UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

REESTRUCTURACIÓN DE LA PLATAFORMA DE RED LAN
DE UNA EMPRESA CERVECERA

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

LUÍS ÁNGEL ZAMORA CONTRERAS

PROMOCIÓN
2007-1

LIMA-PERU
2011

REESTRUCTURACIÓN DE LA PLATAFORMA DE RED LAN DE UNA EMPRESA CERVECERA

A mi padre Willy y a mi madre Fátima,

por siempre creer en mi

y su apoyo constante

en mi formación y en mi vida

SUMARIO

En el presente informe se describe la reestructuración de la plataforma de red LAN de una empresa cervecera, la cual fue realizada con la finalidad de hacerla más robusta y escalable, tanto a nivel de usuarios, servicios y dispositivos.

La reestructuración de la LAN se justificaba debido a su obsolescencia. Esto impedía la eficiente implementación de nuevos servicios y satisfacer las necesidades de crecimiento a nivel de usuarios y dispositivos de red. La plataforma de red LAN contaba con switches de acceso no administrables lo que: 1) provocaba conflictos en la plataforma, 2) Hacía ineficiente el control y administración de los puntos de red, 3) Dificultaba la detección y solución de fallas

Por lo expuesto es que se decide la modernización la red LAN de la empresa cervecera asegurando: 1) La conectividad a mayor velocidad de los diversos equipos de comunicación a nivel usuario (Laptops, PCs, impresoras, scanners, etc.), 2) el acceso a recursos de red (intranet) al personal de la empresa cervecera, 3) calidad de servicio (QoS) en data, voz y video, para la implementación posterior de telefonía IP y 4) la administración y configuración de los equipos de comunicación a nivel consola o aplicativos web (Switches).

La nueva red LAN se torna más robusta al cambiar los switches de acceso por otros más modernos y al modificar la topología. La topología involucra el cambio de la estructura al incorporar switches de alta disponibilidad así cómo switches de distribución. La nueva estructura jerárquica se replica para proporcionar redundancia a la LAN.

ÍNDICE

INTRODUCCIÓN

El trabajo surge por la necesidad de contar con una red LAN moderna, para las cuatro plantas y cincuenta distribuidoras de la empresa cervecera situadas a nivel nacional, que permitiera el crecimiento a nivel de servicios, usuarios y dispositivos de red, asegurándose la robustez de las comunicaciones, una calidad de servicio de voz y datos, la administración de los dispositivos de red a nivel de consola y el acceso a intranet, con la consecuente mejora de seguridad.

El proyecto descrito planteó la reestructuración de la red LAN para todas las sedes de la empresa cervecera con una estimación de tiempo de doce meses desde la aprobación del proyecto hasta su culminación, incluyéndose el tiempo de espera para la adquisición de equipos.

Se puso como límite de inversión económica para el equipamiento (hardware y software), el cableado estructurado, el envió de los equipos a las sedes, y el traslado y viáticos de los administradores de red LAN un total máximo de 1'500,000 USD.

El proyecto se planteó, cómo una de sus metas principales, proporcionar una plataforma adecuada para hacer uso de la telefonía IP y periféricos (handheld). Sin embargo la incorporación de estos equipos eran parte de otro proyecto, que viene siendo implementado dada la finalización de los trabajos de reestructuración.

Parte también importante del proyecto de modernización de la LAN era la mejora del desempeño que se traducía en la reducción del número de fallas y así cómo de su tiempo de resolución. Para ello se considera brindar una mayor robustez la plataforma y brindar redundancia a nivel LAN con respecto a las plantas, mientras que en las distribuidoras sólo existirá la redundancia a nivel WAN, soportada por el proveedor.

La seguridad de la red a nivel usuario era primordial, por tanto se propone el cambio de los switches de acceso por switches administrables. Esto permite un mayor control por puerto de usuario, ya que se activan o desactivan los puertos, según sea la necesidad de la sede, además de establecer fácilmente reglas de acceso.

El presente informe no incluye la descripción de los trabajos realizados en cableado estructurado (sólo plantas), debido a que éstos fueron realizados por terceros aprovechando el tiempo de espera de los equipos solicitados para implementar la modernización de la LAN.

El informe se ha basado en uno de los proyectos que han sido parte del desempeño

profesional del autor por tres años en el diseño de redes.

El informe se divide en cuatro capítulos principales: 1) Planteamiento de ingeniería del problema, 2) Marco teórico conceptual, 3) Metodología para la solución del problema y finalmente 4) Cronograma y presupuesto.

En el primer capítulo se realiza el planteamiento de ingeniería del problema, describiendo el problema, el objetivo del trabajo, la evaluación y justificación del proyecto, además de la precisión de los alcances del informe. Finalmente presentar una síntesis del diseño y los trabajos realizados presentado.

El segundo capítulo se divide en cinco partes: 1) La red como plataforma (mensajes, dispositivos, medios y protocolos), 2) LAN (tecnologías y topologías), 3) Dispositivos de la Red (jerarquía de redes), 4) Switches (operaciones básicas y características), 5) los medios de red (medios de cobre y medios de fibra).

El tercer capítulo está dividido en tres secciones; primeramente se hace un análisis de la solución, estableciendo la situación previa de la empresa y las necesidades a cubrir; en esta sección se hace el dimensionamiento, selección y configuración de los dispositivos, y la formulación de la topología. La segunda sección presentará la ingeniería del proyecto, describiendo en detalle la configuración y topología para cada tipo de sede (Plantas y distribuidoras), siendo similar para cada caso. En la tercera sección se describe el equipamiento utilizado. Las plantillas de configuración de los dispositivos son parte de los anexos del informe.

En el cuarto capítulo se proporciona el cronograma de los trabajos y el presupuesto del proyecto.

Se agradece a la empresa cervecera, dueña de la infraestructura LAN, por haber posibilitado la utilización del proyecto de reestructuración para los fines académicos concernientes a este informe de suficiencia

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

En este capítulo se realiza el planteamiento de ingeniería del problema, para ello primero se describe el problema y luego se expone el objetivo del trabajo, también se evalúa el problema y se precisan los alcances del informe, para finalmente presentar una síntesis del diseño presentado.

1.1 Descripción del Problema

La obsolescencia de la plataforma de red LAN de la empresa cervecera para los nuevos servicios y necesidades a corto y largo plazo, debido a su antigüedad.

La plataforma de red era plana, esto quiere decir que sólo se contaba con los routers, y además con switches de acceso no administrables lo que, a medida que crecía la red (tanto en usuarios, servicios y dispositivos de red), provocaba conflictos en la plataforma y hacía laborioso el control y administración de los puntos de red. Esto ocasionaba la demora en la detección y solución de fallas (troubleshooting). La implementación de nuevos servicios hacía más caótica esta situación.

1.2 Objetivos del trabajo

Optimización de la plataforma de red LAN de las diferentes sedes a nivel nacional de la empresa cervecera (sedes de Lima y Plantas ubicadas en la parte Norte, Sur, y Centro de nuestro país), con proyección a soportar crecimiento global de usuarios y nuevos servicios.

Esto se logrará mediante la reestructuración de la plataforma de red LAN, la cual debe cumplir con lo siguiente:

- Conectividad a mayor velocidad de los diversos equipos de comunicación a nivel usuario, tales como Laptops, PCs, impresoras, scanners, etc.
- Acceso a recursos de red (intranet) al personal de la empresa cervecera.
- Calidad de servicio (QoS) en data, voz y video.
- Administración y configuración de los equipos de comunicación a nivel consola o aplicativos web (Switches).

1.3 Evaluación del problema

Las redes Ethernet a través del tiempo han dejado de ser solo redes para datos. Actualmente las redes Ethernet deben ser diseñadas para la convergencia de servicios

de Voz, Video y Datos.

La red LAN es un pilar fundamental para la operación exitosa de una empresa. Esto será cada vez más crítico debido a la convergencia de aplicaciones de voz, data y video sobre las redes IP.

Las distintas redes LAN de la empresa están clasificadas en dos escenarios:

- Las plantas.- Son las fábricas en donde produce y embotella la cerveza y gaseosas. Estas plantas están situadas en zonas industriales de las ciudades de Pucallpa, Arequipa, Lima y Cuzco. Las plantas no solo son centros de producción; también son centros administrativos que manejan el mercadeo, adquisición de insumos, etc., y necesitan mantener el control, seguridad y constancia de la red, para hacer uso óptimo de sus recursos.
- Distribuidoras.- (aproximadamente 50 a nivel nacional) Son centros de venta al por mayor y de distribución a zonas alejadas. Llevan el control de entrada y salida del producto y esta información, a mediano y corto plazo, sirve para que las plantas hagan una proyección de la producción que sea requerida en un mediano o largo plazo.

El personal calificado de la empresa para dar servicio a la red de cada escenario se clasifica en:

- Administradores de Red: Situados en la sede principal (Planta de Lima), encargados del monitoreo a nivel nacional así cómo el análisis y presentación de propuestas de mejora, tanto para la adquisición de equipos y de software.
- Soporte on site: Personal experto que se sitúa en las diferentes plantas del país. Este personal realiza la supervisión en su local asignado y apoyo a los administradores de red ante cualquier problema en la plataforma LAN.
- Jefes de cómputo: Personal que atiende usuarios en las distribuidoras y apoya a los administradores de red.

Las redes LAN están interconectadas mediante una WAN brindada por el proveedor de servicios de telefónica, quien administra y controla los routers a nivel nacional.

Como toda empresa, las comunicaciones son una parte esencial, tanto a nivel de datos cómo de voz. El uso de la telefonía clásica para comunicarse (llamadas larga distancia) así como de llamadas locales con los distribuidores, representaba un costo considerable. Es por ello que la restructuración de la red, para que brinde telefonía IP, reduciría enormemente los costos, al permitir una comunicación entre las sedes cómo si estuvieran en la misma localidad. La calidad de servicio (QoS) necesita no sólo de la incorporación o recambio de nuevos dispositivos sino también de la redundancia para asegurar la comunicación y su desempeño.

La administración de redes sin una estructura jerárquica adecuada y sin dispositivos

de red administrables, traían como consecuencia una pérdida de tiempo en la detección y resolución de problemas en la red, lo que afectaba directamente a la productividad de la empresa.

La reestructuración completa en las plantas y distribuidoras, era sumamente necesaria ya que la tecnología debía, no sólo actualizarse, sino proyectarse para futuro crecimiento (escalamiento).

1.4 Alcance del trabajo

El proyecto planteó la reestructuración de la red LAN para todas las sedes de la empresa cervecera; es decir las cuatro plantas y las 50 distribuidoras a nivel nacional.

Se hizo una estimación de tiempo de 12 meses desde la aprobación del proyecto hasta su culminación, lo que incluía el tiempo de espera para la adquisición de equipos.

Se puso como límite de inversión económica 1'500,000 USD. Lo que incluía el equipamiento (hardware y software), el cableado estructurado, el envió de los equipos a las sedes, además del traslado y viáticos de los administradores de red LAN.

El proyecto tiene cómo una de sus metas principales, proporcionar una plataforma adecuada para hacer uso de la telefonía IP y periféricos (handheld). La incorporación de estos equipos son parte de otro proyecto, el cual es realizado una vez finalizado el de reestructuración.

Otra meta, era la de asegurar la continuidad del servicio (desempeño), reduciendo el número de fallas y el tiempo de resolución. Se plantea entonces hacer más robusta la plataforma y brindar redundancia a nivel LAN con respecto a las plantas, mientras que en las distribuidoras sólo existirá la redundancia a nivel WAN, soportada por el proveedor.

Otra meta fue la de mejorar la seguridad de la red, a nivel usuario, para lo cual se propone el cambio de los switches de acceso por switches administrables, lo que permite tener más control por puerto de usuario, activando o desactivando los puertos, según sea la necesidad de la sede.

El presente informe no incluye la descripción de los trabajos realizados en cableado estructurado (sólo plantas), éste es efectuado por terceros (empresa calificada en cableado estructurado) durante el tiempo de espera de los equipos comprados.

1.5 Síntesis del trabajo

El proyecto de reestructuración de la plataforma de red LAN, es realizado por los administradores de red (cuatro semanas). Se evaluaron las limitaciones además de las necesidades a cubrir a mediano y corto plazo. Se diseñó la nueva topología de red LAN determinando el hardware, el software y el direccionamiento para cada dispositivo de cada sede.

Luego de la adquisición de los equipos, la cual tuvo un tiempo de espera de 4 meses,

se procedió a la programación de los dispositivos (2 semanas). Las plantillas de configuración de los dispositivos de red se diferencias en cuatro:

- Para switches de acceso.- Tanto para plantas cómo para distribuidoras. El número total de dispositivos es de 164.
- Para switches de distribución.- Sólo para las plantas de la empresa. El número total de dispositivos es de 8.
- Para switches Core.- Sólo para las plantas de la empresa. El número total de dispositivos es de 8.
- Para switches de alta disponibilidad.- Sólo para las plantas de la empresa. El número total de dispositivos es de 8.

Una vez configurados todos los dispositivos (188 equipos) éstos fueron enviados a las distintas localidades (plantas y distribuidoras) para luego ser instaladas y puestas en producción, trabajo que fue realizado por los administradores de la red LAN: el tiempo invertido para las distribuidoras fue de 17 semanas y para las plantas de 8 semanas.

La reestructuración es analizada para dos escenarios: las plantas y las distribuidoras:

1.5.1 Plantas de la empresa

La topología inicial de la red LAN, para las plantas de la empresa, no poseía switches de distribución, solamente switches de acceso (puerto de fibra) directamente conectados a un switch core de fibra, y de ahí al router. El router es administrado por el proveedor WAN. Ver Figura 1.1.

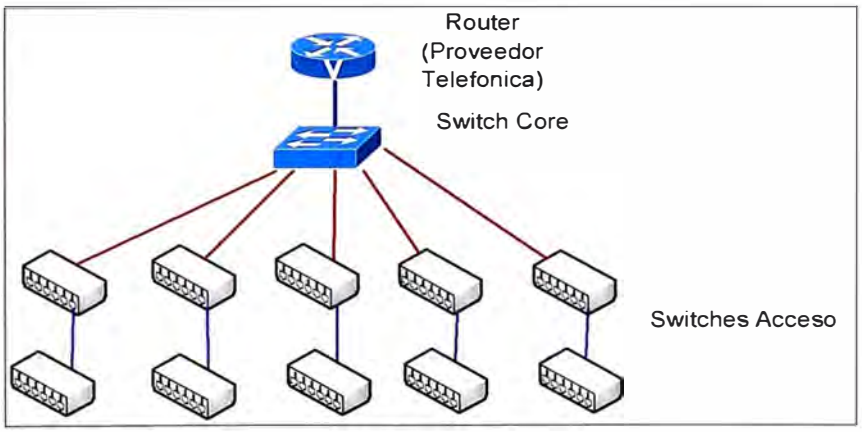

Figura 1.1 Topología inicial

La solución implementada para las plantas incorpora switchs de distribución (de fibra y cobre) además de la redundancia de los switches core. El switch redundante es conectado (de manera similar) vía un switch capa 3 al router adicional colocado por el proveedor WAN. Ver Figura 1.2.

Dado que los switches son los más susceptibles a una falla en una red LAN, fue necesario priorizar la obtención de una plataforma de red óptima. Para ello se consideró realizar la restructuración de toda la plataforma LAN, haciendo uso de equipos Cisco

(Switches Catalyst).

Par el manejo de la redundancia implementada en los switches capa 3 y core se aplica el STP (Spanning Tree Protocol) y para el balaceo de carga y enrutamiento al EIGRP (Enhanced Interior Gateway Routing Protocol), el cual es el adecuado para este tipo de topología.

