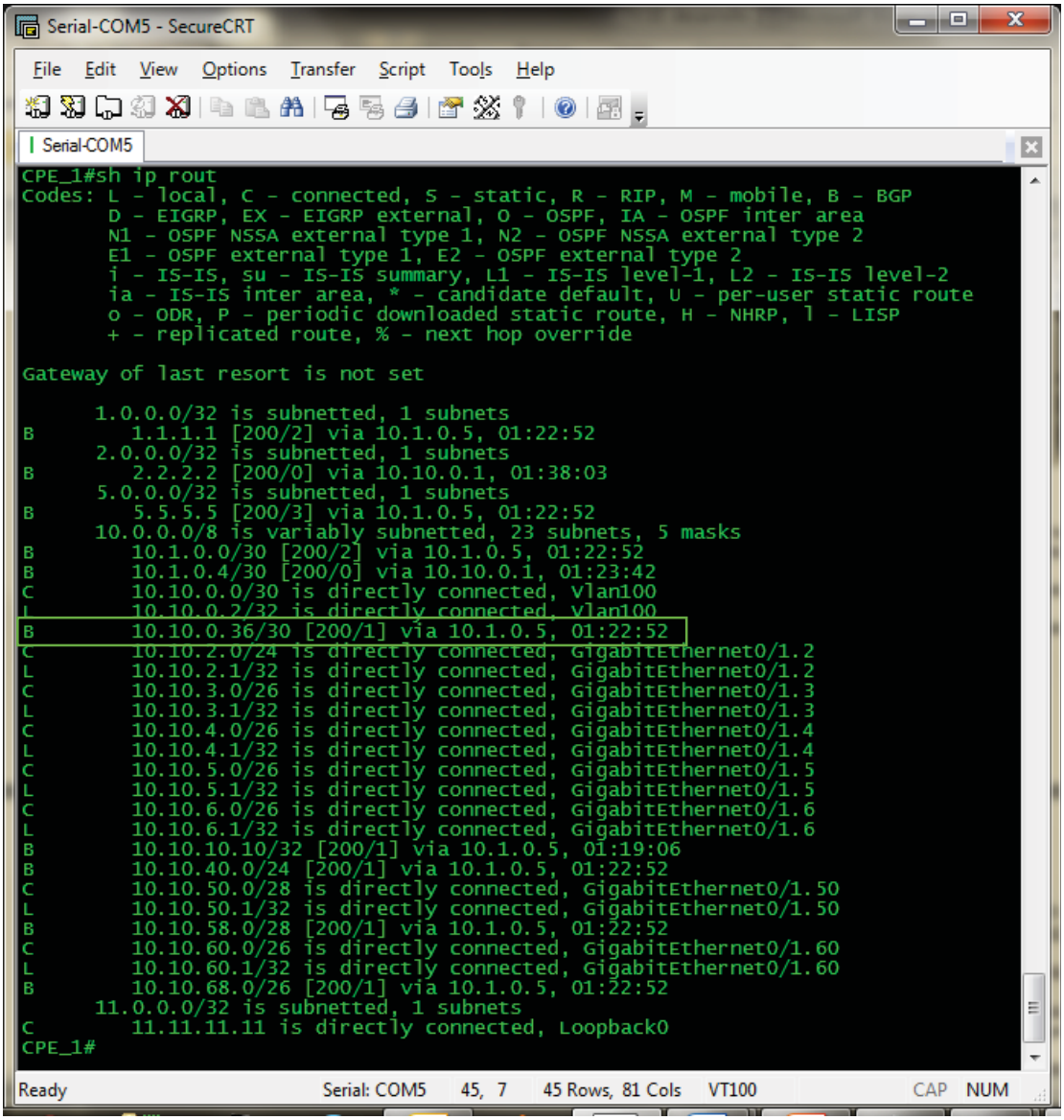


Fig. 7.30. La tabla de rutas IP del equipo CPE_1 hacia las redes remotas.

El resultado muestra todas las rutas hacia las redes remotas aprendidas por el protocolo BGP, y las conexiones físicas directamente en sus interfaces, así mismo indica la vía de salida y la ip del siguiente salto.

- L: identifica que la ruta es link-local. Las redes link-local se crean de forma automática cuando se configura una interfaz con una dirección IP y se activa.
- C: identifica una red conectada directamente. Las redes conectadas directamente se crean de forma automática cuando se configura una interfaz con una dirección IP y se activa.
- B: indica que la ruta se obtuvo de forma dinámica de otro enrutador mediante el protocolo de enrutamiento (BGP).

Analizando una ruta de la figura 3.19

B 10.10.0.36/30 [200/1] vía 10.1.0.5, 01:22:52

La letra B indica que la red 10.10.0.36 fue aprendida por el protocolo BGP

- 10.10.0.36/30: identifica la red destino
- [200/: identifica la distancia administrativa del origen de la ruta
- /1]: identifica la métrica para llegar a la red remota
- 10.1.0.5: identifica la dirección IP del siguiente salto para llegar a la red remota
- 01:22:52: identifica el tiempo transcurrido desde la última comunicación con la ruta.

(7.9.) Resultados de las pérdidas de paquetes.

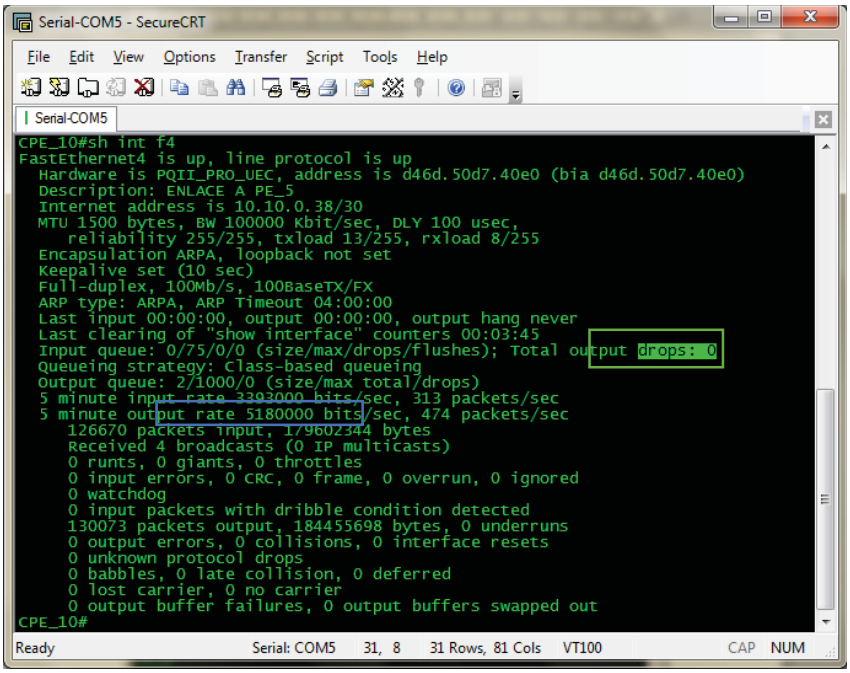


Fig. 7.31. Sin pérdidas de paquetes en la interfaz WAN del equipo CPE_10.

El tráfico de la red en la interfaz WAN del CPE_10 no presenta pérdida paquetes, no hay **congestión de red**, esto se ve en la Fig. 7.31, donde se aprecia:

Recuadro azul: Tasa de transmisión **= 5.180 Mbps**

Recuadro anaranjado: **Drops: 0 ->->-> 0%** de perdida de paquetes.

0% de perdidas paquete en un escenario donde funcionan simultáneamente las tres clases de servicio: Telefonía, Servidores e Internet.

El dimensionamiento para este equipo CPE_10 cubre una tasa de transmisión máxima a 10 Mbps. Es decir que aún no se genera una congestión de la red.
Las pérdidas de paquetes se mostraran cuando alcance tasas de transmisiones mayores a 10 Mbps.

COSTO - BENEFICIO DE LA PROPUESTA

Para calcular el costo se consideran los precios de los componentes utilizados en el desarrollo de la red de datos en la plataforma IP-MPLS.
Puesto que esta es la primera red de datos en la plataforma IP-MPLS de la UNSAAC, se tiene que considerar el costo de todos los componentes que se llegarían a utilizar en todo el proceso de la implementación y ejecución; implica comprar equipos de telecomunicaciones y materiales para acoplar e integrar a red actual.

Los costos se detallan en los cuadros 8.1, 8.2 y 8.3:

UNIVERSIDAD NACIONAL SAN ANTONIO ABAD DEL CUSCO

TESIS INGENIERIA ELECTRÓNICA

ANÁLISIS Y MEJORA DE LA RED DE DATOS DE LA UNSAAC SOBRE LA PLATAFORMA IP-MPLS EN UN BANCO DE PRUEBAS

COSTOS Y PRESUPUESTOS TESIS PRE-GRADO

ITEM	CANT.	DESCRIPCIÓN	Costo Unitario Nuevos Soles	Total en Nuevos Soles
1	1	COSTO DE **EQUIPAMIENTO** DE LA RED PROPUESTA	265,211.20	265,211.20
2	1	**Instalación e Integración** de la red MPLS en la red de datos UNSAAC	15,091.00	15,091.00
3			0.00	0.00
4				
5				
6				
7				
8				
9				
10				
11				

Tesis para optar el Título Profesional de Ingeniero Electrónico:
ANÁLISIS Y MEJORA DE LA RED DE DATOS DE LA UNSAAC SOBRE LA PLATAFORMA IP-MPLS EN UN BANCO DE PRUEBAS

TOTAL EN NUEVOS SOLES S/. **280,302.20**

Br. Joel Lenin Quispe Vilca Br. Edison Yuver Moreno Cardenas

Tabla. 8.1. Resumen del costo dimensionado en el análisis y diseño de la red de datos en la plataforma IP-MPLS.

2	COSTO DE EQUIPAMIENTO DE LA RED PROPUESTA

PRECIO DE LOS EQUIPOS				
No.	Descripción	Cantidad	Costo unitario	Costo total (S/.)
1	CISCO 3945E /K9	5	32,011.20	160,056.00
2	CISCO 1921 /K9	10	1,597.14	15,971.40
3	SWITCH CISCO CATALYST 2960	10	1,877.58	18,775.80
4	Servidor Ibm X3400 M3 7379	20	3,115.00	62,300.00
5	FIBRA OPTICA SM SC/SC 3MTS DUPLEX	10	80.00	800.00
6	SOFTWARE DE ADMINISTRACION	1	308.00	308.00
7	LICENCIA DE MPLS	20	350.00	7,000.00
8				0.00
9				0.00
10				0.00
11				0.00
12				0.00
	TOTAL			265,211.20

Tabla. 8.2. Costo de equipos de telecomunicaciones.

Se realiza la propuesta con los precios del mercado que están ofertadas por las páginas web y local de ventas en la ciudad de Lima por lo que se estima otro presupuesto para el transporte de estos equipos y materiales por transportistas de carga Lima – Cusco.

Se estima diez días de montaje de equipos de telecomunicaciones en los diferentes puntos como son el data center y facultades y veinte días más para realizar las pruebas de integración del servicio y capacitación.

2	Instalación e Integración de la red MPLS en la red de datos UNSAAC

ALQUILER DE EQUIPOS Y HERRAMIENTAS							
No.	Descripción			Cantidad	Dias	Costo unitario	Costo total (S/.)
		Costo	Años				
1	Equipos de protección personal	35.00	0.1	1	10	2.50	25.00
2	Laptop	3,500.00	2.0	2	30	5.00	300.00
3	Transporte combi personal de trabajo			4	30	2.00	240.00
4	Caja de Herramientas ethernet	350.00	2.0	1	10	1.00	10.00
5	ETIQUETADORA BROTHER 24mm	350.00	2	1	10	1.00	10.00
6	Camara digital EpsonES95 16MP	250.00	2	1	10	1.00	10.00
7	Transporte de traslado de equipos hasta la UNSAAC			1	2	578.00	1,156.00
	TOTAL						1,751.00

MATERIALES					
No.	Descripción	Cantidad	Unidad	Costo unitario	Costo total (S/.)
1	PATCH CORD CAT 6 CERTIFICADOS DE 1,5 MTS	40	UND	7.00	280.00
2	CABLE UTP cat.6 SATRA	100	MTS	1.50	150.00
3	PRECINTOS	1	CTO	12.00	12.00
4	CARTUCHO DE ETIQUETADORA 24mm	1	UND	70.00	70.00
5					0.00
	TOTAL				512.00

CONSUMIBLES					
No.	Descripción	Cantidad	Unidad	Costo unitario	Costo total (S/.)
1	Papel Bon	200	UND	0.10	20.00
2	Marcadores indelebles	2	UND	1.00	2.00
3	Impresiones a color y blanco y negro	20	UND	0.30	6.00
4					0.00
5					0.00
	TOTAL				28.00

MANO DE OBRA							
No.	Descripción	Cantidad	Días	H-h / día	H-h total	Costo unitario	Costo total (S/.)
1	Ingeniero Electrónico Residente	2	30	5	300	40.00	12,000.00
2	Técnico de instalación	2	10	4	80	10.00	800.00
3					0		0.00
4							0.00
	TOTAL				380.00		12,800.00

SUBTOTAL		15,091.00
GASTOS GENERALES	0.0%	0.00
UTILIDAD	0.0%	0.00
TOTAL		15,091.00

Tabla. 8.3. Costo de materiales, administrativos, mano de obra de la instalación e integración de la red propuesta.

