

UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA



**PROYECTO DE TELEEDUCACIÓN PARA ESCUELAS DE
PACASMAYO EMPLEANDO TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIÓN**

**INFORME DE SUFICIENCIA
PARA OPTAR EL TÍTULO PROFESIONAL DE:
INGENIERO ELECTRÓNICO**

**PRESENTADO POR:
PATRICK MARCEL OSORIO ESPINOZA**

**PROMOCIÓN
2008-II**

**LIMA-PERÚ
2013**

**PROYECTO DE TELEEDUCACIÓN PARA ESCUELAS DE
PACASMAYO EMPLEANDO TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIÓN**

A mis padres,
A mi familia,
A mi alma mater

SUMARIO

En el presente trabajo se explica el planteamiento para la ejecución de un proyecto de teleeducación para escuelas de Pacasmayo empleando tecnologías de la información y comunicación (TIC).

La necesidad de su ejecución parte de la iniciativa de la empresa privada de ejecutar un proyecto social. La empresa es Cementos Pacasmayo, la cual desea afianzar los lazos empresa-comunidad, mejorando así las condiciones en el ámbito educativo en pro del desarrollo de la sociedad.

El informe se enfoca en la solución de comunicaciones, teniendo en cuenta el equipamiento TIC a fin de dimensionarlo al igual que los demás servicios asociados a la solución educativa.

El informe de suficiencia abarca el diseño de la plataforma tecnológica, la cual considera los siguientes alcances:

- Conectividad.- Es decir lo correspondiente a los servicios de red privada virtual aplicando políticas de calidad de servicio y accesos a la nube de internet.
- Infraestructura.- La topología de redes y comunicaciones (routers, switches, servidores, etc), así como equipamiento básico relacionado a la educación: netbooks, equipo de videoconferencia y software educativo asociado.
- Software.- Es el soporte lógico de las técnicas educativas: Classroom manager, Metasys School server y software de protección de equipos en casos de robo.

ÍNDICE

INTRODUCCIÓN	1
CAPÍTULO I	
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA	3
1.1 Descripción del problema	3
1.2 Objetivos del trabajo.....	3
1.3 Evaluación del problema	3
1.3.1 Introducción.....	3
1.3.2 Soluciones para el desarrollo social.....	3
1.3.3 TIC para la educación.....	4
1.4 Alcance del trabajo	9
CAPÍTULO II	
MARCO TEÓRICO CONCEPTUAL	10
2.1 Red Privada Virtual - VPN	10
2.1.1 Aspectos generales	10
2.1.2 Razones para implementar VPNs.....	11
2.1.3 Modelo Arquitectura VPNs	11
2.2 Servicios Red Privada Virtual IP-VPN.....	13
2.2.1 Modos de acceso	13
2.2.2 Infraestructura de Red IP-MPLS	14
2.2.3 Aplicaciones	15
2.2.4 Beneficios.....	16
2.3 Multiprotocol Label Switching - MPLS.....	16
2.3.1 Principales ventajas MPLS	17
2.3.2 Términos más utilizados en MPLS.....	17
2.3.3 Modo de operación.....	18
2.3.4 Red Privada Virtual - MPLS.....	19
2.4 Calidad de Servicio.....	20
2.4.1 Descripción general.....	20
2.4.2 Calidad de Servicio en Arquitectura MPLS	21
2.4.3 Parámetros calidad de servicio.....	24
2.4.4 Arquitectura de Servicios Diferenciados (DIFFSERV).....	24
2.4.5 Definición del Campo de Servicios Diferenciados.....	25
CAPÍTULO III	
METODOLOGÍA DE LA SOLUCIÓN	27

3.1	Evaluación de alternativas de Comunicaciones	27
3.1.1	Tecnologías disponibles	27
3.1.2	Elección de tecnología.....	29
3.2	Elección de medio de acceso, enlaces, parámetros de calidad y equipos	30
3.2.1	Elección de medio de acceso para los enlaces	30
3.2.2	Dimensionamiento de los enlaces	32
3.2.3	Determinación de los Parámetros de Calidad de Servicio para la solución.....	34
3.2.4	Dimensionamiento de equipamiento.....	34
3.3	Topología de la solución.....	37
3.3.1	Servicio de comunicaciones en los Centros Educativos	38
3.3.2	Descripción de equipos de comunicaciones	41
3.4	Configuración de Calidad de servicio para la solución	45
3.4.1	Asignación de las clases de servicio.....	45
3.4.2	Funcionamiento del exceso de tráfico en cada clase para la solución	47
3.4.3	Configuración de las Clases de Servicio en los Centros Educativos.....	48
3.5	Disponibilidad del servicio para la solución.....	49
3.6	Requerimientos técnicos para implementación.....	50
3.6.1	Condiciones eléctricas.....	50
3.6.2	Condiciones ambientales.....	52
3.6.3	Condiciones para la provisión de un ingeniero residente	52
3.7	Aspectos complementarios de los servicios.....	53
3.7.1	Sistema operativo del ambiente de enseñanza	53
3.7.2	Aplicaciones para la enseñanza	53
3.7.3	Plataforma en línea	55
CAPÍTULO IV		
COSTOS Y CRONOGRAMA.....		56
4.1	Análisis de costos.....	56
4.2	Cronograma de trabajos	57
CONCLUSIONES Y RECOMENDACIONES		59
ANEXO A		
GLOSARIO DE TÉRMINOS		60
BIBLIOGRAFÍA.....		62

INTRODUCCIÓN

El trabajo surge por la necesidad de la Empresa Cementos Pacasmayo para afianzar los lazos empresa-comunidad, mejorando las condiciones de vida en pro del desarrollo de la zona de influencia en donde se ejecuta sus trabajos de producción.

Para ello la empresa decide brindar a tres escuelas de Pacasmayo una solución de teleeducación empleando tecnologías de la información y comunicación (TIC).

Para la plataforma de comunicaciones se eligió una red IP-VPN propiedad de Telefónica del Perú. Este es un servicio de interconexión de redes locales distribuidas soportado sobre la infraestructura MPLS, que permite la óptima integración de puntos geográficamente distantes y aplicaciones en diversos ámbitos de las necesidades humanas como la educación y salud.

A fin de diseñar la red de comunicaciones del proyecto, se tiene en cuenta algunos parámetros fundamentales para cada sitio, tales como la tasa de transferencia de datos máxima, los dispositivos a comunicar por la red WAN, el tipo de acceso a emplear, etc.

El tráfico es prioritariamente de la aplicación educacional HP Metasys Education Solution dicho software permite el control de todos los equipos conectados en la red para el manejo de todos los aplicativos educativos, también se considera una salida a internet de toda la red a través del Datacenter de Telefónica del Perú. Adicionalmente también se considera equipos de videoconferencia para educación a distancia.

El presente informe de suficiencia está organizado en cuatro capítulos:

- Capítulo I "Planteamiento de ingeniería del problema".- En este capítulo introductorio se realiza la descripción de las necesidades educativas del caso de estudio (los tres colegios). Así mismo se establecen los objetivos y alcances del proyecto (plataforma tecnológica). Se amplían conceptos sobre el desarrollo social y TIC para la educación.

La topología desarrollada es un modelo que tiene un centro de gestión centralizado ya que se aprovecha las ventajas de una correcta consolidación de la información en los servidores, lo que permite tener sustanciales ahorros, mejorar la gestión y contar con un único sistema de información.

- Capítulo II "Marco Teórico Conceptual".- En este capítulo se exponen las bases teóricas conceptuales más importantes para la comprensión del sistema descrito en el presente informe. Se desarrollan los siguientes ítems: Red Virtual Privada (VPN), Servicios IP-VPN, MPLS, Calidad de servicio.

- Capítulo III "Metodología de la solución".- El presente capítulo está organizado en los siguientes ítems: Evaluación de plataforma tecnológica de comunicaciones (elección de la plataforma, medio de acceso y determinación de los parámetros de calidad), dimensionamiento de los enlaces, topología de la solución (incluye servicios de comunicaciones y equipamiento), calidad de servicio (Descripción Clases de Servicio, Tratamiento del exceso de tráfico en cada clase), disponibilidad del servicio, requerimientos técnicos para implementación (Condiciones eléctricas, Tablero de distribución, Transformador de aislamiento, Pozo de tierra, Estabilizador/UPS, Voltajes de salida, Condiciones ambientales, Ventilación, Humedad, Condiciones para la provisión de un ingeniero residente), aspectos complementarios de los servicios (Sistema operativo del ambiente de enseñanza, Aplicaciones para la enseñanza, Plataforma en línea).
- Capítulo IV "Costos y cronograma".- En el presente capítulo se tocan los temas involucrados al presupuesto y al cronograma del proyecto de ingeniería.

CAPÍTULO I PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

En este capítulo introductorio se realiza la descripción de las necesidades educativas del caso de estudio (los tres colegios). Así mismo se establecen los objetivos y alcances del proyecto (plataforma tecnológica).

1.1 Descripción del problema

Necesidad de ejecutar un proyecto social por parte de la empresa Cementos Pacasmayo, para afianzar los lazos empresa-comunidad, mejorando las condiciones de vida en pro del desarrollo de la comunidad donde opera.

1.2 Objetivos del trabajo

Plantear un proyecto de teleeducación para escuelas de Pacasmayo empleando tecnologías de la información y comunicación.

1.3 Evaluación del problema

La presente información se basa en la documentación presentada para el Proyecto de Educación para Escuelas de Pacasmayo [1]. Esta sección está organizada en tres ítems.

1.3.1 Introducción

El Perú se encuentra en un franco proceso de crecimiento nunca antes visto. Los ciudadanos de sus regiones y provincias desean aprovechar las oportunidades del crecimiento del país. Todo esto hace que se deba afrontar el gran reto de mejorar los servicios a los ciudadanos de las distintas localidades.

1.3.2 Soluciones para el desarrollo social

Se desarrollan a continuación dos aspectos fundamentales relacionados a la problemática:

a. Retos del desarrollo social

Estos son resumidos en la Tabla 1.1

Tabla 1.1 Retos del desarrollo social (Fuente: referencia [1])

Retos	Acciones
Mejorar la Seguridad Ciudadana	Aumentando la productividad de las fuerzas de seguridad disponibles.
Mejorar la Educación	Aumentando la productividad de los profesores, la motivación de los alumnos conectándolos al mundo.

Mejorar los servicios de Salud	Aumentando la productividad y calidad de los servicios de salud, racionalizando el uso de los recursos disponibles.
Impulsar el desarrollo	Mejorando los servicios básicos para potenciar las capacidades de nuestros ciudadanos para aprovechar las oportunidades del desarrollo.

b. Mejora de los servicios ciudadanos

Mediante el uso de la Tecnología de Información y de Comunicaciones se busca mejorar los servicios básicos de la población. La tabla 1.2 resume los antecedentes y lo que se quiere lograr.

Tabla 1.2 Antecedentes (Fuente: referencia [1])

Antes	Después
Falta de Seguridad, real o percibida	Dar más seguridad a nuestra población
Educación desconectada del mundo y de los avances tecnológicos	Mejorar la educación de nuestros estudiantes
Servicios de Salud insuficientes o Ineficientes	Mejorar los servicios de salud de nuestros hospitales

1.3.3 TIC para la educación

Los principales problemas a resolver son [1]:

- Ausentismo de los alumnos a clase debido al aburrimiento y falta desinterés en la escuela
- Bajo rendimiento en los cursos debido al pobre desarrollo del aprendizaje significativo.
- Falta de atención y motivación debido a los pocos materiales didácticos que permitan combinar un experiencia vivencial con multimedia
- Fuente de información limitada desfasada debido a no contar con medios de acceso a otras fuentes de conocimiento como bibliotecas virtuales internacionales.
- Poca o limitada aplicación de las mejores prácticas educativas debido a la falta de herramientas para la gestión y seguimiento.

Para ello se propone la aplicación de las TICs. Básicamente se plantea dotar las aulas de computadoras personales, ya sea cableada o inalámbricamente. Estas opciones deben disponer un servidor por cada local (escuela) y conectadas mediante una IP VPN (red privada virtual). Los servidores estarán conectados a su propia LAN y en caso de que uno de los servidores “caiga”, el servidor de otro local asumirá el tráfico y servicio de las computadoras “clientes” del servidor caído.

El Data Center de telefónica cumple la función de habilitar un portal educativo. El Data Center debe contener:

- Repositorio de software de educación.
- El controlador de los ordenadores de la solución (todas las PCs)

- Un servidor de autenticación y registro.
- Un servidor encargado de monitorear la operatividad de los servidores de cada escuela

La Figura 1.1 resume lo antes mostrado.

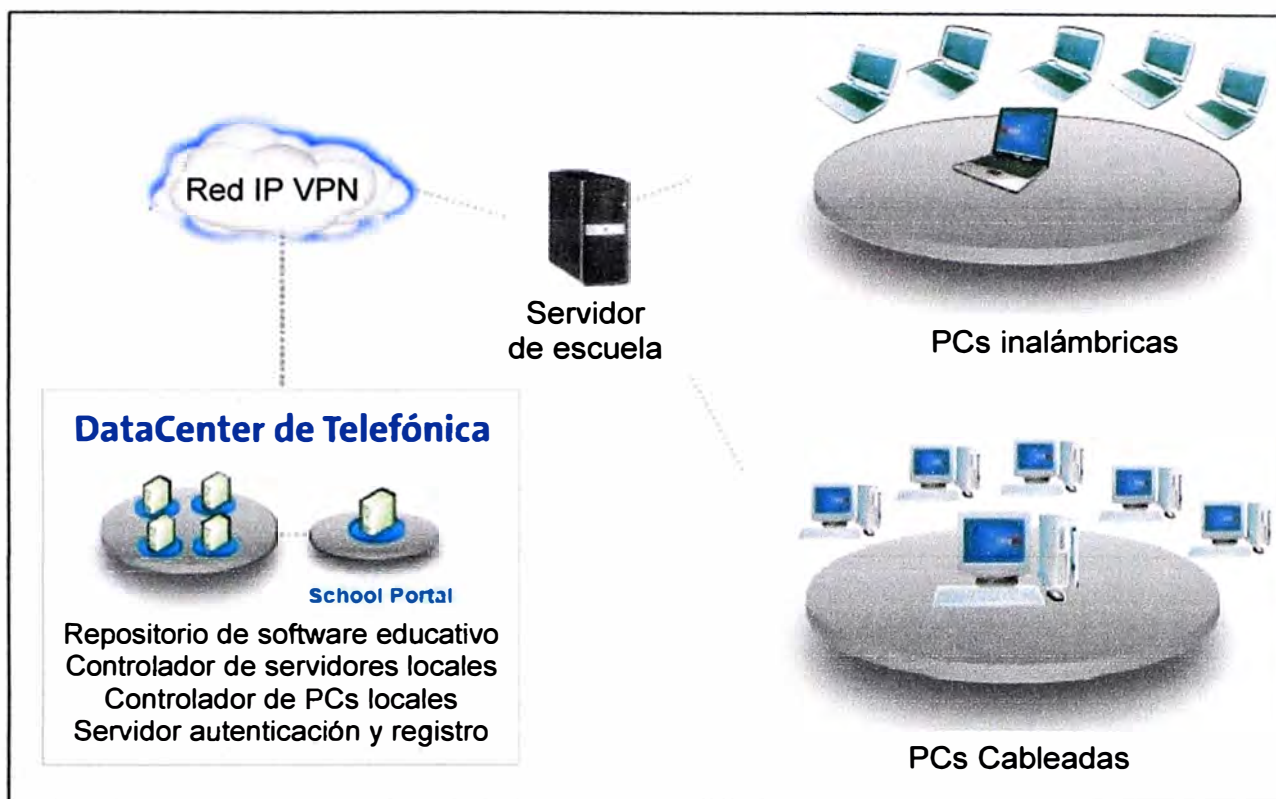


Figura 1.1 Resumen de solución (Fuente: referencia [1])

Un mayor detalle de la topología de comunicaciones elegida para la presente solución se desarrolla en el capítulo III.

Respecto a los equipos de cómputo para el usuario final se tiene lo siguiente:

- PCs para alumno.- Se considera la opción de brindar equipos HP Mini 1000 (Figura 1.2) para cada alumno. Asimismo se podría contar con las siguientes funcionalidades en caso se soliciten las mismas: software antirrobo y software de monitoreo.



Figura 1.2 HP Mini 1000 (Fuente: Fabricante)

- PCs para profesores.- La solución considera PC desktops para los profesores, habilitados con el software HP Classroom Manager, el cual le permitirá al profesor monitorear, controlar y desplegar los contenidos que desee en las PCs de los alumnos

Respecto al HP Classroom Manager, esta es una herramienta para monitorear, controlar e interactuar con los estudiantes dentro de un aula digital (Figura 1.3). Sus principales características son:

- Controlar las PCs del aula desde una única estación.
- Ver pantalla de los estudiantes; compartir escritorios.
- Encuestas y exámenes en tiempo real & monitoreo de resultados.
- Transferencia de archivos; crear diario de clase.
- Controlar impresoras y dispositivos.
- Internet controlado.

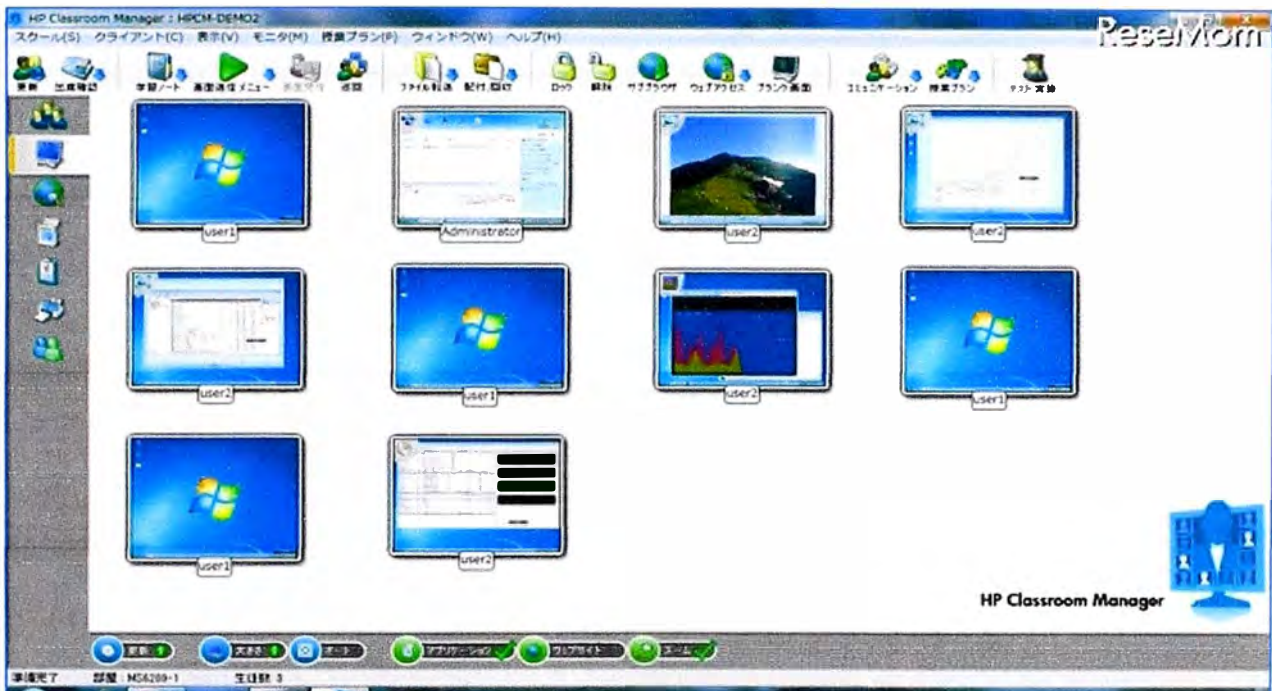


Figura 1.3 Ejemplo de Pantalla de docente (Fuente: referencia [1])

Es necesario, precisar algunos aspectos sobre los servidores:

Servidor de Contenidos en las escuelas.- Se considera la instalación de un servidor de contenidos en cada escuela donde se implemente la solución. Este servidor le permitirá a los alumnos acceder a los contenidos del software educativo de Schola y del servicio Educared, lo cual le permitirá a los alumnos incrementar la cantidad y mejorar calidad de la información a ser consultada.