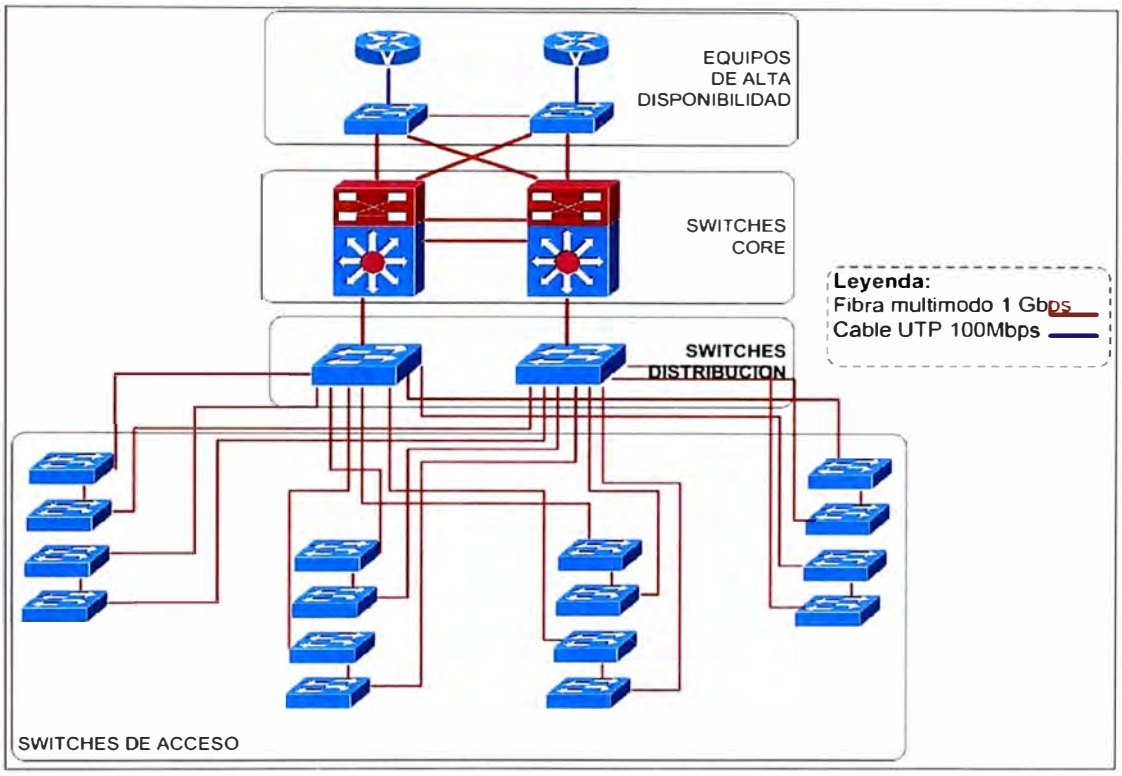

Figura 1.2 Topología implementada

1.5.2 Distribuidoras

La topología de la red LAN de las distribuidoras no ha sido modificada. Esta consiste básicamente de un router conectado a un switch de acceso y luego en cascada con otros (uno o dos) switch de acceso, según la necesidad. Ver Figura 1.3

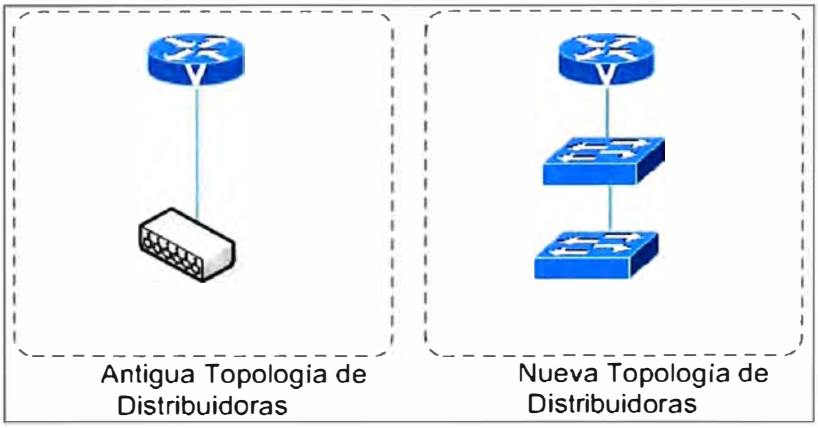

Figura 1.3 Topología Distribuidoras

La mejora en las LAN de las distribuidoras en sí ha sido el cambio y agregación de equipos, para que puedan soportar el crecimiento de usuarios y nuevos servicios de red.

CAPÍTULO II
MARCO TEÓRICO CONCEPTUAL

En el presente capítulo son expuestos los aspectos teóricos que fundamentan la solución de ingeniería, haciendo énfasis en la LAN, materia del informe de suficiencia. El capítulo está dividido en: 1) La red como plataforma, 2) Red LAN (Local Area Network), 3) Dispositivos de la Red, 4) Switches, 5) los medios de red.

2.1 La red como plataforma

Poder comunicarse en forma confiable con todos en todas partes es de vital importancia para la vida personal y comercial.

Para respaldar el envío inmediato de los millones de mensajes que se intercambian entre las personas de todo el mundo, se confía en una Web de redes interconectadas. Estas redes de información o datos varían en tamaño y capacidad, pero todas las redes tienen cuatro elementos básicos en común (Ver Figura 2.1)

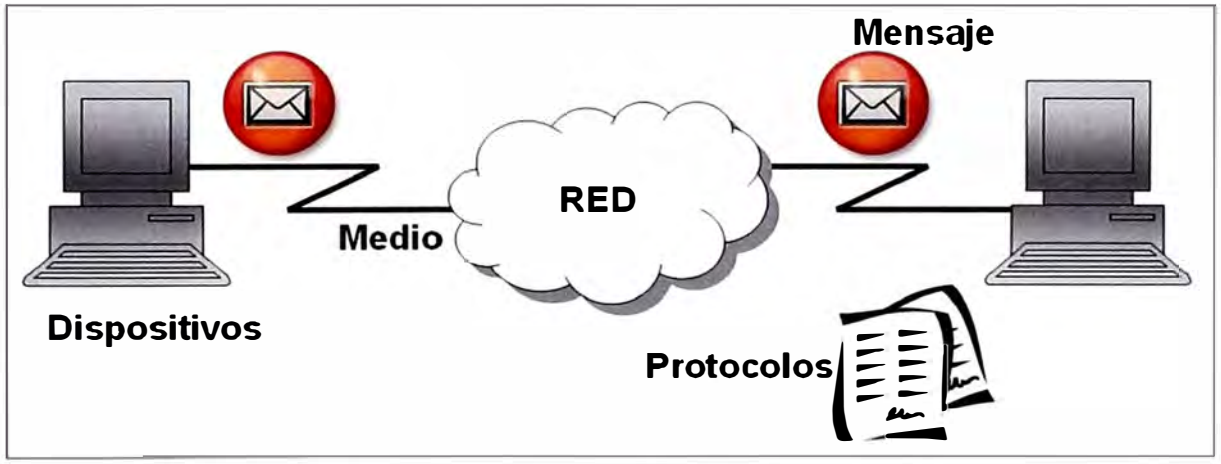

Figura 2.1 Los 4 elementos de una red: Dispositivos, medios, mensajes y reglas

2.1.1 Mensaje

Es la primera etapa del viaje desde la computadora al destino, el mensaje instantáneo se convierte en un formato que puede transmitirse en la red. Todos los tipos de mensajes tienen que ser convertidos a bits, señales digitales codificadas en binario, antes de ser enviados a sus destinos. Esto es así sin importar el formato del mensaje original: texto, video, voz o datos informáticos. Una vez que el mensaje instantáneo se convierte en bits, está listo para ser enviado a la red para su remisión.

2.1.2 Dispositivos

Una computadora es sólo un tipo de dispositivo que puede enviar y recibir mensajes

por una red. Muchos otros tipos de dispositivos pueden conectarse a la red para participar en servicios de red. Entre esos dispositivos se encuentran teléfonos, cámaras, sistemas de música, impresoras y consolas de juegos.

Además de la computadora, hay muchos otros componentes que hacen posible que los mensajes instantáneos sean direccionados a través de kilómetros de cables, cables subterráneos, ondas aéreas y estaciones de satélites que puedan existir entre los dispositivos de origen y de destino. Uno de los componentes críticos en una red de cualquier tamaño es el router.

Un router une dos o más redes, como una red doméstica e Internet, y pasa información de una red a otra. Los routers en una red funcionan para asegurar que el mensaje llegue al destino de la manera más rápida y eficaz.

2.1.3 Medios

Para enviar el mensaje instantáneo al destino, la computadora debe estar conectada a una red local inalámbrica o con cables. Las redes locales pueden instalarse en casas o empresas, donde permiten a computadoras y otros dispositivos compartir información y utilizar una conexión común a Internet.

Las redes inalámbricas hacen factible el uso de dispositivos con redes en cualquier parte, en una oficina, en una casa e inclusive al aire libre. Fuera de la casa o la oficina, la red inalámbrica está disponible en zonas activas públicas como restaurantes, empresas, habitaciones de hoteles y aeropuertos.

Muchas de las redes instaladas utilizan cables para proporcionar conectividad. Ethernet es la tecnología de red con cable más común en la actualidad. Los hilos, llamados cables, conectan las computadoras a otros dispositivos que forman las redes. Las redes con cables son mejores para transmitir grandes cantidades de datos a alta velocidad y son necesarias para respaldar multimedia de calidad profesional.

2.1.4 Protocolos

Aspectos importantes de las redes son reglas o protocolos. Estas reglas son las normas que especifican la manera en que se envían los mensajes, cómo se direccionan a través de la red y cómo se interpretan en los dispositivos de destino. Por ejemplo: en el caso de la mensajería instantánea Jabber, los protocolos XMPP (Extensible Messaging and Presence Protocol), TCP (Transmission Control Protocol) e IP (Internet Protocol) son importantes conjuntos de reglas que permiten que se realice la comunicación.

La estandarización de los distintos elementos de la red permite el funcionamiento conjunto de equipos y dispositivos creados por diferentes compañías. Los expertos en diversas tecnologías pueden contribuir con las mejores ideas para desarrollar una red eficiente sin tener en cuenta la marca o el fabricante del equipo.

2.2 Red LAN (Local Area Network)

Una LAN es una red que conecta los ordenadores en un área; las redes LAN se pueden conectar entre ellas a través de líneas telefónicas y ondas de radio. Un sistema de redes LAN conectadas de esta forma se llama una Red de área ancha o WAN (Wide Area Network) Las estaciones de trabajo y los ordenadores personales en oficinas normalmente están conectados en una red LAN, lo que permite que los usuarios envíen o reciban archivos y compartan el acceso a los archivos y a los datos.

Cada ordenador conectado a una LAN se llama un Host. Cada Host (ordenador individual) en un LAN tiene su propia CPU con la cual ejecuta programas, pero también puede tener acceso a los datos y a los dispositivos en cualquier parte en la LAN. Esto significa que muchos usuarios pueden compartir dispositivos tales como impresoras láser, así como datos. Los usuarios pueden también utilizar la LAN para comunicarse entre ellos, enviando E-mail o chateando.

Algunas de las facilidades que brinda el uso de una red local son:

- Compartir los recursos existentes: impresoras, módems, escáner, etc.
- Acceder a servicios de información internos (Intranet) y externos (Internet).
- Intercambiar archivos.
- Uso del correo electrónico.
- Permite conexiones remotas a los distintos recursos.
- Copias de seguridad centralizadas.

En las siguientes dos secciones se desarrollarán los aspectos esenciales de una LAN; es decir: 1) Las tecnologías y 2) las topologías

2.2.1 Tecnologías

Las tecnologías de mayor difusión son: a) La tecnología Token Ring y b) La tecnología Ethernet.

a. Token Ring

La Tecnología Token Ring originalmente fue desarrollada por IBM en los años 1970s, con topología lógica en anillo y técnica de acceso de paso de testigo. El primer diseño de una red de Token-Ring es atribuido a E. E. Newhall en 1969.

IBM publicó por primera vez su topología de Token-Ring en marzo de 1982, cuando esta compañía presento los papeles para el proyecto 802 del IEEE. IBM anunció un producto Token-Ring en 1984, y en 1985 éste llegó a ser un standard de ANSI/IEEE, debido al apoyo de la primera empresa informática mundial.

La red Token-Ring es una implementación del standard IEEE 802.5, en el cual se distingue más por su método de transmitir la información que por la forma en que se conectan las computadoras.

La IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), ha desarrollado una serie de estándares (IEEE 802.X) en los que se definen los aspectos físicos (cableado, topología física y eléctrica) y de control de acceso al medio de redes locales. Estos estándares se han reconocido internacionalmente (ANSI, ISO, etc.), y adoptado por ISO en una serie equivalente ISO 8802.X.

La norma 802.5 que ha realizado el IEEE define redes con anillo lógico en un anillo físico (también se puede configurar el anillo lógico sobre una topología física de estrella) y con protocolo MAC de paso de testigo (Token Ring). La norma prevé distintos niveles de prioridad (codificados mediante unos bits incluidos en el testigo). Las velocidades de transmisión normalizadas son de 1,4, 16, 20 y 40 Mbit/s (la más común es de 16 Mbit/s), existen diferentes tipos de cableado: UTP, STP y cable coaxial.

Hasta finales de 1988, la máxima velocidad permitida en este tipo de redes era de 4 Mbps, con soporte físico de par trenzado. En esa fecha se presentó la segunda generación Token Ring-II, con soporte físico de cable coaxial y de fibra óptica, y velocidades de hasta 16 Mbps. Sin embargo, las redes antiguas, con cable de par trenzado, debían recablearse si se querían utilizar las prestaciones de las de segunda generación, lo cual representa un buen ejemplo de la importancia que las decisiones sobre cableado tienen en la implantación de una red de área local.

b. Ethernet

Diseñado originalmente por Digital, Intel y Xerox por lo cual, la especificación original se conoce como Ethernet DIX. Posteriormente en 1.983, fue formalizada por el IEEE como el estándar Ethernet 802.3.

La velocidad de transmisión de datos en Ethernet es de 10Mbits/s en las configuraciones habituales pudiendo llegar a ser de 100Mbits/s en las especificaciones Fast Ethernet. Al principio, sólo se usaba cable coaxial con una topología en BUS, sin embargo esto ha cambiado y ahora se utilizan nuevas tecnologías como el cable de par trenzado (10 Base-T), fibra óptica (10 Base-FL) y las conexiones a 100 Mbits/s (100 Base-X o Fast Ethernet). La especificación actual se llama IEEE 802.3u.

Ethernet opera a través de dos capas del modelo OSI: Capa Física y Enlace de Datos

b.1 Capa Física

Implica señales, streams (corrientes continuas) de bits que se transportan en los medios, componentes físicos que transmiten las señales a los medios y distintas topologías. La Capa Física de Ethernet tiene un papel clave en la comunicación que se produce entre los dispositivos, Las características de la Capa Física no permiten el reconocimiento de quien envía o recibe información, ya que esta capa solo tiene manejo a nivel de bits, los cuales tienen solo dos estados, cero o uno. La Capa física presenta las

siguientes limitaciones:

- No se puede comunicar con capas superiores
- No pueden identificar dispositivos
- Solo reconoce streams de bits
- No puede determinar la fuente de la transmisión cuando transmite múltiples dispositivos

Las variaciones entre las familias Ethernet se dan en la capa física (Ver Tabla 2.1), donde se tienen diferentes velocidades de operación para medios de par trenzado y medios de fibra óptica:

- 10 Mbps - Ethernet 10Base-T
- 100 Mbps - Fast Ethernet
- 1000 Mbps - Gigabit Ethernet
- 10 Gbps - 10 Gigabit Ethernet

Tabla 2.1 Ethernet existentes

Tipo de Ethernet	Ancho de banda	Tipo de medio	Duplex	Distancia max.
10Base-5	10 Mbps	Coaxial thicknet	Half	500 m
10Base-2	10 Mbps	Coaxial thinnet	Half	185 m
10Base-TX	10 Mbps	UTP Cat3/Cat5	Half	100 m
100Base-TX	100 Mbps	UTP Cat5	Half	100 m
100Base-TX	200 Mbps	UTP Cat5	Full	100 m
100Base-FX	100 Mbps	Fibra multimodo	Half	400 m
100Base-FX	200 Mbps	Fibra multimodo	Full	2 Km.
1000Base-T	1 Gbps	UTP Cat5e/Cat6	Full	100 m
1000Base-SX	1 Gbps	Fibra multimodo	Full	550 m
1000Base-LX	1 Gbps	Fibra monomodo	Full	2 Km.
10GBase-LX4	10 Gbps	Fibra multimodo	Full	300 m
10GBase-LX4	10 Gbps	Fibra monomodo	Full	10 km
10GBase-T	10 Gbps	UTP Cat6a/Cat7	Full	100 m

b.2 Capa Enlace de Datos

Las subcapas de enlace de datos (MAC y LLC) contribuyen significativamente a la compatibilidad de tecnología y la comunicación con la PC.

La subcapa de Control de Acceso al Medio o MAC (Medium Access Control) se ocupa de los componentes físicos que se utilizarán para comunicar la información y prepara los datos para transmitirlos a través de los medios. La subcapa Control de Enlace Lógico o LLC (Logical Link Control) sigue siendo relativamente independiente del equipo físico que se utilizará para el proceso de comunicación.