El hecho de emplear enrutadores de Servicios Integrados de segunda generación para el diseño de la red de datos de la UNSAAC, reduce el consumo de recursos en la red, lo que permite un mejor procesamiento de los datos que se transmiten en ella. Esto incrementa aún más la escalabilidad de este tipo de soluciones, y permite que la red soporte diferentes tipos de servicio como voz, video y acceso a Internet. Además, el corto tiempo de convergencia obtenido en esta solución, permite afirmar que en caso de existir eventos que puedan hacer que una sesión BGP caiga, ésta se recuperará rápidamente, reduciendo así el tiempo de indisponibilidad de servicio hacia los usuarios.[82]

MPLS como toda tecnología nueva, satisface ciertas características que para el usuario son de gran importancia en el desarrollo de sus aplicaciones y sus demandas, por ello los beneficios más

[82]http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/1500/MENENDEZ_AVILA_RICARDO_SOLUCION_MPLS_VPN.pdf?sequence=1

sobresalientes que el usuario tendrá al ser implementada una solución MPLS en el núcleo de su red de datos son:

Con las nuevas aplicaciones de MPLS se pueden priorizar las calidades de los servicios por medio de "Acuerdos de Niveles de Servicios" (Service Level Agreements), que sirven para optimizar la velocidad para flujos específicos de video y voz, aprovechando al máximo las transferencias de archivos, proporcionándole al usuario garantía y seguridad de una conexión estable y sin limitaciones de tiempo, permitiendo menos retardos y aprovechando al mismo tiempo los beneficios de red de Internet, como sucede con las aplicaciones multimedia que se ejecutan en tiempo real.[83]

Una de las características fundamentales es el manejo de un gran Ancho de Banda, actualmente y dependiendo de los recursos disponibles se tienen velocidades del orden de Megabits por segundo, pero la tendencia es lograr el rango de los Gigabits por segundo.

Para aplicaciones de Sistema de Control a distancia de equipos muy sofisticados en los cuales demasiado retardo de la información de Control entre el equipo y el manipulador remoto puede resultar fatal, es de vital importancia reducir este retardo al mínimo posible, lo cual se logra con la combinación de una gran Ancho de Banda y la priorización de los servicios y técnicas avanzadas de enrutamiento que ofrece MPLS, con lo cual se logran retardos realmente muy pequeños en el orden de los milisegundos, características que permite mantener en un nivel adecuado el retardo de la información; muy importante sobre todo para sistemas de control de dispositivos a distancia.

[83] http://repositorio.utp.edu.co/dspace/bitstream/11059/1311/1/0046T172.pdf

CONCLUSIONES

CONCLUSIONES PARCIALES.

- En la red de datos sobre la plataforma IP-MPLS propuesta soporta una capacidad doble que el actual ancho de banda (150 Mbps) que se maneja, y la modularidad que toda red debe poseer a futuro. La arquitectura propuesta full mesh garantiza la fiabilidad y rapidez en el procesamiento de datos para la comunicación de los usuarios finales.

- El equipamiento mencionado en el capítulo IV está diseñado para soportar tecnología MPLS, tipos de tráfico, calidad de servicio, protocolos de enrutamiento que cumplen con los requerimientos de una red IP-MPLS. Además el equipamiento que se propone es flexible a cualquier red, esto ayuda a la integración en la red actual. Los enrutadores que se mencionan trabajan con puertos gigabitethernet la cual respalda a la categoría Ethernet que está instalada en la ciudad de Perayoc, y se podrá acoplar a los diferentes enlaces de fibra mediante convertidor de medio, de luz a electricidad.

- Se llegó a implementar en software GNS3 la red propuesta, llegando a validar la conectividad entre todas las subredes creadas, y administrar todos los equipos mediante una IP virtual denominada loopback de gestión. Logrando una mejor controlabilidad del administrador de red por la accesibilidad práctica. En el laboratorio realizado en equipos reales de marca CISCO se obtuvo pruebas satisfactorias según la teoría y diseño propuesto, se probó conectividad y saturación de los canales de los diferentes tipos de tráfico.

- Al ver los resultados de la tabla 7.1 se notó que los tiempos para el tráfico cos3 no varían demasiado puesto que este tipo de tráfico es en tiempo real y prioridad alta por sus características, con respecto a los 2 tipos de trafico cos2 y cos1 son menos sensibles y se nota la diferencia en el aumento de tiempos de respuesta con respecto a la demanda de usuarios o descargas. Además la visualización de los parámetros de marcación de paquetes en las interfaces de entrada de los enrutadores, la cual clasifican los diferentes tipos de tráfico; se visualiza la calidad de servicio en las interfaces de salida de los enrutadores según se ha creado las listas de acceso de prioridad y diferenciar los tiempos de respuesta de acuerdo a la prioridad con que viaja el paquete de información. Se analiza las tablas de enrutamiento del mecanismo IP-MPLS y el protocolo BGP visualizando el trayecto y las subredes que se anuncian y recepciona en la tabla de los enrutadores, además de las actualizaciones constantes que se realiza en los enrutadores nos ayuda a tener un mejor status de nuestra red

- Los beneficios del costo de implementar esta red IP-MPLS en la UNSAAC son: Ahorros de costes, dependiendo de la combinación específica de aplicaciones y de la configuración de la red IP-MPLS de la UNSAAC, los servicios pueden reducir los costes entre un 10 y un 25% frente a otros servicios de datos comparables. Soporte de QoS, hace referencia a la priorización del tráfico en tiempo real, una prestación clave cuando se quiere introducir voz y vídeo en las redes de datos. Rendimiento mejorado, debido a la naturaleza de "muchos a muchos" de los servicios la red IP-MPLS, se reduce el número de saltos entre puntos, lo que se traduce directamente en una mejora de los tiempos de respuesta y del rendimiento de las aplicaciones. Recuperación ante desastres, permiten conectar los centros de datos y otros emplazamientos

clave mediante múltiples conexiones redundantes a la nube MPLS y, a través de ella, a otros sitios de la red. Preparación para el futuro, la red IP-MPLS representa "el camino del futuro".

CONCLUSIÓN GENERAL.

- Una vez analizados e interpretados los resultados arrojadas por los instrumentos de recolección de datos aplicados, se obtuvo como resultados la fiabilidad en acceso a la red de nuestros usuarios, la red garantiza un crecimiento a futuro a nivel físico y lógico, seguridad en la red y fácil administración. Así mismo el método de balancear la carga del tráfico mediante el protocolo BGP y políticas de servicio creados, escogiendo la mejor ruta para su destino; adecuar la comunicación y petición a mayor intensidad en la INTRANET aprovechando la abundante información académica de la UNSAAC.

  Además se pudo determinar que cada uno de los objetivos planteados en esta investigación fueron alcanzados satisfactoriamente, ya que quedó plasmado un análisis sistemático que permite conocer los fundamentos básicos de las tecnologías que conforman este estudio, de la misma manera quedaron plasmados tanto aspectos técnicos (QoS, acceso al medio, y optimización del tráfico) como no técnicos (operatividad, productividad y aspectos económico) evidenciando que los servicios de transporte de datos que ofrecen la red IP-MPLS propuesta para este estudio, son considerados aceptables, sin embargo, la inclusión de tecnologías que implementen mejoras tanto técnicas - operativas como económicas, siempre serán fundamentales para mantener los ideales de excelencia en la calidad de los servicios prestados en la UNSAAC.

RECOMENDACIONES Y COMENTARIOS

- La orientación básica de las recomendaciones es que; los logros, se deben consolidar y de ser posible, mejorar y superar; las deficiencias o distorsiones, se deben corregir; las carencias, se deben cubrir con las implementaciones o adquisiciones que sean necesarias; las limitaciones se deben de superar.

- Implementar y poner en funcionamiento el diseño de la red de datos en la plataforma IP-MPLS que proponemos; por los beneficios que trae como son Ingeniería de tráfico, fácil administración de la red, unificación de los diferentes tipos de tráfico, los recursos físicos están diseñados para un crecimiento del BW en el futuro; para que la UNSAAC tenga una Intranet independiente. Todo ello traería a los usuarios dentro de la universidad como: docentes, alumnos y administrativos optimizar la productividad y afianzar el aspecto académico.

- Realizar pruebas con la mayor cantidad de equipos que aparece en la Fig. 4.22. La topología lógica de la Red General de datos en la plataforma IP-MPLS de la UNSAAC, ya que la muestra para en el análisis de la tesis, es una limitante para ver el funcionamiento general de toda la red de datos en la plataforma IP-MPLS propuesto debido a que solo se tiene pocos equipos.
  El estudio necesario es ver la convergencia y funcionamiento paralelo de los diferentes tipos de servicio por medio de protocolo BGP.

- Conseguir la licencia del MPLS para realizar y tener un banco pruebas general en equipos enrutadores y switches, hacer un análisis más profundo del funcionamiento del protocolo MPLS, como la conmutación de etiquetas; Conectividad en malla, Administración de QoS, Optimización de rutas, Redundancia en el backbone, Priorización de tráfico y Convergencia IP voz/datos/video, ya que la licencia es una limitante a la hora de realizar las pruebas en equipos reales.

- Para mejorar el análisis de ingeniería de tráfico en la red de datos en la plataforma IP-MPLS, se podría aumentar dos tipos de tráfico a la existente, al final el análisis seria de cinco clases de servicio, la marcación de paquetes que la realizan en la LAN del enrutador como la aplicación de Calidad de Servicio (QoS) en la salida o la WAN del enrutador; contaría de un estudio más detallado. El estudio pasaría al estudio de colas.

- Fomentar a desarrollar un proyecto de investigación acerca de la digitalización de toda la información que la universidad tiene como: Libros, tesis, archivos documentarios y todo archivo físico. La implementación de una biblioteca virtual es un proyecto de investigación que abre nuevos horizontes de conocimiento y estudio.

- La red de datos de la UNSAAC en la plataforma IP-MPLS propuesta está orientada a ser una INTRANET, el cual tiene como objetivo organizar el escritorio de cada docente, alumno y administrativo con mínimo costo, tiempo y esfuerzo para ser más productivo, rentable, oportuno, seguro y competitivo.

- Implementar en una simulación con equipos reales la red de datos en la UNSAAC sobre la plataforma IP-MPLS propuesta, obteniendo además de la licencia del MPLS para los

enrutadores, y realizar un análisis más detallado lo cual ayudara a verificar el estudio de los diferentes niveles de servicio, mayor fiabilidad y el transporte de un tráfico óptimo.
Además se recomienda que en base a este proyecto de investigación den comienzo a nuevos proyectos de investigación como una biblioteca virtual, digitalización de la información de la Universidad.

- Realizar el estudio de diseño de cableado estructurado en cobre y fibra óptica actual para obtener el dimensionamiento adecuado y futuro según estándares de cableado estructurado ya que según datos de la red de datos de la UNSAAC la cantidad de usuarios ha aumentado a gran escala.

- Tener en cuenta las medidas de seguridad eléctrica para el sistema instalado, tanto para garantizar el funcionamiento ininterrumpido de la Red de voz y datos, como para proteger los equipos y al personal de posibles fallas eléctricas.

- Se puede apreciar el gran crecimiento de usuarios y acceso a la red en corto tiempo. Es claro que la demanda de servicios seguirá exigiendo mayor velocidad e incrementando usuarios, esto lleva de la mano al cambio de equipamiento para poder satisfacer el procesamiento de la información a mayor requerimiento. Las redes LAN a largo plazo deberían ser inalámbricas, seguras, inteligentes y más orientadas a los servicios que a la velocidad.

BIBLIOGRAFÍA

ALEJANDRO E. CABALLERO ROMERO, Guías Metodológicas Para los Planes y Tesis de Maestrías y Doctorados, Lima: Ugraph S.A.C., 2011.

ROBERTO HERNANDEZ SAMPIERI, Metodología de la investigación, 5ta Edicion Sampieri., 2008.

REDY ECHARRI ROZAS Y DANTE PACHECO MIRANDA, Diseño de una Red Privada Virtual Para La Universidad Nacional San Antonio Abad del Cusco., Tesis Pregrado en Ingeniería Informática y de Sistemas, 2008.

MARTHA ODILIA TAPASCO GARCIA, MPLS, EL PRESENTE DE LAS REDES IP, Tesis Pregrado en Ingeniería de Sistemas y Computación, 2008.

M. SC. INGENIERO ELÉCTRICO SIDNEI DE OLIVERA GUERRA, Una Propuesta De Arquitectura Mpls/Diffserv Para Proveer Mecanismos De Calidad De Servicio (Qos) En El Transporte De La Telefonía Ip, Tesis Doctoral, 2004.

EDISON XAVIER BAYAS MOPOSITA Y MÓNICA JEANETH CUNALATA PILLA, "Análisis del Rendimiento de Frame Relay vs Ethernet sobre Una Arquitectura MPLS", Tesis de Grado, 2013.

PABLO BELZARENA, Ingeniería de Trafico en Línea en Redes MPLS Aplicando la Teoría de Grandes Desviaciones, Tesis Doctoral, 2003.

JAVIER IGOR DOMÉNICO Y LUNA VICTORIA GARCÍA, Medición y Análisis de Tráfico En Redes MPLS, Tesis de Grado, 2007.

CISCO 3900 SERIES INTEGRATED SERVICES ROUTERS DATA SHEET.
http://www.cisco.com/c/en/us/products/collateral/routers/3900-series-integrated-services-routers-isr/data_sheet_c78_553924.html

CISCO IOS IP ROUTING: BGP COMMAND REFERENCE.
http://www.cisco.com/c/en/us/td/docs/ios/iproute_bgp/command/reference/irg_book.pdf

BGP - CISCO PRESS
http://www.ciscopress.com/articles/article.asp?p=762938&seqNum=3

COMPARACIÓN DE CARACTERISTICAS DE ROUTER CISCO.
www.cisco.com/c/en/us/products/routers/3900-series-integrated-services-routers-isr/series-comparison.html

LECTURAS RECOMENDADAS

RFC: Request For Comments, solicitud de comentarios, son una serie de publicaciones del grupo de trabajo de ingeniería de internet que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc. y comentarios e ideas sobre estos.

A continuación se listan algunas RFC que pueden resultar de interés.