Servidor Centralizado.- La solución incluye el alojamiento de un servidor en el Data Center de Telefónica del Perú, el cual servirá para la consolidación de la información recolectada de los servidores de contenidos de cada escuela y para el acceso de contenidos en caso se presente alguna falla en los servidores locales en cada escuela.

Consecuentemente, para un óptimo uso de las herramientas, se considera necesario capacitar a los profesores en el uso del software de Schola y en la manera de utilizar esta herramienta como un complemento de su metodología de enseñanza.

También se considera realizar evaluaciones periódicas a los alumnos a fin de medir el avance de sus conocimientos en las áreas de razonamiento verbal y matemático.

Se instalarán los equipos de comunicaciones necesarios para el correcto funcionamiento de la solución, permitiendo el acceso a Internet de los alumnos. La presente solución está considerando un despliegue LAN alámbrico.

Los alcances de la metodología educativa son:

- Niveles de Inicial y Primaria.
- Utilización de la plataforma educativa y de monitoreo.
- Lógico Matemática y Comprensión Lectora.
- Evaluación a estudiantes de 2do grado de Primaria.
- Capacitación al 100% de docentes de ambos niveles.
- Un facilitador local permanente para monitoreo durante todo el año escolar.

Las etapas a nivel de solución educativa se presentan en la Figura 1.4



Figura 1.4 Etapas de la solución educativa (Fuente: referencia [1]).

Las etapas de la capacitación-evaluación se presentan en la Figura 1.5.



Figura 1.5 Etapas de la capacitación-evaluación (Fuente: referencia [1]).

El sistema de administración considera lo siguiente (Figura 1.6):

- Control de ingreso de usuarios.

- Control de programación curricular.
- Control de usuarios y perfiles.
- Buzón de sugerencias.



Figura 1.6 Entorno de administración (Fuente: referencia [1])

Respecto a las actividades se tiene (Figura 1.7):

- Selección de actividades.
- Selección de idiomas.
- Seguimiento de estadísticas.
- Configuración general.

Código	Actividad	Grado ↑	Saber	Acciones
DV - 3a.I.a-b	Mi familia y sus integrantes. Roles de los miembros de la familia.	3 a 4 años	Familia	<input checked="" type="checkbox"/> <input type="checkbox"/>
DV - 3a.I.c	Mi familia escolar.	3 a 4 años	Familia	<input checked="" type="checkbox"/> <input type="checkbox"/>
DV - 3a.II.c	Intercambio de nuestros productos.	3 a 4 años	Cosecha	<input checked="" type="checkbox"/> <input type="checkbox"/>
DV - 3a.II.a-b	Conocemos los productos que se cosechan en mi comunidad. La cosecha de la papa.	3 a 4 años	Cosecha	<input checked="" type="checkbox"/> <input type="checkbox"/>
DV - 3a.III.c	Cuidemos nuestro cuerpo.	3 a 4 años	Nuestro Cuerpo	<input checked="" type="checkbox"/> <input type="checkbox"/>
DV - 3a.III.a-b	¿Cómo es mi cuerpo? Nuestros sentidos.	3 a 4 años	Nuestro Cuerpo	<input checked="" type="checkbox"/> <input type="checkbox"/>

Figura 1.7 Entorno de actividades (Fuente: referencia [1])

Los beneficios de la solución educativa se muestran en la Figura 1.8



Figura 1.8 Beneficios de la solución educativa (Fuente: referencia [1])

Nota:

Dada la coyuntura socio económica de la zona es que La empresa Pacasmayo decide implementar la solución educativa para tres colegios, cumpliendo así con sus objetivos institucionales relacionados con la comunidad

1.4 Alcance del trabajo

El informe se enfoca en la solución de comunicaciones, teniendo en cuenta el equipamiento TIC a fin de dimensionarlo al igual que los demás servicios que se brinde para la solución educativa.

Se consideran tres aulas en Pacasmayo, para un aproximado de 20 alumnos por colegio, que servirán para todo el alumnado.

El informe de suficiencia abarca el diseño de la plataforma tecnológica. Esta contempla los siguientes alcances:

- Conectividad.- Es decir lo correspondiente a los servicios de Red Privada Virtual (VPN), aplicación de políticas de calidad y salida a internet.
- Infraestructura.- La topología de redes y comunicaciones (routers, switches, servidores), así como equipamiento básico relacionado a la educación: netbooks, equipos de videoconferencia, proyector y ecran.
- Software.- Es el soporte lógico de las técnicas educativas: Classroom manager, Metasys School Server.

CAPÍTULO II MARCO TEÓRICO CONCEPTUAL

En este capítulo se exponen las bases teóricas conceptuales más importantes para la comprensión del sistema descrito en el presente informe.

Se desarrollan los siguientes ítems: Red Virtual Privada (VPN), Servicios de Red Privada Virtual IP-VPN, MPLS y Calidad de servicio.

2.1 Red Privada Virtual - VPN

En esta sección se desarrolla lo relacionado a las Redes Privadas Virtuales (VPN). Se desarrollan los aspectos generales, las ventajas de las VPNs, así como los modelos de arquitectura [2][3].

2.1.1 Aspectos generales

Una VPN es una estructura de red que emula una red privada sobre infraestructura pública existente. Brinda comunicación a nivel de las capas 2 ó 3 del modelo OSI. La VPN pertenece generalmente a una compañía y le permite tener diferentes locales interconectados a través de la infraestructura de un proveedor de servicios. Esto es posible ya que la tecnología permite crear un túnel de encriptación a través de la Internet u otra red pública de tal forma que permita a los usuarios que se encuentran en los extremos del túnel disfrutar de la seguridad, privacidad y funciones que antes estaban disponibles sólo en redes privadas [2][3]. Como se muestra en la Figura 2.1.

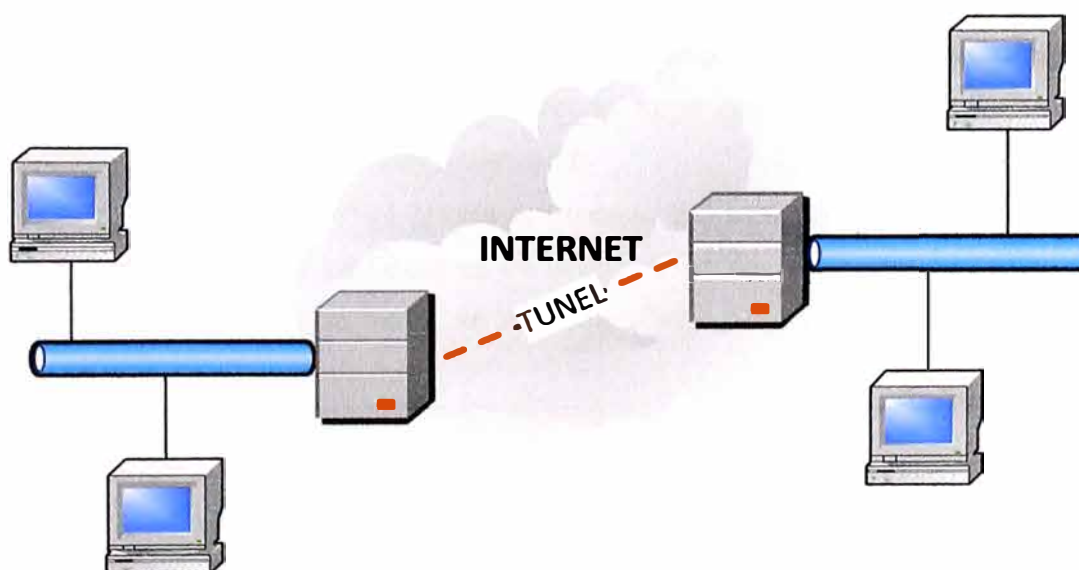


Figura 2.1 VPN a través de Internet (Fuente: Elab. propia)

El equivalente a esta red VPN sería un enlace privado punto a punto (peer to peer), que es sumamente costoso si se trata de extender la red a grandes distancias, debido al requerimiento de cableado y equipos en la localidad a la cual se quiera llegar.

2.1.2 Razones para implementar VPNs

Son las siguientes [3]:

- Reducción de costo.- Para una implementación de red que abarque empresas alejadas geográficamente ya no será indispensable en términos de seguridad realizar enlaces mediante líneas dedicadas (punto a punto). En su lugar, se puede emplear un acceso ADSL es de bajo costo, brinda un ancho de banda alto y está disponible en la mayoría de zonas urbanas. Los usuarios remotos móviles podrán ahorrar costos de llamadas telefónicas de larga distancia, realizándolas a través de un acceso local a Internet.
- Alta seguridad.- Las redes VPN utilizan altos estándares de seguridad para la transmisión de datos, comparables con una red punto a punto. Protocolos como 3DES (Triple data encryption standard) el cual cumple la función de encriptar la información a transferir y el protocolo IPSec (IP Security) para manejo de los túneles mediante software brindan un alto nivel de seguridad al sistema. También se emplean varios niveles de autenticación para el acceso a la red privada mediante llaves de acceso, para validar la identidad del usuario.
- Escalabilidad.- No es necesario realizar inversiones adicionales para agregar usuarios a la red. El servicio se provee con dispositivos y equipos configurables y manejables. La desarrollada infraestructura de los proveedores de Internet hace innecesario realizar un enlace físico que puede significar una gran inversión de dinero y de tiempo.
- Compatibilidad con tecnologías de banda ancha.- Una VPN puede aprovechar infraestructura existente de banda ancha inalámbrica, TV cable o conexiones de alta velocidad del tipo ADSL o ISDN. Con ello brinda un alto grado de flexibilidad al momento de configurar la red. Se pueden emplear tecnologías como Voz sobre IP (VoIP), que permiten ahorrar en telefonía de larga distancia.
- Mayor productividad.- Una VPN brinda un acceso durante mayor tiempo, que significa una mayor productividad de los usuarios de la red. Además, con la consecutiva reducción en las necesidades de espacio físico, se fomenta el teletrabajo así como otras actividades como teleeducación y telemedicina.

2.1.3 Modelo Arquitectura VPNs

Son dos, Overlay VPN y el Peer-to-peer VPN [2].

a. Modelo Overlay VPN

Inicialmente las VPNs se implementaron basadas en tecnologías como Frame Relay o ATM, donde el proveedor brinda conectividad a nivel de Capa 2 a los routers del cliente.

Éste modelo era el llamado Modelo Overlay. El proveedor es el dueño de los routers de borde (Edge Routers) que se conectan a la red del cliente, o los administra. La idea es tener a los routers físicamente en el local del cliente.

Este modelo es sencillo de entender pues separa claramente las responsabilidades del cliente y del proveedor. El proveedor brinda al cliente un grupo de líneas dedicadas virtuales (emuladas), llamadas VCs, que pueden estar constantemente disponibles (PVCs) o ser establecidas bajo demanda (SVCs). El usuario establece una comunicación de router a router entre los equipos de cliente o Customer Premises Equipment (CPE) a través de las VCs. Los datos del protocolo de enrutamiento son intercambiados entre los CPE, y el proveedor no tiene conocimiento alguno de la estructura interna de la red del cliente, como se puede apreciar en la Figura 2.2.

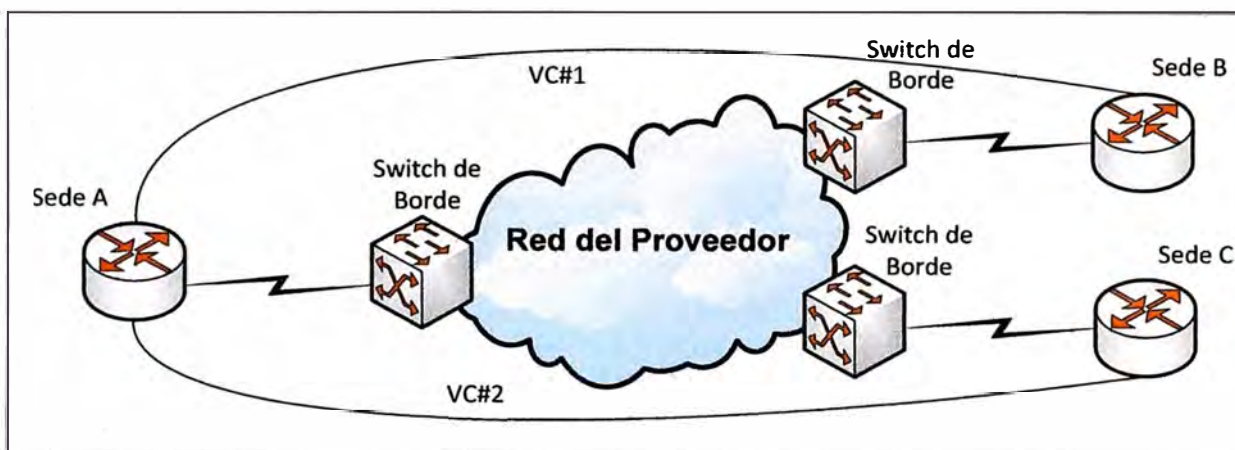


Figura 2.2 Modelo Overlay VPN (Fuente: Elab. propia)

b. Modelo Peer-to-peer VPN

El modelo peer-to-peer también fue utilizado inicialmente, aunque no fue tan popular. La razón principal es que no es tan fácil de desplegar y mantener debido a que necesita listas de distribución, filtros de paquetes IP, o túneles GRE. Este modelo fue introducido para contrarrestar las desventajas del modelo Overlay. En las VPNs peer-to-peer, el equipo de borde del proveedor o Provider Edge (PE) es un router que intercambia las rutas directamente con el router CPE. Como se puede apreciar en la figura 2.3.



Figura 2.3 Modelo Peer-to-peer VPN (Fuente: Elab. propia)

La Tabla 2.1 muestra una comparación entre ambos esquemas.

Tabla 2.1 Comparación entre esquemas de modelos de conexión (Fuente: Ref. [3])

Modelo Overlay (Backbone Frame-Relay/ATM)	Modelo Peer-to-Peer (Backbone IP)
Conmutación veloz de tramas en el backbone (capa 2)	Velocidad de conmutación de paquetes dependiente de plataforma.
Total independencia entre redes de clientes (VPN en capa 2)	Redes de clientes sujetas a compartir una misma tabla de rutas
Puede transportar cualquier protocolo de capa 3.	Cualquier otro protocolo a transportar debe pasar encapsulado en paquetes IP
Esquema de QoS limitado, versatilidad adicional depende del protocolo de capa 3 utilizado	Esquema de QoS para aplicaciones basado en marcación de paquetes o reserva de ancho de banda
Cada cliente nuevo implica la creación de circuitos nuevos (PVCs) en el backbone (Más configuración en más equipos)	Cada cliente nuevo sólo implica la creación del circuito de acceso y del enrutamiento
Utilización no óptima de troncales FR/ATM	Troncales IP con dimensionamiento óptimo
Utilización no óptima de acceso central en esquemas hub & spoke	Utilización óptima del ancho de banda en accesos (full-mesh virtual)
Acceso de cliente a servicios en el proveedor implica nuevos circuitos en capa 2	Fácil acceso a servicios en el proveedor (data center) a través de troncales IP existentes
Elección de la mejor ruta hecha en capa 3	Elección de la mejor ruta según protocolo de enrutamiento basado sólo en métricas fijas
Se complica el intercambio de rutas debido a los múltiples vecinos del CPE	Enrutamiento simple para el cliente, ya que el CPE intercambia rutas con uno o pocos PE
Enrutamiento engorroso entre los locales del cliente	Enrutamiento óptimo entre las sedes del cliente, pues los PE conocen su topología de red
Para asignar ancho de banda, el cliente debe especificar el perfil de tráfico exacto de local a local	El cliente debe especificar el ancho de banda inbound y outbound sólo para cada local

2.2 Servicios Red Privada Virtual IP-VPN

El servicio IP VPN es un servicio de conexión de redes que utiliza como medio de transporte la red IP MPLS de Telefónica del Perú la cual permite ofrecer calidad de servicio en la transmisión de datos, voz y video. Adicionalmente se puede extender la red a nivel internacional sin alterar la infraestructura local [6].

2.2.1 Modos de acceso

A nivel local existen diferentes modos de acceso a la casa del cliente. El servicio IP VPN con Acceso Ethernet como acceso en la última milla, permite la conexión de redes de área local remotas (LANs) con prestaciones similares a las que se obtendrían dentro de un mismo edificio, con elevada escalabilidad de ancho de banda, desde 2 Mbps hasta 400Mbps, además de las características mostradas en la tabla 2.2:

Tabla 2.2 Características de servicios IP-VPN (Fuente: Ref [6])

Acceso Ethernet TDM	Simétrico	Medio de acceso	Dedicado	Fibra óptica, Cobre, Radio
		Interfaces y protocolos de acceso	Dedicado	E1, Protocolo Ethernet, Interfaces 10/100 y 1000
	Clases de servicio (QoS)		Datos (Plata)	Orientado a tráfico transaccional y storage IP
			Multimedia (Oro)	Orientado a tráfico en tiempo real (VoIP, video IP)
	Simétrico	Simétricos Dedicados	Velocidades (Acceso y Caudal)	2 Mbps, 4 Mbps, 10 Mbps, 20 Mbps, 30 Mbps, 40 Mbps, 50 Mbps, 60 Mbps, 70 Mbps, 80 Mbps, 90 Mbps, 100 Mbps, 200 Mbps y 400 Mbps.
Informes		Configuración, estadísticas de utilización		
Equipos CE	Routers o Switch		Alquiler, venta o propietario	
Equipos terminales de red	Media-converter o Multiplexor			

2.2.2 Infraestructura de Red IP-MPLS

La infraestructura de red sobre la que se soporta el servicio presenta las siguientes características:

- Utilización de nodos de red de tecnología NORTEL, JUNIPER y CISCO, suministradores líderes en el mercado de equipos de conmutación para transmisión de datos.
- Núcleo de red (backbone) contruidos sobre enlaces de 34, 45, 155 y 622 Mbps.
- Arquitectura de red completamente redundante, tanto en nodos como en enlaces.
- Existencia de un Centro Internacional de Control (CIC) con amplias capacidades de supervisión, operación y control, y en funcionamiento 24 horas/día, 365 días/año.

Todo ello, otorga fiabilidad y capacidad de transmisión elevada al servicio IP VPN.

Tabla 2.3 Características de la Red IP-VPN (Fuente: Ref [3])

Atributos	Clases de servicio (QoS)		Datos	Orientado a Tráfico transaccional
			Multimedia	Orientado a Tráfico en tiempo real ó de misión crítica
	Simétrico	Simétricos Dedicados	Velocidades de Acceso	64 Kbps, 128 Kbps, 192 Kbps, 256 Kbps, 384 Kbps, 512 Kbps, 1024 Kbps, 2048 Kbps, 34 Mbps, 45Mbps y 155 Mbps.
			Caudal IP	32 Kbps, 48 Kbps, 64 Kbps, 96 Kbps, 128 Kbps, 192 Kbps, 256 Kbps, 384 Kbps, 512 Kbps, 768 Kbps, 1024 Kbps, 1554 Kbps, 2048 Kbps, 34 Mbps, 45 Mbps. Se consideraran también los anchos de banda en incrementos de 1 Mbps, entre los 2 Mbps y 34 Mbps

El servicio IP VPN con Acceso TDM como acceso en la última milla soporta de los 64Kbps hasta los 2Mbps, es un servicio simétrico de interconexión de redes que utiliza como base la red IP MPLS de Telefónica del Perú, lo cual permite ofrecer calidad de servicio en la transmisión de datos, voz y video.