La Capa de enlace de datos presenta las siguientes ventajas:

- Se conecta con las capas superiores mediante control de enlace lógico (LLC).
- Utiliza esquemas de direccionamiento para identificar dispositivos

- Utiliza tramas para organizar los bits en grupos
- Utiliza control de acceso al medio (MAC) para identificar fuentes de transmisión.

A continuación es explicado con mayor detalle estas dos subcapas:

i) Control de enlace lógico (LLC)

Es el que permite la conexión con las capas superiores; cómo fue mencionado, Ethernet separa las funciones de la capa de Enlace de datos en dos subcapas diferenciadas: la subcapa Control de enlace lógico (LLC) y la subcapa Control de acceso al medio (MAC). Las funciones descritas en el modelo OSI para la capa de Enlace de datos se asignan a las subcapas LLC y MAC. La utilización de dichas subcapas contribuye notablemente a la compatibilidad entre diversos dispositivos finales.

Para Ethernet, el estándar IEEE 802.2 describe las funciones de la subcapa LLC y el estándar 802.3 describe las funciones de la subcapa MAC y de la capa física (Ver Figura 2.2). El Control de enlace lógico se encarga de la comunicación entre las capas superiores y el software de red, y las capas inferiores, que generalmente es el hardware. La subcapa LLC toma los datos del protocolo de la red, que generalmente son un paquete Ipv4, y agrega información de control para ayudar a entregar el paquete al nodo de destino. La Capa 2 establece la comunicación con las capas superiores a través del LLC.

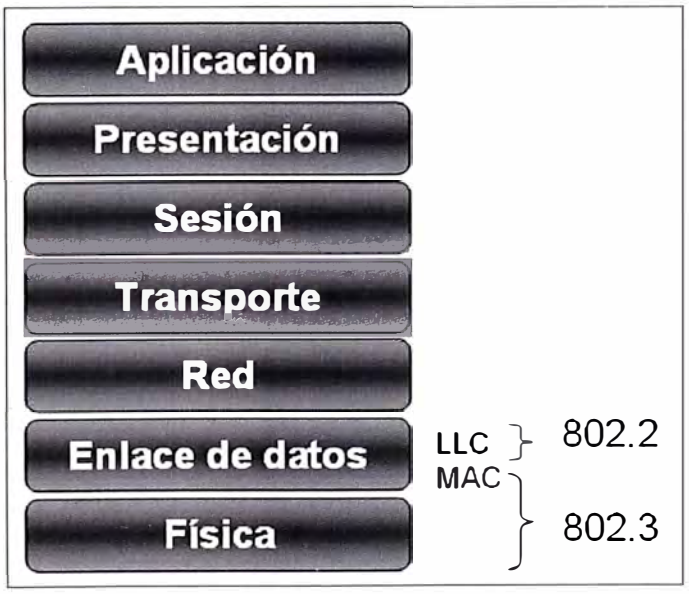

Figura 2.2 Ethernet en el modelo OSI

El LLC se implementa en el software y su implementación depende del equipo físico. En una computadora, el LLC puede considerarse como el controlador de la Tarjeta de interfaz de red (NIC). El controlador de la NIC (Tarjeta de interfaz de red) es un programa que interactúa directamente con el hardware en la NIC para pasar los datos entre los medios y la subcapa de Control de Acceso al medio (MAC).

El control de enlace lógico (LLC) coloca información en la trama que identifica qué

protocolo de capa de red está siendo utilizado por la trama. Esta información permite que varios protocolos de la Capa 3, tales como IP e IPX, utilicen la misma interfaz de red y los mismos medios.

ii) El control de acceso al medio (MAC)

Proporciona a la capa de enlace de datos el direccionamiento y la delimitación de datos de acuerdo con los requisitos de señalización física del medio y al tipo de protocolo de capa de enlace de datos en uso.

El MAC es el mecanismo encargado del control de acceso de cada estación al medio. El MAC puede realizarse de forma distribuida cuando todas las estaciones cooperan para determinar cuál es y cuándo debe acceder a la red. También se puede realizar de forma centralizada utilizando un controlador. Si más de un dispositivo realiza una transmisión simultáneamente, las señales físicas colisionan y la red debe recuperarse para que pueda continuar la comunicación.

La subcapa MAC controla la colocación de tramas en los medios y el retiro de tramas de los medios. Como su nombre lo indica, se encarga de administrar el control de acceso al medio. Esto incluye el inicio de la transmisión de tramas y la recuperación por fallo de transmisión debido a colisiones.

Las técnicas de control de acceso al medio

Las técnicas de control de acceso al medio pueden ser síncronas o asíncronas. Las síncronas hacen que la red se comporte como de conmutación de circuitos, lo cuál no es recomendable para LAN y WAN. Las asíncronas son más aceptables ya que las LAN actúan de forma impredecible y por tanto no es conveniente el mantenimiento de accesos fijos. Las asíncronas se subdividen en 3 categorías: rotación circular, reserva y competición. Como serán descritas a continuación.

- Rotación circular: se va rotando la oportunidad de transmitir a cada estación, de forma que si no tiene nada que transmitir, declina la oferta y da paso a la siguiente estación. La estación que quiere transmitir, sólo se le permite una cierta cantidad de datos en cada turno. Este sistema es eficiente cuando casi todas las estaciones quieren transmitir algo, de forma que el tiempo de transmisión se reparte equitativamente. Pero es ineficiente cuando sólo algunas estaciones son las que desean transmitir, ya que se pierde mucho tiempo rotando sobre estaciones que no desean transmitir.
- Reserva: esta técnica es adecuada cuando las estaciones quieren transmitir un largo periodo de tiempo, de forma que reservan ranuras de tiempo para repartirse entre todas las estaciones.
- Competición: en este caso, todas las estaciones que quieren transmitir compiten para poder hacerlo (el control de acceso al medio se distribuyen entre todas las estaciones).

Son técnicas sencillas de implementar y eficientes en bajas cargas pero muy ineficientes para cargas altas (cuando hay muchas estaciones que quieren el acceso y además transmiten muchos datos).

Trama Ethernet

En la Capa de Enlace se recibe la Unidad de Data de Protocolo de la Capa de Red (PDU). La estructura de la trama de Ethernet agrega encabezados y tráilers a la PDU para encapsular el mensaje que se envía. Una trama Ethernet se compone de los siguientes campos (Figura 2.3):

Figura 2.3 Campos de trama Ethernet

- Preámbulo: Este campo tiene una extensión de 7 bytes que siguen la secuencia.
- Inicio. Es un campo de 1 byte con la secuencia <<10101011>>, que indica que comienza la trama.
- Dirección de destino: Es un campo de 2 o 6 bytes que contiene la dirección del destinatario. Aunque la norma permite las dos longitudes para este campo, la utilizada en la red de 10 Mbps es la de 6 bytes. Esta dirección puede ser local o global. Es local cuando la dirección sólo tiene sentido dentro de la propia red, y suele estar asignada por el administrador de red.
- Una dirección global (dirección MAC o dirección Ethernet) es única para cada tarjeta de red.
- Dirección de origen: Es semejante al campo de dirección de destino, pero codifica la dirección MAC de la estación que originó la trama, es decir, de la tarjeta de red de la estación emisora.
- Campo Longitud/Tipo: (2 bytes) define la longitud exacta del campo Datos de la trama. Esto se utiliza posteriormente como parte de la FCS para garantizar que el mensaje se reciba adecuadamente. En este campo debe ingresarse una longitud o un tipo. Sin embargo, sólo uno u otro podrá utilizarse en una determinada implementación. Si el objetivo del campo es designar un tipo, el campo Tipo describe qué protocolo se implementa. El campo denominado Longitud/Tipo sólo aparecía como Longitud en las versiones anteriores del IEEE y sólo como Tipo en la versión DIX. Estos dos usos del campo se combinaron oficialmente en una versión posterior del IEEE, ya que ambos usos eran comunes. El campo Tipo de la Ethernet II se incorporó a la actual definición de

trama del 802.3. La Ethernet II es el formato de trama de Ethernet que se utiliza en redes TCP/IP. Cuando un nodo recibe una trama, debe analizar el campo Longitud/Tipo para determinar qué protocolo de capa superior está presente. Si el valor de los dos octetos es equivalente a 0x0600 hexadecimal o 1536 decimal o mayor que éstos, los contenidos del campo Datos se codifican según el protocolo indicado.

- Encabezado y Datos: Los campos Datos y Relleno (de 46 a 1500 bytes) contienen los datos encapsulados de una capa superior, que es una PDU de Capa 3 genérica o, con mayor frecuencia, un paquete IPv4. Todas las tramas deben tener al menos 64 bytes de longitud. Si se encapsula un paquete pequeño, el Pad se utiliza para aumentar el tamaño de la trama hasta alcanzar este tamaño mínimo.
- Secuencia de verificación de trama: (FCS) (4 bytes) se utiliza para detectar errores en la trama. Utiliza una comprobación cíclica de redundancia (CRC). El dispositivo emisor incluye los resultados de una CRC en el campo FCS de la trama. El dispositivo receptor recibe la trama y genera una CRC para detectar errores. Si los cálculos coinciden, significa que no se produjo ningún error. Los cálculos que no coinciden indican que los datos cambiaron y, por consiguiente, se descarta la trama (Figura 2.4). Un cambio en los datos podría ser resultado de una interrupción de las señales eléctricas que representan los bits.

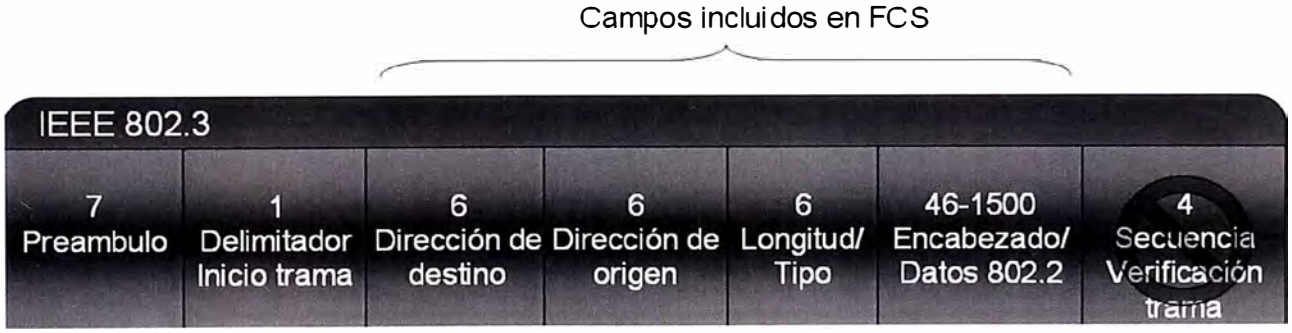

Figura 2.4 Secuencia de verificación de trama

2.2.2 Topologías de la Red LAN

La topología se refiere a la forma en que están interconectados los distintos equipos (nodos) de una red. Un nodo es un dispositivo activo conectado a la red, como un ordenador o una impresora. Un nodo también puede ser dispositivo o equipo de la red como un concentrador, conmutador o un router.

Las topologías de red más usadas son: Anillo, Bus y Estrella, y serán descritas a continuación.

a. Anillo

Topología en la que los ordenadores o nodos están enlazados formando un círculo a través de un mismo cable (Figura 2.5). Las señales circulan en un solo sentido por el círculo, regenerándose en cada nodo. En la práctica, la mayoría de las topologías lógicas

en anillo son en realidad una topología física en estrella.

b. Bus

Una topología de bus consiste en que los nodos se unen en serie con cada nodo conectado a un cable largo o bus, formando un único segmento (Figura 2.6). A diferencia del anillo, el bus es pasivo, no se produce regeneración de las señales en cada nodo. Una rotura en cualquier parte del cable causará, normalmente, que el segmento entero pase a ser inoperable hasta que la rotura sea reparada. Como ejemplos de topología de bus tenemos 10BASE-2 y 10BASE-5.

c. Estrella

Lo más usual en ésta topología es que en un extremo del segmento se sitúe un nodo y el otro extremo se termine en una situación central con un concentrador. La principal ventaja de este tipo de red es la fiabilidad, dado que si uno de los segmentos tiene una rotura, afectará sólo al nodo conectado en él. Otros usuarios de los ordenadores de la red continuarán operando como si ese segmento no existiera. 10BASE-T Ethernet y Fast Ethernet son ejemplos de esta topología. Figura 2.7

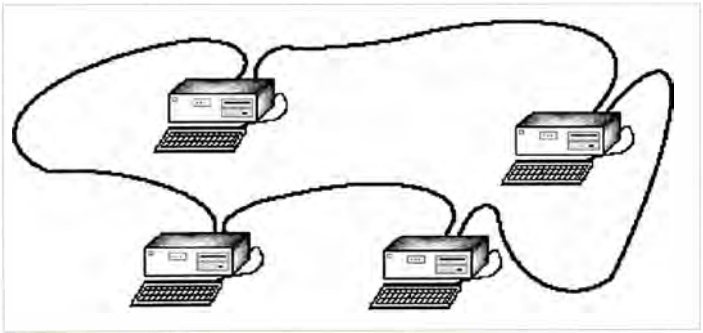

Figura 2.5 Topología Anillo

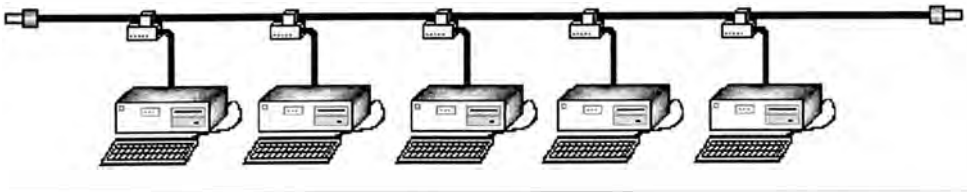

Figura 2.6 Topología Bus

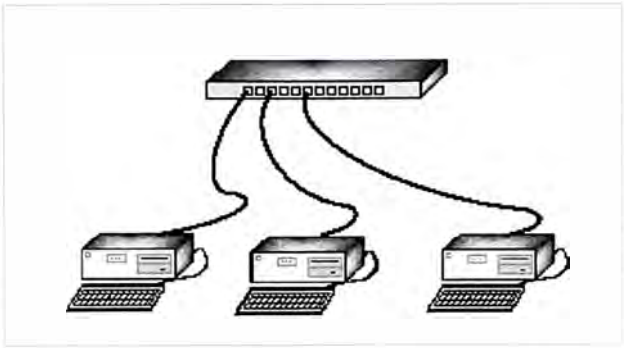

Figura 2.7 Topología estrella

2.3 Dispositivos de la Red

Los dispositivos de red para proporcionar conectividad y para trabajar detrás de escena y garantizar que los datos fluyan a través de la red conectan los hosts individuales a la red y pueden conectar varias redes individuales para formar una internetwork. (Figura 2.8).

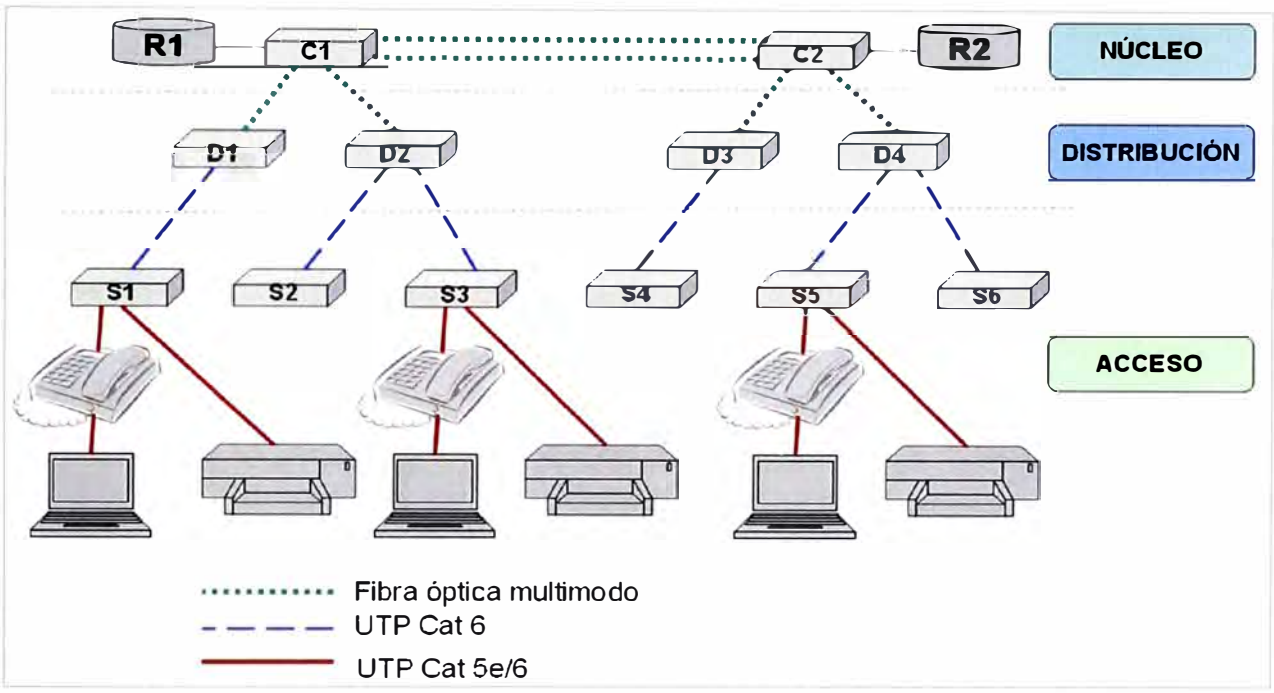

Figura 2.8 Dispositivos en una Red Lan y medios comunes

Los siguientes son ejemplos de dispositivos de red:

- Dispositivos de acceso a la red (hubs, switches y puntos de acceso inalámbricos),
- Dispositivos de internetworking (routers),
- servidores de comunicación y módems, y
- Dispositivos de seguridad (firewalls).