BGP:
RFC 1771 A border Gateway Protocol 4 (BGP–4)
RFC 1773 Experience with the BGP-4 Protocol
RFC 1772 Application of the Border Gateway Protocol in the Internet

EGP:
RFC 904 Exterior Gateway Protocol Formal Specification

IP:
RFC 1753 The recommendation for the IP next generation protocol
RFC 2893– Transition Mechanisms for IPv6 Hosts and Routers

MPLS:
RFC 3031 Multiprotocol Label Switching Architecture
RFC 3036 LDP Specification

OSPF:
RFC 1583 OSPF Version 2
RFC 1793 Extending OSPF to Support Demand Circuits
RFC 1584 Multicast Extensions to OSPF
RFC 1403 BGP OSPF Interaction
RFC 1245 OSPF Protocol Analysis
RFC 1246 Experience with the OSPF Protocol

ANEXOS

ANEXO A.
”LICITACIÓN PÚBLICA INTERNACIONAL N° 001-2004-UNSAAC, ADQUISICIÓN DE BIENES E INTEGRACIÓN DE LA RED DE CONECTIVIDAD DE LA UNSAAC”

e-Business Distribution Perú S.A.

Postor: e-Business Distribution Perú S.A.
Calle Antequera Nº 777 – Lima 27 – Perú
☎Tel (511) 2216560 - ☎Fax (511) 4228197

Señores
UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO
Av. De La Cultura N° 733 – Ciudad Universitaria Perayoc
Cusco

Licitación Pública Internacional N° 0001-2004-UNSAAC
Adquisición de Bienes e Instalación de la Red Integral de Conectividad de la UNSAAC

SOBRE N° 1 – PROPUESTA TECNICA 2ª Parte

ALCATEL BUSINESS PARTNER

San Isidro, 28 de junio del 2004

tyco
Electronics
AMP NETCONNECT

Tyco Electronics del Perú S.A.C.
Calle Paz Soldán 170, Of. 301, San Isidro
Lima, Perú

Telef. (51-1)221-4105, Fax. (51-1)421-0368

00775

GC-NETCONNECT-636-2004

Lima, 24 de Junio del 2004

Señores
Universidad Nacional San Antonio Abad Cuzco
Presente.-

Ref.: Licitación Pública Internacional N° 0001-2004-UNSAAC
Adquisición de Bienes e Instalación de la Red Integral de Conectividad de la UNSAAC

Estimados Señores:

Tenemos el agrado de informar a ustedes que la **División AMP NETCONNECT** está presente en Perú desde 1999 para ofrecer al Mercado Informático Peruano, una completa gama de productos **AMP** orientados a satisfacer las más exigentes demandas de "SOLUCIONES DE CABLEADOS ESTRUCTURADOS".

Es importante destacar, que con la reciente adquisición de **AMP** y **RAYCHEM** por parte del Holding **Tyco International Ltd. Company**, esto ha permitido crear la Empresa **Tyco Electronics** orientada principalmente a ofrecer al Mercado Mundial, Componentes y Sistemas Electrónicos de **alto rendimiento** para satisfacer las más exigentes necesidades de Redes de Cableados Estructurados de nuestros Clientes.

Las razones que nos motivaron para abrir una oficina en Perú, se orientan principalmente a poder ofrecer a nuestros Clientes, **un gran almacén con productos en stock y Garantía técnica de rendimiento y/o productos por 25 años** para nuestros **Sistemas de Cableados Estructurados**, Ingeniería de apoyo en Proyectos especiales y toda la Logística necesaria para asistir a nuestros Socios Tecnológicos.

En esta oportunidad, queremos presentar a la compañía **E-BUSINESS DISTRIBUTION PERÚ S.A.**, con RUC N°20474529291, autorizados a comercializar nuestros productos **AMP**, y uno de nuestro selecto grupo de **integradores, diseñadores e instaladores de redes certificados**, representada por la señora Mirtha Reinkendorf en su calidad de

Tyco Electronics del Perú S.A.C.
Calle Paz Soldán 170, Of. 301, San Isidro
Lima, Perú

Fono: (51-1)221-4165, Fax: (51-1)421-0368

00776

Gerente General, quien se presentará a la presente Licitación con nuestros productos AMP para lo cual queremos informarle que en caso sea favorecida con la buena pro, Tyco Electronics una vez culminado el proyecto, y luego de hacer una Auditoría de Red del 5% de la misma, proporcionará el "**Certificado de Garantía de Productos y Rendimiento por 25 años**" directamente a nombre de la **Universidad Nacional San Antonio Abad Cuzco.**

Adjuntamos certificados expedidos por Lloyd´s Register Quality Assurance de ISO 9001 para nuestras Plantas de Producción y Centros de Distribución en América.

Sin otro particular y quedando a la espera de cualquier consulta adicional que deseen formularnos al respecto,

Les saluda muy atentamente,

César Villar
Sales & Technical Support Engineer
AMP NETCONNECT
Tyco Electronics del Perú

00778

Av. del Libertador 6250 - 8° Piso
C1428ARS - Buenos Aires, Argentina
Tel. (54-11) 5556-3200 / Fax (54-11) 5556-3266
http://lat.3com.com/lat

Lima, 25 de Junio del 2004

Sres. UNIVERSIDAD SAN ANTONIO DE ABAD CUSCO
Licitacion Publica Internacional Nro. 001-2004-UNSAAC
"Adquisición de bienes e instalacion de la red de conectividad de la UNSAAC"

CERTIFICADO DE DISTRIBUCION

Por medio de la presente, 3Com Corporation , certifica que la empresa E-BUSINESS DISTRIBUTION PERU S.A. , es Distribuidor Autorizado en el Perú de la completa línea de productos que esta distribuye en la región.

Con esto, nuestra empresa garantiza el respaldo a la solución ofertada por el Distribuidor anteriormente individualizado.

Atentamente,

Cesar Huaylinos Rojas
Country Manager Peru-Bolivia

eBD

TrendCorp
SEGURIDAD EN INTERNET

00773

Lima, 28 de junio 2004

Señores
Licitación pública internacional N°001-2004-UNSAAC
"ADQUISICION DE BIENES E INSTALACION DE LA RED DE CONECTIVIDAD DE LA UNSAAC
Presente.-

Por medio de la presente, informamos a usted que, Trendcorp S.A es distribuidor representante de la linea Netscreen en el Perú y como estrategia de ventas locales, poseemos canales válidos para desarrollar mejor la linea y apoyarlos en todo el servicio que los clientes finales requieran.

E-Business Distribution Perú S.A. empresa constituida según leyes de la República del Perú es un canal autorizado de los productos de Netscreen y como tal , cuenta con los derechos de comercializar y brindar soporte técnico para los productos de esta última.

De igual forma, certificamos que E-Business Distribution Perú S.A.; cuenta con los recursos humanos calificados en la República del Perú, para soportar, instalar, configurar y mantener los productos de Netscreen.

Adicionalmente, la empresa E-Business Distribution Perú S.A.contará con el soporte y apoyo técnico local de la empresa Trendcorp S.A. y esta a su vez del apoyo internacional de Netscreen, que asegura el buen funcionamiento de los productos que fabrica y/o promueve a nivel mundial.

Atentamente

Luis E. Tapia
Regional Sales Manager for Latin America
Juniper- Netscreen

Leslie Puelles Risco
Gerente Comercial
Trendcorp S.A.

eBD

ALCATEL

03783

Bogotá, D.C. 23 de junio de 2004

Señores
UNSAAC
Lima

CERTIFICACION

Alcatel Enterprise Solution División certifica que actualmente e-Business Distribution Perú S.A. es distribuidor autorizado de los productos de voz y datos marca Alcatel, para el mercado empresarial y está autorizado para distribuir, instalar y dar soporte a éstos equipos en el territorio peruano.

e-Business Distribution Perú S.A. cuenta con certificación técnica de fábrica para ofrecer los servicios de soporte y mantenimiento de los equipos suministrados, además cuenta con el apoyo directo de Alcatel para el diseño de soluciones para proyectos de telecomunicaciones y el apoyo de fábrica con visitas frecuentes de nuestros ingenieros.

Cordialmente,

Jorge Silva
Andean Regional Manager
Alcatel Enterprise Solution División

e-Business Distribution Perú S.A.

eBD

ANEXO B.
“INFORME TECNICO: INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE RED INALÁMBRICA CISCO PARA UNIVERSIDAD DE SAN ANTONIO ABAD DEL CUSCO UNSAAC– CAMPUS PERAYOC”

INFORME TECNICO de:

Instalación, Configuración y Puesta en marcha de Red Inalámbrica Cisco para Universidad de San Antonio Abad del Cusco UNSAAC– campus Perayoc

Julio 2013

Tabla de contenido

CONTROL DE CAMBIOS

Versión	Fecha de Versión	Revisado por	Comentario	Detalle de cambio
1.0	06/06/2013	Ing. Jorge Luis Coveñas	Emisión Inicial	
2.0	0/07/2013	Ing. Jorge Luis Coveñas	Cambios en plan de IP	Cambio de rangos IP para usuarios de la red WiFi (desde página 17)

INTRODUCCIÓN

El presente documento es un informe técnico acerca de la instalación, configuración y puesta en marcha de la Red Inalámbrica basada en *Cisco Unified Wireless Network* según los requerimientos indicados por el personal responsable de RCU-UNSAAC designado para este proyecto.

Los siguientes archivos forman parte del informe técnico y se entregan en medio digital.

Item	Nombre de archivo	Comentarios
1	ESXi-5.1.0-799733-custom-Cisco-2.1.0.3	Instalador de VMware EXSi 5.1.0
2	PI-VA-1.2.1.12-small.ova	Instalador de máquina virtual y Cisco Prime Infraestructure 1.2
3	VMware-viclient-all-5.1.0-786111.exe	Instalador de cliente VMware para acceso a máquina virtual.
4	Prime Infrastructure 1.2 Base License and Software.zip	Licencia base Cisco Prime Infraestructure 1.2.
5	Prime Infrastructure 1.2 - Lifecycle - 50 Device Lic PAK.zip	Licencia para 50 dispositivos en Cisco Prime Infraestructure 1.2.

DATOS GENERALES

CLIENTE	**Universidad de San Antonio Abad del Cusco - UNSAAC**	
UBICACION	Ciudad Universitaria de Perayoc	Av. de la Cultura, Nro. 733, Cusco.
CONTACTO EN SITIO	Ing. Fernando Tagle Carbajal	Director de la Red de Comunicaciones – UNSAAC (RCU)
	email: ftaglec@unsaac.edu.pe	

LISTA DE MATERIALES – INVENTARIO

Item	Equipo	Tipo	Modelo	N° de Serie	Comentarios
1	1A	Biblioteca	AIR-CAP1552E-A-K9	FTX1704P0UF	En torre, PWRINJ en gabinete. Conectado a puerto 42 de
2	2A	Ciencias Administrativas	AIR-CAP1552E-A-K9	FTX1704P0QZ	En poste, PWRINJ en gabinete.
3	3A	Enfermería	AIR-CAP1552E-A-K9	FTX1704P0UG	En poste, PWRINJ en gabinete
4	4A	Medicina	AIR-CAP1552E-A-K9	FTX1704P0QU	En poste, PWRINJ en caja NEMA en azotea.
5	5A	Ing. Geológica	AIR-CAP1552E-A-K9	FTX1704P0QM	En poste, PWRINJ en gabinete
6	6A	Ciencias de la Comunicación	AIR-CAP1552E-A-K9	FTX1704P0UK	En poste, PWRINJ en gabinete
7	7A	CEPRU	AIR-CAP1552E-A-K9	FTX1704P0UE	En poste con PWRINJ en caja NEMA
8	8A	Ing. Eléctrica	AIR-CAP1552E-A-K9	FTX1704P0QV	En poste, PWRINJ en gabinete
9	9A	Educación / Derecho	AIR-CAP1552E-A-K9	FTX1704P0QS	En poste, PWRINJ en aula
10	10A	Comedor Antiguo	AIR-CAP1552E-A-K9	FTX1704P0QN	En poste con PWRINJ en caja NEMA
11	11A	Ing. Civil	AIR-CAP1552E-A-K9	FTX1704P0UH	En azotea de Arquitectura, PWRINJ en aula.
12	12A	SINDUC	AIR-CAP1552E-A-K9	FTX1704P0QW	En poste con PWRINJ en caja NEMA
13	13A	Ing. Química	AIR-CAP1552E-A-K9	FTX1704P0QP	En poste, PWRINJ en gabinete
14	14A	Arquitectura	AIR-CAP1552E-A-K9	FTX1704P0QQ	En azotea de Pabellón C, PWRINJ en aula.
15	15A	Ciencias Químicas	AIR-CAP1552E-A-K9	FTX1704P0R1	En pared, PWRINJ en gabinete.
16	16A	Pabellón Administrativo (por entrada de Av. La Cultura)	AIR-CAP1552E-A-K9	FTX1704P0UJ	En poste, PWRINJ en gabinete
17	17A	Ciencias Sociales	AIR-CAP1552E-A-K9	FTX1704P0QX	En poste, PWRINJ en gabinete de Pab. Administrativo.
18	18A	Parque Tricentenario	AIR-CAP1552E-A-K9	FTX1704P0QR	En poste, PWRINJ en aula
19	19A	Parque de la Exposición	AIR-CAP1552E-A-K9	FTX1704P0QY	En poste, PWRINJ en gabinete de Cs. Contables.
20	20A	Estacionamiento	AIR-CAP1552E-A-K9	FTX1704P0QK	En poste, PWRINJ en gabinete de RCU.
21	21A	Biblioteca	AIR-CAP1552E-A-K9	FTX1704P0VG	En azotea de RCU con PWRINJ en caja NEMA.
22	22A	Ing. Metalúrgica	AIR-CAP1552E-A-K9	FTX1704P0QT	En pared, PWRINJ en gabinete.
23	1B	Centro de Idiomas	AIR-LAP1142N-A-K9	FTX1704K00U	En balcón, 4to piso, conectado a switch Alcatel con PWRINJ.