- IP VPN Intranet: Permite la creación de redes virtuales seguras y fiables para el intercambio de información entre los elementos en una organización. Cada intranet es identificada en la red mediante un identificador llamado VPN IP único, creando de esta forma redes privadas virtuales independientes sin posibilidad de intercambio de información entre ellas. Así la red IP MPLS garantiza la seguridad en toda las redes el cliente.

- IP VPN Extranet: Permite la formación de redes privadas virtuales entre organizaciones con redes independientes integrando los elementos que interactúan en la cadena de valor de una organización como por ejemplo clientes y proveedores manteniendo la seguridad y privacidad en las comunicaciones.

2.2.3 Aplicaciones

El Servicio IP VPN está dirigido para aquellas soluciones que deseen crear un entorno Intranet, en el cual todas los puntos conectados puedan compartir entre sí todo tipo de aplicaciones (datos, voz, video y multimedia), independientemente de dónde estén localizadas; e incluso extender sus procesos hacia otros puntos de interés para intercambiar información dentro de un entorno Extranet común; demandando los siguientes requerimientos [6]:

- Comunicaciones integradas de Redes de Área Local (LANs) dispersas geográficamente.
- Solución económica en entornos fuertemente mallados, permitiendo conectividad todos-contratodos.
- Clases de Servicio que prioricen aplicaciones críticas, según el tipo de tráfico cursado (Voip, SNA, SAP, video, etc.)
- Facilidad en la incorporación de nuevas sedes.
- Formación de Intranets y Extranets.
- Solución de VPN segura.
- Soluciones de última tecnología.

Con los accesos Ethernet puede además implementar las siguientes aplicaciones:

- Diseñado para negocios que necesitan gran ancho de banda para extender su LAN y /o implementar servicios de almacenamiento (storage) en IP.
- Arquitectura de Disaster Recovery en IP.
- Acceso a los servicios de la Red IP.
- Arquitectura de sistemas del tipo Cliente-Servidor.

- Integración con otros servicios como Hosting y Housing en el Data Center de Telefónica del Perú.
- Teleeducación, telemedicina, transmisión de noticias.
- Interconexión de puntos de venta

2.2.4 Beneficios

El servicio en su conjunto otorga además los siguientes beneficios [6]:

- Disponer de una Red Privada Virtual con tecnología MPLS (Multiprotocol Label Switching), la cual permite establecer un “grupo cerrado de usuarios” para comunicaciones de voz, datos, video, multimedia con calidad de servicio, seguridad y confiabilidad.
- Configurar redes privadas virtuales del tipo “todos contra todos” (el alcance de esta configuración es definida por el cliente), seguras, de bajo retardo y con priorización de tráfico según las aplicaciones, entre todos los puertos participantes de las conexiones IP del cliente, extremo a extremo.
- Ofrecer con calidad de servicio en tres niveles: oro, plata y bronce, etc diferenciados por la prioridad en la asignación de recursos para la transmisión de las aplicaciones en red (voz, datos, vídeo, entre otros). Por cada enlace se pueden definir anchos de banda diferentes para cuatro niveles de calidad de servicio disponibles, los cuales se definen dependiendo de las aplicaciones que el cliente curse por dicho enlace.

2.3 Multiprotocol Label Switching - MPLS

MPLS es un protocolo que se ubica entre la capa de red y la capa de enlace de datos del modelo OSI. MPLS es implementado en WAN y Backbones de proveedores de servicio. El protocolo MPLS describe los mecanismos para realizar la conmutación de etiquetas sobre la WAN. La Figura muestra la estructura del paquete con etiquetas MPLS.

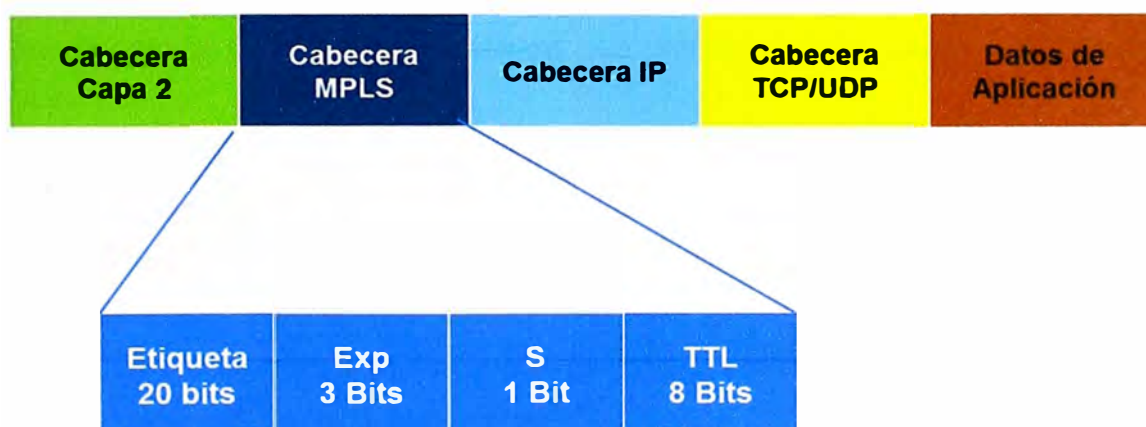


Figura 2.4 Paquete con Etiquetas MPLS (Fuente: Ref. [5])

Funcionalmente el protocolo MPLS añade una cabecera MPLS a cada paquete IP que ingresa a la WAN, esta acción cambia la forma en como los enrutadores de la WAN

envían y procesan los paquetes IP.

Lo que viaja por la WAN ahora son paquetes IP más una cabecera MPLS de 3 Bytes. La cabecera MPLS es insertada sobre la capa de enlace de datos y bajo la capa de red. La cabecera MPLS consta de cuatro campos un campo de etiqueta, campo pila, campo experimental (usado para QoS) y campo TTL.

El campo de mayor relevancia es el campo etiqueta ya que en base a este campo los enrutadores saben cómo enviar los paquetes IP etiquetados.

2.3.1 Principales ventajas MPLS

Entre las ventajas de la tecnología MPLS se pueden resaltar [5]:

- Es multi-protocolo tanto hacia arriba (L3) como hacia abajo (PWE3).
- Uso eficiente del ancho de banda en accesos (full-mesh virtual).
- Conmutación rápida de paquetes basado en etiquetas y no direcciones IP destino.
- Redes de clientes totalmente independientes (MPLS-VPN).
- Trabaja con QoS (Calidad de Servicio) basado en marcación de paquetes.
- Permite aplicar Ingeniería de Tráfico (TE).
- La creación de una nueva VPN sólo implica la creación del circuito de acceso y del enrutamiento.

2.3.2 Términos más utilizados en MPLS

Son los siguientes [7]:

- LSR (Label Switching Router): Nodo interno de la red MPLS capaz de conmutar y enrutar paquetes analizando la etiqueta adicionada a cada uno de estos.
- Edge LSR (Edge Label Switch Router) o LER (Label Edge Router): Nodo de borde que maneja tráfico entrante y saliente de la red MPLS. El Edge LSR de entrada adiciona la etiqueta a MPLS a cada paquete y el de salida la extrae y enruta según la capa de Red.
- LDP (Label Distribution Protocol): Protocolo que establece sesiones TCP entre LSR/LERs para intercambiar las etiquetas que estos utilizarán para la conmutación de paquetes.
- TDP (Tag Distribution Protocol): Protocolo similar a LDP, propietario de Cisco.
- LIB (Label Information Base): Base de datos formada en un LSR/LER que contiene información de etiquetas e interfaces asociadas a las redes destino.
- FEC (Forwarding Equivalence Class): Es una clase que agrupa un conjunto de paquetes que se enviarán en base a una característica común (dirección destino, clase QoS, etc). Los paquetes que pertenezcan al mismo FEC, usarán el mismo camino a lo largo de toda la red MPLS y la misma etiqueta de salida.
- LSP (Label Switched Path): Camino unidireccional definido con QoS y formado por una secuencia de LSRs sobre el cual se envían los paquetes que pertenecen al mismo FEC.

- Traffic Engineering (TE): Proceso de control de flujo de tráfico a través de la red, que optimiza el uso de recursos con el objetivo de mejorar su rendimiento.

2.3.3 Modo de operación

En el enrutamiento tradicional al llegar un paquete IP al enrutador, este analiza la cabecera IP del paquete entrante y obtiene la dirección IP destino a la cual va dirigido el paquete, luego en base a esta dirección, el enrutador analiza su tabla de enrutamiento y realiza la búsqueda de coincidencia más larga luego mapea la dirección destino con una ruta de su tabla, con lo cual obtiene la interfaz de salida y el próximo salto al cual debe enviar el paquete IP [7][8].

Al agregar el protocolo MPLS este proceso en los enrutadores de la WAN cambia. Primero, se establece un LSP entre los routers que van a transmitir el tráfico FEC. Los LSPs hacen las veces de túneles de transporte e incluyen los parámetros QoS específicos del flujo, que sirven para determinar la cantidad de recursos a reservar para el LSP y las políticas de desechado y la cola de procesos en cada LSR.

En toda WAN se tiene los enrutadores de borde y los enrutadores de núcleo. Los enrutadores de borde son aquellos que están en la periferia de la red y están conectados a dispositivos que no son parte de la WAN. En la siguiente figura 2.5 se muestra una WAN MPLS.

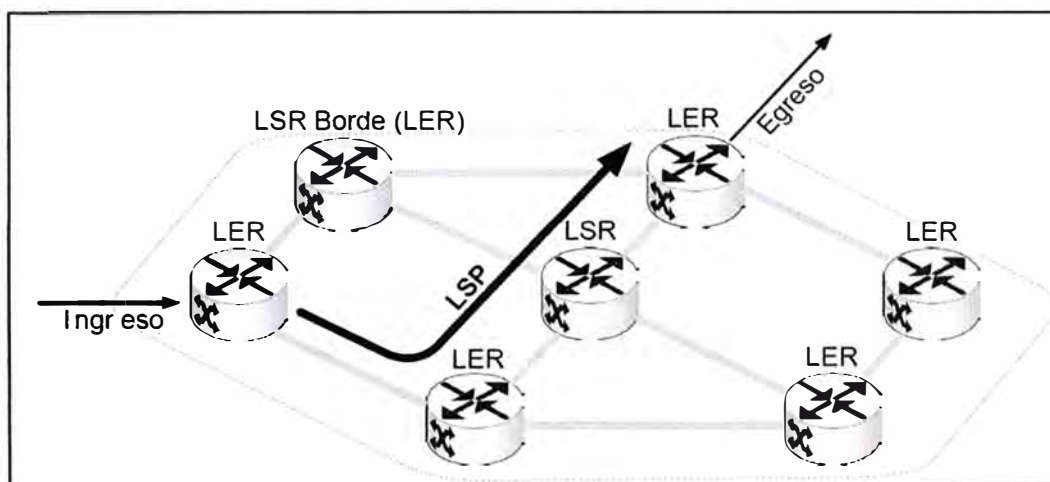


Figura 2.5 Red de área amplia con tecnología MPLS (Fuente: Ref. [7]).

Los enrutadores de núcleo son aquellos que están en el centro de la WAN y todas sus interfaces están conectadas a enrutadores de la WAN. En un dominio MPLS a los enrutadores de borde se les llama LER y a los enrutadores de núcleo LSR. Los LER son los encargados de añadir la cabecera MPLS a cada paquete IP que ingrese a la WAN, los LSR deben conmutar las etiquetas contenidas en las cabeceras MPLS.

Antes de ingresar al dominio MPLS, el Edge LSR (LER) determina los servicios de red que se requiere. Luego, asigna el paquete a una FEC y a un LSP particular, lo etiqueta y lo envía. Si no existe ningún LSP, el enrutador de borde trabaja en conjunto con los

demás LSRs para definirlo. Una vez dentro del dominio MPLS, en cada LSR cuando se recibe un paquete IP este paquete contiene una cabecera MPLS y el enrutador analiza la cabecera MPLS y no la cabecera IP.

Al abrir la cabecera MPLS el enrutador busca el valor de etiqueta del paquete y luego analiza su base de información de envío de etiquetas (LIB) (no su tabla de enrutamiento) posteriormente envía el paquete. Esto significa que por cada LSR que atreviese un paquete IP el valor de la etiqueta cambia, esta conmutación de etiquetas a lo largo de la ruta de un flujo de paquetes IP da origen a lo antes ya mencionado como ruta conmutada por etiquetas (LSP).

Los LSR/LEs extraen las etiquetas de su LIB el mismo que se obtiene vía protocolos de señalización. El protocolo de señalización de MPLS es el protocolo de distribución de etiquetas (LDP). Mediante LDP cada enrutador del dominio MPLS aprende las etiquetas, converge su tabla LIB y obtiene la información necesaria para enviar los paquetes IP etiquetados. LDP se utiliza junto con un protocolo de enrutamiento en el dominio MPLS. Primero se realiza el intercambio de la información de enrutamiento, después converge la tabla de enrutamiento, luego cada LSR realiza su asignación local de etiquetas asignando un valor de etiqueta a cada ruta que tenga en su tabla de enrutamiento. Posteriormente se establecen adyacencias entre LSR vía el puerto TCP 646 para iniciar la sesión LDP. Mediante el protocolo LDP cada LSR intercambia sus etiquetas con las del enrutador vecino. Cuando se da por finalizada la sesión LDP cada LSR tendrá su LIB. La LIB es muy similar a la tabla de enrutamiento con la diferencia de que cada ruta en la LIB contiene un valor de etiqueta.

2.3.4 Red Privada Virtual - MPLS

Es un mecanismo el cual permite que los proveedores de servicios utilizar su backbone IP/MPLS para proporcionar servicios de VPN a sus clientes, también se conoce como VPNs MPLS MP-BGP porque MP-BGP se utiliza para el intercambio de la información de enrutamiento entre sitios remotos sobre la WAN y MPLS se utiliza para enviar tráfico de VPN [9].

Un sitio está conectado a la red del proveedor de servicios (SP) por una interfaz. El SP asocia la interfaz a una tabla de enrutamiento y envío VPN (VRF) en un PE. En la arquitectura VPN MPLS MP-BGP se definen 3 tipos de dispositivos el CE, el PE y el P.

El dispositivo de borde cliente (CE) puede ser un conmutador de capa dos pero típicamente el CE es un enrutador que establece adyacencia con el PE directamente conectado. Después de establecer adyacencia el enrutador CE anuncia las rutas locales del sitio VPN y aprende rutas remotas desde el PE.

El enrutador de borde del proveedor (PE) intercambia información de enrutamiento

con el enrutador CE. Para intercambiar la información de enrutamiento se puede usar enrutamiento estático a algunos protocolos de enrutamiento como RIP, OSPF, EIGRP o EBGP. Cada enrutador PE mantiene una VRF para cada uno de los sitios directamente conectado. El enrutador interno proveedor (P) es cualquier enrutador en la red del proveedor que no une a CEs. Los enrutadores P funcionan como LSR de MPLS enviando y conmutando etiquetas. En la figura 2.6 se muestra la arquitectura de una VPN MPLS MP-BGP

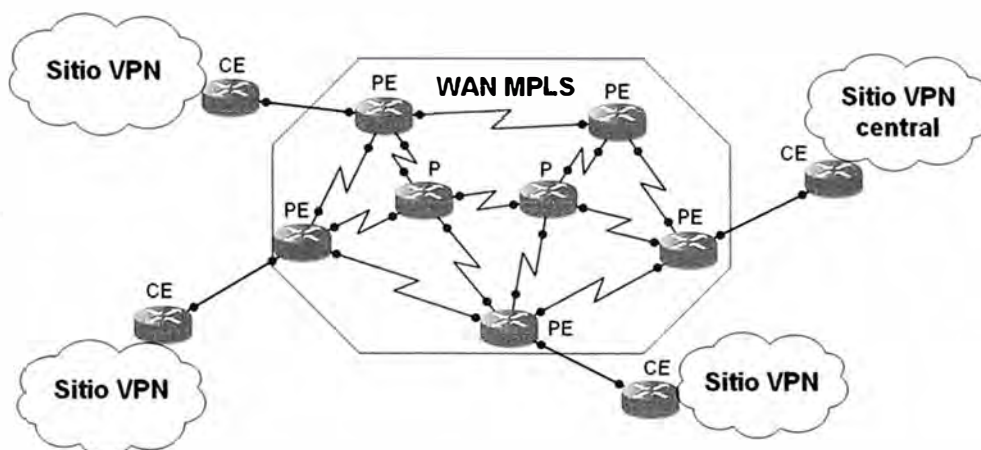


Figura 2.6 Red privada virtual sobre MPLS (Fuente: Ref. [9]).

Dos flujos de control son necesarios para el establecimiento de la VPN. El primer flujo de control es el intercambio de la información de enrutamiento entre sitios remotos esto es realizado a través del protocolo MP-BGP. El segundo flujo de control es el establecimiento de la ruta conmutada por etiquetas (LSP) vía el protocolo LDP, luego ocurre el tráfico de datos entre sitios remotos.

2.4 Calidad de Servicio

Aquí se tratará uno de los conceptos y fundamentos principales que presentará la red a implementar. Esto se trata de la calidad de servicio o QoS (Quality of Service) aplicada sobre la red MPLS [9].

2.4.1 Descripción general

La calidad de servicio definirá la manera que deberá ser tratado cierto flujo de datos dentro de la red, es decir, las características que este presentará. De esta manera se podrá dar un trato especial a cada tipo de aplicación y utilizar los recursos de la red necesarios y suficientes para su transporte. Mediante este mecanismo se podrá determinar el delay, jitter y probabilidad de pérdida de los paquetes pertenecientes a aplicaciones específicas.

En la actualidad, la ITU-T (International Telecommunication Union) y la IETF (Internet Engineering Task Force) han propuesto diversas arquitecturas para dar solución a los requerimientos de Calidad de Servicios presentes en el mercado.

Entre los modelos propuestos por la ITU-T están [9]:

- DBW (Dedicated Bandwidth o Capacidad de Transferencia con Anchura de banda Dedicada).
- SBW (Statistical bandwidth o Capacidad de Transferencia con anchura de banda Estadística).
- Best Effort o de transferencia de tipo mejor esfuerzo.

Estas arquitecturas definen las características del flujo de datos según los siguientes parámetros:

- IPTD (Retardo de transferencia de paquetes IP): Se refiere al retardo que sufre un paquete cuando es transmitido entre dos puntos de referencia cualesquiera, siendo estos puntos por lo general origen y destino.
- IPDV (Varianza del retardo de paquetes IP): Se refiere al jitter o variación del retardo. Esta variación difícilmente sigue algún comportamiento fijo o predecible, es decir, el valor que se obtiene de muestra en muestra es variable. Tráficos sensibles al retardo dependen mucho de este parámetro para su funcionamiento.
- IPER (Tasa de errores en los paquetes IP): Se refiere al porcentaje de paquetes enviados erróneamente en la transmisión total. Estos errores suelen darse por fallas en la codificación o decodificación.
- IPLR (Tasa de pérdida de paquetes IP): Se refiere al porcentaje de paquetes descartados Del total que hayan sido transmitidos. Estas pérdidas suelen darse por saturación del ancho de banda, expiración del TTL (tiempo de vida), etc.