La administración de datos mientras fluyen a través de la red también es una función de los dispositivos de red. Estos dispositivos utilizan la dirección host de destino, conjuntamente con información sobre las interconexiones de la red, para determinar la ruta que deben tomar los mensajes a través de la red.

Los dispositivos de red realizan las siguientes funciones:

- Regenerar y retransmitir señales de datos,
- Mantener información sobre qué rutas existen a través de la red y de la internetwork,
- Notificar a otros dispositivos los errores y las fallas de comunicación,
- Direccionar datos por rutas alternativas cuando existen fallas en un enlace,
- Clasificar y direccionar mensajes según las prioridades de QoS (calidad de servicio), y
- Permitir o denegar el flujo de datos en base a configuraciones de seguridad.

Para una gestión eficiente, una LAN se estructura de manera jerárquica, en la que los

switches poseen características adecuadas a la capa en la que trabajan (núcleo o core, distribución y acceso). La LAN básicamente es gestionada por switches (S1, D1, C1), el router es un dispositivo para internetworking, es decir que permite que distintas LANS puedan comunicarse entre si. Los switchs serán desarrollados en la siguiente sección

Gran parte de la Ethernet moderna utiliza switches para los dispositivos finales y opera en full duplex. Los switches brindan mucho más throughput (volumen de trabajo o de información que fluye a través de un sistema) que los hubs (Concentradores) y aumentan el rendimiento tan notablemente. La pertinencia de usar un hub en vez de un switch se debe a tres razones:

- **Disponibilidad**: los switches de LAN no se desarrollaron hasta comienzos de la década de 1990 y no estuvieron disponibles hasta mediados de dicha década. Las primeras redes Ethernet utilizaban hubs de UTP y muchas de ellas continúan funcionando hasta el día de hoy.
- **Económicas**. En un principio, los switches resultaban bastante costosos. A medida que el precio de los switches se redujo, la utilización de hubs disminuyó y el costo es cada vez menos un factor al momento de tomar decisiones de implementación.
- **Requisitos**: Las primeras redes LAN eran redes simples diseñadas para intercambiar archivos y compartir impresoras. Para muchas ubicaciones, las primeras redes evolucionaron hasta convertirse en las redes convergentes de la actualidad, lo que originó una necesidad imperante de un mayor ancho de banda disponible para los usuarios individuales. En algunos casos, sin embargo, será suficiente con un hub de medios compartidos y estos productos permanecen en el mercado.

2.4 Switches

Los switches son los dispositivos que se emplean y se recomiendan para las LAN actuales, permiten la segmentación de las LAN en distintos dominios de colisión. Cada puerto del switch implica un dominio de colisión distinto y brinda la integridad del ancho de banda al Host conectado a dicho puerto. Figura 2.9

Figura 2.9 Switchs Catalyst

Los switches pueden operar en modo half duplex y full duplex, cuando está operando en el modo half duplex, las colisiones quedan limitadas al nodo o nodos conectados al puerto del switch, para lo cual el método de control de acceso al medio CSMA/CD estará activo.

En las redes modernas, las conexiones son full duplex, esto implica que las conexiones troncales entre switches, conexiones con otros dispositivos como APs (puntos de acceso inalámbricos), routers, PCs, etc., son full duplex y el método de control de acceso al medio quedará desactivado, porque no habrá colisiones.

El switch administra la información a nivel de tramas; para tomar una decisión de reenvío de trama lee la dirección MAC destino y busca en una tabla interna o tabla MAC el puerto donde tiene que ser enviada esa trama para que llegue a su destino.

2.4.1 Operaciones básicas

Son aprendizaje, actualización, inundación, reenvío selectivo y filtrado; son explicados a continuación.

a. Aprendizaje

La tabla MAC debe llenarse con las direcciones MAC asociadas a sus puertos correspondientes. Cuando una trama llega al switch por uno de sus puertos, se graba la dirección MAC Origen de dicha trama y se asocia al puerto por donde llegó, este paso se repite para cada puerto del switch hasta llenar la tabla.

b. Actualización

Cada entrada MAC aprendida en la tabla MAC tiene un temporizador en reversa, normalmente de 300 segundos, que se utiliza para eliminar entradas antiguas, cuando el temporizador llega a cero, se volverá a actualizar la próxima ves que el switch reciba una trama del nodo por el mismo puerto.

c. Inundación

El switch realizará una inundación, lo que significa que enviará la trama por todos los puertos menos por el cual fue recibido, esto sucede cuando no sabe a que puerto de salida corresponde el envío de la trama porque no tiene la entrada del destino en su tabla MAC.

d. Reenvío selectivo

Si el switch tiene una la entrada destino de la trama que recibe entonces realizará un reenvío selectivo al puerto correspondiente.

e. Filtrado

En algunos casos la trama no se reenvía, se filtra. Esto sucede cuando al analizar la MAC destino de la trama, se encuentra que está dirigida a un Host cuya dirección MAC está asociada al mismo puerto por donde llegó la trama.

2.4.2 Características

Los switches, básicamente son dispositivos de capa de enlace, ya que administran la información a nivel de tramas; limitan los dominios de colisión pero expanden el dominio de Broadcast. Esto significa que al recibir una trama con una dirección MAC Broadcast, reenviarán la trama por todos sus puertos, menos por el cual fue recibido. Esta característica permite el funcionamiento de diversas aplicaciones a los nodos de la red, cómo por ejemplo, el uso del Protocolo de Solicitud de Dirección o ARP (Address Resolution Protocol) que sirve para solicitar la dirección MAC de algún otro nodo, para que sea posible enviarle una trama; otra aplicación conocida es el uso del Protocolo de Configuración Dinámica de Host o DHCP (Dynamic Host Configuration Protocol), que se usa cuando un Host de la red requiere que un servidor le asigne una configuración IP para acceder a los servicios de la red.

También hay switches de propiedades avanzadas que analizan, no solo la trama, también pueden analizar el paquete IP y tomar decisiones de envío en base a la información de IP destino. Estos switches son llamados Switches Multicapa.

a. Factores de forma de los switches

Son las características claves de un switch, como por ejemplo, si tiene la opción PoE, de la denominación en ingles Power Over Ethernet, si es de configuración fija o modular, si es apilable o no es apilable o el grosor medido en bastidores.

b. Switches de configuración fija

A este tipo de switches no es posible agregarle mayores características de las que originalmente ya vienen, por ejemplo si se adquiere un switch fijo de 24 puertos FastEthernet y se requiere posteriormente añadir un puerto para conexión de fibra, no será posible ya que no tiene ranuras para aceptar ningún otro puerto o módulo de ampliación. En redes de alta densidad de puntos de red, es preferible optar por switches modulares.

c. Switches modulares

Estos Switches ofrecen mayor flexibilidad, el tamaño del chasis va directamente ligado al número de tarjetas en línea que puedan agregarse, las tarjetas en línea son las que contienen los puertos.

d. Switches apilables

Los switches apilables pueden conectarse con un cable especial backplane. Se pueden apilar hasta nueve switches de forma redundante y todos operan como si fueran un solo switch, sin tener que gastar puertos de red para su interconexión. La redundancia da confiabilidad, en caso una de las conexiones backplane caiga. Estas conexiones backplane, por lo general, son más veloces que los puertos de línea.

e. Rendimiento

Al seleccionar un switch, se debe tener en cuenta la densidad de puertos del switch, tasa de reenvío y agregado de ancho de banda.

f. Densidad de puerto

Es el número de puertos disponibles en un switch único. Las altas densidades de puerto permiten mejor uso del espacio y la energía. Con switches modulares y con el agregado de tarjetas de línea se puede lograr una alta densidad de puerto.

g. Velocidades de envío

Las tasas de envío definen la capacidad de procesamiento del switch por estimación de la cantidad de datos que puede procesar por segundo. Al adquirir un switch, es importante saber este parámetro, ya que si la velocidad de reenvío es muy baja, el switch no trabajará a la velocidad completa de cable en todos los puertos al mismo tiempo. La velocidad de cable es la velocidad que cada puerto puede lograr.

h. Agregado de enlaces

Es la propiedad que permite establecer dos o más enlaces operando como si fuera un solo enlace, lo cual produce un aumento del ancho de banda de enlace. Las aplicaciones de agregado de enlace se dan para mitigar los cuellos de botella. Los enlaces troncales de la red que no se dan abasto para el tráfico que fluye por ellos pueden apoyarse en los agregados de enlace, siempre y cuando se tengan puertos disponibles. En el caso de los Switches Catalyst CISCO con puertos Gigabit, se pueden establecer agregados de enlace hasta de 8 puertos, lo cual permite un ancho de banda de 8 Gbps.

i. Switches PoE

Power over Ethernet permite que un switch provea energía a un dispositivo por el cableado de red existente. Con esta característica se suelen alimentar de energía teléfonos IP y APs, por lo que no es necesario preocuparse por tener tomas de energía cerca a estos dispositivos en la instalación; solo basta que el cable de red pueda llegar al dispositivo. Se debe tener en cuenta que la característica PoE eleva el precio del switch, por lo que se debe justificar esta funcionalidad en la red.

j. Funciones de capa 3

Un Switch de Capa 3 tiene todos los niveles de control y seguridad con los que un ruteador normalmente cuenta. Existen mecanismos de seguridad para prevenir que un usuario indeseado se conecte a la red, incluso a nivel físico.

Estos switches pueden filtrar información no deseada incluso de los usuarios que tienen permitido el acceso a la red, para prevenir ataques a servidores, bases de datos, o proteger aplicaciones con ciertos niveles de seguridad. También cuentan con mecanismos de protección para evitar que un usuario no deseado pueda infiltrarse a la

configuración del switch.

Un Switch de Capa 3 cuenta con la suficiente "inteligencia" para interactuar con el tráfico que va o viene de la Internet, y participa con ella en el manejo eficiente de los diferentes tipos de tráfico como Voz sobre IP por ejemplo, que ya es una realidad. Un switch de Capa 2 simplemente no tiene nada que hacer al respecto. Además, a un Switch de Capa 3 se le pueden agregar funcionalidades que van más allá de la Capa 3, como Server Load Balancing, por ejemplo. Un Switch de Capa 3 tiene la capacidad para distinguir cuando los puertos donde se conectan los servidores de la empresa están, ocupados, saturados o caídos, de tal manera que pude reenviar eficientemente el tráfico y las peticiones de los usuarios de la red, hacia aquellos puertos que puedan responder.

Un Switch de Capa 2, no entiende este concepto y en el caso de que se presente esta situación, no hacen más que reintentar y retransmitir, generando más tráfico y empeorando la situación. La tendencia tecnológica es así como eventualmente los Switches de Capa 2, remplazaron a los concentradores (HUB), los nuevos mecanismos de conmutación en Capa 3, están sustituyendo a los switches de Capa 2, por sus rendimientos, sus altas funcionalidades, sus mecanismos redundantes y de tolerancia a fallas, su mejor control y su escalabilidad. Eventualmente una empresa que requiera de nuevas aplicaciones, que demande comunicación hacia y de la Internet, y que requiera de altos mecanismos de seguridad, tendrá que migrar hacia la conmutación de Capa 3. La funcionalidad Capa 3 del Switch nivel 3, es ideal para las oficinas pequeñas o medianas, sucursales, escuelas y universidades con grupos de trabajo segmentados.

Los Beneficios clave del switch de Capa 3 son:

- Facilidad de uso: Fácil despliegue y mantenimiento debido a su enrutamiento dinámico, que actualiza automáticamente la red Capa 3 sin intervención manual,
- Rendimiento: Switches Capa 3 con velocidad alámbrica, con conexiones 10/100 para computadora de escritorio, diseñadas para conectividad de alto rendimiento. La asignación de prioridades para los paquetes ofrece el rendimiento óptimo para aplicaciones de tiempo real, como voz y video,
- Escalabilidad: Soporta hasta 2,000 rutas externas, permitiendo su escalamiento a medida que crece la red,
- Seguridad: Mejora la seguridad con registro en la red basado en normas, ACL (Listas de Control de Acceso), encriptación Secure Shell y Secure Sockets Layer, y
- Costo Total de Propiedad: Solución de bajo costo optimizada para lugares de borde de grupos de trabajo.

k. Características del switch en la capa de acceso

Se le llama switch de acceso a todo switch que facilita la conexión de nodo final,

nodos finales, como PCs, teléfonos IP, cámaras IP y APs. Teniendo en cuenta los factores de forma, rendimiento y funcionalidad, analicemos ahora otras características de hardware y de configuración indispensables para nuestro diseño, como la velocidad de los puertos, seguridad de puerto, soporte de VLANs y calidad de servicio o QoS.

l. Seguridad de puerto

La seguridad de puerto permite asegurar que uno o un grupo de nodos seleccionados puedan conectarse a un puerto. Por ejemplo, si se configuran los puertos de un switch con seguridad de puerto, se asocian las direcciones de un nodo o un grupo de nodos a cada puerto y solo se permite el acceso a la red a estos nodos asociados. En caso un nodo no asociado intente ingresar a la red por uno de los puertos, el switch detecta la intrusión y el puerto cae eléctricamente, haciendo necesaria la intervención del administrador del switch para reactivarlo.

m. VLANs

Una VLAN es una subred lógica. En un switch se pueden crear muchas VLAN y cada una es un dominio de Broadcast. De esta forma, se puede separar el tráfico de áreas en una empresa; esto permite el mejor manejo y administración del ancho de banda. Una aplicación común en redes actuales, es separar el tráfico de voz en una VLAN llamada VLAN de voz: el tráfico de datos estará separado del tráfico de voz, el cual es muy sensible a los retardos.

n. Velocidad de puerto

Teniendo en cuenta los requisitos de rendimiento, los puertos de switch de acceso comercial son Fast Ethernet y Gigabit Ethernet. Para aplicaciones de telefonía IP y tráfico de datos, es suficiente con puertos Fast Ethernet que permiten una tasa de 100 Mbps, pero en caso se requiera un mayor rendimiento se opta por Gigabit Ethernet que permite hasta 1000 Mbps. El uso de velocidades más altas de puerto también eleva el costo del switch.

o. QoS

Significa Calidad de Servicio.Una red convergente admite tráfico de voz, video y datos, para lo cual los switches de acceso deben admitir QoS para poder diferenciar y priorizar cierto tráfico. Por ejemplo, con QoS, el switch puede brindar prioridad al paso del tráfico de voz en los enlaces troncales, minimizando su retardo.

p. Spanning Tree protocol

Es un protocolo de red de nivel dos (nivel de enlace de datos) de la capa OSI. Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (usados en el sistema desarrollado para garantizar la disponibilidad de las conexiones). El protocolo Spanning Treee permite a los dispositivos

de interconexión la activación o desactivación automática de los enlaces de conexión, garantizando que la topología está libre de bucles. Este propotocllo es transparente a las estaciones de usuario.

q. EIGRP

De sus siglas en inglés (Enhanced Interior Gateway Routing Protocol),. El Protocolo de enrutamiento de gateway interior mejorado es un protocolo (Cisco Systems) de enrutamiento híbrido; ofrece algoritmos mejorados de vector de distancias y del estado de enlace. Este protocolo es avanzado y se basa en las características asociadas a los protocolos del estado de enlace. EIGRP reúne las funcionalidades de actualizaciones parciales y la detección de vecinos. EIGRP es más fácil de configurar que otros protocolos. Este protocolo mejora la convergencia y opera con mayor eficiencia que otros protocolos lo que permite que una red tenga una arquitectura mejorada.