Item	Equipo	Tipo	Modelo	N° de Serie	Comentarios
24	2B	Ing. Eléctrica	AIR-LAP1142N-A-K9	FTX1704KO10	En viga, 3er piso, switch Cisco.
25	3B	Biblioteca, Hall	AIR-LAP1142N-A-K9	FTX1704K011	En viga, 3er piso, switch Cisco.
26	4B	No asignado	AIR-LAP1142N-A-K9	FTX1704K00X	En caja.
27	5B	Patio Pabellón C.	AIR-LAP1142N-A-K9	FTX1704K00Z	En pared, 3er piso, switch CIsco
28	6B	Centro de Idiomas	AIR-LAP1142N-A-K9	FTX1704K00W	En balcón, 2do piso, conectado a switch Alcatel con PWRINJ.
29	7B	Ciencias Químicas	AIR-LAP1142N-A-K9	FTX1704K00V	En pared, pasillo 1er piso, conectado a switch Alcatel con PWRINJ.
30	8B	Contabilidad	AIR-LAP1142N-A-K9	FTX170400Y	En techo, 2do piso, conectado a switch 3Com con PWRINJ.
31	9B	Of. Admisión - Pab. Industrial	AIR-LAP1142N-A-K9	FTX1704K012	En balcón, 3er piso, conectado a switch Alcatel con PWRINJ.
32	1C	Nuevo Comedor	AIR-LAP1262N-A-K9	FTX1704K06Y	En techo, 3er piso, switch CIsco
33	2C	Derecho	AIR-LAP1262N-A-K9	FTX1704K06X	En la Biblioteca de Derecho
34	3C	Turismo	AIR-LAP1262N-A-K9	FTX1704K06W	En pared, Mesh, con fuente de poder AC.
35	4C	Auditorio Pabellón C	AIR-LAP1262N-A-K9	FTX1704K06U	En techo, switch Cisco.
36	5C	Ciencias Sociales	AIR-LAP1262N-A-K9	FTX1704K06V	En caja.
37	6C	Medicina	AIR-LAP1262N-A-K9	FTX1704K06T	En viga, 3er piso, switch Cisco.
38	1D	Sistemas e Informática	AIR-CAP3602E-A-K9	FTX1704GH2C	En pared, 2do piso, conectado a switch Alcatel con PWRINJ.
39	2D	Electrónica	AIR-CAP3602E-A-K9	FTX1704GH2A	En viga, pasillo 4to piso, switch Cisco.
40	3D	Biblioteca, RCU	AIR-CAP3602E-A-K9	FTX1704GH2B	En pared, oficina RCU, switch Cisco.
41	SW1	Ing. Metalúrgica	WS-C2960S-24PD-L	FOC1643W231	
42	SW2	Ing. Geológica	WS-C2960S-24PD-L	FOC1643X445	
43	SW3	Ing. Eléctrica	WS-C2960S-48FPD-L	FOC1703W35W	
44	SW4	Educación	WS-C2960S-24PD-L	FOC1643W22D	
45	SW5	Obras	WS-C2960S-24PD-L	FOC1643W22M	
46	SW6	Comedor	WS-C2960S-24PD-L	FOC1643X43L	
47	SW7	Arquitectura	WS-C2960S-48FPD-L	FOC1703W35R	
48	SW8	Ing. Civil	WS-C2960S-24PD-L	FOC1643W22S	
49	SW9	Pabellón C	WS-C2960S-48FPD-L	FOC1703W35L	
50	SW10	Ing. Química	WS-C2960S-48FPD-L	FOC1703Z3JF	
51	SW11	Pabellón Administrativo	WS-C2960S-48FPD-L	FOC1703W35P	
52	SW12	Ciencias Sociales	WS-C2960S-24PD-L	FOC1643W22U	
53	SW13	Administración	WS-C2960S-48FPD-L	FOC1703Z3JH	

Item	Equipo	Tipo	Modelo	N° de Serie	Comentarios
54	SW14	Aulas generales	WS-C2960S-48FPD-L	FOC1703W34Z	
55	SW15	Medicina	WS-C2960S-48FPD-L	FOC1703W35X	
56	SW16	Centro de Salud	WS-C2960S-24PD-L	FOC1643W22X	
57	SW17	Enfermería	WS-C2960S-24PD-L	FOC1643W22R	
58	SW18	Economía	WS-C2960S-24PD-L	FOC1643W22K	
59	SW19	Datacenter – RCU	WS-C2960S-48FPD-L	FOC1703Z3JK	
60	WLC	Datacenter – RCU	AIR-CT5508-K9	FCW1703L0GC	
61	UCSC	Datacenter – RCU	UCSC-C220-M3S	FCH1701V0H5	

SOLUCIÓN IMPLEMENTADA

1.1.REEMPLAZO DE SWITCHES ALCATEL POR CISCO

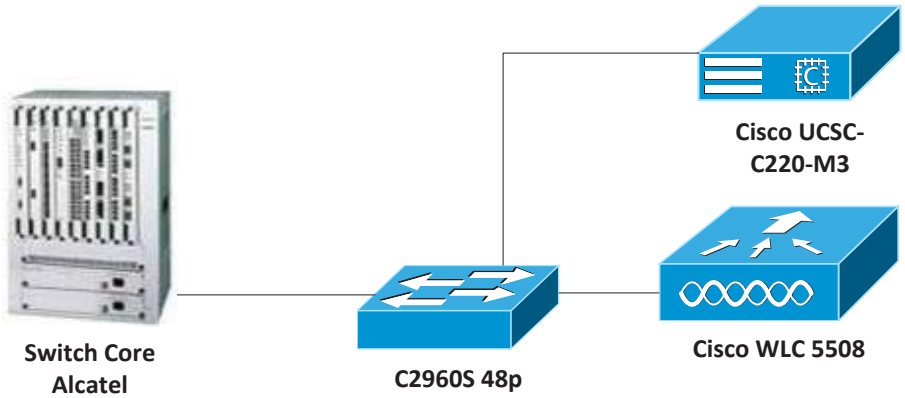
La red LAN de la UNSAAC tiene un switch de Core Alcatel, como switches de distribución cuenta con switches 3Com y como switches de acceso se usaban switches Alcatel y 3Com.
El pedido del cliente fue reemplazar los switches de acceso Alcatel que indicó por los nuevos switches Cisco. En principio, se trata de un cambio de equipo por otro con la misma configuración de VLANs y distribución de VLANs por puerto LAN.
Con esto, la topología física y lógica anterior a los reemplazos de switch se mantiene.

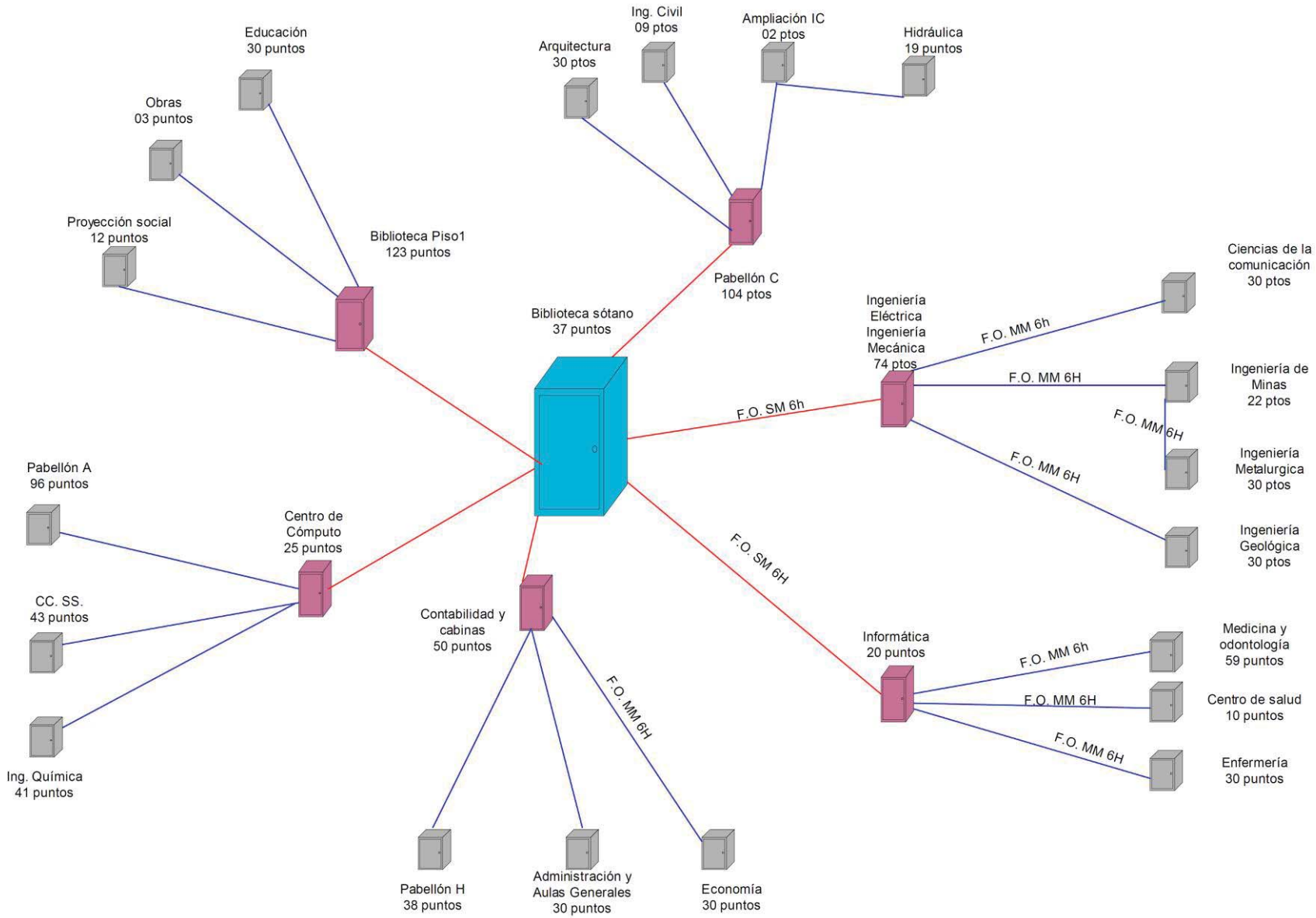
LISTA DE VLANS POR SWITCH CISCO

Dispositivo	Ubicación	Comentarios
SW1	Ing. Metalúrgica	Uplink FO MM, LC-ST
SW2	Ing. Geológica	Uplink FO MM, LC-ST
SW3	Ing. Eléctrica	
SW4	Educación	Uplink FO MM, LC-ST
SW5	Obras	
SW6	Comedor	
SW7	Arquitectura	Uplink FO MM, LC-ST
SW8	Ing. Civil	Uplink FO MM, LC-ST
SW9	Pabellón C	Uplink FO MM, LC-LC
SW10	Ing. Química	Uplink FO MM, LC-ST
SW11	Pab. Administrativo	
SW12	Ciencias Sociales	
SW13	Administración	Uplink FO MM, LC-ST
SW14	Aulas generales	Uplink FO MM, LC-ST
SW15	Medicina	Uplink FO MM, LC-ST
SW16	Centro de salud	Uplink FO MM, LC-ST
SW17	Enfermería	Uplink FO MM, LC-ST
SW18	Economía	Uplink FO MM, LC-ST
SW19	RCU – Datacenter	

La Universidad mediante la Red de Comunicaciones UNSAAC (RCU) tiene las funciones de operación y mantenimiento de los switches existentes (Alcatel y 3Com).
Los cambios de configuración solicitados a RCU para este proyecto fueron:

- Agregar las VLAN en toda la red.
- Permitir las VLANs mencionadas en los puertos troncales.
- Asignar un puerto del switch Core Alcatel para conexión con el switch Cisco del Datacenter y Configurar dicho puerto. El cliente asignó el puerto 10 del Core Alcatel 7800 para este fin.