2.4.2 Calidad de Servicio en Arquitectura MPLS

La arquitectura MPLS provee de un circuito virtual o LSP a través de los diferentes nodos que conforman la red MPLS. Gracias a este tipo de funcionamiento, el circuito virtual creado provee de un trato igualitario a los diferentes tráficos que se envían bajo a un mismo túnel LSP bajo una etiqueta FEC en particular. Estudios relacionados a la Calidad de Servicio en diferentes escenarios son de interés actualmente dado que, a comparación con las demás arquitecturas, MPLS ofrece escalabilidad, simplicidad, velocidad, entre otros. Las facilidades que ofrece esta arquitectura para la implementación de Calidad de Servicio son las que se explicarán a continuación [9]:

a. Velocidad frente al esquema de enrutamiento IP.

En efecto, la conmutación de etiquetas es más rápida y eficiente en primer lugar porque se produce en la capa inmediatamente anterior a la capa de red. En segundo lugar, el envío o forwarding se hace en base a un campo específico de la cabecera de la tecnología de conmutación; véase el caso de Frame Relay cuyo campo de identificación de camino es el DLCI Data Link Connection Identifier, en el caso de ATM el campo de

identificación es el VCI Virtual Circuit Identifiers. En MPLS, el campo de identificación de camino es el campo Label el cual representa una FEC y un camino en la red. En tercer lugar, el proceso de clasificación del tráfico solo se da en los routers de entrada y el proceso inverso en el router de salida.

b. Procesamiento más rápido de la cabecera MPLS.

En el caso particular de MPLS solo se necesita tener en cuenta los campos Label, TTL para el envío del tráfico y en ciertos casos dependiendo del tipo de SLA que se haga, los campos correspondientes a Stacking para envío interdominio y el campo Experimental EXP para implementar prioridades. En el caso de IP, se deben de procesar muchos campos como dirección origen, destino, TTL (IPv4), opciones (IPv4), Hop Limit (IPv6), Payload, entre otros campos lo cual retrasa el envío y procesamiento de los paquetes en los nodos de la red, además de que este proceso se repite en cada nodo de la red.

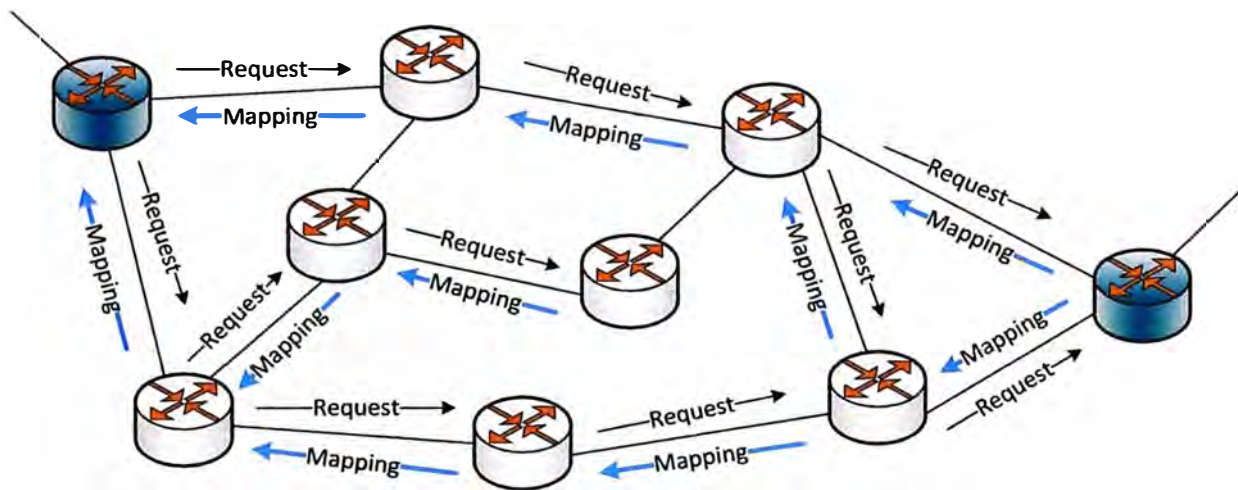


Figura 2.7 Esquema de Envío en la Arquitectura MPLS. Uso de Etiquetas (Fuente: [9])

c. Facilidad de Implementación

Cualquiera de las formas que existe para el correcto funcionamiento de la arquitectura MPLS requiere de poca señalización entre los nodos. Las contramedidas que se pueden tomar en caso de fallas, protocolos de enrutamiento, entre otras tecnologías de capas superiores y/o inferiores no afecta el funcionamiento de la arquitectura, es decir, para cualquier cambio en cualquier capa la arquitectura se amolda a los posibles cambios sin la intervención del administrador de la red MPLS.

d. Adaptabilidad frente a la capa de red como a la capa de enlace

La arquitectura MPLS se localiza entre la capa de red y la capa de enlace, se vale de la conmutación para el envío del tráfico y de los protocolos de enrutamiento para la creación de las tablas de conmutación y de rutas alternas para diferentes fines. Como se puede observar, MPLS utiliza la capa superior inmediata así como la inferior pero su funcionamiento no depende de estas. Además, MPLS se adapta perfectamente a las tecnologías de capa de enlace; tales como ATM, PPP, Frame Relay, la Familia Ethernet;

así como a cualquier tecnología de capa de red como IPv4, IPv6.

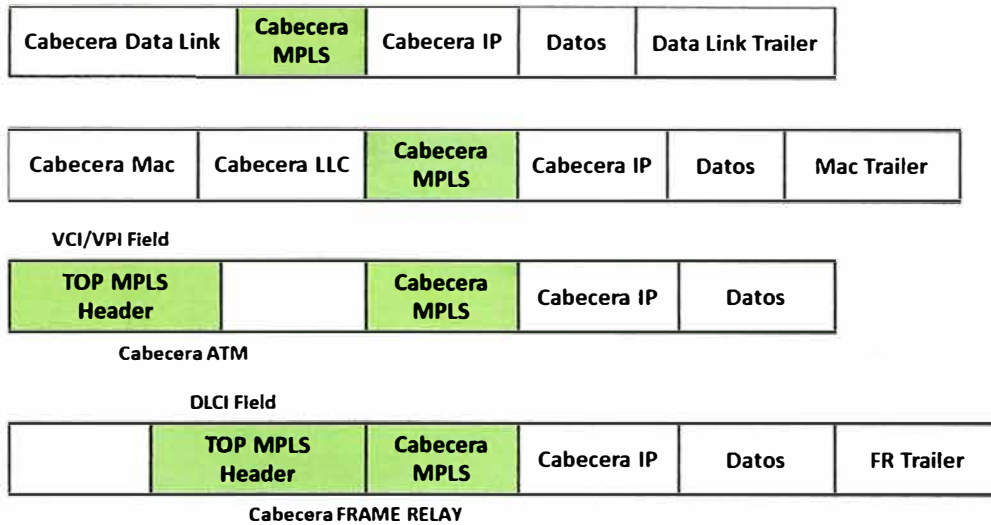


Figura 2.8 Capas de enlace (Fuente: Ref. [9])

- Se acomoda a los modelos de Calidad de Servicio (QoS) de la ITU-T. Gracias al campo experimental EXP el cual cuenta con 3 bits, se puede priorizar los diferentes tipos de tráfico cursados en el mismo túnel LSP. Nótese que con 3 bits se puede obtener 8 tipos de prioridades, lo cual coincide con el número de clases que ha sido propuesta por la ITU-T. Esta característica se suma al hecho de que MPLS es capaz de reservar recursos a través de un mismo así como de diferentes dominios. Puede entenderse que una Clase de Servicio pueda ser implementada bajo una reserva de recursos para ciertos tipos de tráfico provenientes de un cliente y dentro de esta reserva de recursos se daría prioridad a los tráfico que la necesiten.
- Permite la implementación de Ingeniería de Tráfico. Gracias a nuevos protocolos de enrutamiento como a mejoras a otros protocolos de capas superiores, MPLS tiene la capacidad de cambiar dinámicamente de ruta. Las nuevas rutas pueden ser generadas por protocolos de capa de red destinados a crear la tabla de enrutamiento bajo ciertas métricas, así también se aplicarán ciertas políticas en estos mismos protocolos para una mejor evaluación de los recursos de la red. Además estudios sobre posibles alternativas, impacto en la Calidad de Servicio (QoS) se llevan a cabo actualmente como la utilización del protocolo RSVP-TE RSVP Traffic Engineering.
- Permite la implementación de Balanceo de Carga. Al igual que la posibilidad de Ingeniería de Tráfico se puede implementar en los nodos que manejan MPLS es proporcionada por los protocolos de capas superiores, así también el balanceo de carga se puede proporcionar a la red usando estos mismo protocolos según lo crea lo más conveniente el administrador de red. Esta funcionalidad se suele combinar con otras características de MPLS como ingeniería de Tráfico ya que así se evitaría la creación de congestión como la subutilización tanto de los enlaces como de los recursos de los nodos

con menores capacidades existentes en la red pero que en un instante de tiempo con media a alta congestión podrían convertirse en la mejor ruta de cierto tipo de tráfico con lo que se podría evitar pérdidas y retardos en el tráfico que cursa la red.

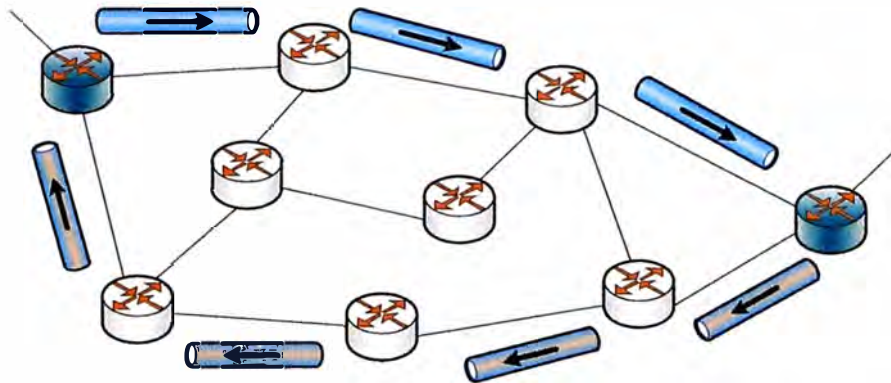


Figura 2.9 Envío de tráfico por diferentes caminos para evitar congestiones (Fuente: [9])

2.4.3 Parámetros calidad de servicio

La tabla 2.4 resume los parámetros de calidad de servicio considerados para la medición de los requerimientos de la solución.

Tabla 2.4 Parámetros de calidad de servicio

Parámetro	Unidades	Significado
Velocidad de Transmisión	Kbps	Indica el caudal necesario para una correcta transmisión.
Retardo (delay) o Latencia	ms	El tiempo medio que se tardan en llegar los paquetes.
Jitter	ms	La fluctuación que se puede producir en el retardo.
Tasa de Perdidas	%	Proporción de paquetes perdidos respecto a los paquetes enviados.

2.4.4 Arquitectura de Servicios Diferenciados (DIFFSERV)

El modelo de servicios diferenciados o DiffServ (Differentiated Services) es propuesto por la IETF (Grupo Especial sobre Ingeniería de Internet) para realizar la clasificación del tráfico IP en un número limitado de clases de servicio.

Los DiffServ no establecen una ruta extremo a extremo para conocer el estado de la red sino con todos los dispositivos de red con clases de servicio configuradas se llega a obtener un resultado preferente para priorizar el tráfico con respecto a los demás cuando la red está congestionada. Los servicios diferenciados son propuestos para resolver problemas que aparecen en los servicios integrados y en RSVP, siendo el modelo DiffServ más escalable, flexible y sencillo.

El modelo DiffServ propone la división del tráfico en función de su tipo de tráfico,

resolviendo el problema de la señalización marcando el mismo paquete en los campos de su cabecera.

DiffServ (servicios diferenciados) proporciona CoS (clases de servicio) a agregados de tráficos unidireccionales. En un dominio DiffServ diferentes tráficos de salida de usuarios se asocian hacia una misma clase DiffServ. Estas constituyen, por lo tanto, un agregado de tráfico que se identifica con un DiffServ Code Point (DSCP- Código de Prefijo de Servicios Diferenciados) determinado y presenta las siguientes características:

- Se basa en el marcado de paquetes únicamente. No hay reserva de recursos por tráfico, no hay protocolo de señalización, no hay información de estado en los routers.
- En vez de distinguir tráficos individuales clasifica los paquetes en categorías según la clase de servicio requerida.
- Los routers tratan cada paquete según su categoría (que viene marcada en la cabecera del paquete). La política de control y la política de admisión sólo se ha de efectuar en los routers de entrada a la red del proveedor y en los que atraviesan fronteras entre proveedores diferentes (normalmente en las fronteras entre sistemas autónomos).

La Arquitectura de Servicios Diferenciados (Diffserv) está basado en un modelo simple de tratamiento del tráfico, utilizado para grandes redes enrutadas. La sofisticada clasificación, marcado de los paquetes, política y operaciones de acondicionamiento necesitan sólo ser implementadas en los elementos de frontera de la red.

El marcado de paquetes se realiza mediante la asignación de un código específico DSCP, que es todo lo que se necesita para identificar a cada clase de tráfico. La clase de tráfico es la agregación de todos los tráficos bajo el mismo criterio de clasificación. En la figura 2.10 se puede ver cómo se implementa servicios diferenciados en los routers Cisco.



Figura 2.10 Implementación de DiffServ en los routers (Fuente: Cisco)

2.4.5 Definición del Campo de Servicios Diferenciados

Un campo de cabecera, llamado DS, es definido para los Servicios Diferenciados, tal

como se muestra en la figura 2.11.



Figura 2.11 Campo de DS (Fuente: Cisco)

Seis bits del campo DS se usan DSCP, que indican el tratamiento que debe recibir este paquete en los routers. CU (Currently Unused – actualmente sin uso) reservado. Este campo se utiliza actualmente para control de congestión. El campo DSCP dentro del campo DS es capaz de tener hasta 64 valores distintos. La tabla 2.5 muestra las 64 combinaciones que puede tener el campo DSCP.

Tabla 2.5 Códigos DSCP (Fuente: Cisco)

DSCP	PHB	DSCP	PHB	DSCP	PHB	DSCP	PHB
000 000	CS0 (DB)	010 000	CS2	100 000	CS4	110 000	CS6
000 001	EXP/LU	010 001	EXP/LU	100 001	EXP/LU	110 001	EXP/LU
000 010	-	010 010	AF21	100 010	AF41	110 010	-
000 011	EXP/LU	010 011	EXP/LU	100 011	EXP/LU	110 011	EXP/LU
000 100	-	010 100	AF22	100 100	AF42	110 100	-
000 101	EXP/LU	010 101	EXP/LU	100 101	EXP/LU	110 101	EXP/LU
000 110	-	010 110	AF23	100 110	AF43	110 110	-
000 111	EXP/LU	010 111	EXP/LU	100 111	EXP/LU	110 111	EXP/LU
001 000	CS1	011 000	CS3	101 000	CS5	111 000	CS7
001 001	EXP/LU	011 001	EXP/LU	101 001	EXP/LU	111 001	EXP/LU
001 010	AF11	011 010	AF31	101 010	-	111 010	-
001 011	EXP/LU	011 011	EXP/LU	101 011	EXP/LU	111 011	EXP/LU
001 100	AF12	011 100	AF32	101 100	-	111 100	-
001 101	EXP/LU	011 101	EXP/LU	101 101	EXP/LU	111 101	EXP/LU
001 110	AF13	011 110	AF33	101 110	EF	111 110	-
001 111	EXP/LU	011 111	EXP/LU	101 111	EXP/LU	111 111	EXP/LU

CAPÍTULO III METODOLOGÍA DE LA SOLUCIÓN

Basado en lo ya explicado el capítulo I, este capítulo se enfoca a exponer la metodología de la solución de ingeniería.

El presente capítulo está organizado en los siguientes ítems: Evaluación de las alternativas tecnológicas de Comunicaciones, elección del medio de acceso, topología de la solución (incluye servicios de comunicaciones y equipamiento), calidad de servicio, disponibilidad del servicio, requerimientos técnicos para implementación, aspectos complementarios de los servicios.

3.1 Evaluación de alternativas de Comunicaciones

En esta sección se hará la evaluación de tecnologías disponibles para brindar la solución de telecomunicaciones y así mismo se describirá a la tecnología seleccionada.

3.1.1 Tecnologías disponibles

Es necesario recalcar que las redes privadas virtuales orientadas a la conexión pueden ser constituidas sobre infraestructura capa 2 o 3. Las redes VPNs orientadas a conexión de capa 2 son las redes punto a punto en modelo overlay, como lo es Frame-Relay y las conexiones virtuales de ATM. Por otro lado, las VPNs construidas mediante túneles IPSec (con encriptación para garantizar privacidad) corresponden a redes constituidas sobre capa 3 en malla completa o parcial.

Las VPNs de acceso son orientadas a la conexión mediante circuitos conmutados que proveen una conexión segura para el acceso remoto entre individuos (usuarios móviles y viajeros) y una red extranet o intranet corporativa a través de la red compartida de un proveedor de servicios. Las deficiencias de las VPNs orientadas a la conexión radican en su escalabilidad, específicamente dichas VPNs en caso de no contar con conexiones de malla entre sus sitios ocasionan ruteo deficiente.

Las redes privadas virtuales no orientadas a la conexión no requieren de un conectionado lógico predefinido o de la provisión de circuitos virtuales entre dos extremos para establecer entre este tipo de redes tenemos las VPN IP convencionales el cual básicamente ofrece la conexión de los routers de los clientes a la red backbone.

El proveedor de servicios configura típicamente múltiples protocolos dinámicos de ruteo corriendo además múltiples procesos de ruteo en sus routers de backbone para el

servicio de sus clientes. Los clientes perciben una red VPN IP privada por virtud de la combinación de listas de acceso, procesos y protocolos de ruteo.

Los mayores inconvenientes que se presentan a los proveedores de manejo de servicios IP son la escalabilidad y la complejidad de implementación. El número disponible de protocolos y procesos de ruteo soportados por las plataformas de cada router obliga a los proveedores a implementar routers separados por cada VPN de cliente en el punto de presencia del proveedor.

En este mismo tipo se tiene Las VPNs MPLS, el protocolo MPLS separa tráfico y provee privacidad sin la necesidad de encriptación o protocolos de túneles de Capa 2, con lo cual, simplifica enormemente el proceso de provisión. MPLS resuelve los problemas de escalabilidad encontrados en los desarrollos de Frame-Relay y ATM ya que permite a los proveedores de servicios provisionar múltiples VPNs para diversos clientes sin la necesidad de configurar decenas de cientos de circuitos virtuales para cada uno de los grupos cerrados de usuarios. Además, permite que el cliente corra sus propios protocolos de ruteo.

El modelo MPLS requiere que los routers CE (routers en casa del cliente) intercambien información de ruteo directamente con los routers de borde del proveedor, en lugar de que cada CPE intercambie la información con cada uno de los restantes CPE. Los miembros de una VPN son identificados como pertenecientes a un grupo cerrado por medio de etiquetas. Dichas etiquetas transportan información del próximo salto, los atributos de los servicios, y un identificador de VPN, que mantiene la comunicación dentro de un ámbito privado (VPN).

Los paquetes que ingresan en la red del proveedor desde un router CPE son procesados, y las etiquetas son asignadas al mismo basándose en la interface física por la cual dicho paquete provino. Las etiquetas son aplicadas empleando la funcionalidad de las tablas VRF (Virtual Router Forwarding). Las tablas de envío son predeterminadas, y los paquetes son analizados en el LSR de ingreso o PE (router de borde del proveedor)

Los dispositivos de core o P (router en el backbone del proveedor) tienen la función solamente de conmutar paquetes etiquetados. MPLS hace que las redes backbone de ruteo de los proveedores provean capacidad de VPN y visibilidad de Capa 3 aun sobre infraestructuras de Capa 2. Esto último permite crear grupos cerrados de usuarios y asociar servicios con ellos.