2.5 Los medios de red

La comunicación a través de una red es transportada por un medio. El medio proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino.

Las redes modernas utilizan principalmente tres tipos de medios para interconectar los dispositivos y proporcionar la ruta por la cual pueden transmitirse los datos. Estos medios son:

- hilos metálicos dentro de los cables (Cables UTP),
- Fibras de vidrio o plásticas (cable de fibra óptica), y
- Transmisión inalámbrica.

La codificación de señal que se debe realizar para que el mensaje sea transmitido es diferente para cada tipo de medio. En los cables UTP los datos se codifican dentro de impulsos eléctricos que coinciden con patrones específicos. Las transmisiones por fibra óptica dependen de pulsos de luz, dentro de intervalos de luz visible o infrarroja. En las transmisiones inalámbricas, los patrones de ondas electromagnéticas muestran los distintos valores de bits.

Los diferentes tipos de medios de red tienen diferentes características y beneficios. No todos los medios de red tienen las mismas características ni son adecuados para el mismo fin. Los criterios para elegir un medio de red son:

- La distancia en la cual el medio puede transportar exitosamente una señal,
- El ambiente en el cual se instalará el medio,
- La cantidad de datos y la velocidad a la que se deben transmitir, y
- El costo del medio y de la instalación.

2.5.1 Medios de cobre

El medio más utilizado para las comunicaciones de datos es el cableado que utiliza

alambres de cobre para señalizar bits de control y datos entre los dispositivos de red. El cableado utilizado para las comunicaciones de datos generalmente consiste en una secuencia de alambres individuales de cobre que forman circuitos que cumplen objetivos específicos de señalización.

Otros tipos de cableado de cobre, conocidos como cables coaxiales, tienen un conductor simple que circula por el centro del cable envuelto por el otro blindaje, pero está aislado de éste. El tipo de medio de cobre elegido se especifica mediante el estándar de la capa física necesario para enlazar las capas de Enlace de datos de dos o más dispositivos de red. Ver Figura 2.10.

Estos cables pueden utilizarse para conectar los Hosts de una LAN a los dispositivos intermedios, como routers o switches. Los cables también se utilizan para conectar dispositivos WAN a un proveedor de servicios de datos, como una compañía telefónica. Cada tipo de conexión y sus dispositivos complementarios incluyen requisitos de cableado estipulados por los estándares de la capa física.

Los medios de red generalmente utilizan conectores y tomas. Estos elementos ofrecen conexión y desconexión sencillas. Además, puede utilizarse un único tipo de conector físico para diferentes tipos de conexiones. Por ejemplo, el conector RJ-45 se utiliza ampliamente en las LAN con un tipo de medio y en algunas WAN con otro tipo.

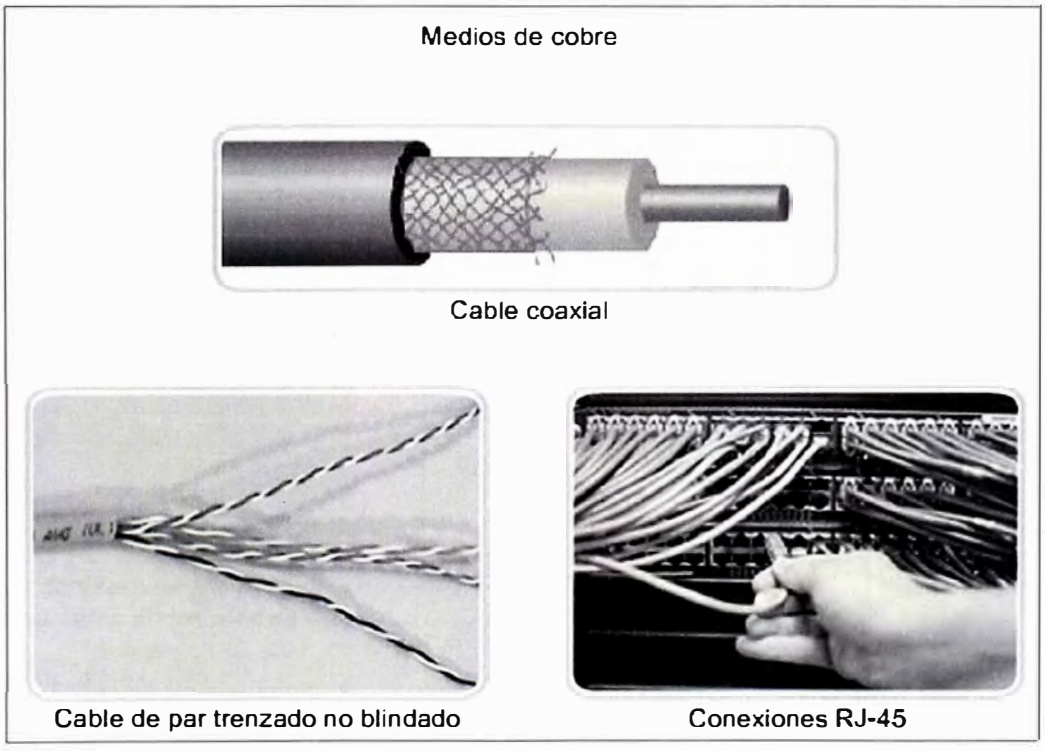

Figura 2.10 Tipos de cables Cobre

A continuación se desarrollarán los siguientes aspectos referidos a los medios de cobre: Interferencia de señal externa, Cable de par trenzado no blindado, estándares de cableado UTP, tipos de cable UTP, seguridad de los medios de cobre, y conectores

comunices de medios de cobre

a. Interferencia de señal externa

Los datos se transmiten en cables de cobre como impulsos eléctricos. Un detector en la interfaz de red de un dispositivo de destino debe recibir una señal que pueda decodificarse exitosamente para que coincida con la señal enviada. Los valores de voltaje y sincronización en estas señales son susceptibles a la interferencia o "ruido" generado fuera del sistema de comunicaciones. Estas señales no deseadas pueden distorsionar y corromper las señales de datos que se transportan a través de los medios de cobre. Las ondas de radio y los dispositivos electromagnéticos como luces fluorescentes, motores eléctricos y otros dispositivos representan una posible fuente de ruido (Figura 2.11).

Los tipos de cable con blindaje o trenzado de pares de alambre están diseñados para minimizar la degradación de señales debido al ruido electrónico. La susceptibilidad de los cables de cobre al ruido electrónico también puede estar limitada por:

- La selección del tipo o categoría de cable más adecuado para proteger las señales de datos en un entorno de networking determinado.
- El diseño de una infraestructura de cables para evitar las fuentes de interferencia posibles y conocidas en la estructura del edificio.
- La utilización de técnicas de cableado que incluyen el manejo y la terminación apropiados de los cables.

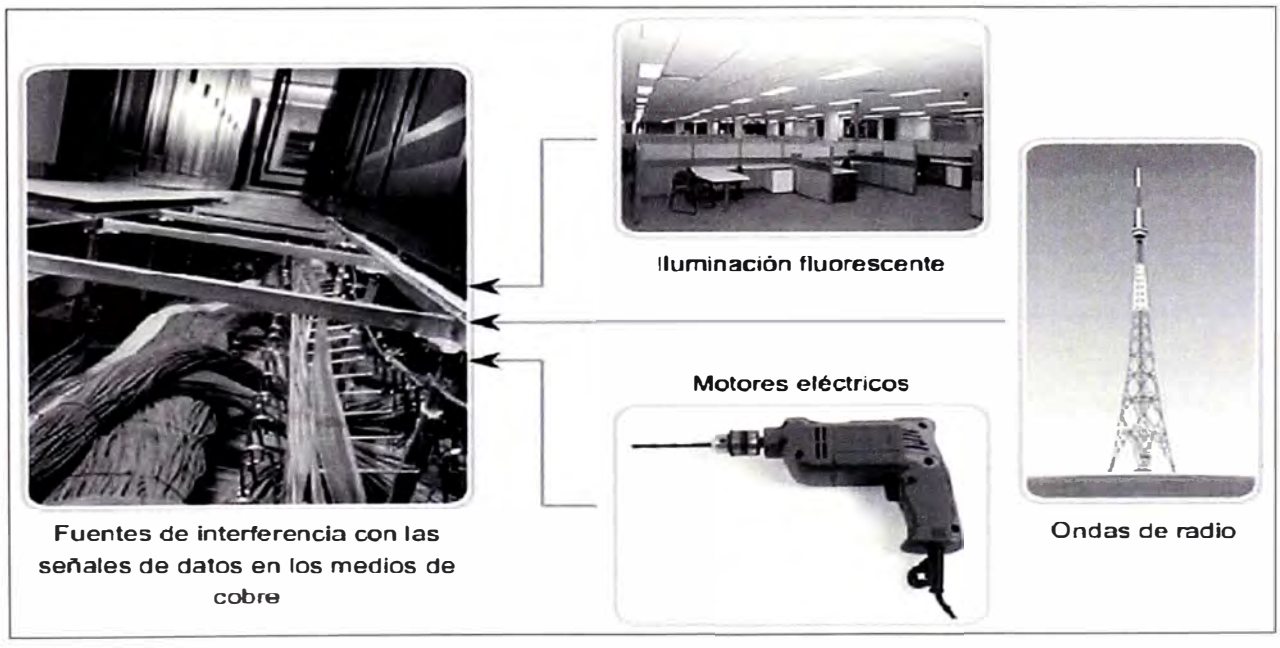

Figura 2.11 Causas de interferencia externa con los medios de cobre

b. Cable de par trenzado no blindado (UTP)

El cableado de par trenzado no blindado (UTP), como se utiliza en las LAN Ethernet, consiste en cuatro pares de alambres codificados por color que han sido trenzados y cubiertos por un revestimiento de plástico flexible (Figura 2.12).

El trenzado cancela las señales no deseadas. Cuando dos alambres de un circuito eléctrico se colocan uno cerca del otro, los campos electromagnéticos externos crean la misma interferencia en cada alambre. Los pares se trenzan para mantener los alambres lo más cerca posible.

Cuando esta interferencia común se encuentra en los alambres del par trenzado, el receptor los procesa de la misma manera pero en forma opuesta. Como resultado, las señales provocadas por la interferencia electromagnética desde fuentes externas se cancelan de manera efectiva.

Este efecto de cancelación ayuda además a evitar la interferencia proveniente de fuentes internas denominada crosstalk, el cual se define cómo la interferencia ocasionada por campos magnéticos alrededor de los pares adyacentes de alambres en un cable. Cuando la corriente eléctrica fluye a través de un alambre, se crea un campo magnético circular a su alrededor.

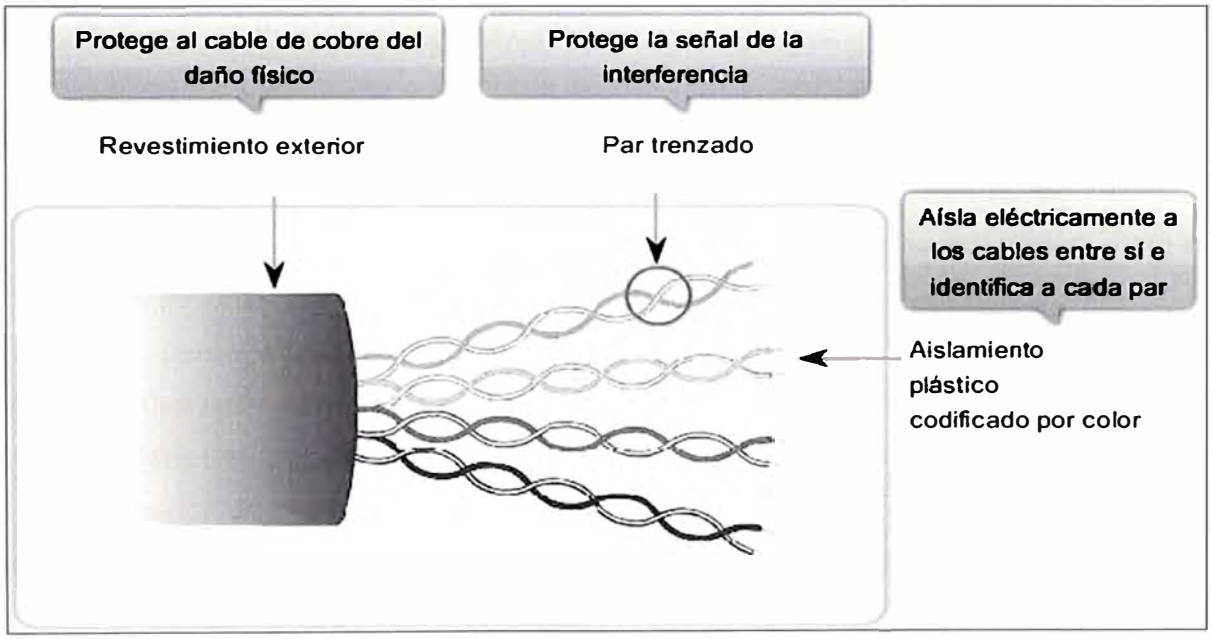

Figura 2.12 Cable de par trenzado no blindado (UTP)

Cuando la corriente fluye en direcciones opuestas en los dos alambres de un par, los campos magnéticos, como fuerzas equivalentes pero opuestas, producen un efecto de cancelación mutua. Además, los distintos pares de cables que se trenzan en el cable utilizan una cantidad diferente de vueltas por metro para ayudar a proteger el cable de la crosstalk entre los pares.

c. Estándares de cableado UTP

El cableado UTP que se encuentra comúnmente en el trabajo, las escuelas y los hogares cumple con los estándares estipulados en conjunto por la Asociación de las Industrias de las Telecomunicaciones (TIA) y la Asociación de Industrias Electrónicas (EIA). TIA/EIA-568A estipula los estándares comerciales de cableado para las

instalaciones LAN y es el estándar de mayor uso en entornos de cableado LAN. Algunos de los elementos definidos son:

- Tipos de cables
- Longitudes de los cables
- Conectores
- Terminación de los cables
- Métodos para realizar pruebas de cable

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) define las características eléctricas del cableado de cobre. IEEE califica el cableado UTP según su rendimiento. Los cables se dividen en categorías según su capacidad para transportar datos de ancho de banda a velocidades mayores.

Por ejemplo, el cable de Categoría 5 (Cat5) se utiliza comúnmente en las instalaciones de FastEthernet 100BASE-TX. Otras categorías incluyen el cable de Categoría 5 mejorado (Cat5e) y el de Categoría 6 (Cat6).

Los cables de categorías superiores se diseñan y fabrican para admitir velocidades superiores de transmisión de datos.

A medida que se desarrollan y adoptan nuevas tecnologías Ethernet de velocidades en gigabits, Cat5e es el tipo de cable mínimamente aceptable en la actualidad. Cat6 es el tipo de cable recomendado para nuevas instalaciones edilicias.

Algunas personas conectan redes de datos utilizando los sistemas telefónicos existentes. Generalmente, el cableado de estos sistemas es algún tipo de UTP de categoría inferior en comparación con los estándares actuales de Cat5+.

La instalación de cableado menos costoso pero de calificación inferior resulta poco útil y limitada. Si se decide adoptar posteriormente una tecnología LAN más rápida, es posible que se requiera el reemplazo total de la infraestructura del cableado instalado.

d. Tipos de Cable UTP

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

Según las diferentes situaciones, es posible que los cables UTP necesiten armarse según las diferentes convenciones para los cableados.

Esto significa que los alambres individuales del cable deben conectarse en diferentes órdenes para distintos grupos de pins en los conectores RJ-45.

A continuación se mencionan los principales tipos de cables que se obtienen al utilizar convenciones específicas de cableado:

- Cable directo y cable cruzado de Ethernet, cable de Consola

Es posible que la utilización de un cable de conexión cruzada o de conexión directa en forma incorrecta entre los dispositivos no dañe los dispositivos pero no se producirá la conectividad y la comunicación entre los dispositivos. Éste es un error común de laboratorio. Si no se logra la conectividad, la primera medida para resolver este problema es verificar que las conexiones de los dispositivos sean correctas.

e. Seguridad de los medios de cobre

Se clasifican en dos:

e.1 Peligro por electricidad:

Uno de los posibles problemas de los medios de cobre es que los alambres de cobre pueden conducir la electricidad de manera no deseada. Debido a este problema, el personal y el equipo podrían estar sujetos a diferentes peligros por electricidad.

Un dispositivo de red defectuoso podría conducir la corriente al chasis de otros dispositivos de red. Además, el cableado de red podría representar niveles de voltaje no deseados cuando se utiliza para conectar dispositivos que incluyen fuentes de energía con diferentes potenciales de conexión a tierra.