Educación
30 puntos
Obras
03 puntos
Proyección social
12 puntos
Biblioteca Piso1
123 puntos
Arquitectura
30 ptos
Ing. Civil
09 ptos
Ampliación IC
02 ptos
Hidráulica
19 puntos
Pabellón C
104 ptos
Biblioteca sótano
37 puntos
F.O. SM 6h
Ingeniería
Eléctrica
Ingeniería
Mecánica
74 ptos
F.O. MM 6h
Ciencias de la
comunicación
30 ptos
F.O. MM 6H
Ingeniería de
Minas
22 ptos
F.O. MM 6H
F.O. MM 6H
Ingeniería
Metalurgica
30 ptos
Ingeniería
Geológica
30 ptos
F.O. SM 6H
Informática
20 puntos
F.O. MM 6h
Medicina y
odontología
59 puntos
F.O. MM 6H
Centro de salud
10 puntos
F.O. MM 6H
Enfermería
30 puntos
Pabellón A
96 puntos
Centro de
Cómputo
25 puntos
CC. SS.
43 puntos
Ing. Química
41 puntos
Contabilidad y
cabinas
50 puntos
F.O. MM 6H
Pabellón H
38 puntos
Administración y
Aulas Generales
30 puntos
Economía
30 puntos

1.2. IMPLEMENTACIÓN DE RED INALÁMBRICA

La red inalámbrica de la UNSAAC está basada en un Cisco Wireless LAN Controller 5508. Es decir se trata de la arquitectura de red Cisco Unified Wireless Network.
Con esta arquitectura los Access Point se registran en el Controller. La configuración de los SSID y esquemas de seguridad correspondientes se configuran en el Controller de manera centralizada.
Se tiene Access Point Outdoor e Indoor con los siguientes modelos:

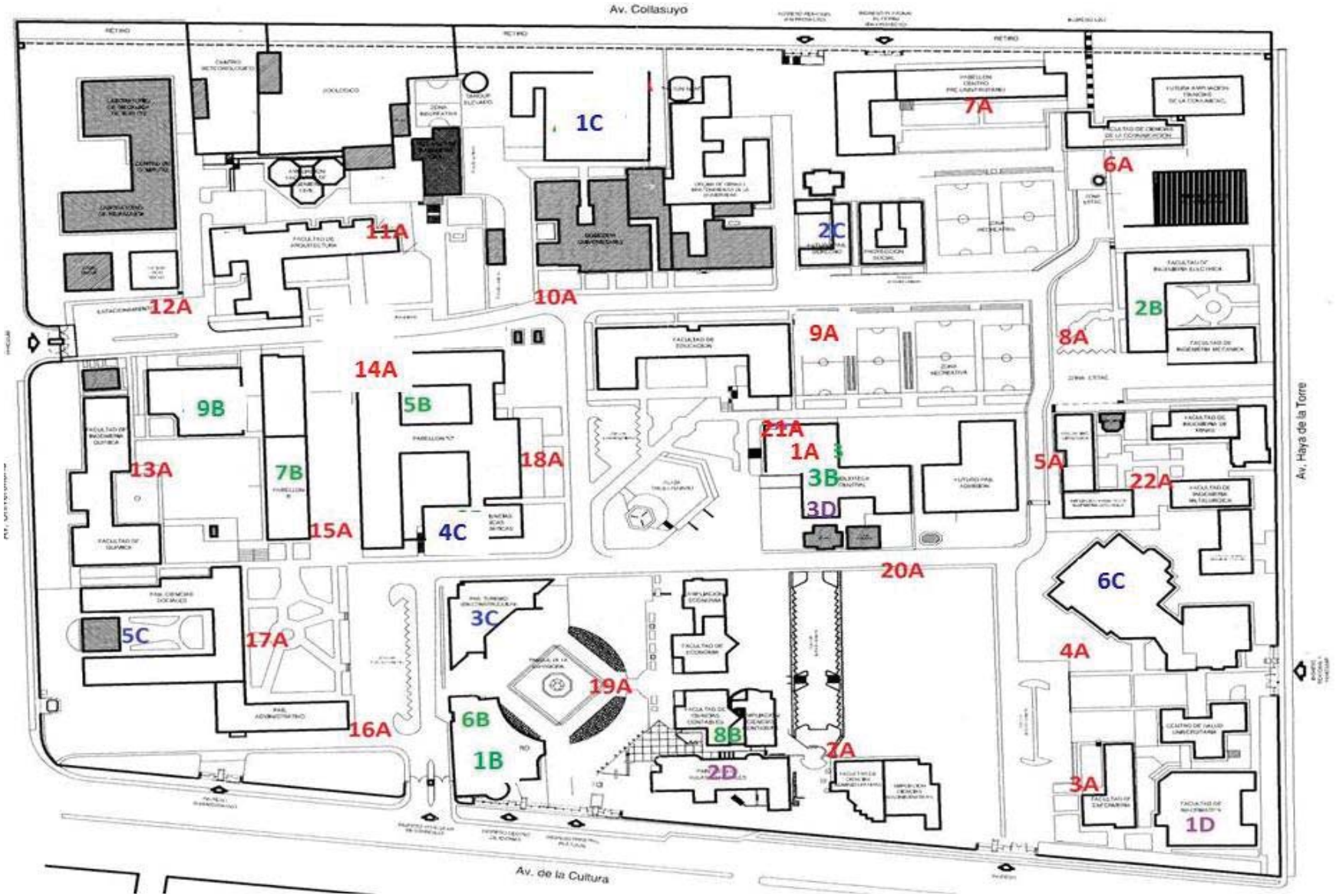
Tipo	Modelo	Part Number	Cantidad	Comentarios
A	Outdoor	AIR-CAP1552E-A-K9	22	Se conectan en topología Mesh Outdoor, con un AP como RootAP y el resto como MeshAP
B	Indoor	AIR-LAP1142N-A-K9	9	Se conectan a la red wired en puertos tipo Access VLAN 70 (untag). En los casos de conectarse con switches no-Cisco se usa Power Injector.
C	Indoor	AIR-LAP1262N-A-K9	6	De manera similar a tipo B. Con excepción el AP nombrado 3C el cual se conecta a la red Mesh Outdoor.
D	Indoor	AIR-CAP3602E-A-K9	3	De manera similar a tipo B.

Los Access Point se han instalado siguiendo las indicaciones del cliente acerca de la ubicación y alimentación de energía AC.
En el caso de los AP Outdoor se instalaron en postes y adosados a pared, para lo cual se utilizaron estructuras metálicas con tubos de 2”para el montaje de los AP.
Se coordinó con el cliente la asignación de los puertos de switches a utilizar para la conexión de los Access Point.

WIRELESS LAN CONTROLLER - AIR-CT5508-K9

- Se instaló en rack del Datacenter designado por RCU.
- Se instalaron los 02 adaptadores SFP-GLC-T en los puertos **1** y **3**.
- Se conectan los puertos 1 y 3 con el switch Cisco Catalyst 2960S de Datacenter.

PLANO DE UBICACIÓN DE ACCESS POINT



COMENTARIOS ADICIONALES

1.3. CISCCO WIRELESS LAN CONTROLLER

El Cisco Wireless LAN Controller **AIR-CT5508-100-K9** soporta una fuente de poder redundante AC. Para esto se tiene una bahía libre en la parte posterior del equipo.

Part Number	Product Name
AIR-PWR-5500-AC=	5500 Series Wireless Controller Redundant AC Power Supply

Actualmente el Controlador tiene licencia para 100 Access Points. En caso de necesitar soporte de más Access Points se debe adquirir una licencia de upgrade.

Part Number	Product Description
L-LIC-CT5508-UPG	Primary upgrade SKU: Pick any number or combination of the following options under this SKU to upgrade one or many controllers under one product authorization key
L-LIC-CT5508-5A	5 AP Adder License for the 5508 Controller (eDelivery)
L-LIC-CT5508-25A	25 AP Adder License for the 5508 Controller (eDelivery)
L-LIC-CT5508-50A	50 AP Adder License for the 5508 Controller (eDelivery)
L-LIC-CT5508-100A	100 AP Adder License for the 5508 Controller (eDelivery)
L-LIC-CT5508-250A	250 AP Adder License for the 5508 Controller (eDelivery)

1.4. SERVIDOR DE MONITOREO

El servidor de monitoreo Cisco **UCSC-C220-M3S** soporta una fuente de poder redundante AC. Para esto se tiene una bahía libre en la parte posterior del equipo. El código de la fuente de poder instalada es la siguiente:

Part Number	Product Name
UCSC-PSU-450W	450W power supply for C-series rack servers

Por otra parte el servidor está con la siguiente configuración de CPU, memoria y disco duro:

Part Number	Product Name
UCS-CPU-E5-2609	2.4 GHz E5-2609/80W 4C/10MB Cache/DDR3 1066MHz
UCS-MR-1X082RY-A	8GB DDR3-1600-MHz RDIMM/PC3-12800/dual rank/1.35v
A03-D500GC3	500GB 6Gb SATA 7.2K RPM SFF hot plug/drive sled mounted

La capacidad máxima del servidor es el siguiente:

Part Number	Product Name
Procesadores	Hasta 2 procesadores INTEL XEON familia E5-2600.
Disco duros	Hasta 8 discos duros de 2.5”SAS, SATA o SDD, acceso-frontal, hot-swap.

1.5. ACCESS POINT TIPO A

El modelo de Access Point Outdoor **AIR-CAP1552E-A-K9** se han instalado con alimentación POE mediante los Power Injector **AIR-PWRINJ1500-2=**. Estos Access Point tienen una salida POE que se desactiva cuando el Access Point se alimenta mediante Power Injector. Para poder usar esta salida de energía, lo cual puede servir para alimentar con POE a una cámara IP, por ejemplo, se debe alimentar el Access Point mediante energía AC por medio del siguiente cable **AIR-CORD-R3P-40NA=**

Por otra parte, se tiene la posibilidad de conectar este modelo de Access Point a la red cableado mediante enlace de fibra óptica para lo cual se requiere adquirir el Kit de fibra óptica de acuerdo a las necesidades del cliente:

Fiber SFPs for the Cisco Aironet 1520 Series

SKU	Description
GLC-FE-100BX-URGD	100BaseBX10-U Rugged SFP module
GLC-LX-SM-RGD	1000BaseLX single-mode Rugged SFP module
GLC-SX-MM-RGD	1000BaseSX multimode Rugged SFP module

En todos los casos los conectores son LC. El adaptador se debe instalar en el Access Point siguiendo las guías de instalación de hardware.

ANEXO C.
MEMORANDUM Nro 02-RCU-2014-UNSAAC

UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO
RED DE COMUNICACIONES UNSAAC

MEMORANDUM Nro. 02-RCU-2014-UNSAAC

DE	:	Ing. **Roger J. Coaquira Castillo** DIRECTOR de la Red de Comunicaciones UNSAAC.
A	:	**Ing. Yesenia Concha Ramos** Jefe de operaciones de la Red de Comunicaciones UNSAAC
ASUNTO	:	Permiso de acceso al Data Center y Gabinetes de la UNSAAC
FECHA	:	Cusco, 18 de Noviembre del 2014

Por medio del presente comunico a Usted, sírvase dar acceso al Data Center y Gabinetes de las diferentes facultades de la UNSAAC a los Bachilleres Edison Yuver Moreno Cardenas y Joel Lenin Quispe Vilca, con el objetivo de que desarrollen su tesis de investigación referente a la red de datos actual de la UNSAAC.

Atentamente.

Universidad Nacional de San Antonio Abad del Cusco
RED DE COMUNICACIONES - UNSAAC
Ing. Roger Coaquira Castillo
DIRECTOR

RJCC
cc./Arch.

ANEXO D.
DIRECTORIO TELEFONICO DE LA UNSAAC 2016

ANEXO E.
CAPACIDADES DE PROCESAMIENTO DE ROUTERS DE SERVICIOS INTEGRADOS DE SEGUNDA GENERACIÓN (ISR G2) EN LOS SERVICIOS DE INTERNET Y RED PRIVADA VIRTUAL (RPV).

INTERNET

Modelo Router	BW (Mbps)	Código Comercial
881 (IOS UNIVERSAL DATA) + Advanced IP Services	14 M	7976
881 (IOS UNIVERSAL) + Advanced IP Services	14 M	AATL
CISCO1921 K9 (Cisco 1921 IOS UNIVERSAL)	53 M	8751
CISCO1941 K9 (Cisco 1941 IOS UNIVERSAL)	70 M	9809
CISCO2901/K9 (Cisco 2901-2921 IOS UNIVERSAL)	80 M	9553
CISCO2911/K9 (Cisco 2901-2921 IOS UNIVERSAL)	85 M	9810
CISCO2921/K9 (Cisco 2901-2921 IOS UNIVERSAL)	105 M	9811
CISCO2951/K9 (Cisco 2901-2921 IOS UNIVERSAL)	115 M	9812
CISCO3925E/K9 (Cisco 2901-2921 IOS UNIVERSAL)	165 M	9816
CISCO3945E/K9 (Cisco 2901-2921 IOS UNIVERSAL)	225 M	9821
CISCOASR1001 (Advanced IP Services + 2xSFP-GE-T +SFP-GE-L)	1 G	AAFK
Cisco ISR 4451-X IOS XE UNIVERSAL (IP BASE)	1 G	AAUX
Cisco ASR 1002-X IOS XE UNIVERSAL + Advanced Enterprise Services License 957800751 c11143	4 G	AAUY

RPV

Modelo Router	BW Mbps (sin NAT)	BW Mbps (con NAT)	Código Comercial
881 (IOS UNIVERSAL DATA) + Advanced IP Services	80 M	30 M	7976
881 (IOS UNIVERSAL) + Advanced IP Services	80 M	30 M	AATL
CISCO1921 K9 (Cisco 1921 IOS UNIVERSAL)	188 M	45 M	8751
CISCO1941 K9 (Cisco 1941 IOS UNIVERSAL)	250 M	60 M	9809
CISCO2901/K9 (Cisco 2901-2921 IOS UNIVERSAL)	285 M	65 M	9553
CISCO2911/K9 (Cisco 2901-2921 IOS UNIVERSAL)	325 M	75 M	9810
CISCO2921/K9 (Cisco 2901-2921 IOS UNIVERSAL)	395 M	85 M	9811
CISCO2951/K9 (Cisco 2901-2921 IOS UNIVERSAL)	490 M	115 M	9812
CISCO3925E/K9 (Cisco 2901-2921 IOS UNIVERSAL)	680 M	170 M	9816
CISCO3945E/K9 (Cisco 2901-2921 IOS UNIVERSAL)	860 M	200 M	9821
CISCOASR1001 (Advanced IP Services + 2xSFP-GE-T +SFP-GE-L)	1 G	1 G	AAFK
Cisco ISR 4451-X IOS XE UNIVERSAL (IP BASE)	1 G	1 G	AAUX
Cisco ASR 1002-X IOS XE UNIVERSAL + Advanced Enterprise Services License	4 G	4 G	AAUY

ANEXO F.
TABLAS DE LA DISTRIBUCIÓN DE VLANS EN LA UNSAAC.