De acuerdo a lo descrito anteriormente, en la Tabla 3.1 se presenta una comparación entre las diferentes tecnologías VPN y las características más relevantes de las mismas teniendo en cuenta la seguridad, escalabilidad, y otros factores que impactan directamente en los recursos de las redes de los proveedores de servicios y usuarios.

Tabla 3.1 Resumen Comparativo de Tecnologías para implementación VPN.

Características Relevantes	Comentario	VPN – Circuitos Virtuales Capa 2	VPN – Túneles Capa 3	VPN - MPLS
Grado de facilidad para configurar y operar la red	Debe poseer un monitoreo avanzado y automatizado para rápidamente agregar nuevos servicios y operar los existentes.	Medio	Bajo	Alto
Nivel de seguridad	Debe estar diseñado para prevenir ataques del tipo DoS y conservar los datos de los clientes.	Medio	Alto	Medio
Grado de escalabilidad	Debe poder escalar en las nuevas necesidades de los clientes y adaptarse a sus requerimientos.	Medio	Bajo	Alto
Grado de implementación de QoS	Debe ser capaz de asignar prioridad al tráfico crítico o sensible y manejar congestión a lo largo de diferentes anchos de banda.	Alto	Bajo	Alto

Por tanto se concluye que para la presente solución educativa, la plataforma tecnológica más adecuada es la VPN sobre MPLS por la facilidad en la configuración de la red, la escalabilidad el cual nos va a permitir incorporar más centros educativos en el futuro y el alto grado de implementación de QoS (Calidad de servicio).

3.1.2 Elección de tecnología

Para la plataforma de comunicaciones se eligió una Red Privada Virtual (IP-VPN) propiedad de Telefónica del Perú.

Este es un servicio de interconexión de redes locales distribuidas soportado sobre la infraestructura MPLS, que permite la óptima integración de puntos geográficamente distantes y aplicaciones en diversos ámbitos de las necesidades humanas como la educación y medicina [1].

La red de Telefónica del Perú Una (IP VPN) funciona por una plataforma MPLS que sirve como base para la entrega de una amplia variedad de servicios emergentes

basados en IP para el rango completo de 56 Kbps – 40 Gbps. Esta es una red única que soporta una variedad de aplicaciones de datos, voz y video. El uso de esta solución brinda dos ventajas notorias:

- La red MPLS reduce el costo operativo mediante la convergencia.
- Las IP VPN eliminan los costos de la ingeniería y la administración de pasos y rutas de interconexión tipo rueda con centro y rayos.

La solución implica la colocación de router en los puntos a comunicar (datos, señales y administración de pasos entre dicho equipo y la red).

La operatividad de los routers simplifica al proveedor del servicio (Telefónica del Perú) la activación de servicios tales como VoIP y transmisión de video (Videoconferencia). Adicionalmente MPLS sirve como el gran consolidador para combinar diferentes tecnologías de acceso siendo la VPN única.

El servicio IP VPN MPLS de Telefónica del Perú, está basado en el estándar de IETF RFC 2547bis (MPLS de nivel 3). Es por tanto un servicio de VPNs basada en protocolo IP. La plataforma de red IP MPLS mantiene entornos de enrutamiento separados e independientes para cada VPN (más conocido como Virtual Routing Table - VRFs), de forma que asegura la separación completa de cada entorno de usuario, pudiendo ofrecer servicios de VPN sin ningún tipo de restricción sobre el direccionamiento utilizado por el usuario sobre una misma red IP/MPLS.

Las características fundamentales del servicio VPN IP MPLS son:

- Una red cerrada y segura: el tráfico de datos se limita a comunicar sitios previamente configurados y que forman parte de la solución, sin intercambiar datos con el exterior.
- Es convergente: transporte de tráfico de voz, datos y video en la misma VPN
- Maneja adecuadamente las aplicaciones conforme al perfil del sitio: las clases de servicio permiten al servicio IP VPN MPLS la posibilidad de que el usuario pueda definir las calidades de servicio por aplicación datos, voz y video.
- Es gestionado: el servicio cuenta con un Centro de gestión que monitoriza y gestiona la red 24x7x365.
- Tiene una amplia capilaridad: la empresa proveedora de servicios posee gran cobertura nacional e internacional, por lo que se proporciona gran facilidad para expansiones de red de forma ágil y sencilla.

3.2 Elección de medio de acceso, enlaces, parámetros de calidad y equipos

Esta sección desarrolla los aspectos relacionados al dimensionamiento de los enlaces y la determinación de los parámetros de calidad para la solución.

3.2.1 Elección de medio de acceso para los enlaces

Para el medio de acceso se requiere contar enlaces principales (no se considera

respaldo) en todos los centros educativos con diversidad de rutas hacia dos nodos distintos de acceso en la red del proveedor. La tabla 3.2 muestra las características de las tecnologías existentes.

Tabla 3.2 Comparación de características de tecnologías para el medio de acceso

Características	Fibra Óptica	Cobre	Microondas
Distancia entre repetidores (Kms)	40	1.5	30
Atenuación (dB / km) para un Sistema de 56 Mbps	Baja	Media	Alta
Delay máximo (mseg)	30	30	100
Inmunidad a la interferencia estática y fuentes de ruido	Alta	Media	Baja
Resistencia a extremos ambientales. Son menos afectadas por líquidos corrosivos, gases y variaciones de temperatura	Alta	Media	Baja
Inmunidad a la inducción magnética	Alta	Media	Baja
La seguridad en cuanto a instalación y mantenimiento	Alta	Alta	Baja
Confiabilidad y Privacidad	Alta	Alta	Baja

- Medio de acceso de Cobre.- El medio de acceso de cobre es un medio barato y es una buena opción para bajas velocidades de transmisión, máximo 1 E1 lo cual significa que no es un medio que brinde escalabilidad, además ofrece enlaces simétricos dedicados garantizando así el correcto funcionamiento de aplicaciones como videoconferencia como lo demanda la presente solución tecnológica. Adicionalmente al ubicarse las sedes en un área urbana cuenta con servicios de telefonía lo cual indica que el acceso por par de cobre es viable.

- Medio de acceso de fibra óptica.- El medio de acceso de fibra óptica en términos de confiabilidad es mejor que otras tecnologías existentes. En la Tabla 3.2 se aprecia que la fibra óptica es un mejor medio por el tipo de información que la solución educativa requiere transportar, libre de interferencias y garantizando la seguridad y escalabilidad necesarias para la implementación de una red confiable y de alta capacidad, sin restricciones ni factores externos que puedan afectar su desempeño.

- Medio de Acceso Inalámbrico.- El medio de acceso inalámbrico es ventajoso en el aspecto económico porque, en comparación de un medio de fibra óptica, para su implementación no requieren de licencias municipales y se requieren menos trabajos de

obras civiles. Sin embargo, este medio está sujeta a licencias de uso del espectro dependiendo en que banda se desea operar, además presenta desventajas en el aspecto técnico como la seguridad y confiabilidad en comparación del medio de fibra óptica, como puede observarse en la Tabla 3.2.

Considerando que la presente solución incluye un enlace al Datacenter de Telefónica el cual ya cuenta con una conexión a la red IP MPLS del proveedor por ser un nodo de su red se concluye que la mejor alternativa para las sedes es hacer uso del cobre como medio de acceso de última milla por las condiciones que se tienen en relación de disponibilidad, costo y cumplimiento de los requisitos mínimos.

3.2.2 Dimensionamiento de la velocidad de los enlaces

Primero se indica la topología que se utilizará para la solución, esto puede ser una red del tipo “full-meshed”(todos contra todos) o del tipo “hub-and-spoke” (centralizado).

El tipo “full-meshed” permite que todos los sitios estén interconectados con el resto de los sitios que son parte de la red, esto nos indica que el patrón de tráfico es del tipo “peer-to-peer” o sea punto a punto. La tecnología VPN/MPLS permite diseñar la red en full-meshed al mismo o inclusive a menor costo que el diseño en hub-and-spoke. Solo dependerá del tipo de solución o interés del usuario final en la elección del mismo.

En el presente trabajo las sedes establecerán conexiones unas con otras para compartir información además establecerán sesiones de videoconferencia por lo cual decidimos que nuestra red será una full-meshed.

En la solución se tiene un tráfico que es en tiempo real el cual demanda un tratamiento especial para que se ejecute de manera óptima. La parte de videoconferencia se considera trabajar con los equipos Polycom QDX6000 (elección en el punto 3.2.4.b) por su gran calidad y facilidad de uso que aumenta la productividad y ofrece un rápido retorno de la inversión.

Dicho sistema de videoconferencia ofrece una resolución de vídeo de DVD de alta calidad y audio con calidad de CD junto con capacidades de uso compartido de contenido fáciles de usar.

Con ello se obtiene una gran resolución de vídeo a bajo costo, comenzando por 256 Kbps, con un sistema optimizado para un ancho de banda bajo hasta un óptimo de 1024 Kbps, este último será utilizado en la presente solución educativa.

Estos equipos de videoconferencia junto con las políticas de calidad de servicio de la plataforma tecnológica de comunicaciones mantendrán la calidad de vídeo y audio en toda la red, para ello también se cuenta con la tecnología Polycom Lost Packet Recovery (LPR) que nos permite recuperar los paquetes perdidos.

El equipo de videoconferencia soporta un estándar de video H.264 trabajando a una resolución de 1024x768 (XGA) o 800x600 (SVGA) además se podrá contar de una claridad de voz natural y nítida incluso cuando varios interlocutores hablen a la vez con Polycom StereoSurround, el cual utiliza audio de 22 kHz.

Se considera que la sede del Datacenter concentrará la mayoría de los servicios almacenados en el servidor y se utilizará como gateway de acceso a Internet, por lo tanto la distribución de tráfico no será uniforme entre las diferentes sucursales y ya no solo dependerá de la cantidad de usuarios por sucursal sino también por la gran parte del tráfico de datos que deberá pasar en forma obligada por el Datacenter debido a la centralización del servidor.

Tomando como promedio de utilización de ancho de banda por usuario 25Kbps para tráfico de datos comprendido entre las diferentes aplicaciones, programas y servicios propios de la solución educativa; y otros 25Kbps promedio para navegación en internet. Se puede inferir que cada usuario utilizará 50Kbps de ancho de banda en forma entrante "input" y en forma saliente "output", haciendo un promedio de 1024Kbps por cada sede y una suma total de 3072Kbps para el Datacenter

Por lo tanto haciendo una suma del tráfico generado por la videoconferencia y el promedio por tráfico de datos e internet se tiene que el enlace de cada sede debe de ser de aproximadamente 2Mbps y un enlace para el tráfico de datos e internet en el Datacenter de 3Mbps.

El resumen del dimensionamiento de los enlaces de cada sede se muestra en la Tabla 3.3

Tabla 3.3 Especificación de los servicios (Fuente: Telefónica del Perú)

ITEM	Local	Servicio propuesto	Velocidad	Medio de acceso
1	Centro Educativo 1	IP VPN 1:1	02 Mbps	Par de Cobre
2	Centro Educativo 2	IP VPN 1:1	02 Mbps	Par de Cobre
3	Centro Educativo 3	IP VPN 1:1	02 Mbps	Par de Cobre
4	Datacenter TdP	IP VPN 1:1	03 Mbps	Fibra Óptica
5	Datacenter TdP	Infointernet	03 Mbps	Fibra Óptica

3.2.3 Determinación de los Parámetros de Calidad de Servicio para la solución

Para una buena calidad de información a transferirse se maneja un SLA (Acuerdo de disponibilidad de servicio) que determina los rangos adecuados de los parámetros críticos en la red con los que se permita ejecutar de manera correcta las aplicaciones en la red. Dichos parámetros son mostrados en la Tabla 3.4 [1]:

Tabla 3.4 Descripción de parámetros (Fuente: referencia [1])

POP to POP	Retardo	Jitter	Perdida de Paquetes
Capital – Capital	< 5.1ms	< 4.1ms	< 0.21
Capital – Ciudades Principales	< 15.1ms	< 5.1ms	< 0.31

A continuación se explica la importancia para el establecimiento de los parámetros.

- Tiempo de Latencia: Para la solución este es un punto muy crítico al momento de iniciar una sesión de videoconferencia. El rango total permitido de retraso (delay) para una comunicación de audio y video en un sentido es aproximadamente de 125 ms a 150 ms más allá de ello la comunicación es defectuosa. Algunos equipos terminales tratan de compensar esto con bancos de memoria que almacenan los datos que arriban primero, para sincronizarlos con los de latencia más alta [9].
- Fluctuación Temporal – Jitter: Conocido como la variación en el tiempo de la llegada de los paquetes, esto debido a la congestión que sufre la red, pérdida de la sincronización o por el seguimiento de diversas rutas de los paquetes para llegar a su destino. Este parámetro es garantizado por el operador de servicios.(Consultar Tabla 3.4) [9].
- Pérdida de Paquetes: La solución esta propensa a sufrir pérdidas de paquetes IP como resultado de un congestionamiento de la red o corrupción de datos, las comunicaciones como la videoconferencia que son en tiempo real están basadas en el protocolo UDP, el cual no está orientado a conexión y si se produce una pérdida de paquetes no se reenvía. Además para tráfico en tiempo real como la voz, la retransmisión de paquetes perdidos en el nivel de transporte no es práctica por ocasionar retardos adicionales [9]. Por ello es un punto que está considerado en el SLA para garantizar una comunicación fluida en tiempo real.

Una adecuada asignación de velocidad de transmisión para cada tipo de servicio es vital para poder ofrecer calidad de servicio. Las comunicaciones de video facilitan a los estudiantes y docentes permanecer en la misma sintonía y trabajar con mayor eficiencia, permitir a los docentes el uso compartido de contenidos, desde presentaciones hasta recursos multimedia aumenta aún más su efectividad en la enseñanza.

3.2.4 Dimensionamiento de equipamiento de comunicación

En esta sección se analiza y dimensiona el routers y el equipo de videoconferencia.

a. Dimensionamiento Equipo router

Para dimensionar un router CISCO se debe tener en cuenta la cantidad de paquetes por segundo (PPS) que puede procesar el router y la funcionalidad que se quiera habilitar (QoS, NAT, FW, IPSec, etc).

Si es solo IP (Datos) como lo demanda la presente solución, el modelo 1905 puede procesar un aproximado de 290,000 paquetes por segundo al 100% de capacidad, si se hace el cálculo con paquetes de 64 Bytes, se podría decir que puede trabajar hasta con 148.48 Mbps de ancho de banda. Esto con la simple formula: $\text{Mbps} = [(\text{Packet Size}) \times 8 \times \text{PPS}] / 1000000$

Con esto se ve que el equipo soportaría el tráfico de datos que demanda la presente solución educativa en una red VPN MPLS. Para un correcto análisis es necesario también comprender el escenario de implementación y los servicios adicionales a usar.

El escenario de implementación es de un router de borde para salida a internet y conexión a la red IP-MPLS, que realiza HQoS, ACL más no funcionalidades de seguridad (túneles VPN, IPSEC), ni NAT.

Para medir el rendimiento del equipo, debemos conocer cuál es el tamaño usual del paquete de tráfico de Internet, para ello en la industria es usado un término denominado "Internet Mix" o IMIX para describir el tráfico de Internet típico que pasa un poco de equipo de red tales como routers, switches o servidores de seguridad. Cuando se mide el rendimiento del router utilizando equipos de medición con IMIX se supone que el rendimiento que se asemejan a lo que se ve en la vida real.

El perfil de tráfico IMIX se utiliza en la industria para simular los patrones de tráfico del mundo real y la distribución de paquetes. El perfil de tráfico IMIX se basa en un muestreo estadístico realizado en los routers de Internet, y aparecen en los distintos niveles de granularidad, como "simple " y "completo".

- 1518 bytes x 15 paquetes (15%).
- 594 bytes x 24 paquetes (24%).
- 64 bytes x 61 paquetes (61%).

El promedio es dado por $\text{Bytes} = [(1518 \times 15) + (594 \times 24) + (64 \times 61)] / 100 = 409 \text{ bytes}$

Se debe considerar también la utilización del CPU, ya que la mayoría de los proveedores de servicios (ISP) fijan las alarmas de la CPU a 60 o 65 por ciento.

Para la colocación de rendimiento de los routers Cisco ISR G2, el umbral de la CPU se establece en el uso de 75 por ciento. Esta configuración proporciona un indicador válido para la forma en que el router se comporta en un entorno de producción.

Bajo estos parámetros, el fabricante CISCO ha realizado una medición del rendimiento de los equipos CISCO de la serie 1900, donde se muestra el efecto en la

performance del equipo cuando se utilizan los múltiples servicios que se incluyen en el IOS del equipo.

En el escenario donde el router 1905 utilice los servicios de ACLs, NAT, HQoS, al 75% de utilización del CPU, el equipo soportaría 200 Mbps de ancho de banda, esto se puede validar en el documento: Cisco Integrated Services Routers—Performance Overview publicado por CISCO.

En conclusión después del análisis realizado se considera en el diseño al equipo CISCO modelo 1905. Por tanto la solución quedaría según lo mostrado en la Figura 3.1

b. Dimensionamiento Equipo de Videoconferencia

Para definir el modelo y marca del equipo de videoconferencia se toma en consideración lo siguiente:

- Revisión de las características técnicas de los equipos para verificar su empleabilidad.
- No se tiene una restricción por parte del cliente en la elección del equipo de videoconferencia.

En la Tabla 3.5 muestra marcas y modelos de equipos que cumplen estas especificaciones

Tabla 3.5 Equipos y Características (Fuente: Fabricante)

	Marca/Modelo del equipo		
Característica	Tandberg 770 MXP	Polycom QDX 6000	Aethra Vega X3
Estándar de Video	H.261, H.263, H.263+, H.263++	H.264, H.263, H.261	H.261, H.263++, H.264, H.239, H.241
Resolución de Video	4SIF (704 x 480) pixeles 4CIF (704 x 576) pixeles CIF (352 x 288) pixeles QCIF (176 x 144) pixeles	4SIF/4CIF 16:9 SIF (352 x 240) pixels CIF (352 x 288) pixels QSIF (176 x 120) pixels QCIF (176 x 144) pixels	4CIF 704 x 576 pixels FCIF 352 x 288 pixels QCIF 176 x 144 pixels 4CIF 704 x 576 pixels
Velocidad de Transmisión	168Kbps – 336Kbps	256 Kbps – 2 Mbps, optimo 1024 Kbps	64Kbps-2Mbps sobre IP
Entrada de Video	1x MiniDin, S-video 1 x RCA camera / aux 1 x RCA VCR 1 x DVI/SXGA: PC	2 x S-Video, uno para la cámara 2 x Composite 1 x VGA	Integrated Y/C, Para la cámara RCA Aux Composite DVI_I XGA

Salida de Video	1x MiniDin, S-video 1 x RCA / VCR 1 x RCA / dual monitor 1 x DVI/XGA:	Component 720p 2 x S-Video / VGA 2 x RCA	1x RCA Monitor Composite 1xDVI_I XGA Out
Estándar de Audio	G.711, G.722, G.722.1, G.728	G.719, G.722, G.722.1, G.711, G.728	G.711,G.728, G.722, G.722.1
Entrada de Audio	2xConectores XLR para microfonos 1xRCA VCR (R) 1x RCA VCR/DVD (L)	2xR-J9 Para micrófonos analógicos 2 x Dual RCA	1xRCA Línea de Audio
Salida de Audio	2 x Dual RCA	1 x RCA	1xRCA / S/PDIF (mono/stereo) 1 x RCA / VCR
Interfaces de Red	1 x LAN / Ethernet (RJ-45) 10/100 Mbit LAN 1 x PC card slot (PCMCIA) for wireless LAN	1xRJ45 10/100 Mbit LAN 2 x RS232 (1 para el control camara)	1 x BRI RJ-45 2 x RJ-45 Ethernet 10/100BASE-T full-duplex
Software de Gestión	TANDBERG Management Suite	CMA software	Interface Web
Precio (US\$)	8560.00	6,800.00	7,350.00

Es importante indicar que el proveedor de servicios como parte de sus soluciones integrales de comunicaciones mantiene relaciones comerciales con ciertas marcas de equipos de multimedia como es el caso de Polycom bajo un acuerdo marco, el cual se ve reflejado en el precio especial del equipo. Dado que todos los equipos cumplen con los requerimientos mínimos necesarios para la presente solución, se propone el de menor costo. En conclusión se considerará para el diseño el equipo Polycom QDX 6000.