Estos casos son posibles cuando el cableado de cobre se utiliza para conectar redes en diferentes edificios o pisos que utilizan distintas instalaciones de energía. Por último, el cableado de cobre puede conducir voltajes provocados por descargas eléctricas a los dispositivos de red.

Como consecuencia, las corrientes y los voltajes no deseados pueden generar un daño a los dispositivos de red y a las computadoras conectadas o bien provocar lesiones al personal. Para prevenir situaciones potencialmente peligrosas y perjudiciales, es importante instalar correctamente el cableado de cobre según las especificaciones relevantes y los códigos de edificación.

e.2 Peligros de incendio

El revestimiento y aislamiento de los cables pueden ser inflamables o producir emanaciones tóxicas cuando se calientan o se queman. Las organizaciones o autoridades edilicias pueden estipular estándares de seguridad relacionados para las instalaciones de hardware y cableado.

f. Conectores comunes de medios de cobre

Los diferentes estándares de la capa física especifican el uso de distintos conectores. Estos estándares establecen las dimensiones mecánicas de los conectores y las propiedades eléctricas aceptables de cada tipo de implementación diferente en el cual se implementan.

Si bien algunos conectores pueden parecer idénticos, éstos pueden conectarse de manera diferente según la especificación de la capa física para la cual fueron diseñados.

El conector RJ-45 definido por ISO 8877 se utiliza para diferentes especificaciones de la capa física en las que se incluye Ethernet. Otra especificación, EIA-TIA 568, describe los códigos de color de los cables para colocar pines a las asignaciones (diagrama de pines) para el cable directo de Ethernet y para los cables de conexión cruzada.

Si bien muchos tipos de cables de cobre pueden comprarse prefabricados, en algunas situaciones, especialmente en instalaciones LAN, la terminación de los medios de cobre pueden realizarse en sitio. Estas terminaciones incluyen conexiones engarzadas para la terminación de medios Cat5 con tomas RJ-45 para fabricar patch cables y el uso de conexiones insertadas a presión en patch panels 110 y conectores RJ-45. La figura muestra algunos de los componentes de cableado de Ethernet.

2.5.2 Medios de fibra

El cableado de fibra óptica utiliza fibras de plástico o de vidrio para guiar los impulsos de luz desde el origen hacia el destino. Los bits se codifican en la fibra como impulsos de luz. El cableado de fibra óptica puede generar velocidades muy superiores de ancho de banda para transmitir datos sin procesar.

La mayoría de los estándares actuales de transmisión aún necesitan analizar el ancho de banda potencial de este medio.

a. Comparación de medios de Cobre con los medios de Fibra

Las fibras utilizadas en los medios de fibra óptica son inmunes a la interferencia electromagnética y no conduce corriente eléctrica no deseada cuando existe un problema de conexión a tierra.

Las fibras ópticas pueden utilizarse en longitudes mucho mayores que los medios de cobre sin la necesidad de regenerar la señal, ya que son finas y tienen una pérdida de señal relativamente baja. Algunas especificaciones de la capa física de fibra óptica admiten longitudes que pueden alcanzar varios kilómetros.

Algunos de los problemas de implementación de medios de fibra óptica:

- Más costoso (comúnmente) que los medios de cobre en la misma distancia (pero para una capacidad mayor)
- Se necesitan diferentes habilidades y equipamiento para terminar y empalmar la infraestructura de cables
- Manejo más cuidadoso que los medios de cobre

En la actualidad, en la mayor parte de los entornos empresariales se utiliza principalmente la fibra óptica como cableado backbone para conexiones punto a punto con una gran cantidad de tráfico entre los servicios de distribución de datos y para la interconexión de los edificios en el caso de los campus compuestos por varios edificios. Ya que la fibra óptica no conduce electricidad y presenta una pérdida de señal baja, es

ideal para estos usos.

b. Fabricación de cable de fibra óptica

Los cables de fibra óptica consisten en un revestimiento exterior de PVC y un conjunto de materiales de refuerzo que la rodean (Figura 2.13).

El revestimiento rodea la fibra de plástico o de vidrio y está diseñado para prevenir la pérdida de luz de la fibra.

Se requieren dos fibras para realizar una operación full duplex ya que la luz sólo puede viajar en una dirección a través de la fibra óptica. Los patch cables de la fibra óptica agrupan dos cables de fibra óptica y su terminación incluye un par de conectores de fibra únicos y estándares. Algunos conectores de fibra aceptan fibras receptoras y transmisoras en un único conector.

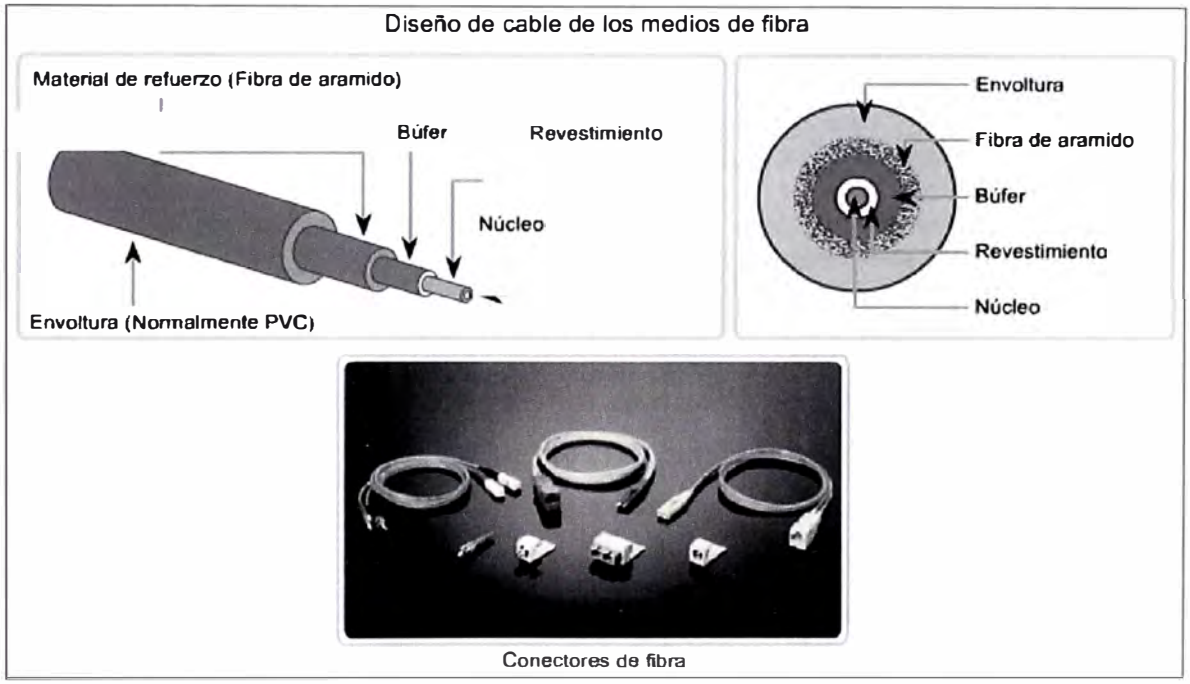

Figura 2.13 Características de los medios Físicos.

c. Fibra Multimodo y Monomodo

En términos generales, los cables de fibra óptica pueden clasificarse en dos tipos: monomodo y multimodo (Figura 2.14).

La fibra óptica Monomodo transporta un sólo rayo de luz, generalmente emitido desde un láser. Este tipo de fibra puede transmitir impulsos ópticos en distancias muy largas, ya que la luz del láser es unidireccional y viaja a través del centro de la fibra.

La fibra óptica Multimodo a menudo utiliza emisores LED que no generan una única ola de luz coherente. En cambio, la luz de un LED ingresa a la fibra multimodo en diferentes ángulos. Los tendidos extensos de fibra pueden generar impulsos poco claros al recibirlos en el extremo receptor ya que la luz que ingresa a la fibra en diferentes ángulos requiere de distintos períodos de tiempo para viajar a través de la fibra. Este

efecto, denominado dispersión modal, limita la longitud de los segmentos de fibra multimodo.

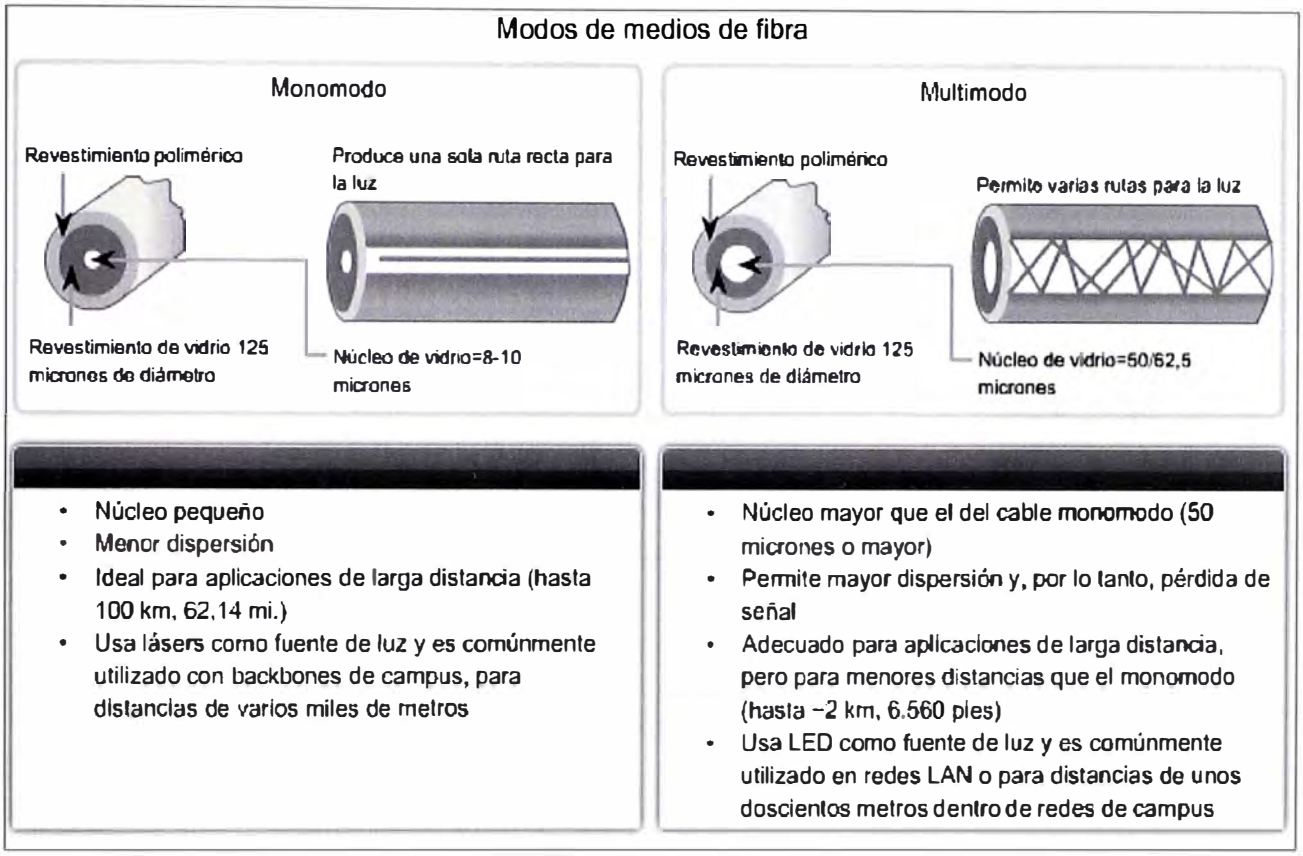

Figura 2.14 Modos de medios de fibra

La fibra multimodo y la fuente de luz del LED que utiliza resultan más económicas que la fibra monomodo y su tecnología del emisor basada en láser.

d. Conectores comunes de fibra Óptica

Los conectores de fibra óptica incluyen varios tipos. La figura muestra algunos de los tipos más comunes:

- Punta Recta (ST) (comercializado por AT&T): un conector muy común estilo Bayonet, ampliamente utilizado con fibra multimodo.
- Conector suscriptor (SC): conector que utiliza un mecanismo de doble efecto para asegurar la inserción positiva. Este tipo de conector se utiliza ampliamente con fibra monomodo.
- Conector Lucent (LC): un conector pequeño que está adquiriendo popularidad en su uso con fibra monomodo; también admite la fibra multimodo.

La terminación y el empalme del cableado de fibra óptica requiere de equipo y capacitación especiales. La terminación incorrecta de los medios de fibra óptica producen una disminución en las distancias de señalización o una falla total en la transmisión.

Tres tipos comunes de errores de empalme y terminación de fibra óptica son:

- Desalineación: los medios de fibra óptica no se alinean con precisión al unirlos.

- Separación de los extremos: no hay contacto completo de los medios en el empalme o la conexión.
- Acabado final: los extremos de los medios no se encuentran bien pulidos o puede verse suciedad en la terminación.

Se recomienda el uso de un Reflectómetro óptico de dominio de tiempo (OTDR) para probar cada segmento del cable de fibra óptica. Este dispositivo introduce un impulso de luz de prueba en el cable y mide la retrodispersión y el reflejo de la luz detectados en función del tiempo. El OTDR calculará la distancia aproximada en la que se detectan estas fallan en toda la longitud del cable.

Se puede realizar una prueba de campo al emitir una luz brillante en un extremo de la fibra mientras se observa el otro extremo. Si la luz es visible, entonces la fibra es capaz de transmitir luz. Si bien esta prueba no garantiza el funcionamiento de la fibra, es una forma rápida y económica de detectar una fibra deteriorada.

CAPÍTULO III
METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA

En el presente capítulo se expone la ingeniería del proyecto de reestructuración de la plataforma LAN. Éste ha sido desarrollado teniendo cómo referencia lo ya descrito en el capítulo 1; en las secciones 1.4 y 1.5.

El capítulo está dividido en tres secciones: Primero se hará un análisis de la solución, estableciendo la situación previa de la empresa y las necesidades a cubrir; en esta sección se hace el dimensionamiento, selección y configuración de los dispositivos, y la formulación de la topología.

A continuación se presenta la ingeniería del proyecto, describiendo en detalle la configuración y topología para cada tipo de sede (Plantas y distribuidoras), siendo similar para cada caso. Finalmente se describe el equipamiento utilizado. Las plantillas de configuración de los dispositivos serán parte de los anexos del informe.

3.1 Análisis de la solución

Se muestra en esta sección la situación previa de la empresa y las necesidades a satisfacer a mediano plazo. Esta sección es donde se dimensiona, selecciona y configura los dispositivos, además de definir la topología más óptima.

3.1.1 Descripción situacional de la topología previa a la solución

Cómo fue mencionado en anteriores capítulos, se planteó la reestructuración de la red LAN para todas las sedes de la empresa cervecera; en las cuatro plantas (Lima, Arequipa, Cuzco y Pucallpa) y las 50 distribuidoras a nivel nacional.

La reestructuración de toda la plataforma se hacía necesaria debido al incremento de servicios y usuarios que saturaban a la red LAN, además, se contemplaba usar otros servicios. Esto implicaba el uso de una red que ya no las soportaría en su estado actual debido a su antigüedad topológica y de equipamiento de comunicaciones.

Las metas impuestas para la reestructuración de la red LAN fueron:

1. Priorizar y asegurar la continuidad del servicio (desempeño), reduciendo el número de fallas y el tiempo de resolución de estas.
2. Proporcionar una plataforma que garantice un óptimo uso de la telefonía IP y de diversos periféricos (handheld, impresoras, equipos de video conferencia), sin causar problemas en la calidad del servicio, según sea la aplicación.

3. Mejorar la seguridad de la red a nivel de equipo de comunicación y usuario.

4. Permitir el crecimiento de la red sin que se vea afectado los requerimientos mencionados.

3.1.2 Alternativas de solución

Para el logro de las metas se debe seleccionar la correcta topología y equipamiento:

1. Para priorizar y asegurar la continuidad del servicio se plantea, con respecto a las plantas, una estructura más robusta y además brindar redundancia a nivel LAN; mientras que para las distribuidoras se plantea una redundancia a nivel WAN, soportada por otro proveedor.

2. Para el uso de telefonía IP y equipos periféricos, se plantea la adquisición de dispositivos de red con QoS (Calidad de Servicio). Estos dispositivos de red también deben ser capaces de proveer energía a los periféricos (incluso al teléfono IP) para que no dependan de la red eléctrica para ser energizados y puestos en producción; en sí los dispositivos de red deberán ser de tipo PoE (Power over Ethernet).