a) **VLANS DE DATOS.**

DISTRIBUCION DE VLANS EN LA UNSAAC						
VLAN	**NOMBRE**	**DIRECCION IP SUBRED**	**MASCARA**	**DIRECCION IP**	**mascara IP**	**BW (Mbps)**
2	ING ELECTRICA	10.10.2.0/24	0	10.10.2.1	255.255.255.0	3
3	ING GEOLOGICA	10.10.3.0/26	192	10.10.3.1	255.255.255.192	2
4	ING METALURGICA	10.10.4.0/26	192	10.10.4.1	255.255.255.192	1
5	ING DE MINAS	10.10.5.0/26	192	10.10.5.1	255.255.255.192	3
6	ING MECANICA	10.10.6.0/26	192	10.10.6.1	255.255.255.192	3
8	EDUCACION	10.10.8.0/26	192	10.10.8.1	255.255.255.192	3
9	OBRAS	10.10.9.0/24	0	10.10.9.1	255.255.255.0	3
10	DERECHO	10.10.10.0/25	128	10.10.10.1	255.255.255.128	3
11	BIBLIOTECA CENTRAL	10.10.11.0/25	128	10.10.11.1	255.255.255.128	5
12	RED DE COMUNICACIONES	10.10.12.0/26	192	10.10.12.1	255.255.255.192	3
13	CEPRU	10.10.13.0/27	224	10.10.13.1	255.255.255.224	3
14	ING ELECTRONICA	10.10.14.0/24	0	10.10.14.1	255.255.255.0	3
15	COMUNICACIÓN	10.10.15.0/26	192	10.10.15.1	255.255.255.192	3
17	CONTROL DE CALIDAD	10.10.17.0/26	192	10.10.17.1	255.255.255.192	2
18	PERSONAL	10.10.18.0/26	192	10.10.18.1	255.255.255.192	3
19	ING QUIMICA	10.10.19.0/27	224	10.10.19.1	255.255.255.224	1.5
20	COMEDOR	10.10.20.0/27	224	10.10.20.1	255.255.255.224	3
21	ARQUITECTURA	10.10.21.0/26	192	10.10.21.1	255.255.255.192	3
22	ING CIVIL	10.10.22.0/26	192	10.10.22.1	255.255.255.192	3
23	QUIMICA	10.10.23.0/26	192	10.10.23.1	255.255.255.192	2
24	INST SISTEMAS	10.10.24.0/24	0	10.10.24.1	255.255.255.0	4
25	CENTRO DE COMPUTO	10.10.25.0/24	0	10.10.25.1	255.255.255.0	3
26	PABELLON C	10.10.26.0/24	0	10.10.26.1	255.255.255.0	5
27	TURISMO	10.10.27.0/25	128	10.10.27.1	255.255.255.128	1
29	RED WIRELESS	10.10.128.0/16	0	10.10.128.1	255.255.128.0	29
32	ADMINISTRACION	10.10.32.0/26	192	10.10.32.1	255.255.255.192	3
33	CENTRO DE IDIOMAS	10.10.33.0/26	192	10.10.33.1	255.255.255.192	3
34	CONTABILIDAD	10.10.34.0/25	128	10.10.34.1	255.255.255.128	3
35	AULAS GENERALES	10.10.35.0/27	224	10.10.35.1	255.255.255.224	3
36	ENFERMERIA	10.10.36.0/26	192	10.10.36.1	255.255.255.192	3
37	ING DE SISTEMAS	10.10.37.0/24	0	10.10.37.1	255.255.255.0	4
38	MEDICINA	10.10.38.0/26	192	10.10.38.1	255.255.255.192	3
39	CENTRO DE SALUD	10.10.39.0/27	224	10.10.39.1	255.255.255.224	2
40	PABELLON ADMINISTRATIVO	10.10.40.0/24	0	10.10.40.1	255.255.255.0	5
41	CIENCIAS SOCIALES	10.10.41.0/24	0	10.10.41.1	255.255.255.0	3
42	ECONOMIA	10.10.42.0/26	192	10.10.42.1	255.255.255.192	3

b) VLANS DE SERVIDORES

VLANS DE SERVIDORES						
VLAN	**NOMBRE**	**DIRECCION IP SUBRED**	**MASCARA**	**DIRECCION IP**	**mascara IP**	**BW (Mbps)**
50	SERVIDORES 1	10.10.50.0/28	240	10.10.50.1	255.255.255.240	6
51	SERVIDORES 2	10.10.51.0/28	240	10.10.51.1	255.255.255.240	6
52	SERVIDORES 3	10.10.52.0/28	240	10.10.52.1	255.255.255.240	3
53	SERVIDORES 4	10.10.53.0/28	240	10.10.53.1	255.255.255.240	1
54	SERVIDORES 5	10.10.54.0/28	240	10.10.54.1	255.255.255.240	8
55	SERVIDORES 6	10.10.55.0/28	240	10.10.55.1	255.255.255.240	2
56	SERVIDORES 8	10.10.56.0/28	240	10.10.56.1	255.255.255.240	4
57	SERVIDORES 9	10.10.57.0/28	240	10.10.57.1	255.255.255.240	4
58	SERVIDORES 10	10.10.58.0/28	240	10.10.58.1	255.255.255.240	2
59	SERVIDORES PRINCIPAL	10.10.59.0/28	240	10.10.59.1	255.255.255.240	-

c) VLANS DE TELEFONIA

VLANS DE TELEFONIA						
VLAN	**NOMBRE**	**DIRECCION IP SUBRED**	**MASCARA**	**DIRECCION IP**	**mascara IP**	**BW (Mbps)**
60	TELEFONIA 1	10.10.60.0/26	192	10.10.60.1	255.255.255.192	2
61	TELEFONIA 2	10.10.61.0/26	192	10.10.61.1	255.255.255.192	2
62	TELEFONIA 3	10.10.62.0/26	192	10.10.62.1	255.255.255.192	1.5
63	TELEFONIA 4	10.10.63.0/27	224	10.10.63.1	255.255.255.224	0.512
64	TELEFONIA 5	10.10.64.0/26	192	10.10.64.1	255.255.255.192	3
65	TELEFONIA 6	10.10.65.0/27	224	10.10.65.1	255.255.255.224	1.5
66	TELEFONIA 8	10.10.66.0/27	224	10.10.66.1	255.255.255.224	2
67	TELEFONIA 9	10.10.67.0/27	224	10.10.67.	255.255.255.224	2
68	TELEFONIA 10	10.10.68.0/26	192	10.10.68.1	255.255.255.192	3.5

d) VLANS DE CAMARAS

VLANS DE CAMARAS						
VLAN	**NOMBRE**	**DIRECCION IP SUBRED**	**MASCARA**	**DIRECCION IP**	**mascara IP**	**BW (Mbps)**
70	CAMARAS	10.10.70.0/27	224	10.10.70.1	255.255.255.224	1

ANEXO G.
PLANTILLAS DE CONFIGURACIÓN DE LOS EQUIPOS PE Y CPE DE LA RED DE DATOS DE LA UNSAAC SOBRE LA PLATAFORMA IP/MPLS.

PE_1

```
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname PE_1
!
boot-start-marker
boot-end-marker
!
clock timezone GMT -5 0
!
no aaa new-model
memory-size iomem 5
ip cef
!
no ip domain lookup
ip domain name lab.local
!
enable secret cisco
!
interface Loopback0
 description GESTION
 ip address 1.1.1.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/0
 description ENLACE A PE_2
 ip address 10.1.0.5 255.255.255.252
 mpls ip
 duplex full
 speed 100
 no shutdown
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip flow ingress
 ip virtual-reassembly in
!
interface GigabitEthernet0/1
 description ENLACE A PE_3
 ip address 10.1.0.13 255.255.255.252
```

```
 mpls ip
 duplex full
 speed 100
 no shutdown
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip flow ingress
 ip virtual-reassembly in
!
interface GigabitEthernet0/2
 description ENLACE A PE_4
 ip address 10.1.0.17 255.255.255.252
 mpls ip
 duplex full
 speed 100
 no shutdown
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip flow ingress
 ip virtual-reassembly in
!
interface GigabitEthernet0/3
 description ENLACE A PE_5
 ip address 10.1.0.1 255.255.255.252
 mpls ip
 duplex full
 speed 100
 no shutdown
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip flow ingress
 ip virtual-reassembly in
!
router ospf 10
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 10
 router-id 1.1.1.1
 log-adjacency-changes
 redistribute bgp 100 subnets
 network 1.1.1.1 0.0.0.0 area 10
 network 10.1.0.0 0.0.0.3 area 10
 network 10.1.0.4 0.0.0.3 area 10
 network 10.1.0.12 0.0.0.3 area 10
 network 10.1.0.16 0.0.0.3 area 10
 default-information originate
```

```
!
no ip http server
no ip http secure-server
!
banner motd ^CCC

&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&
&&&&&
&                                   &
&                                   &
&      Tesis: ANALISIS Y MEJORA DE LA RED          &
&      DE DATOS DE LA UNSAAC SOBRE LA PLATAFORMA     &
&      IP/MPLS EN UN BANCO DE PRUEBAS              &
&                                   &
&      Tesistas:                       &
&      EDISON YUVER MORENO CARDENAS                &
&      JOEL LENIN QUISPE VILCA                 &
&      > FACULTAD DE INGENIERIA ELECTRONICA         &
&                                   &
&      ADVERTENCIA: Se prohibe copiar la tesis      &
&      de investigacion. Derechos Reservados.       &
&                                   &
&                                   &
&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&
&&&&&


^C
!
line con 0
 exec-timeout 0 0
 password cisco
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 password cisco
 login
!
end
```

CPE_1

```
service timestamps debug datetime localtime
service timestamps log datetime localtime
```

```
service password-encryption
!
hostname CPE_1
!
boot-start-marker
boot-end-marker
!
clock timezone GMT -5 0
!
no aaa new-model
memory-size iomem 5
ip cef
!
enable secret cisco
!
class-map match-any qos5
 match ip dscp cs6
 match ip dscp cs5
class-map match-any qos2
 match ip dscp cs2
 class-map match-any qos1
 match ip dscp cs1
!
policy-map wan
 class qos5
    priority 2048
    police 2048000 384000 768000 conform-action transmit  exceed-action drop  violate-action
drop
 class qos2
    bandwidth 6144
    police 6144000 1152000 2304000 conform-action transmit  exceed-action set-dscp-transmit
cs1 violate-action set-dscp-transmit 8
 class qos1
    bandwidth 12288
 class class-default
    fair-queue
!
policy-map Shape20480
 class class-default
    shape average 20481000
  service-policy wan
!
class-map match-any P2
match ip dscp cs2
match access-group name qos2
class-map match-any P5
match ip dscp cs5
match access-group name qos5
```

```
!
policy-map SetDscpLan
 class P5
set ip dscp cs5
class P2
  set ip dscp cs2
 class class-default
  set ip dscp cs1
!
interface Loopback0
 description GESTION
 ip address 11.11.11.11 255.255.255.255
!
interface GigabitEthernet0/0/0
 description ENLACE A PE_2
 switchport access vlan 100
 no ip address
 load-interval 30
 duplex full
 speed 100
!
interface Vlan100
 description ENLACE A PE_2
 ip address 10.10.0.2 255.255.255.252
 no shutdown
 no ip redirects
 no ip proxy-arp
 load-interval 30
 service-policy output Shape20480
!
interface GigabitEthernet0/1
 description LAN FACULTAD CPE_1
 no ip address
 load-interval 30
 duplex full
 speed 100
 no shutdown
!
interface GigabitEthernet0/1.2
 description LAN ING ELECTRICA
 encapsulation dot1Q 2
 ip address 10.10.2.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip flow ingress
 ip virtual-reassembly in
 service-policy input SetDscpLan
```

```
!
interface GigabitEthernet0/1.3
 description LAN ING GEOLOGICA
 encapsulation dot1Q 3
 ip address 10.10.3.1 255.255.255.192
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip flow ingress
 ip virtual-reassembly in
 service-policy input SetDscpLan
!
interface GigabitEthernet0/1.4
 description LAN ING METALURGICA
 encapsulation dot1Q 4
 ip address 10.10.4.1 255.255.255.192
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip flow ingress
 ip virtual-reassembly in
 service-policy input SetDscpLan
!
interface GigabitEthernet0/1.5
 description LAN ING MINAS
 encapsulation dot1Q 5
 ip address 10.10.5.1 255.255.255.192
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip flow ingress
 ip virtual-reassembly in
 service-policy input SetDscpLan
!
interface GigabitEthernet0/1.6
 description LAN ING MECANICA
 encapsulation dot1Q 6
 ip address 10.10.6.1 255.255.255.192
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip flow ingress
 ip virtual-reassembly in
 service-policy input SetDscpLan
!
interface GigabitEthernet0/1.50
 description SERVIDORES 1
 encapsulation dot1Q 50
```

```
 ip address 10.10.50.1 255.255.255.240
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip flow ingress
 ip virtual-reassembly in
 service-policy input SetDscpLan
!
interface GigabitEthernet0/1.60
 description TELEFONIA 1
 encapsulation dot1Q 60
 ip address 10.10.60.1 255.255.255.192
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip flow ingress
 ip virtual-reassembly in
 service-policy input SetDscpLan
!
router bgp 100
 no synchronization
 bgp router-id 11.11.11.11
 bgp log-neighbor-changes
 network 11.11.11.11 mask 255.255.255.255
 network 10.10.2.0 mask 255.255.255.0
 network 10.10.3.0 mask 255.255.255.192
 network 10.10.4.0 mask 255.255.255.192
 network 10.10.5.0 mask 255.255.255.192
 network 10.10.6.0 mask 255.255.255.192
 network 10.10.50.0 mask 255.255.255.240
 network 10.10.60.0 mask 255.255.255.192
 neighbor WAN_PE_2 peer-group
 neighbor WAN_PE_2 remote-as 100
 neighbor WAN_PE_2 password unsaac
 neighbor WAN_PE_2 timers 10 30
 neighbor WAN_PE_2 soft-reconfiguration inbound
 neighbor 10.10.0.1 peer-group WAN_PE_2
 neighbor 10.10.0.1 description ENLACE PE_2
 no auto-summary
!
ip http server
no ip http secure-server
!
ip access-list extended qos5
 permit ip 10.10.60.0 0.0.0.63 10.10.61.0 0.0.0.63
 permit ip 10.10.60.0 0.0.0.63 10.10.62.0 0.0.0.63
 permit ip 10.10.60.0 0.0.0.63 10.10.63.0 0.0.0.31
 permit ip 10.10.60.0 0.0.0.63 10.10.64.0 0.0.0.63
```