3.3 Topología de la solución

La Figura 3.1 muestra la topología de solución. En él se puede ver los centros educativos involucrados, así como el equipamiento a instalar. La nube representa la conectividad IP VPN entre los centros educativos y el Data Center de Telefónica del Perú.

El tráfico es prioritariamente de la aplicación educativa HP Metasys Education Solution dicho software permite el control de todos los equipos conectados en la red para el manejo de todos los aplicativos educativos. Adicionalmente también se considera equipos de videoconferencia para educación a distancia [1]. Este modelo tiene un centro de gestión centralizado ya que se aprovecha las ventajas de una correcta consolidación de la información en los servidores, lo que permite tener sustanciales ahorros, mejorar la gestión y contar con un único sistema de información. Para que este modelo resulte

exitoso, se debe contar con un sistema de alta disponibilidad que asegure que los servidores de educación se encuentren siempre disponibles y con la información actualizada. Por este motivo se estableció el sistema de gestión del sistema de educación en Datacenter de Telefónica del Perú.

En la Figura 3.2 se muestra la salida a Internet de la solución que será a través del Data Center de Telefónica del Perú como un punto único para toda la red educativa. Al ser este tráfico no prioritario se aplicará una clase de servicio de mejor esfuerzo (Best-Effort). De acuerdo a lo referido en el punto 3.2.1, los tres colegios considerados en la solución ubicados en la ciudad de Pacasmayo contarán con un enlace IP VPN con las calidades de servicio brindados por el proveedor de servicios el cual se detalla en la Tabla 3.6.

Tabla 3.6 Calidades de servicio (Fuente: Elab. propia)

Local	Servicio propuesto	Velocidad	Clase multimedia	Clase datos	Clase Best Effort	Medio de acceso
Centro Educativo 1	IP VPN 1:1	02 Mbps	1024 Kbps	512 Kbps	512Kbps	Par de Cobre
Centro Educativo 2	IP VPN 1:1	02 Mbps	1024 Kbps	512 Kbps	512Kbps	Par de Cobre
Centro Educativo 3	IP VPN 1:1	02 Mbps	1024 Kbps	512 Kbps	512Kbps	Par de Cobre
Datacenter TdP	IP VPN 1:1	03 Mbps	-	1536 Kbps	1536 Kbps	Datacenter
Datacenter TdP	Infointernet	03 Mbps	-	-	-	Datacenter

A continuación se describen los servicios de comunicaciones y equipamientos involucrados en la solución.

3.3.1 Servicio de comunicaciones en los Centros Educativos

Los tres centros educativos considerados en la solución están ubicados en la localidad de Pacasmayo contarán cada una con un enlace IP VPN con acceso TDM cuyo medio de acceso será par de cobre. Dichos enlaces serán configurados a una velocidad de 02 Mbps. Estos enlaces utilizarán par de cobre como medio de acceso a través de un equipo Modem HDSL, a este equipo MODEM se conectará el equipo router marca CISCO modelo 1905 el cual será configurado para soportar las aplicaciones de videoconferencia y solución educativa [11] [12] [13].

- Acceso : Simétrico (TDM)
- Velocidad : 2048 Kbps
- Caudal Multimedia : 1024 Kbps
- Caudal datos : 1024 Kbps
- DCE : MODEM HDSL
- DTE : ROUTER CISCO 1905

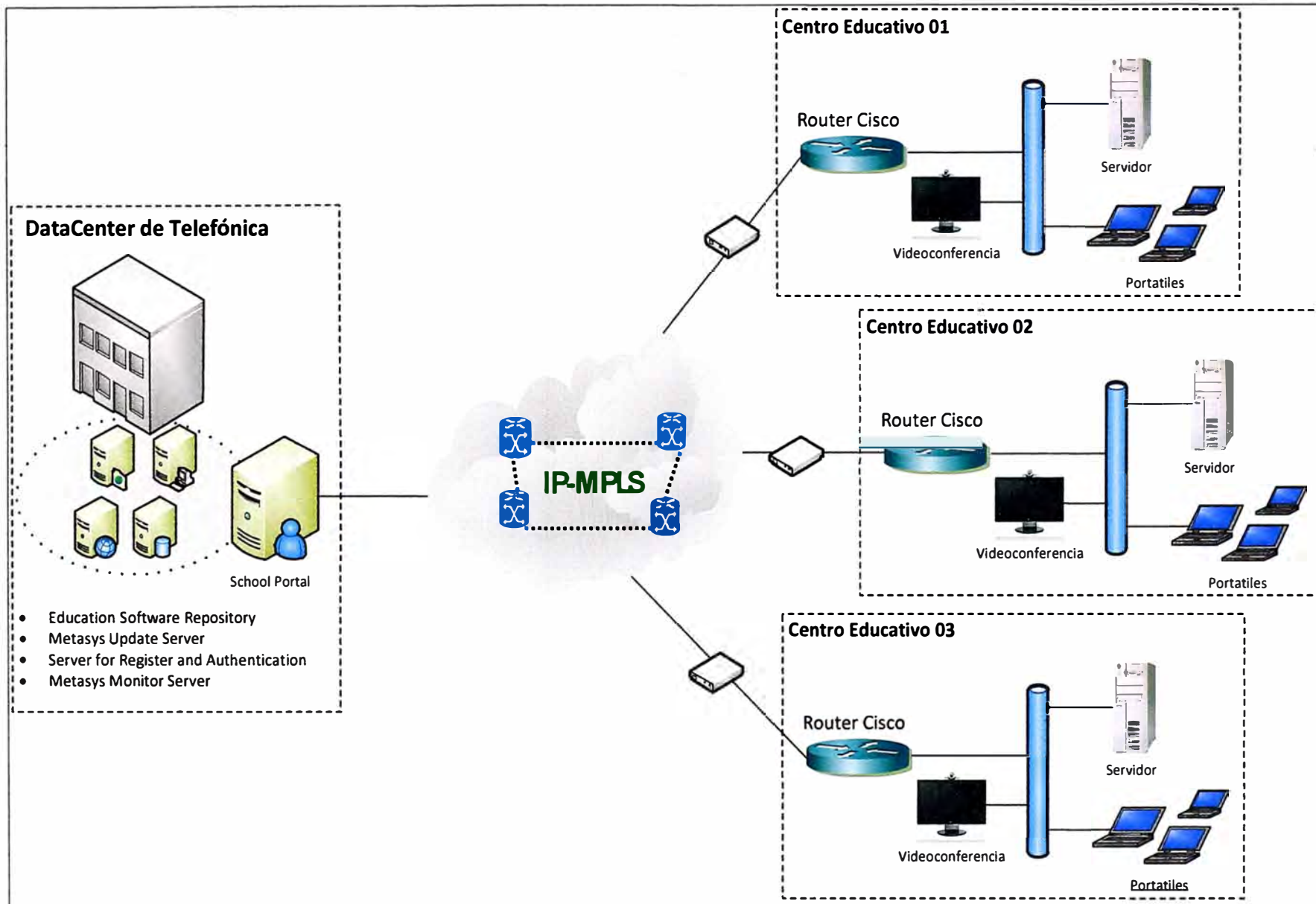


Figura 3.1 Topología de red (Fuente: Elaboración propia)

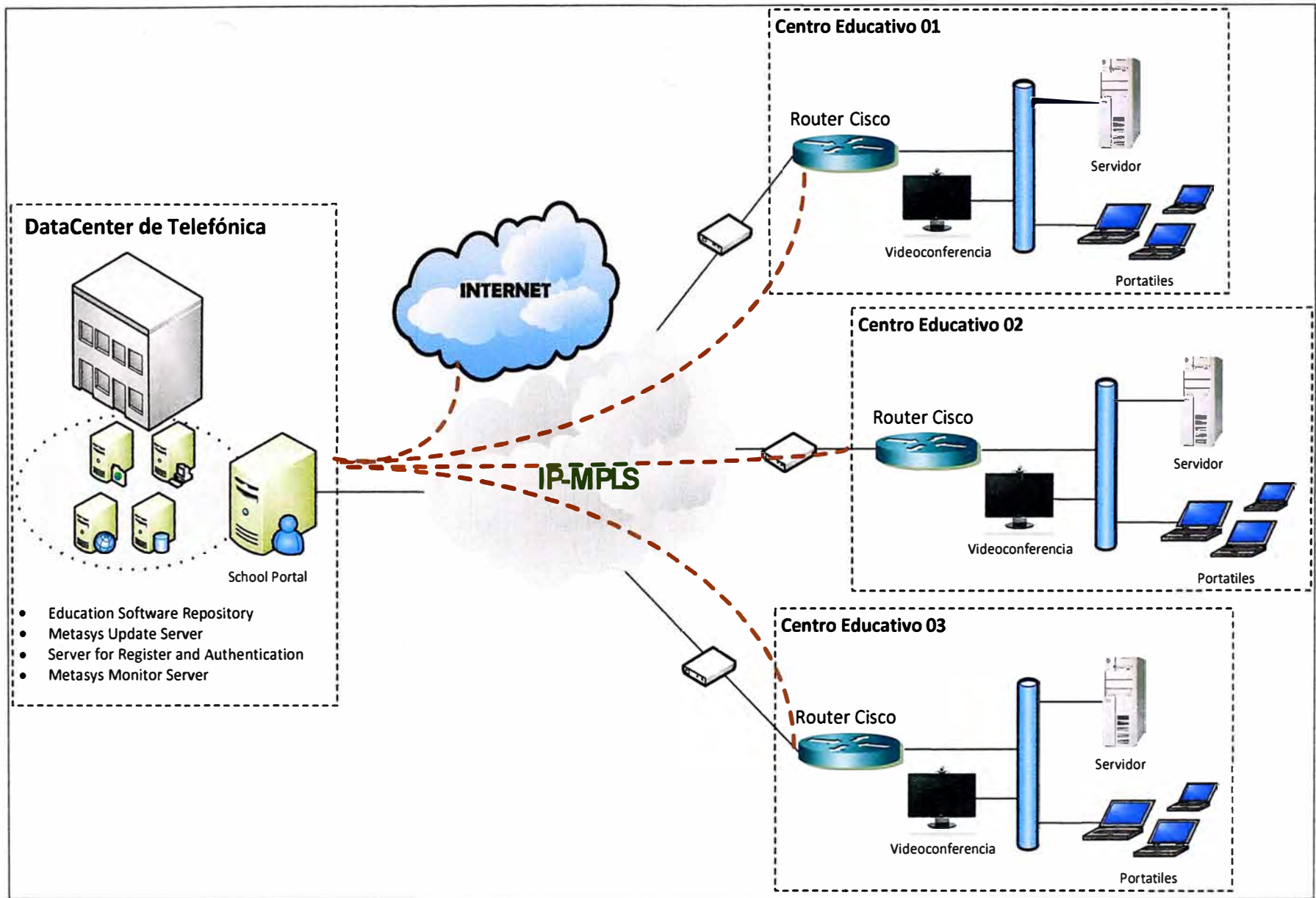


Figura 3.2 Salida a Internet de la solución (Fuente: Elaboración propia)

En el Data Center de Telefónica del Perú se encontrará alojado el servidor central parte importante de la solución de educación, este es un sitio que ya dispone de la infraestructura de comunicaciones necesaria para conectarse a la red IP VPN de los centros educativos así como servidores para el almacenamiento de datos.

En el Data Center se contará con un enlace IP VPN con acceso Ethernet de 03 Mbps de velocidad a fin de permitir el acceso al Servidor Central por parte de los distintos alumnos y profesores que forman parte de la solución de educación. Además este sitio será un punto singular de la red IP VPN por lo cual también se contará con un acceso a Internet que permitirá la salida de todas las PCs consideradas en la solución a Internet.

- Acceso : SIMÉTRICO (Ethernet)
- Velocidad : 3072 Kbps
- Caudal datos : 3072 Kbps

3.3.2 Descripción de equipos de comunicaciones

Aquí describe el equipamiento involucrado en la solución de comunicaciones explicando los aspectos técnicos y funcionales [11] [12] [13].

a. Router

Para la solución se utilizará el Cisco 1905 Integrated Services Router serie (ISR G2) pues nos proporciona datos de alta seguridad, movilidad y servicios de aplicación además ofrece un aumento de los niveles de los servicios de integración de datos con de la seguridad, inalámbrico, la movilidad y los servicios que permite una mayor eficiencias y ahorros de costes. En la Tabla 3.7 se muestra la configuración del router

Tabla 3.7 Configuración del router Cisco 1905

Producto	Descripción
CISCO1905/K9	C1905 Router, 2 GE, HWIC-1T, CAB-SS-V35MT, 256F/256D, IPBase
S19UK9-15102T	Cisco 1900 IOS UNIVERSAL
CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m
CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet
SL-19-IPB-K9	IP Base License for Cisco 1900
CON-SMBS-1905	SMBS 8X5XNBD C1905 Serial Router, 2 GE,1 EHWIC slot

Una característica importante de esta nueva familia de routers CISCO (Figura 3.3) es que cuenta con un único IOS software instalado en cada cisco ISR G2.

Dicho IOS contiene todas las capacidades tecnológicas del router que puede ser activado con licencias dependiendo que aplicación se le quiera dar al equipo, permitiendo al usuario desplegar rápidamente características avanzadas sin necesidad de descargar un nuevo IOS.

Además, por defecto se tiene más memoria que servirá de apoyo a nuevas capacidades.

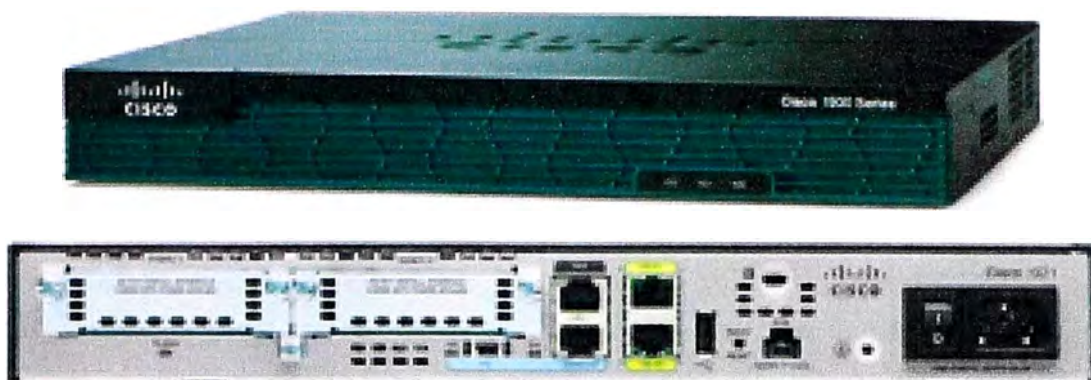


Figura 3.3 Cisco 1905 Integrated Services Router serie (ISR G2) (Fuente: Cisco)

b. Switch

Los switches Cisco Catalyst de las series 2960 ofrecen un sistema de comunicación todo en uno gracias a sus capacidades para datos, conexión de voz y video, asignando prioridad al tráfico de voz o al intercambio de datos para que la entrega de información concuerde con las necesidades que demanda el software educativo.

Este modelo ofrece 24 puertos para la red LAN y cuentan con alimentación por Ethernet (POE) para alimentación de los puntos terminales de la red. En la Tabla 3.8 se muestra la configuración del equipo.

Tabla 3.8 Configuración del switch Cisco Catalyst 2960 (Fuente: Fabricante)

Producto	Descripción
WS-C2960-24TT-L	Catalyst 2960 24 10/100 PoE + 2 T/SFP LAN Base Image
CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m
CON-CSSPD-C29602TT	SHARED SUPP SDS Catalyst 2960 24 10/100 + 2 1000BT LAN

Es importante indicar que la solución no considera equipos que se alimenten vía el switch pero ya se tendría habilitado el switch con POE cuando se desee integrar nuevos servicios en la plataforma como lo es la telefonía IP (Figura 3.4).



Figura 3.4 Switch Cisco Catalyst 2960 (Fuente: Cisco)

c. Equipo de Videoconferencia

Por su manejo de un potente códec, cámara de calidad profesional, audio con calidad de CD y múltiples entradas y salidas de vídeo, el sistema QDX 6000 es compatible con la

mayoría de sistemas de videoconferencia, puentes para conferencias y productos de firewall transversal basados en estándares, entre otros.

Con sus interfaces intuitivas y el cifrado AES altamente seguro de comunicaciones de audio y vídeo, los usuarios pueden realizar llamadas de forma segura y acceder a una videoconferencia en cuestión de segundos.

Los contenidos y otros elementos multimedia se comparten a través de una sencilla interfaz en la que sólo hay que hacer clic, mientras que la tecnología Lost Packet Recovery™ de Polycom brinda unas conferencias ininterrumpidas y sin problemas, incluso en redes saturadas.

Tabla 3.9 Configuración sistema Polycom QDX 6000 (Fuente: Fabricante)

Producto	Descripción
Polycom EagleEye QDX	Cámara de alta resolución
Códec	Para la reproducción de audio y video
Kit de altavoces	Para la salida de audio
Mando a distancia	Control para la realización de videoconferencias y configuraciones
Cables de conexión	Cables para la conexión de equipos y alimentación



Figura 3.5 Sistema Polycom QDX 6000 (Fuente: Fabricante)

d. Servidor

El servidor HP ProLiant ML10 es ideal para la presente solución educativa tecnológica por disponer los recursos necesarios y ser adecuado en cuanto a rentabilidad. Este equipo cuenta con gestión remota HP iLO 3 el cual permite su administración vía remota evitando así gastos por traslado a la ubicación del servidor. Cuenta con un chasis de gran tamaño que permite el flujo de aire al máximo reduciendo considerablemente el fallo de

los componentes por sobrecalentamiento

Su diseño al ser tipo PC de escritorio permite su fácil instalación y comodidad para cualquier ampliación que se desee hacer a alguno de sus componentes con soporte hasta dos unidades de disco duro, siete puertos USB y cuatro ranuras de E/S.

Tabla 3.10 Configuración sistema Polycom QDX 6000 (Fuente: Fabricante)

Producto	Descripción
Procesador	Intel® Pentium® G2130 (2 núcleos, 3,2 GHz, 3 MB, 55 W)
Ranuras de Expansión	(4) PCIe
Memoria	UDIMM de 2 GB (1 x 2 GB)
Disco Duro	(1) SATA LFF
Unidad Óptica	Unidad DVD-ROM JackBlack SATA de media altura

e. Equipo terminal para estudiantes

Las PCs para los estudiantes cuentan con procesador Intel, es una computadora portátil diseñado por Intel. Se integra a los estudiantes y profesores en un sistema de aprendizaje, permitiendo a los estudiantes colaborar, intercambiar información y revisar el material de aprendizaje.