3. Mejorar la seguridad de la red a nivel de equipo de comunicación y usuario.- para lo cual se propone el cambio de lo switches de acceso por switches administrables, lo que permite tener más control por puerto de usuario, activando o desactivando los puertos, según sea la necesidad de la sede.

4. Para el escalamiento de la red LAN, se plantea que los switches a adquirir tengan suficientes puertos disponibles para una ampliación de la red a mediano y largo plazo.

3.1.3 Definición de equipamiento y topología

Esta se realiza tomando en consideración los aspectos discutidos en la sección anterior (3.1.2 Alternativas de solución). La Tabla 3.1 resume las características de los dispositivos de red para cada capa jerárquica en la topología de red implantada

Tabla 3.1 Características de los dispositivos del modelo jerárquico

	Acceso	**Distribución**	**Núcleo**
Agregado de ancho de banda	Si	Si	Si
Fast Ethernet/Gigabit Ethernet	Si		
Gigabit Ethernet/Tera Ethernet		Si	Si
Tasa alta de envío		Si	
Soporte de la capa 3		Si	Si
Seguridad del puerto	Si		
Power over Ethernet (PoE)	Si		
Calidad de servicio (QoS)	Si	Si	Si
Componentes redundantes.		Si	Si
Políticas de seguridad/listas de control de acceso		Si	
Tasa muy alta de envío			Si
VLAN	Si		

a. Robustez de plataforma

La robustez de la plataforma es lograda según se muestra en la Figura 3.1.

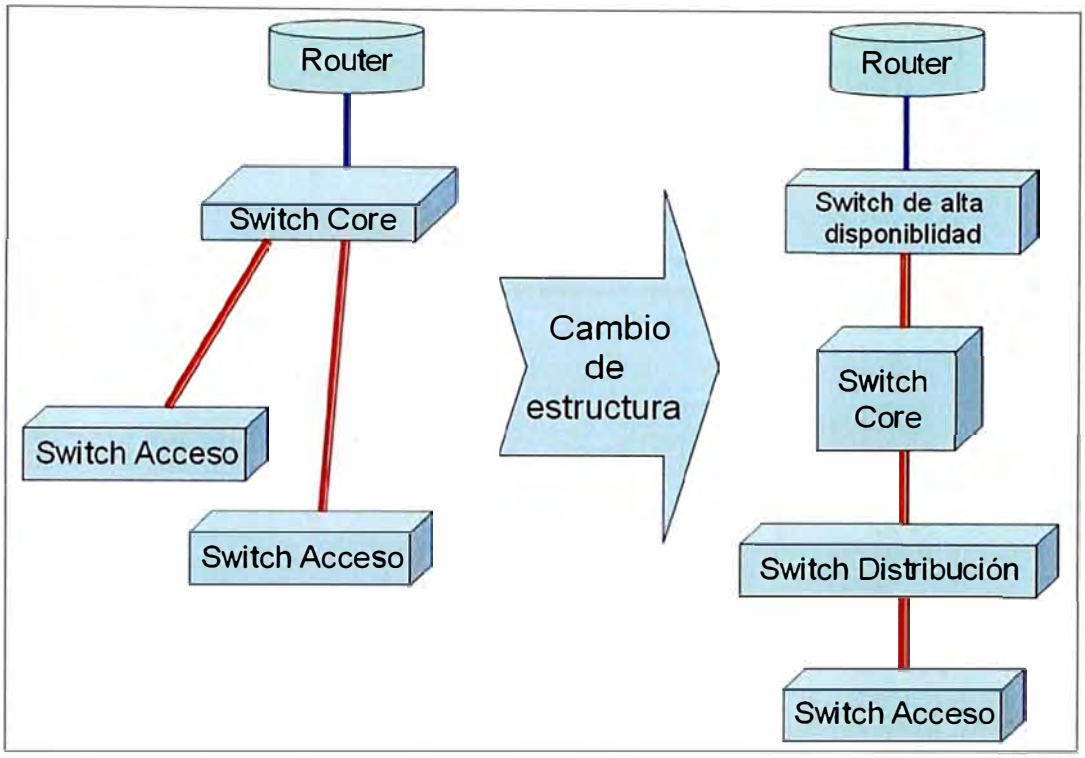

Figura 3.1 Cambio estructural de la plataforma (Plantas)

Los switches de alta disponibilidad son necesarios para poder realizar la contingencia ante la caída del router principal por medio de la creación de una VLAN e implementación del protocolo HSRP (Hot Standby Router Protocol). HSRP es un protocolo propiedad de CISCO que permite el despliegue de routers redundantes tolerantes a fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers.

Los switch core son necesarios para poder lograr una alta tasa de tráfico (throughput) para administrar el tráfico a la capa de distribución. Se requiere un switch core que ofrezca switching de múltiples capas, y que sus entradas sean de fibra.

Los switches de distribución son necesarios para segmentar grupos de trabajo y las políticas de conectividad. Los switches de distribución proveen una ruta de acceso para que los switches de acceso puedan enviar datos entre ellos.

Los switches de acceso son necesarios para conectar los equipos finales y garantizar el acceso a la red. Los switches de acceso no deben llevar a cabo el Forwarding (reenviado) de tráfico entre ellos.

Dado lo expresado líneas arriba, la robustez de la plataforma es lograda mediante el cambio estructural mostrado en la Figura 3.1.

b. La redundancia

Esta será lograda según se muestra en la Figura 3.2.

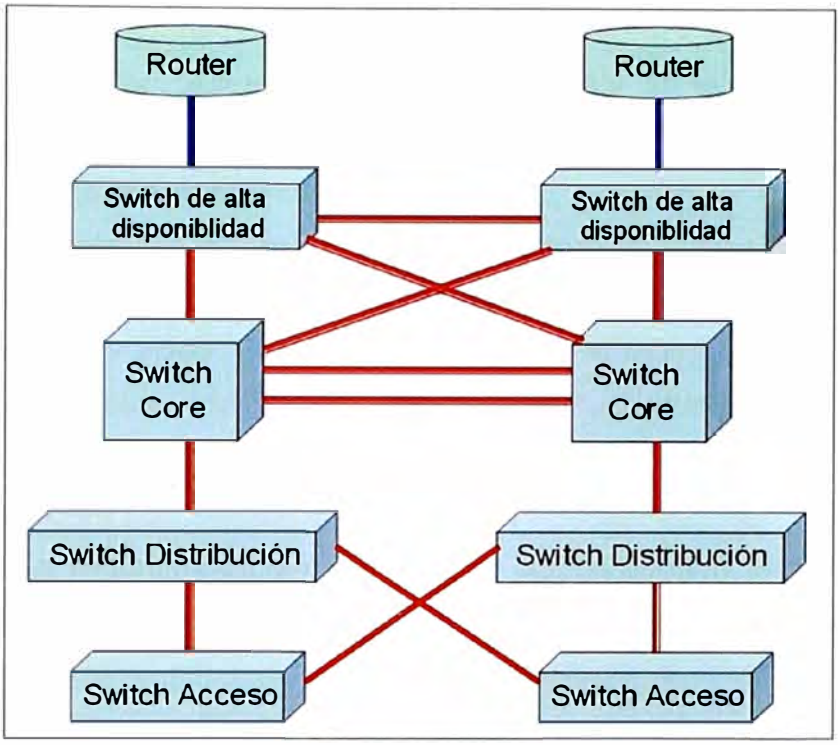

Figura 3.2 Redundancia de la plataforma de red LAN

Se puede apreciar en la Figura 3.2 que la nueva estructura ha sido duplicada y que algunos dispositivos se han enlazado entre sus similares.

Los switches de la capa de acceso se conectan con dos switches diferentes de la capa de distribución para asegurar la redundancia de la ruta. Si falla uno de los switches de la capa de distribución, el switch de la capa de acceso puede conmutar al otro switch de la capa de distribución.

Los switches Core se conectan con los switches de alta disponibilidad asegurándose la redundancia de la ruta a nivel core. Al fallar uno de los switches de la capa de core, el switch de alta disponibilidad envía la información al switch core secundario. Los switches Core se conectan entre si para darle balance a la carga de trabajo, reduciendo así la saturación en la red. Para esta disposición se decide utilizar el protocolo de enrutamiento EIGRP (Enhanced Interior Gateway Routing Protocol) al ofrecer este lo mejor de los algoritmos de vector de distancias y del estado de enlace; además se utiliza el STP (Spanning Tree Protocol) para controlar la ocurrencia de bucles infinitos.

c. Uso de telefonía IP

Para el uso de telefonía IP y equipos periféricos, los switches de acceso deben ser capaces de energizarse independientemente de la red eléctrica. Los nuevos switches de acceso deben tener PoE (Power over Ethernet) para que se energicen mediante el mismo puerto.

d. Calidad de Servicio

La calidad de servicio es implementada en los switches core y de distribución,

mediante la creación de una VLAN y lista de accesos para la administración de los equipos de comunicación. Además de crearse la VLAN de telefonía, se crean otras VLANS: de usuarios (host), de equipos de red (switches administrables) y otra para los otros periféricos (handheld, impresoras, etc.).

La prioridad de consumo de ancho de banda es establecida en el router (administrado por el proveedor WAN): 1) Datos, 2) Voz, 3) Video. La máxima prioridad la tienen las aplicaciones de audio y video. Es el core quien indica al router que tipo de información contiene el paquete (datos, voz o video), según de la VLAN que provenga el paquete. El router prioriza el tráfico según el QoS programado.

e. Seguridad de la red

Para mejorar la seguridad de la red a nivel de equipo de comunicación y usuario, se propone el cambio de switches de acceso no administrables por switches administrables, obteniéndose más control por puerto de usuario, activando o desactivando los puertos, según sea la necesidad de la sede.

En general se plantea el cambio de los dispositivos de red por unos más modernos y de mayor capacidad. Este aspecto alcanza también a la topología de las distribuidoras en donde se cambia solamente el switch no administrable por uno administrable. Esto se puede ver en la Figura 3.3.

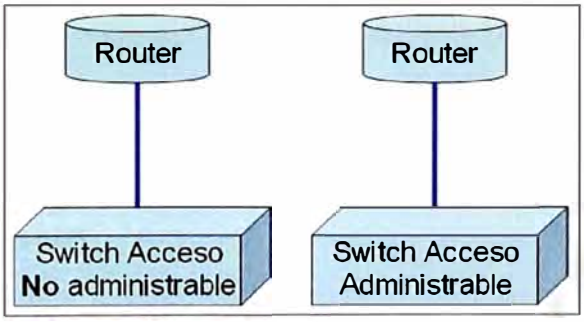

Figura 3.3 Modernización de equipos en Distribuidoras

f. Escalamiento

Para lograr el escalamiento de la red LAN, permitiendo así un crecimiento a mediano y largo plazo, se planificó que los switches a adquirir tengan suficientes puertos disponibles. La Figura 3.4 muestra un ejemplo de ello.

Se plantea la adquisición de un switch core de 12 puertos Gigabits que se conectará a un switch de distribución de 24 puertos, éste brindando conectividad a 8 switch de acceso, como estructura base. Se puede apreciar claramente que es posible soportar un crecimiento a mediano y largo plazo sin afectar el desempeño y la topología implementada. Para un escalamiento futuro, sería necesario primeramente la adquisición de más switches de acceso. Debe destacarse que, aun copando la capacidad del switch de distribución, no será necesario la adquisición de uno adicional, por cuanto los switches

de acceso permiten su conexión en cascada.

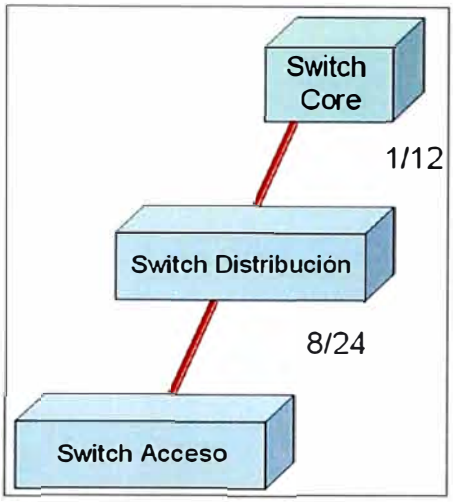

Figura 3.4 Capacidad de escalamiento

g. Conclusión

En resumen se necesitará el siguiente hardware:

- 8 switches core (dos por planta), modelo Catalyst WS-C4510R, de la marca Cisco.
- 8 switches de alta disponibilidad (dos por planta); se elige al Catalyst WS-C3560G-24TS, de la marca Cisco.
- 8 switches de distribución (dos por planta); se elige al Catalyst WS-C3750G-12SS, de la marca Cisco.
- 164 switches de acceso; se elige al Catalyst WS-C2960-24PC-L.

3.2 La ingeniería del proyecto

En esta sección se describirá en detalle la configuración y topología para cada tipo de sede (Plantas y distribuidoras), siendo similar para cada caso.

3.2.1 Redes Virtuales (VLAN)

Se definen las VLANS por su importancia en el nivel de desempeño de red:

- VLAN 1: Usuarios de área administrativa.
- VLAN 2: Usuarios de área de envasado.
- VLAN 3: Usuarios de área de distribución de materiales.
- VLAN 4: Usuarios de área de planta y manufactura.
- VLAN 5: Telefonía IP.
- VLAN 6: Administración de la red.
- VLAN 7: Periféricos (impresoras, fax, etc.).
- VLAN 8: Video cámaras.
- VLAN 10: Servidores

3.2.2 Topología

La Figura 3.5 muestra el esquema final simplificado, la Figura 3.6 el esquema parcial de la Sede Ate, y la Figura 3.7 el esquema total detallado WAN/LAN