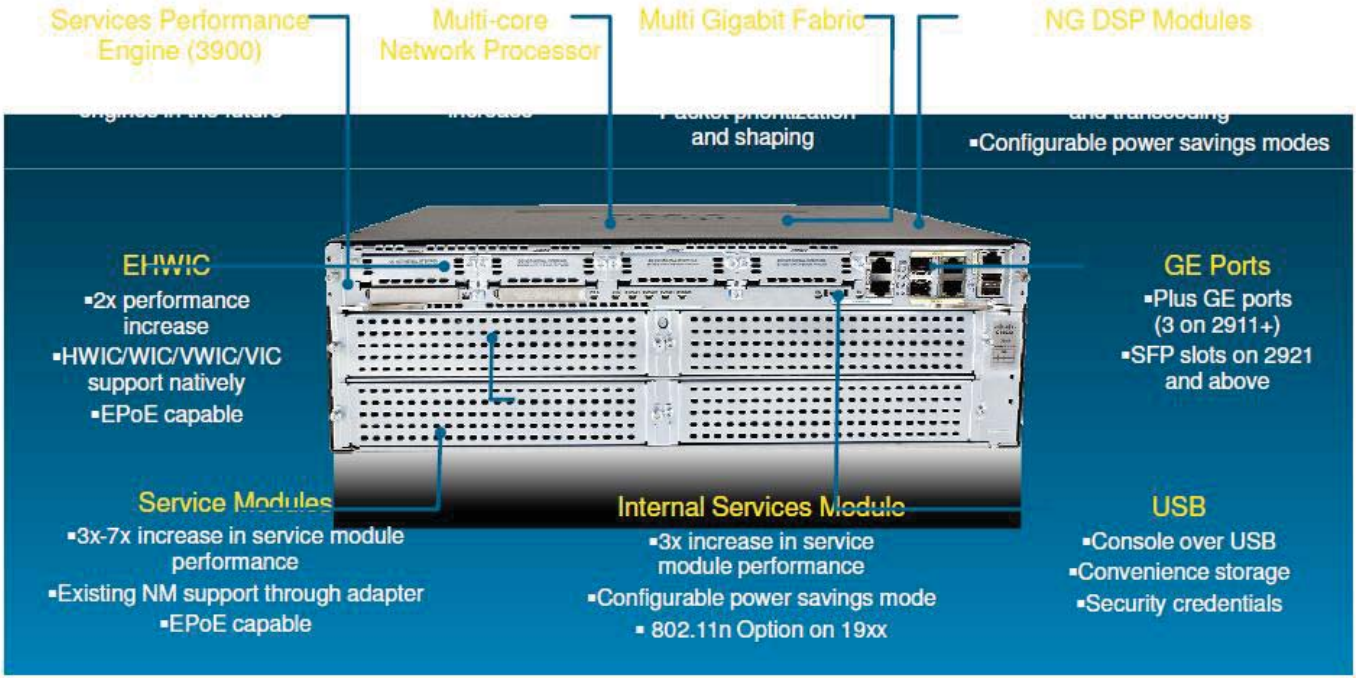
```
 permit ip 10.10.60.0 0.0.0.63 10.10.65.0 0.0.0.31
 permit ip 10.10.60.0 0.0.0.63 10.10.66.0 0.0.0.31
 permit ip 10.10.60.0 0.0.0.63 10.10.67.0 0.0.0.31
 permit ip 10.10.60.0 0.0.0.63 10.10.68.0 0.0.0.63
ip access-list extended qos2
 permit ip 10.10.50.0 0.0.0.15 any
 permit ip any 10.10.51.0 0.0.0.15
 permit ip any 10.10.52.0 0.0.0.15
 permit ip any 10.10.53.0 0.0.0.15
 permit ip any 10.10.54.0 0.0.0.15
 permit ip any 10.10.55.0 0.0.0.15
 permit ip any 10.10.56.0 0.0.0.15
 permit ip any 10.10.57.0 0.0.0.15
 permit ip any 10.10.58.0 0.0.0.15
!
banner motd ^CCC

&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&
&&&&&
&                                       &
&                                       &
&       Tesis: ANALISIS Y MEJORA DE LA RED          &
&       DE DATOS DE LA UNSAAC SOBRE LA PLATAFORMA    &
&       IP/MPLS EN UN BANCO DE PRUEBAS              &
&                                       &
&       Tesistas:                          &
&       EDISON YUVER MORENO CARDENAS               &
&       JOEL LENIN QUISPE VILCA                 &
&       > FACULTAD DE INGENIERIA ELECTRONICA        &
&                                       &
&       ADVERTENCIA: Se prohibe copiar la tesis     &
&       de investigacion. Derechos Reservados.     &
&                                       &
&                                       &
&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&
&&&&&


^C
!

line con 0
 exec-timeout 0 0
```

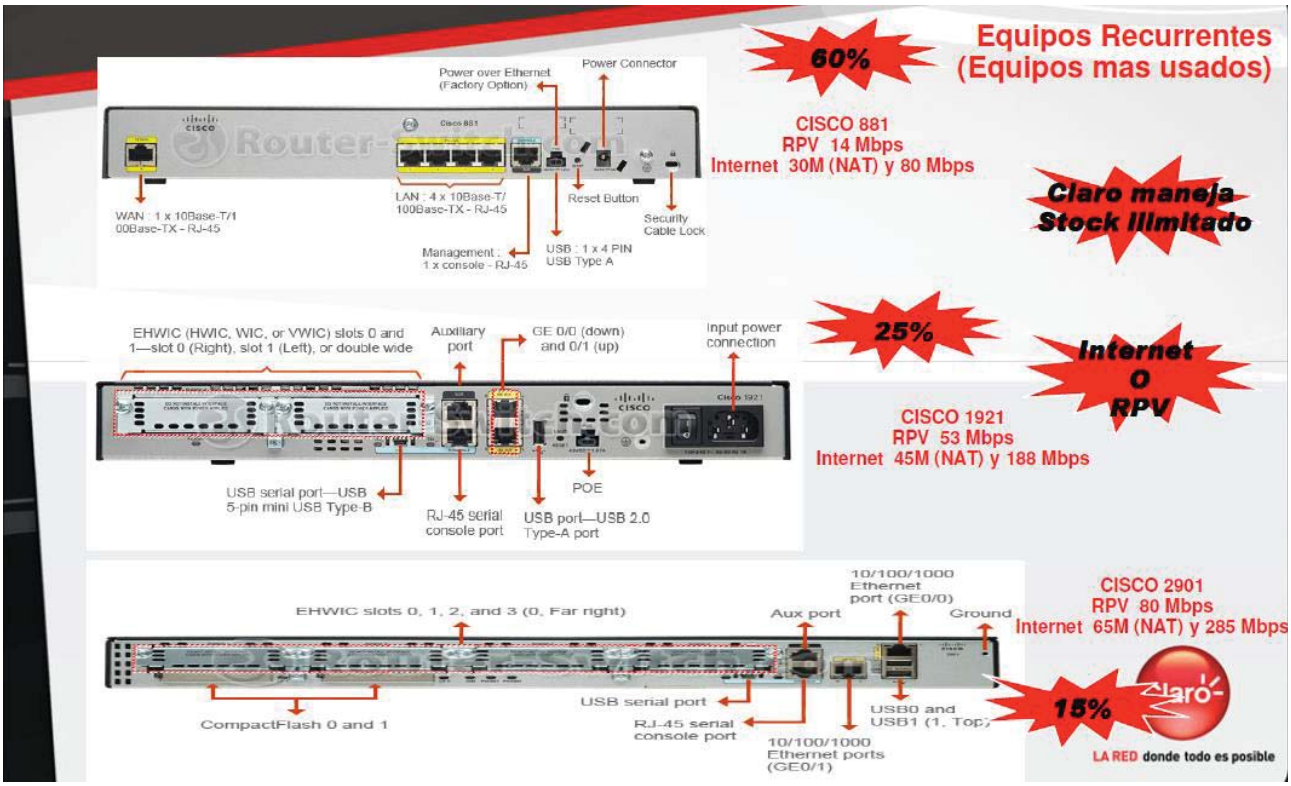
```
 password cisco
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 password cisco
 login
!
end
```

ANEXO H.
CARACTERÍSTICAS TÉCNICAS DE LOS EQUIPOS PROPUESTOS EN EL DISEÑO DE LA RED DE DATOS IP-MPLS.

Next Generation Integrated Services Routers

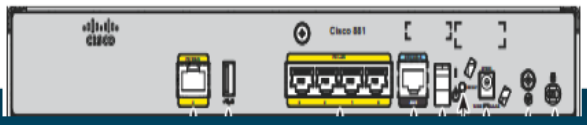
Under the Covers




Equipos Recurrentes
(Equipos mas usados)
60%
Power over Ethernet
(Factory Option)
Power Connector
WAN : 1 x 10Base-T/1
00Base-TX - RJ-45
LAN : 4 x 10Base-T/
100Base-TX - RJ-45
Reset Button
Security
Cable Lock
Management :
1 x console - RJ-45
USB : 1 x 4 PIN
USB Type A
CISCO 881
RPV 14 Mbps
Internet 30M (NAT) y 80 Mbps
Claro maneja
Stock Ilimitado
25%
EHWIC (HWIC, WIC, or VWIC) slots 0 and
1—slot 0 (Right), slot 1 (Left), or double wide
Auxiliary
port
GE 0/0 (down)
and 0/1 (up)
Input power
connection
USB serial port—USB
5-pin mini USB Type-B
RJ-45 serial
console port
USB port—USB 2.0
Type-A port
POE
Internet
O
RPV
CISCO 1921
RPV 53 Mbps
Internet 45M (NAT) y 188 Mbps
EHWIC slots 0, 1, 2, and 3 (0, Far right)
10/100/1000
Ethernet
port (GE0/0)
Aux port
Ground
CompactFlash 0 and 1
USB serial port
RJ-45 serial
console port
USB0 and
USB1 (1, Top)
10/100/1000
Ethernet ports
(GE0/1)
CISCO 2901
RPV 80 Mbps
Internet 65M (NAT) y 285 Mbps
15%
claro
LA RED donde todo es posible

Cisco 880 Series

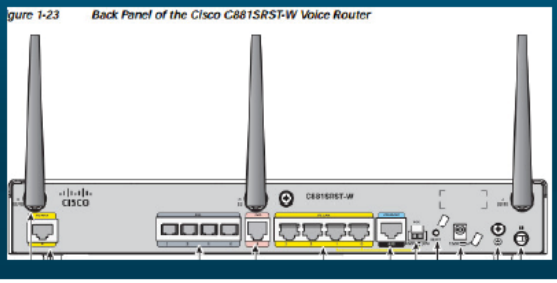
Integrated Services Routers



Models	WAN Interface	LAN Interfaces	802.11g/n Option	Embedded 3G	Integrated ISDN Dial Backup
C881	10/100-Mbps Fast Ethernet	4-port 10/100-Mbps managed switch	No	No	No
Cisco 881	10-/100-Mbps Fast Ethernet	4-port 10-/100-Mbps managed switch	Yes (Cisco 881W)	Yes (Cisco 881G)	No
C886VA	Multimode VDSL2/ADSL2/2+ over ISDN	4-port 10-/100-Mbps managed switch	No	No	Yes

Models	WAN Interface	LAN Interfaces	Voice Ports	802.11g/n Option
Cisco881V	10-/100-Mbps Fast Ethernet	4-port 10-/100-Mbps managed switch	4 foreign-exchange-station (FXS) ports, 2 Basic Rate Interface/BRI) ports, and 1 foreign-exchange-office (FXO) port for public-switched-telephone-network (PSTN) fallback	No
Cisco887VA-V	Multimode VDSL2/ADSL2/2+ over POTS	4-port 10-/100-Mbps managed switch	4 foreign-exchange-station (FXS) ports and 2 Basic Rate Interface/BRI) ports	Yes (Cisco887VA-V-W-K9)
Cisco 881 SRST	10-/100-Mbps Fast Ethernet	4-port 10-/100-Mbps managed switch	4 foreign-exchange-station (FXS) ports and 1 FXO port for public-switched-telephone-network (PSTN) fallback	Yes (Cisco 881 SRSTW)
Cisco 888 SRST	G.SHDSL	4-port 10-/100-Mbps managed switch	4 FXS ports and 1 Basic Rate Interface (BRI) port for PSTN fallback	Yes (Cisco 888 SRSTW)

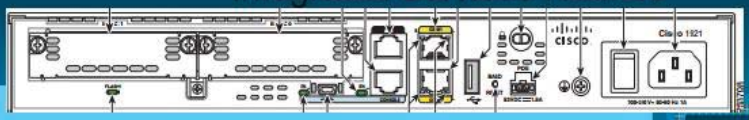
- 15 Mbps WAN Access with Services
  - 256 MB FLASH
  - 1 GB RAM
  - Ports: 4 LAN and 1 WAN



gure 1-23 Back Panel of the Cisco C881SRST-W Voice Router

Cisco 1900 Series

Integrated Services Routers



	1921	1941
SM Slots	0	0
ISM Slots	0	1
EHWIC Slots	2	2
Onboard WAN Ports	2 GE	2 GE
Onboard DSP Slots	0	0
Default Flash	256 MB	256 MB (8GB)
Default DRAM	512 MB	512 MB (2GB)
Form Factor	1RU	2RU

Secure Mobility Platform

- 25Mbps WAN Access with Services
- Factory selectable Integrated wireless 802.11n option
- Desktop form factor with Double Wide HWIC Support