Figura 3.6 Terminales Metasys MeeGo (Fuente: Fabricante)

Permite a los profesores complementar y ampliar sus clases, lo cual es proporcionando por un sistema operativo basado en la plataforma de software Libre. MeeGo combina los proyectos de código abierto Moblin de Intel y Maemo de Nokia en una plataforma de software basada en Linux organizada por la Fundación Linux.

Este sistema operativo cuenta con una innovadora interfaz de usuario optimizada dirigida a los alumnos para la interacción en medios sociales. Diseñado para apoyar el aprendizaje uno a uno, Metasys MeeGo permite a los estudiantes a trabajar juntos, intercambiar información, consumir y crear materiales de aprendizaje en un entorno de colaboración.

El Metasys MeeGo incluye importantes adiciones y mejoras, como la funcionalidad de búsqueda mejorada y soporte a plug-ins, mejora en la interfaz del usuario, soporte a conexiones de dato, gestión de dispositivos Bluetooth, un instalador de aplicaciones integrado y un instalador de medios educativos con mayor rendimiento y estabilidad.

3.4 Configuración de Calidad de servicio para la solución

Es de vital importancia considerar que por la red de la solución va a transmitirse tráfico multimedia para establecer una conexión para la videoconferencia el cual demanda cumplir con ciertos rangos para la latencia, jitter y pérdida de paquetes.

El tráfico de la videoconferencia debe tener mayor prioridad en la red para evitar que al momento que se ejecute la comunicación, la interactividad sea en tiempo real y no se tenga problemas como retardo, congelamiento del video, distorsión de voz y video.

Para un correcto tratamiento de los tráficos, la red VPN IP MPLS define clases de servicio diferentes (QoS) para priorizar los tráficos y /o aplicaciones dentro de la Intranet del usuario. A continuación se describirá las clase de servicios y posteriormente el tratamiento del exceso de tráfico en cada clase [11][13].

3.4.1 Asignación de las clases de servicio

Para tener una idea más clara, las clases de servicio se muestran en la (Figura 3.7.a) y cada una con su propia prioridad (Fig. 3.7.b), [14][15][16]. Para las aplicaciones que serán presentadas.

a. Aplicación Clase de servicio Multimedia

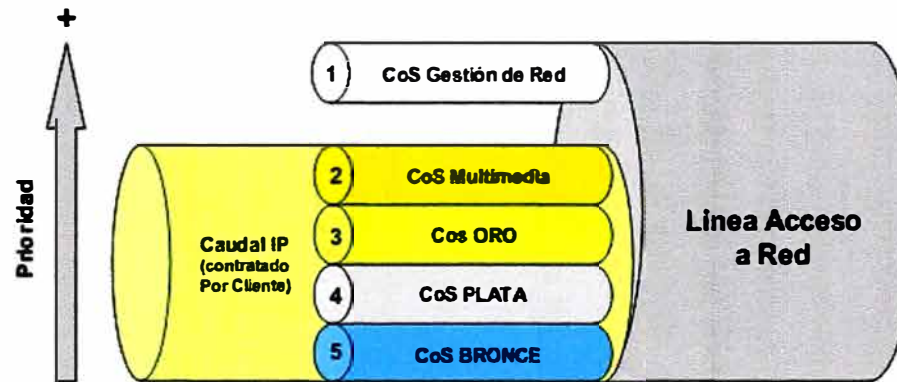
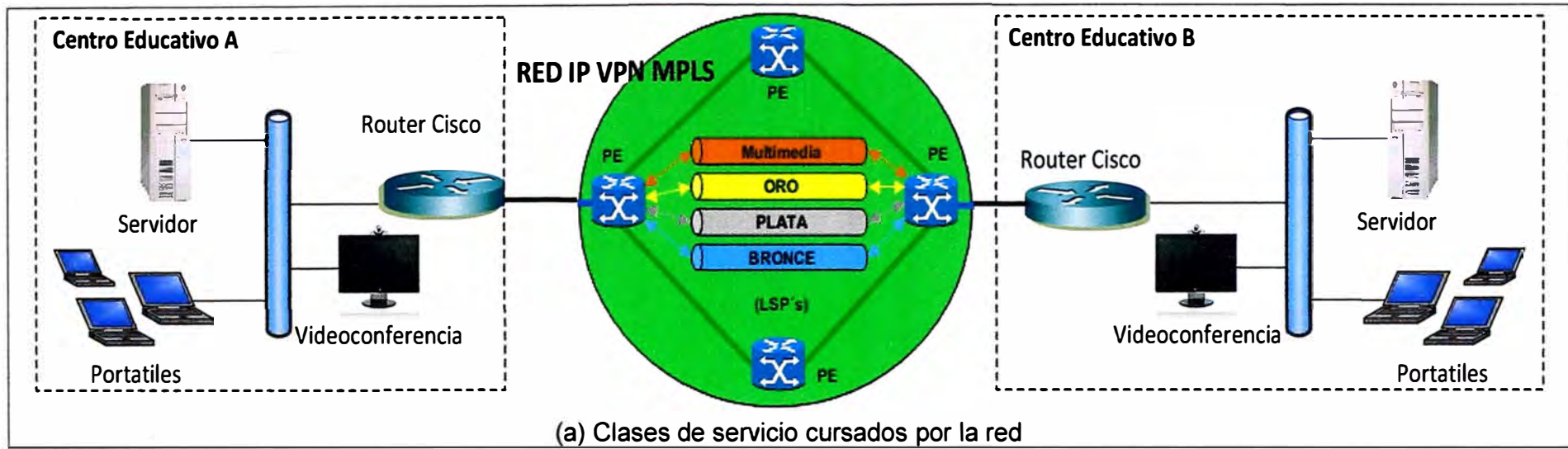
Esta clase será aplicada para marcar el tráfico para la videoconferencia, siendo la más óptima para las aplicaciones de voz y video ya que ofrece alta prioridad de emisión, y por tanto minimización de retardos y jitter, garantizando la transmisión de las comunicaciones de voz corporativas con niveles objetivos de servicio de Retardos de Tránsito, Pérdida de Paquetes y Jitter.

b. Aplicación Clase de servicio Datos (Oro)

Esta clase será aplicada al tráfico propio de la solución educativa ya que ofrece alta prioridad de transmisión, por lo que se asegura una baja tasa de pérdidas, y por tanto apropiada para tráfico crítico para el negocio el usuario como por ejemplo aplicaciones financieras, aplicaciones de control y gestión, etc. Ofrece compromisos de Retardos de Tránsito y Pérdida de Paquetes.

c. Aplicación Clase de servicio por defecto (Plata y Bronce)

Esta clase será aplicada para el tráfico que no ha sido marcado con las dos anteriores por lo cual es considerado como "Best-Effort" (mejor esfuerzo), sin prioridad en la red para ambas clases. Dentro del tráfico no prioritario suelen convivir aplicaciones de Intranet e Internet.



N° CoS	Tipo CoS	ToS	Descripción de Clase de Servicio
1	Gestión	6	Tráfico Gestión: Gestión EDC's Red IP MPLS
2	Multimedia	5	Tráfico Multimedia: Voz y Video sobre IP
3	ORO	3	Tráfico Datos Alta Prioridad: SNA, SAP, Aplicaciones Críticas
4	PLATA	0	Tráfico Datos Baja Prioridad: Intranet
5	BRONCE	1	Tráfico Datos Best Effort: Internet

b) Priorización del tráfico en la red

Figura 3.7 Descripción de Clases de servicio: (Fuente: Elaboración propia).

Esta última (Internet) suelen ir incrementando su demanda de ancho de banda hasta acaparar todo el ancho de banda disponible, dejando sin trabajar a las aplicaciones de Intranet. Para evitar este comportamiento, se definen dos clases de servicio diferenciadas (Plata y Bronce) que permiten contratar un caudal mínimo garantizado para cada una de ellas, de forma que el tráfico en exceso de una de las clases no impida que se curse el caudal mínimo de la otra. Por defecto, se asocia a la clase plata el tráfico corporativo de baja prioridad y a la calidad Bronce, el tráfico de Internet

3.4.2 Funcionamiento del exceso de tráfico en cada clase para la solución

La solución IP VPN MPLS permite la optimización del acceso al ofrecer en todo momento la posibilidad de que el ancho de banda que deja vacante alguna clase pueda ser reutilizado por otra que demande mayor capacidad de transmisión. De este modo, se produce el siguiente tratamiento del exceso de tráfico sobre el caudal asegurado [11][13]:

a. Tratamiento de Tráfico en la Clase de servicio Multimedia

Para la clase de servicio Multimedia, la información transmitida no puede sobrepasar en ningún momento el caudal configurado. En el caso de que se transmitiera más información de la configurada, ésta sería descartada. Cuando no se esté utilizando el caudal Multimedia configurada, éste podrá ser usado por las clases de menor prioridad: Datos, Plata y Bronce.

b. Tratamiento de Tráfico en la Clase Datos

Cuando se envíe más tráfico de la clase Datos del configurado, el excedente será remarcado. Este funcionamiento permitirá que ante una sobrecarga de tráfico Datos y vacancia de cualquier calidad, el caudal Datos excedente se envíe como tráfico Bronce. Por el contrario, cuando no se esté utilizando el caudal Datos contratado, éste podrá ser usado por las clases de menor prioridad: Plata y Bronce.

c. Tratamiento de Tráfico en la Clases de servicio Plata y Bronce

Estas clases podrán emplear el ancho de banda vacante que no utilicen el resto de clases repartiéndoselo en iguales proporciones y transmitiéndose con su misma prioridad (Plata o Bronce según el caso).

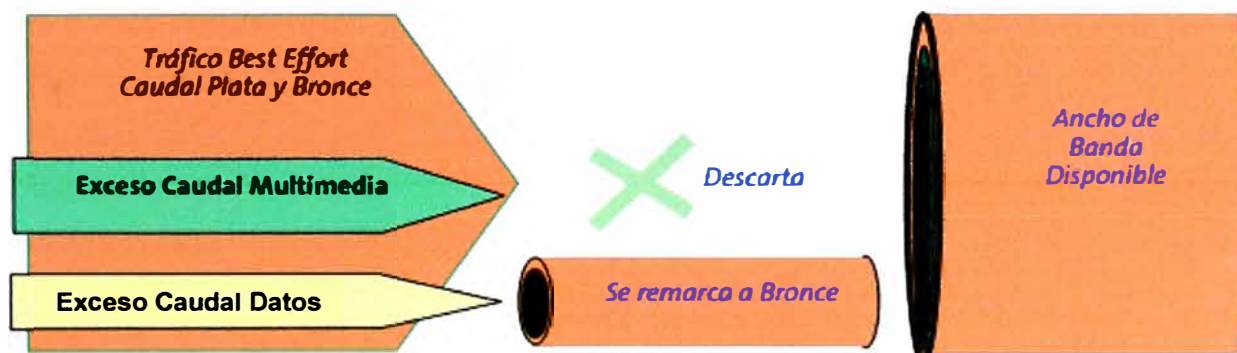


Figura 3.8 Tratamiento del exceso de tráfico (Fuente: Elab. propia)

Cuando una de estas dos clases no genere tráfico, permitirá que éste caudal sea empleado por otra.

3.4.3 Configuración de las Clases de Servicio en los Centros Educativos

De acuerdo a lo definido en el punto 3.3.1 se muestra la configuración de las calidades de servicio en los routers ubicados en los centros educativos.

a. Técnica de Clasificación y Marcación por Clase de Servicio

La clasificación de los paquetes se harán en base a las clases de servicio antes ya descritos. Los paquetes agrupados serán asociados a clases de servicio y hará de la siguiente forma:

- Clase Multimedia destinado a todos los paquetes de voz y video,
- Clase Datos destinado a todos los paquetes de las aplicaciones educativas
- Clase Best Effort destinado a todos los paquetes de intranet e internet

Luego de clasificar estos paquetes de entrada en base a clases de servicio se procederá a aplicar la política de marcación de paquetes para ello se utiliza el DSCP (Punto de código de servicios diferenciados), para la presente solución se utilizará tres tipos de marcación DSCP para diferenciar las clases de servicio:

- CS5: Tráfico de Voz y Videoconferencia
- CS2: Trafico de datos críticos
- CS1: Tráfico restante o datos no críticos.

Clasificación de los Paquetes

```
class-map match-any multimedia
matchip dscp cs5
match access-group name multimedia
class-map match-any datos
match ip dscp cs2
match access-group name datos
```

Política de Marcación

```
policy-map setdscplan
class multimedia
setip dscp cs5
class datos
setip dscp cs2
class class-default
setip dscp cs1
```

b. Técnica de Prevención de Congestión y Encolamiento

Para el encolamiento de baja latencia (LLQ) en base a las clases multimedia, datos y por defecto (best-effort) que agruparan los paquetes que serán marcados con cs5, cs2 y cs1 estos funcionarían como cola de espera. La importancia del encolamiento de baja latencia radica en la priorización estricta que se tiene, reduciendo el jitter en las aplicaciones como videoconferencia, en otras palabras no importa el tipo de tráfico que se esté transmitiendo en un momento determinado, si hay paquetes de la aplicación de videoconferencia en la cola multimedia esta tendrá preferencia poniendo en cola las demás hasta que se termine de enviar el paquete de multimedia.

Para la prevención de congestión del tráfico se tiene que establecer las políticas de calidad de servicio para evitar que cuando el enlace se sature, se genere exceso de tráfico y por ejemplo la videoconferencia siga transmitiéndose afectando los otros tipos de tráfico, el funcionamiento se explicó en el punto 3.4.2

Creación y designación de clases de servicio

```
class-map match-any multimedia
match ip dscp cs5
class-map match-any Datos
match ip dscp cs2
```

Política de Calidad de Servicio

```
policy-map wan
class multimedia
priority 1024
police 1024000 32000 32000 conform-action transmit exceed-action drop
class Datos
bandwidth 512
police 512000 16000 16000 conform-action transmit exceed-action set-dscp-transmit cs1
class bronce
bandwidth 512
class class-default
fair queue
policy-map shape 2048
class class-default
shape average 2048000
service-policy wan
```

3.5 Disponibilidad del servicio para la solución

El Acuerdo de Nivel de Servicio (SLA) es punto importante a considerar para la

solución a manera de garantizar la correcta operatividad de la red brindando soporte y total disponibilidad del sistema. La tasa máxima de pérdida de paquetes deberá ser menor a 1% medido dentro de la red de datos del proveedor de servicios [11][13].

La disponibilidad del servicio será constantemente medida, monitoreada y presentada al usuario final por parte del proveedor de servicios a través de informes mensuales.

La disponibilidad de una red con N sitios conectados es calculada mediante la siguiente formula:

$$\text{Disponibilidad} = \left(1 - \frac{(\text{Tiempo de desconexión})}{(\text{Número de Conexiones}) \times (\text{Periodo de medición})} \right) \times 100 \quad (3.1)$$

- Tiempo de desconexión.- Es la sumatoria de las horas de las averías imputables al proveedor de servicios en el periodo de un mes. No se consideran las horas de averías no imputables al proveedor de servicio, tales como averías por causa del usuario (falta de energía para los equipos, manipulación indebida de los equipos de comunicación, etc) u otras causas como robo de cables y actos de vandalismo.

- Número de Conexiones.- Cantidad de circuitos correctamente operativos considerados dentro de la solución

- Periodo de medición.- Es el tiempo del periodo de medición de la disponibilidad expresado en horas. Para una medición mensual se considera: 30 días x 24 horas.

- Para la presente solución se tienen 03 sitios geográficamente separados los cuales tendrán una disponibilidad asegurada además se tiene un sitio principal ubicado en el Datacenter el cual tendrá una mayor disponibilidad.

De acuerdo a lo descrito líneas arriba, el proveedor nos brindará una disponibilidad definida que se muestran en la tabla 3.11:

Tabla 3.11 Configuración

Local	Medio de Acceso	Tráfico	Disponibilidad (%)
Centro Educativo 1	Cobre	02 Mbps	99.95
Centro Educativo 2	Cobre	02 Mbps	99.95
Centro Educativo 3	Cobre	02 Mbps	99.95
Datacenter	Fibra	03 Mbps	99.99

3.6 Requerimientos técnicos para implementación

En esta sección se definen los requerimientos técnicos para la implementación. Se define los correspondiente a: Condiciones eléctricas, tablero de distribución, transformador de aislamiento, pozo de tierra, estabilizador / ups, voltajes de salida, condiciones ambientales, ventilación, humedad [11][13].

3.6.1 Condiciones eléctricas

Son las siguientes [1]:

- En los ambientes se deberá proporcionar al menos las siguientes condiciones eléctricas:
- Un circuito eléctrico independiente suministrará esta energía.
- Esta debe estar libre de fluctuaciones y deberá ser de 220 volt. / 60 Hertz ó –48VDC según sea el caso.
- El voltaje tierra - neutro no podrá ser superior a 0.7volts, entendiéndose que 0.7 volts son críticos.
- La impedancia no será mayor a 5 Ohms.
- Los armónicos deberán ser los mínimos permitidos.
- No podrán conectarse a este suministro herramientas eléctricas y/o que posean motores como taladros, ni tampoco está permitido utilizar esta misma red para equipos acondicionadores de clima.
- Todos los equipos deberán estar aislados galvánicamente del suministro. Los equipos necesarios para obtener este resultado serán por cuenta del cliente
- El cliente no podrá a modo particular instalar o intervenir eléctricamente los equipos bajo ningún punto de vista.

a. Tablero de distribución

Debe encontrarse empotrado a la pared, ordenado y equipado con una llave exclusivamente para los equipos de comunicaciones y computo. Las llaves deben estar debidamente identificadas y sus características dependerán de la carga para cada sistema, preferiblemente llaves térmicas para prevenir cualquier sobrecarga [1].

b. Transformador de aislamiento

En las oficinas remotas se recomienda instalar estos transformadores para evitar interferencias externas de la línea y que proporcione un punto neutro para el mejor funcionamiento de los equipos [1].

c. Pozo de tierra

Las tomas de alimentación deben estar debidamente polarizados con respecto al punto de tierra y las conexiones de los equipos a la barra de tierra deben ser directas e independientes. En caso que existan varios pozos los equipos de cómputo, comunicaciones y otros que interactúen con ellos deben estar conectados al mismo pozo. El valor del pozo de tierra no debe exceder de 5 ohm [1].

d. Estabilizador / ups

Para la sala de datos se recomienda el uso de un UPS en línea, para garantizar que el suministro eléctrico sea estable e ininterrumpido.

Para las oficinas remotas por lo general utilizan estabilizadores, pero estos no garantizan el suministro continuo solo previenen las variaciones de tensión en la línea. Es recomendable utilizar un UPS pequeño que permita proteger la información ante un corte

de energía [1].

e. Voltajes de salida

Como regla general se considerarán que las fluctuaciones no deberán superar el 0.5% de los valores nominales [1].

De no cumplirse con estas condiciones mínimas, Telefónica no puede asegurar el cumplimiento de los acuerdos de nivel de servicio comprometidos en este documento.

3.6.2 Condiciones ambientales

Los ambientes en donde se instalará los servicios deberán proporcionar al menos las siguientes condiciones ambientales, que asegurarán el correcto funcionamiento de los equipos [1]:

- Sala cerrada y libre de tránsito de personas.
- Sala con la higiene suficiente para evitar la acumulación de polvo u otros residuos que afectan la operación de los equipos.
- Espacio adecuado para maniobrar en los equipos.
- Orden razonable en el cableado para evitar desconexiones involuntarias
- Rango de temperatura adecuado para los equipos, en este caso entre 10°C y 25°C.
- Humedad relativa del aire adecuada para los equipos, en este caso entre 10% y 95%, sin condensación.
- Para la instalación de los equipos de comunicaciones (tales como modem, router, multiplexor, etc.) se debe garantizar espacio suficiente en los racks de comunicaciones.