Cisco 2900 Series

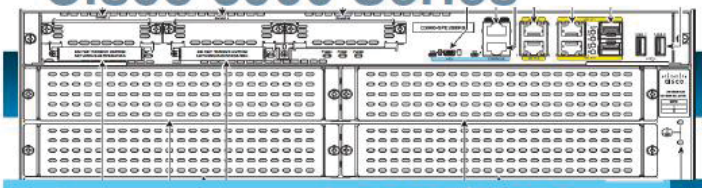
Integrated Services Routers

	2951	2921	2911	2901
SM Slots	2	1	1	0
ISM Slots	1	1	1	1
EHWIC Slots	4	4	4	4
Onboard DSP Slots	3	3	2	2
Onboard WAN Ports	3 GE (1 SFP)	3 GE (1 SFP)	3 GE	2 GE
Default Flash	256 MB	256 MB	256 MB	256 MB
Default DRAM	512 MB	512 MB	512 MB	512 MB
Form Factor	2RU	2RU	2RU	1RU

Secure Collaboration Platform

- Up to 75Mbps WAN Access with Services
- Video-ready DSP support
- Increased service density with Second Services module Slot
- 12 Inch Depth on 2911

Cisco 3900 Series

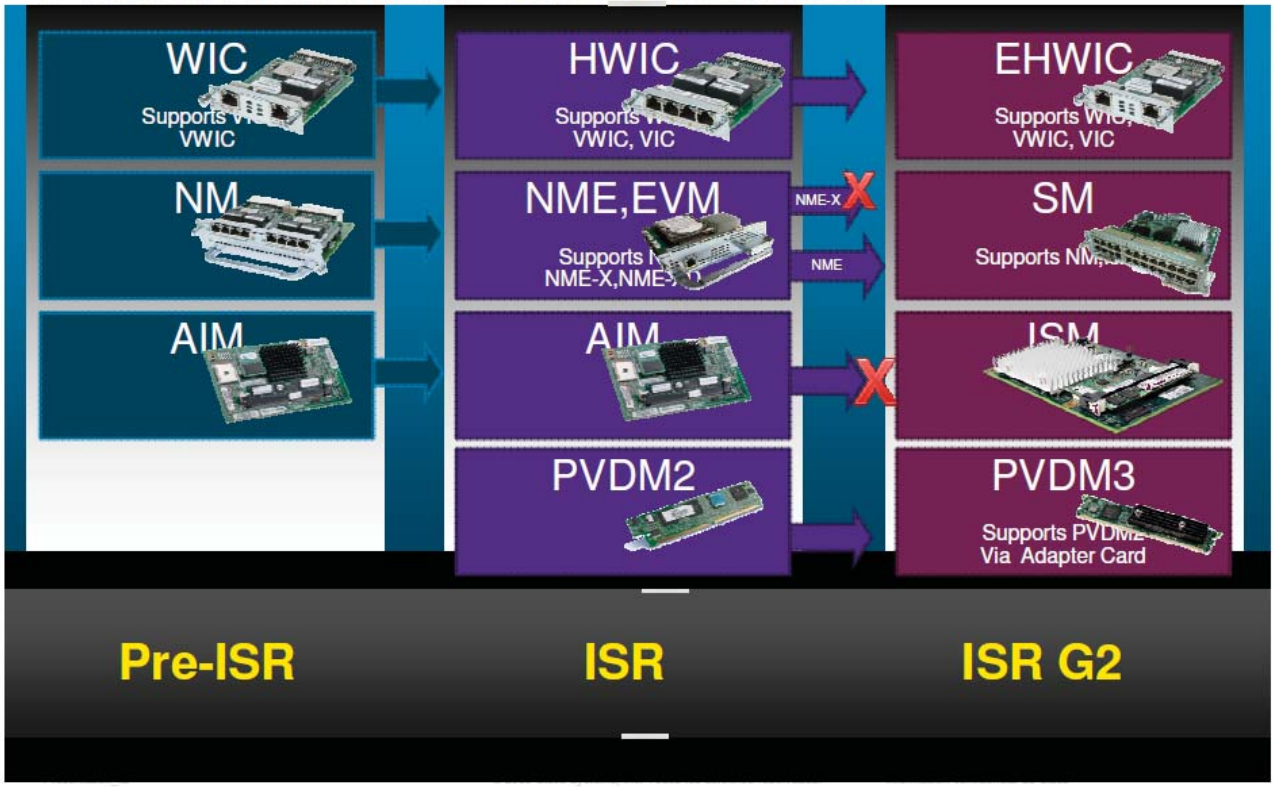


	3945	3925
SM Slots	4	2
ISM Slots	1	1
EHWIC Slots	4	4
Onboard DSP Slots	4	4
Field Upgradeable Motherboards	SPE-150	SPE-100
Integrated Redundant PS	Yes	Yes
Onboard WAN	3GE (2 SFP)	3GE (2 SFP)
Default Flash	256MB	256MB
Default DRAM	1 GB	1 GB
Form Factor	3RU	3RU

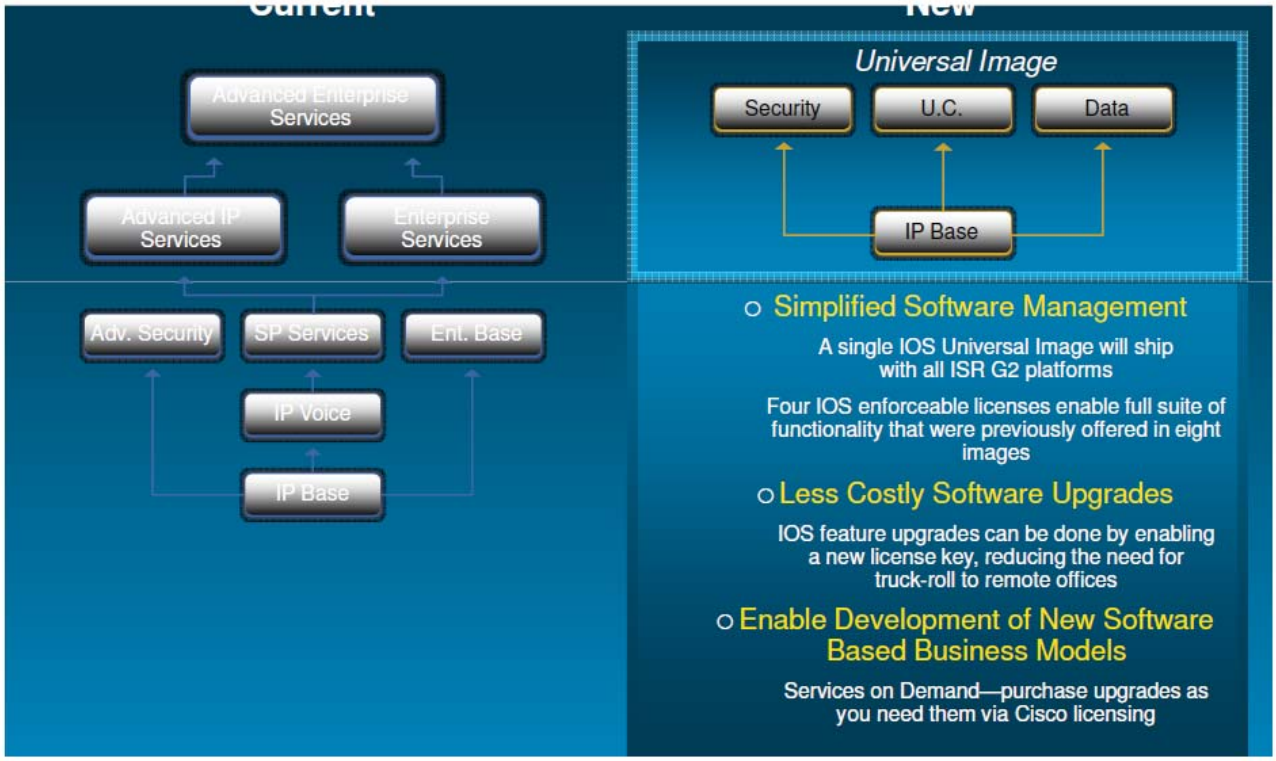
Scalable Rich-media Services Platform

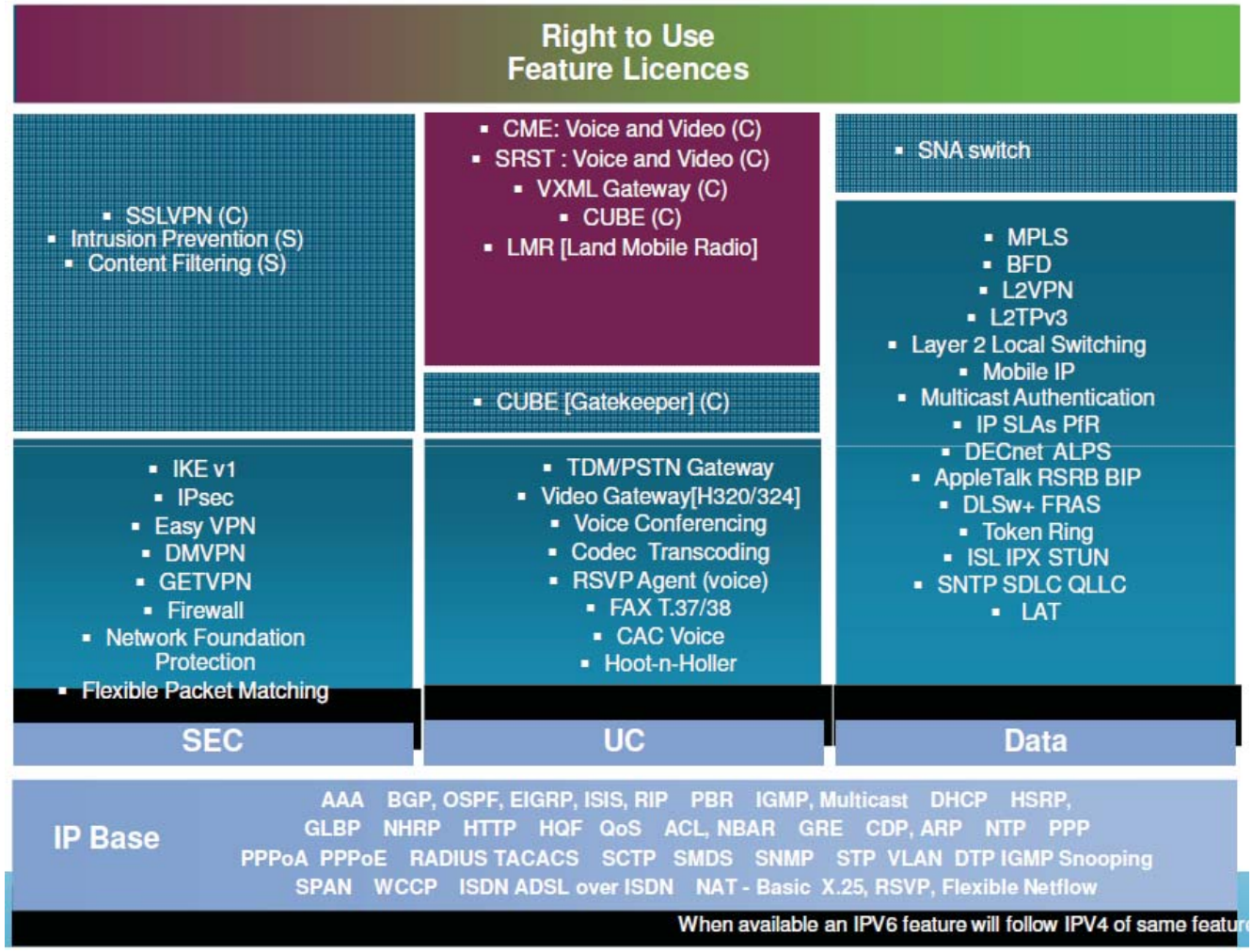
- Up To 150Mbps WAN Access With Services
- Upgradeable services performance engine (SPE) for future expansion
- Configurable dual Integrated Redundant Power supplies
- 2x Default Memory

Platform Module Slot Evolution



IOS Software Packaging Evolution Summary




Right to Use
Feature Licences
SSLVPN (C)
Intrusion Prevention (S)
Content Filtering (S)
CME: Voice and Video (C)
SRST : Voice and Video (C)
VXML Gateway (C)
CUBE (C)
LMR [Land Mobile Radio]
SNA switch
MPLS
BFD
L2VPN
L2TPv3
Layer 2 Local Switching
Mobile IP
Multicast Authentication
IP SLAs PfR
DECnet ALPS
AppleTalk RSRB BIP
DLSw+ FRAS
Token Ring
ISL IPX STUN
SNTP SDLC QLLC
LAT
CUBE [Gatekeeper] (C)
IKE v1
IPsec
Easy VPN
DMVPN
GETVPN
Firewall
Network Foundation Protection
Flexible Packet Matching
TDM/PSTN Gateway
Video Gateway[H320/324]
Voice Conferencing
Codec Transcoding
RSVP Agent (voice)
FAX T.37/38
CAC Voice
Hoot-n-Holler
SEC
UC
Data
IP Base
AAA BGP, OSPF, EIGRP, ISIS, RIP PBR IGMP, Multicast DHCP HSRP,
GLBP NHRP HTTP HQF QoS ACL, NBAR GRE CDP, ARP NTP PPP
PPPoA PPPoE RADIUS TACACS SCTP SMDS SNMP STP VLAN DTP IGMP Snooping
SPAN WCCP ISDN ADSL over ISDN NAT - Basic X.25, RSVP, Flexible Netflow
When available an IPV6 feature will follow IPV4 of same featur

ANEXO I.
NORBERTO JULIAN CURA, DISEÑO EN IMPLEMENTACIÓN DE UNA RED PARA LA TRANSMISIÓN DE DATOS, DIMENSIONAMIENTO.