Asimismo, los equipos de datos deben encontrarse instalados en un área razonable, permitiendo el fácil acceso por delante y por detrás para realizar las actividades de instalación, operación y mantenimiento.

a. Ventilación

Para la sala de datos se debe contar con aire acondicionado y la temperatura no debe exceder los 23°. Por lo general estas salas cuentan con un termómetro que muestra la temperatura ambiente, si es menos de 23° se considera buena, entre 23° y 25° es regular y más de 25° es mala [1].

Para las oficinas remotas el ambiente debe contar como mínimo con ventilación forzada (ventilador) o natural que permita que la temperatura en los equipos no exceda las especificaciones técnicas que son entre 0° y 35 °C.

b. Humedad

Se puede tolerar ambientes donde la humedad no se condense, es decir las partes metálicas del ambiente no deben presentar humedad en su superficie [1].

3.6.3 Condiciones para la provisión de un ingeniero residente

En un centro educativo se deberá proporcionar las siguientes condiciones para el

correcto establecimiento del Ingeniero Residente dentro de su local principal [1]:

- Ubicación idónea de fácil acceso a los equipos de comunicaciones.
- Líneas de comunicaciones (puntos de red, tomas eléctricas, etc.)
- Infraestructura necesaria (mesas, sillas, teléfonos fijos, etc.)

Además de las facilidades de comunicación con los interlocutor/es del cliente.

3.7 Aspectos complementarios de los servicios

Son: Sistema operativo del ambiente de enseñanza, aplicaciones para la enseñanza, plataforma en línea [1].

3.7.1 Sistema operativo del ambiente de enseñanza

Son: Metasys Meego, Metasys Desktop, Metasys School Server [16].

a. Metasys Meego

Es una netbook con sistema operativo que viene con varios elementos como internet, aplicaciones de ofimática y aplicaciones de multimedia exclusivos para el proceso de enseñanza.

b. Metasys Desktop

Sistema operativo basado en Linux y un grupo de aplicaciones integradas para ser usados por los docentes permitiendo un rápido acceso a recursos fundamentales del sistema.

c. Metasys School Server

Sistema operativo basado en Linux en el cual ha sido añadido una serie de servicios que son necesarios para el control, administración y monitoreo del ambiente de enseñanza. El sistema de operación del servidor ha sido específicamente diseñado para el manejo y control de cada PC dentro del ambiente de enseñanza entre principales características son:

- Sincroniza toda información de los estudiantes así como todo el material de trabajo con la información del servidor.
- Permite la definición de las restricciones y políticas de acceso para todos los PCs conectados en el ambiente de enseñanza.
- Instala nuevas versiones del sistema operativo en las PCs de los estudiantes.
- Permite la actualización del software de cada PC.
- Controla los activos del ambiente de enseñanza, prevención de robo y revender partes.
- Funciona como una compuerta para la salida a Internet.

3.7.2 Aplicaciones para la enseñanza

Son; v-Class, PolicyControl, EduSyst Desktop [16].

a. v-Class

Es un software de colaboración en clase que integra a los docentes con los

estudiantes mediante una PC permitiendo que trabajen de manera colaborativa.

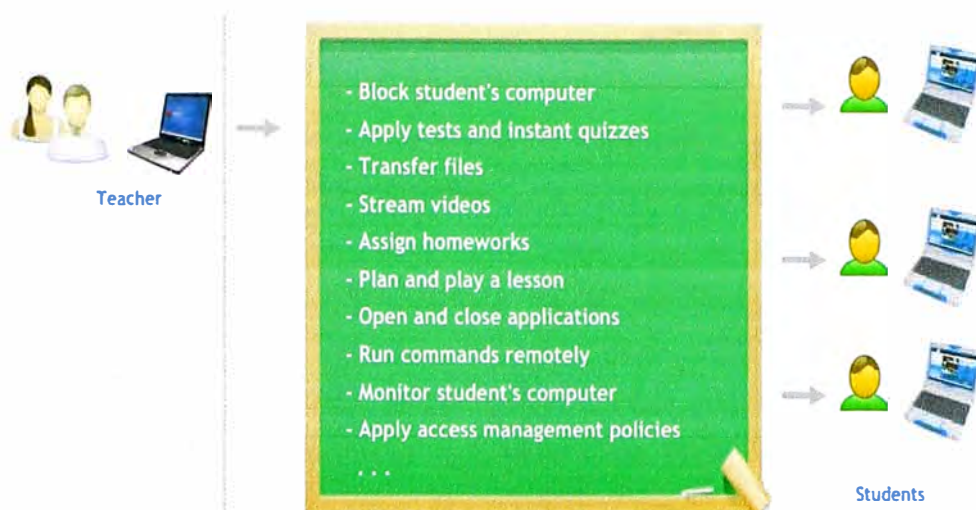


Figura 3.9 v-Class (Fuente: Fabricante)

b. PolicyControl

Una aplicación que permite la creación y modificación de políticas para configurar permisos y restricciones para el acceso a sitios de internet o aplicaciones en una PC donde la política es aplicada.

c. EduSyst Desktop

Un grupo de aplicaciones para la enseñanza y enlaces que sirven como apoyo para el desarrollo de las actividades de enseñanza tanto para los niveles de primaria y secundaria.

Los enlaces nos servirán para seleccionar el contenido de portales educativos de distintos países y lenguajes. Adicionalmente seleccionar aplicaciones en software libre pedagógico global.



Figura 3.10 EduSyst Desktop (Fuente: Fabricante)

3.7.3 Plataforma en línea

Son My Metasys, Metasys Monitor, Arquitectura Metasys [16].

a. My Metasys

Plataforma en línea que permite la venta de los productos Metasys y entrenamiento en su uso, instalación del software y paquetes de actualización.

b. Metasys Monitor

Un sistema que permite al administrador de red controlar y manejar el ambiente de información computacional.

El sistema recoleta información de las computadoras geográficamente distribuidas en la red y presentar dicha información al usuario interesado en reportes y formatos gráficos facilitando el análisis de múltiples usos de recursos

c. Arquitectura Metasys

El sistema de educación Metasys se puede dividir en varios niveles de trabajo.

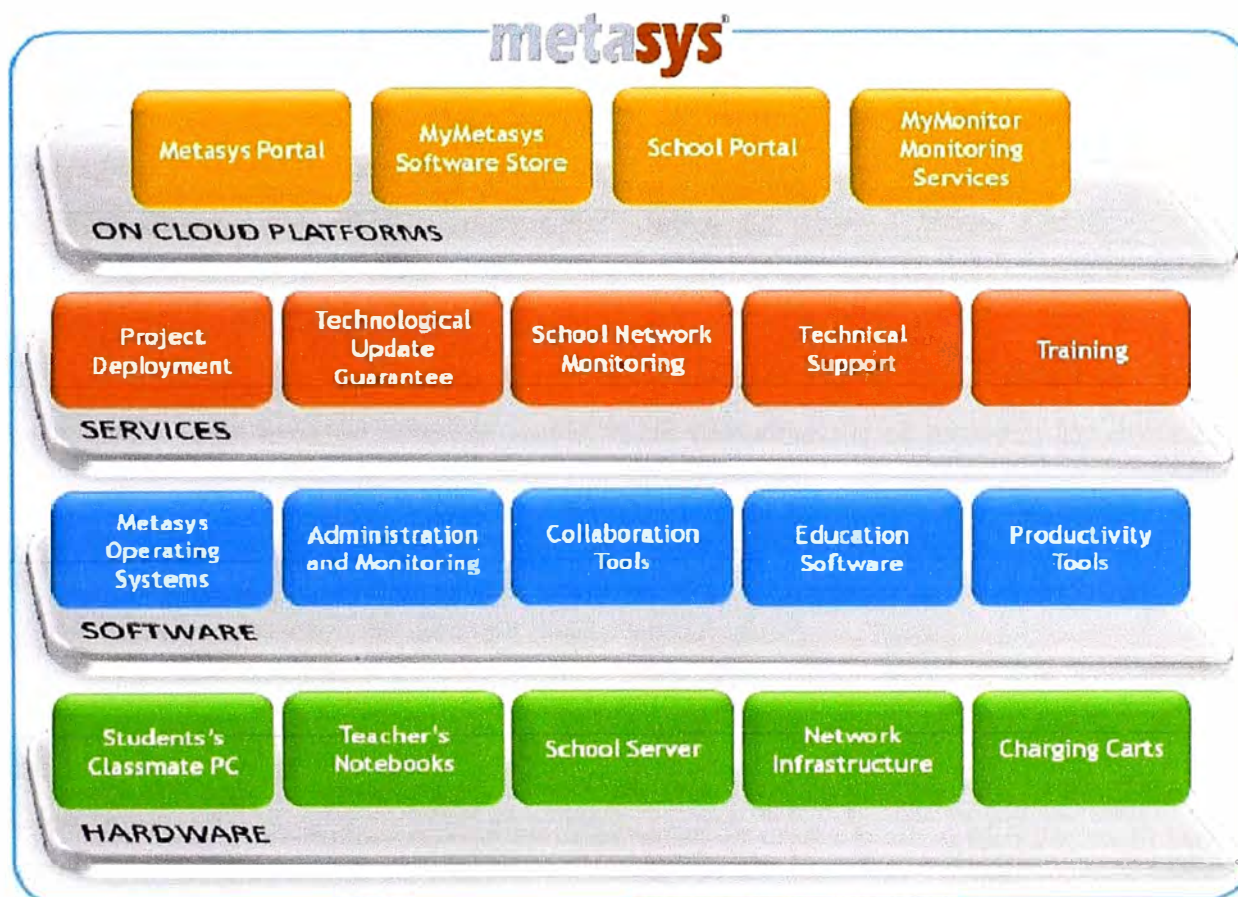


Figura 3.11 Metasys (Fuente: Fabricante)

CAPÍTULO IV COSTOS Y CRONOGRAMA

En el presente capítulo se tocan los temas involucrados al presupuesto y al cronograma del proyecto de ingeniería.

4.1 Análisis de costos

Uno de los puntos fuertes de esta solución es el ahorro en el costo de implementación ya que se hace uso de una plataforma existente y gestionada por el proveedor de servicios garantizándonos una alta disponibilidad en el servicio y el cumplimiento de las políticas de calidad de servicio. La presente solución tiene un gran impacto en el ahorro del costo de su implementación, ya que se utiliza la infraestructura de red del proveedor de servicios, en el capítulo anterior se definió las velocidades que se emplearían para la solución tanto para los servicios de multimedia y datos que son determinados por las calidades de servicio estos valores están dados en Kbps y Mbps. Debido a que el proveedor de servicios ofrece velocidades estándar se utilizarán las velocidades que cubran los requerimientos de la solución.

Para los equipos que no estén asociados a los servicios de conectividad se tendrá un costo como pago único y para los servicios de conectividad se incluyen los equipos de comunicaciones como un pago mensual o recurrente, es importante anotar que el presente proyecto considera el servicio de conectividad por un año.

En la presente solución se está considerando el costo total por los tres colegios donde incluye los equipos y los servicios a instalar, se muestra en la Tabla 4.1.

Tabla 4.1 Costo total (Fuente: Elaboración propia)

Concepto	Componente	Cantidad	P. Unitario	P. Total
Alumnos	Netbook	60	314	18840
	Classroom Manager (mini)	60	19	1140
Docente	PC Desktop	3	888	2664
	Classroom Manager (profesor)	3	200	600
Servidor en Escuela	Servidor HP	3	1380	4140
	Metasys School Server	3	285	855
Infraestructura	Switch Catalyst 2960 (24 ports)	3	1880	5640
	Polycom QDX6000	3	6800	6780
Conectividad 01 año	IP VPN 02 Mbps	36	170	6120
Total				46779

En el local del Datacenter del proveedor de servicios se alojará el servidor central de la solución en donde se habilitara los servicios de conectividad para la comunicación con las sedes remotas también en el Datacenter se habilitará la salida a internet de toda la red.

Como parte de la propuesta se considera el costo de las licencias de los programas a operar en los servidores y PCs los cuales permitirá la gestión para un correcto funcionamiento de la solución educativa, además del costo de la instalación, dichos costos se presentan en la Tabla 4.2.

Tabla 4.2 Costos por servicios en Data Center y Solución educativa (Fuente: Propia)

Concepto	Componente	Cantidad	Precio Unitario	Precio Total
Servidor Central	Servidor Central	1	314	314
	Metasys Enterprise Server	1	896	896
	Alojamiento en DataCenter	12	1200	14400
Conectividad	IP VPN 03 Mbps	12	270	3240
	Infointernet 03 Mbps	12	1200	14400
Solución Educativa	Integración de la solución educativa	1	30000	30000
Total				63250

También como parte de un mejor control y gestión de todos los equipos involucrados en la solución se considera la configuración de los aplicativos necesarios para la solución en cada PCs y servidores, estos costos se presentan en la Tabla 4.3

Tabla 4.3 Costos (Fuente: Propia)

Concepto	Componente	Cantidad	Precio Unitario	Precio Total
Alumnos	Software Antirrobo	60	1.35	81
	Software de Monitoreo	60	2.51	150.6
Docente	Software Antirrobo	3	1.35	4.05
	Software de Monitoreo	3	2.51	7.53
Servidor de Escuela	Software Antirrobo	3	215	645
	Software de Monitoreo	3	590	1770
Servidor Central	Software Antirrobo	1	1640	1640
	Software de Monitoreo	1	19580	19580
Soporte	Mesa de Ayuda	63	48	3024
Total				26902.18

4.2 Cronograma de trabajos

Las etapas implementación de la solución son mostradas en el diagrama Gantt de la Figura 4.1. Es de recalcar que los trabajos se enfocan en el verano de 2014.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Actualmente las redes MPLS de los operadores permiten por sus características que se describieron en el Capítulo III, llevar a cabo este tipo de soluciones brindando una mayor calidad en el servicio para la transmisión de audio y video así como la priorización del tráfico crítico propio de la solución educativa.
2. Al tener una plataforma ya implementada por el operador, permite que la instalación y configuración sea más sencilla de acuerdo a lo que se vio en el capítulo III.
3. Es de vital importancia la existencia de un SLA (Acuerdo de Nivel de Servicio) por parte de los proveedores de servicio donde se garantice los rangos permitidos de los parámetros de calidad como el retardo, jitter y pérdida de paquetes a fin de asegurar el correcto funcionamiento de las aplicaciones críticas y multimedia.
4. La diferencia con anteriores proyectos de esta naturaleza es que la plataforma de comunicaciones implementada se realizaba a través de conexiones de Internet por el tema de costos. Actualmente el costo por acceso VPN a través de MPLS se ha reducido, propiciando el uso de esta tecnología.
5. Esta solución incorpora los nuevos routers Cisco de segunda generación que de acuerdo al dimensionamiento que se presentó en el capítulo III nos permiten integrar diversos servicios diferenciados en un mismo equipo impactando directamente en el ahorro en equipamiento adicional para futuros servicios.

Recomendaciones

1. Es recomendable cumplir con los requerimientos técnicos mínimos tanto ambientales como eléctricos para su correcta implementación, a fin de asegurar la durabilidad de los equipos y evitar inconvenientes con los sistemas.
2. Es indispensable que los equipos portátiles tengan siempre habilitada su aplicativo de seguridad a fin de evitar sean hurtados y si fuera así, su pronta recuperación.
3. Si el número de sedes y sitios para alumnado aumenta es recomendable que se migre los enlaces de cobre de las sedes a fibra óptica a fin de aumentar la velocidad de transmisión.

ANEXO A
GLOSARIO DE TÉRMINOS

3DES	Triple data encryption standard
CIC	Centro Internacional de Control
CoS	clases de servicio
CPE	Customer Premises Equipment
CU	Currently Unused
DBW	Dedicated Bandwidth
DiffServ	Differentiated Services
DSCP	Código de Prefijo de Servicios Diferenciados
FEC	Forwarding Equivalence Class
IETF	Internet Engineering Task Force
IETF	Grupo Especial sobre Ingeniería de Internet
IP Security	IPSec
IPDV	Varianza del retardo de paquetes IP
IPER	Tasa de errores en los paquetes IP
IPLR	Tasa de pérdida de paquetes IP
IPTD	Retardo de transferencia de paquetes IP
ITU-T	International Telecommunication Union
LANs	Redes de Área Local
LDP	Label Distribution Protocol
LER	Label Edge Router
LIB	Label Information Base
LSP	Label Switched Path
LSR	Label Swtiching Router
MPLS	Multiprotocol Label Switching
PE	Provider Edge
POE	Alimentación por Ethernet
QoS	Calidad de Servicio
SBW	Statistical bandwidth
SLA	Nivel de Servicio
SP	proveedor de servicios
TDP	Tag Distribution Protocol
TE	Traffic Engineering
TIC	Tecnologías de la información y comunicación
TTL	tiempo de vida
VoIP	Voz sobre IP
VPN	Red Virtual Privada

BIBLIOGRAFÍA

- [1] Telefónica del Peru, "Proyecto de Educación para Escuelas Pacasmayo V7.0", febrero 2012
- [2] MPLS Fundamentals. Editor: Cisco Press. Estados Unidos: 2006, Ghein Luc De.
- [3] LIMARI RAMIREZ, Víctor Humberto "Tesis de Grado: Protocolos de Seguridad para Redes Privadas Virtuales (VPN)". Universidad Austral de Chile <http://cybertesis.uach.cl/tesis/uach/2004/bmfcil732p/doc/bmfcil732p.pdf>
- [4] MPLS and VPN Architectures. Editor: Cisco Press, Estados Unidos 2002.
- [5] Garcia Giron Giancarlo, Tesis de Grado: Propuesta de Migración de la Red NGN de una operadora Implementada en IP hacia MPLS, Biblioteca Pontificia Universidad Catolica del Perú http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/1063/GARCIA_GIRON_GIANCARLO_MIGRACION_NGN_HACIA_MPLS.pdf?sequence=1
- [6] MPLS-Multiprotocol Label Switching. Version 1.0 Modo de Compatibilidad , Biblioteca Pontificia Universidad Catolica del Perú
- [7] Estudio y Configuración de una VPN MPLS MP-BGP, M. J. Icaran USM España profesores.elo.utfsm.cl/~agv/elo323/2s10/project/MauricioIcaran/VPN%20publiF.doc
- [8] MPLS and VPN Architectures. Editor: Cisco Press Pepelnjak Ivan, Guichard Jim.
- [9] Servicio IP VPN International, Telefonica 2010.
- [10] Servicio Infointernet, Telefonica del Perú, http://cdn.movistar.com.pe/Content/CMS/Archivos/Documentos/9_1_4_Tarifas.pdf
- [11] Servicio IPVPN acceso dedicado, Telefonica del Perú http://cdn.movistar.com.pe/Content/CMS/Archivos/Documentos/9_1_20_Tarifas.pdf
- [12] Polycom QDX6000 Videoconferencing Equipment <http://www.polycom.com/products-services/hd-telepresence-videoconferencing/realpresence-room/realpresence-room-qdx-6000.html>
- [13] Cisco System Rotuers and Switches http://www.cisco.com/cisco/web/solutions/small_business/products/routers_switches/index.html
- [14] Metasys, Educational Solutions http://www.metasys.com.br/index.php?option=com_content&view=article&id=256&Itemid=141&lang=en
- [15] Tandberg, Videoconference Equipment http://www.vsgi.com/products/videoconferencing/tandberg/tandberg_settop_990_880_770_mxp.php
- [16] Aethra Vega X3, Conference Equipment <http://iec.psih.uaic.ro/file/usermanual/Vega%20X3%20user%20manual.pdf>