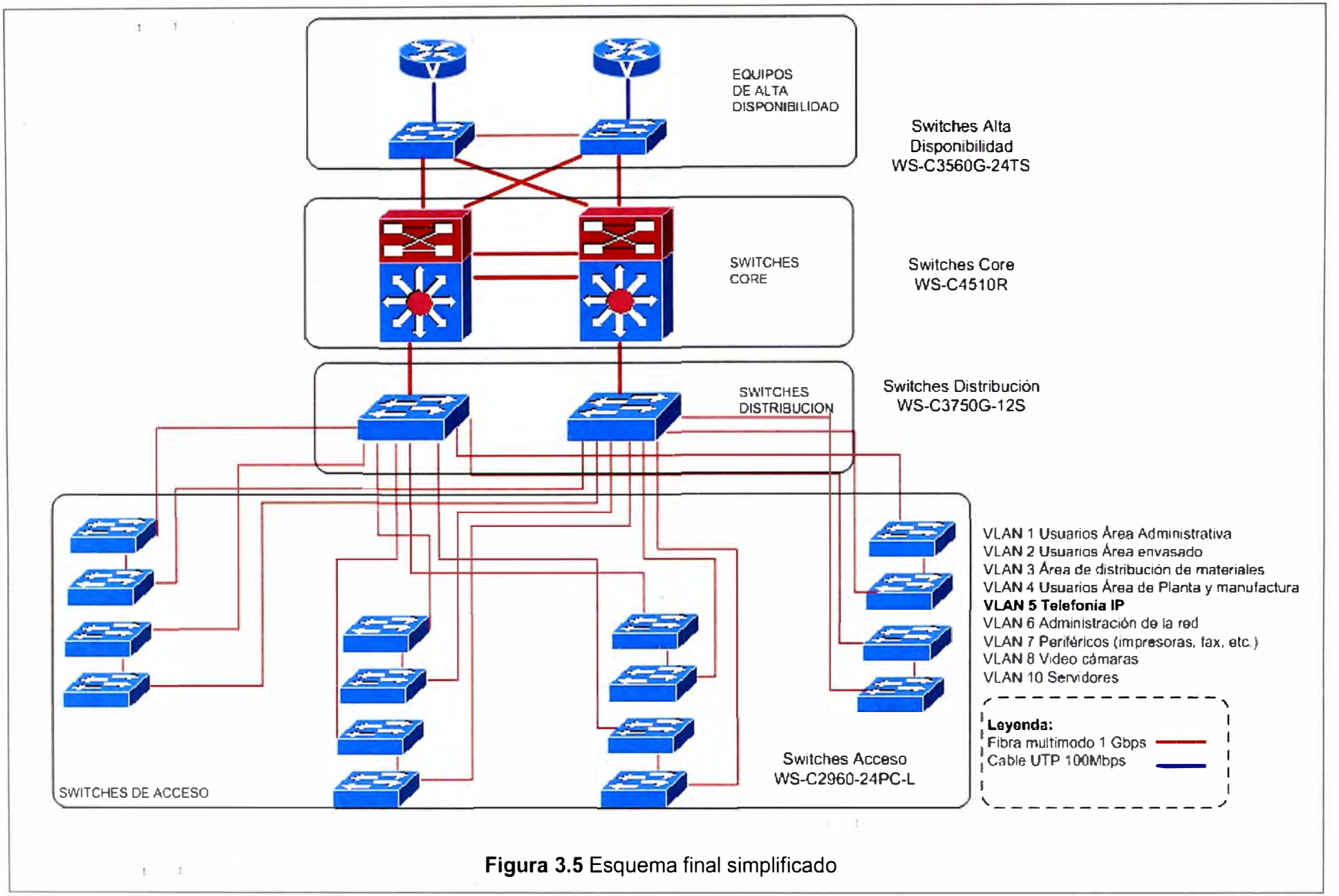

Figura 3.5 Esquema final simplificado

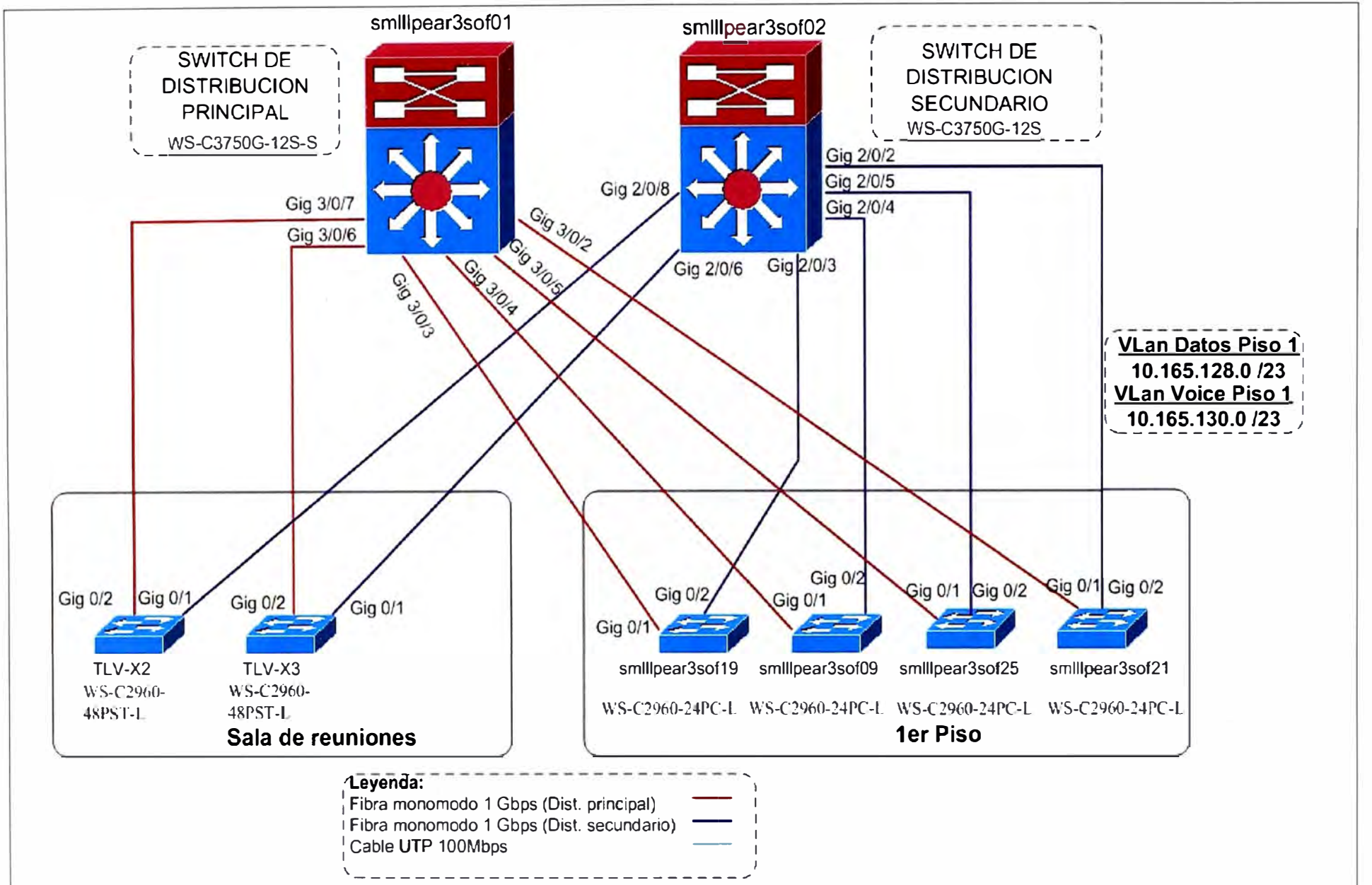

Figura 3.6 Esquema parcial Sede Ate

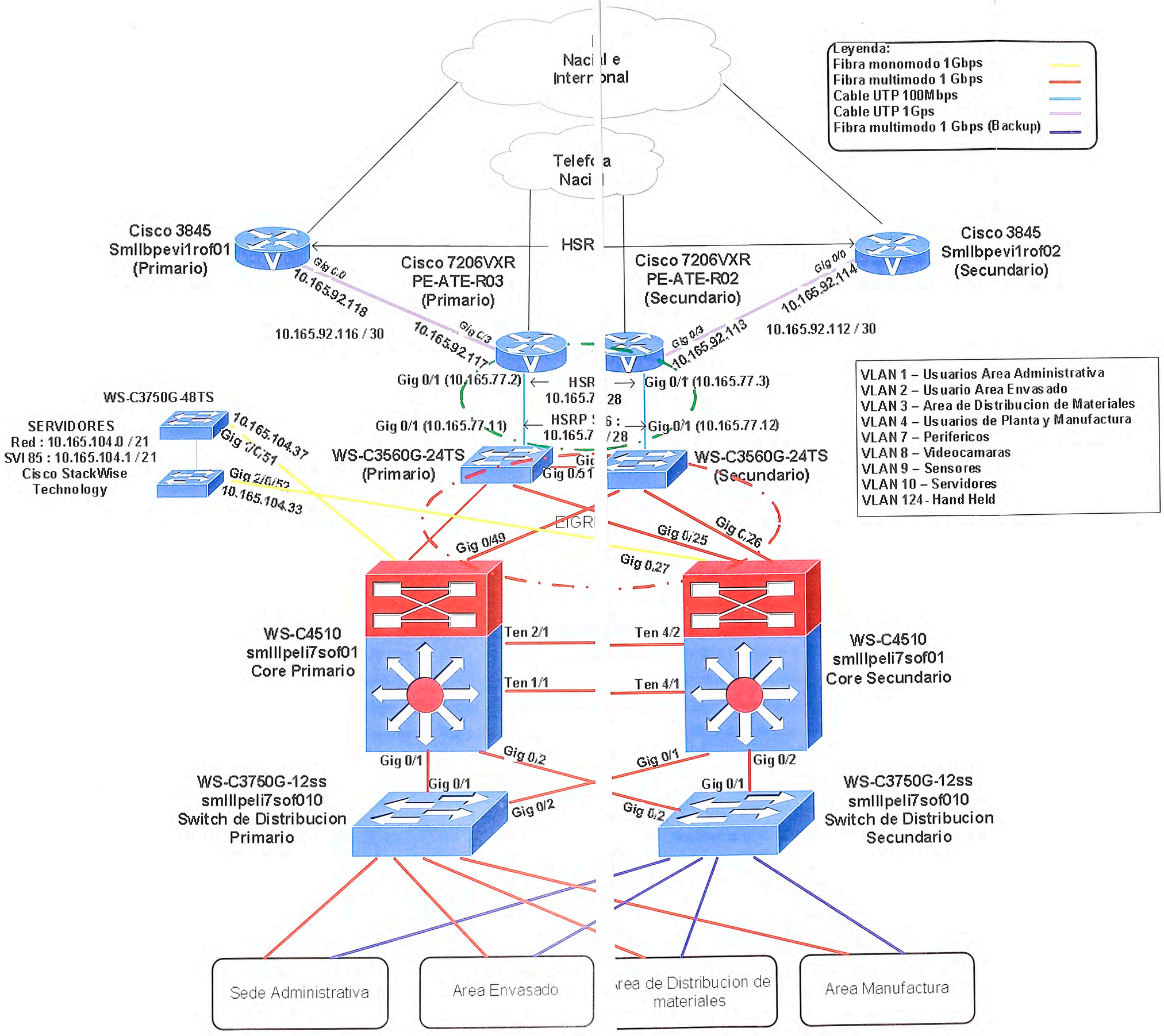

Figura 3.7 E ema total detallado

Dada la complejidad de las LAN, la Figura 3.6 muestra el esquema parcial de la LAN de la Sede de ATE. En ella se puede ver cómo un área está totalmente independizada de otra, en caso de algún incidente en la red sólo afectaría a dicha área, no involucrando a las demás. También se observa la redundancia con respecto a los switches de acceso o borde.

La Figura 3.7, es un esquema total detallado completo de la topología de red WAN/LAN actual. Las IPs asignadas son de referencia así como el subneteo mostrado. No se colocan los verdaderos valores por ser esta información de carácter clasificado para la empresa cervecera.

Aquí se puede observar cómo la estructura LAN se une con la WAN. También se observa a los switches de servidores, que no se mencionaron en el informe por cuanto estos no han sido modificados pero si acoplados a la nueva topología.

También se muestra la redundancia WAN (no es parte de la solución) que está configurada a través de un protocolo HSRP (Hot Standby Router Protocol) que permite el despliegue de routers redundantes tolerantes a fallos en una red. Se indican también las VLANs existentes así cómo las distintas áreas de la empresa cervecera.

3.2.3 Configuración

Las plantillas de configuración de los dispositivos van de acuerdo a su aplicación y localidad. Sólo varían algunos parámetros, pero en general la plantilla sirve facilitar la programación de los dispositivos de red.

- Plantilla Switch WS-C4510R (Core).- Mostrado en el Anexo A.
- Plantilla Switch WS-C3560G-24TS (Alta disponibilidad).- Mostrado en el anexo B.
- Plantilla Switch WS-C3750G-12SS (Distribución).- Mostrado en el Anexo C.
- Plantilla Switch WS-C2960-24PC-L. (Acceso).- Mostrado en el Anexo D.

Lo importante del proyecto, a parte del subneteo, es la configuración en sí. Las plantillas de los anexos describen detalladamente cada aspecto importante. Para hacer didáctica la comprensión de cada configuración, se ha colocado comentarios los cuales se inician con el signo admiración "!". Por ejemplo:

```
! Se asigna el nombre del dispositivo de red.
hostname smlllpeli7sof01
```

La configuración de cada dispositivo ha sido colocada en el anexo en espaciado simple por ser información técnica. Cada plantilla ocupa al menos 8 páginas de instrucciones.

Todos los dispositivos (188 equipos) fueron programados en Lima de acuerdo a su funcionalidad y destino. Luego de ello, los dispositivos fueron enviados a las distintas localidades (plantas y distribuidoras) para luego ser instaladas y puestas en producción.

Este trabajo fue realizado por los administradores de la red LAN, con apoyo de los técnicos locales. El tiempo invertido para las distribuidoras fue de 17 semanas y para las plantas de 8 semanas.

En la actualidad la planta se encuentra totalmente operativa. Y el proyecto de Telefonía IP vienen siendo implementado por etapas, no habiéndose mostrado ningún inconveniente respecto a su desempeño.

En resumen la configuración de cada switch sigue cierta secuencia:

- **Switch WS-C4510R (Core).-** Se asigna nombre propio del equipo, se instala el IOS (Internetwok Operating System), se configura el password de la consola, se configura el password de administrador, se configura el QoS, se configura DHCP para la asignación automática de IP a los periféricos, configuración de spanning tree para evitar los bucles infinitos;

Además se hace la configuración de los dos puertos TenGigabit Ethernet (de alta velocidad), configuración de puerto Gigabit Ethernet, creación de VLANs, Configuracion de Protocolo Eigrp3 para el balanceo de carga y enrutamiento, configuración de rutas estáticas, Configuración de listas de acceso.

- **Switch WS-C3560G-24TS (Alta disponibilidad).-** Se asigna nombre propio del equipo, se instala el IOS (Internetwok Operating System), se configura el password de la consola, se configura el password de administrador, configuración de spanning tree para evitar los bucles infinitos, configuración de seis puertos Gigabit Ethernet, creación de VLANs, Configuración de Protocolo Eigrp3 para el balanceo de carga y enrutamiento, Configuración de listas de acceso.

- **Switch WS-C3750G-12SS (Distribución)**.- Se asigna nombre propio del equipo, se instala el IOS (Internetwok Operating System), se configura el password de la consola, se configura el password de administrador, configuración de spanning tree para evitar los bucles infinitos, configuración de cinco puertos Gigabit Ethernet, creación de VLAN, Configuración de listas de acceso.

- **Switch WS-C2960-24PC-L (Acceso)**.- Se asigna nombre propio del equipo, se instala el IOS (Internetwok Operating System), se configura el password de la consola, se configura el password de administrador, configuración de Fast Ethernet, creación de VLAN, configuración de listas de acceso, configuración del SSH (Secure Shell).

3.3 Equipamiento

Son cuatro los dispositivos utilizados en el proyecto y cuyas características técnicas serán descritas en esta sección: 1) Switch WS-C4510R del Core (Tabla 3.2), 2) Switch WS-C3560G-24TS de alta disponibilidad (Tabla 3.3), 3) Switch WS-C3750G-12SS de distribución (Tabla 3.4), 4) Switch WS-C2960-24PC-L de acceso (Tabla 3.5).

3.3.1 Switch WS-C4510R de Core

Las principales características a describir de este switch son: dimensiones, capacidad de procesamiento (Troughput), conexión Soportada, peso, calidad de servicio, seguridad, supresión de tormentas de broadcast, protocolo IP, administración, Manejo de VLANs, carga y actualización de Software Base.

Tabla 3.2 Switch WS-C4510R de Core

Características	Requerimientos Mínimos
Tipo de equipo	Conmutador Multicapa de operación a nivel 2,3
Espacio	Montable en Rack de 19" (14 RU)
Switched 10/100 Fast Ethernet (RJ-45)	384
Capacidad de Procesamiento (Troughput)	48 Gbps
Conexión Soportada	Puertos con Autesensing: Half y Full Duplex, AutoMdix
Peso	54.50 lb (24.73 kg)
Calidad de Servicio	Estándar 802.1p CoS y clasificación de campo DSCP se proporcionan, mediante el marcado y reclasificación en función de cada paquete con origen y destino la dirección IP, la fuente y la dirección MAC de destino, o la capa TCP 4 o número de puerto UDP
Seguridad	IEEE 802.1x permite a la seguridad dinámica, basada en puertos, que proporciona autenticación de usuario. IEEE 802.1x con asignación de VLAN permite una asignación de VLAN dinámica para un determinado del usuario, independientemente del lugar donde el usuario está conectado.
Supresión de tormentas de broadcast	Control de broadcast
Protocolo IP	IPV4 – IPV6 (Opcional)
Administración	Sistema de administración via CLI, telnet, http y ssh. Soporte de protocolo SNMP y RMON
Carga y Actualización de Software Base	Administración de software base a través de puerto consola, FTP o TFTP
Manejo de VLANs	Hasta 1024 VLAN y hasta 128 instancias de spanning-tree por switch son compatibles La VLAN de voz simplifica las instalaciones de telefonía, manteniendo el tráfico de voz en un aparte VLAN para facilitar la administración y solución de problemas.

3.3.2 Switch WS-C3560G-24TS de alta disponibilidad

Las principales características a describir de este switch son: tipo de equipo, Espacio, capacidad de conmutación (Backplane), capacidad de procesamiento (troughput) conexión soportada, conectores y cableado, PoE, calidad de servicio, seguridad, supresión de tormentas de broadcast protocolo IP, administración, carga y actualización de software base, manejo de VLANs

Tabla 3.3 Switch WS-C3560G-24TS de alta disponibilidad

Características	Requerimientos Mínimos
Tipo de equipo	Conmutador Multicapa de operación a nivel 2,3
Espacio	Montable en Rack de 19" (1 RU)
Capacidad de Conmutación (Backplane)	32 Gbps
Capacidad de Procesamiento (Troughput)	38.7 Mbps
Conexión Soportada	Puertos con Autesensing: Half y Full Duplex, AutoMdix
Conectores y Cableado	puertos 10BASE-T: conectores RJ-45, dos pares de categoría 3, 4, o 5 sin blindaje de par trenzado (UTP)
PoE	Potencia máx. suministrada por puerto: 15,4 W Potencia total dedicado a PoE: 370W total de energía dedicada a PoE: 124W (Cisco Catalyst 3560-8PC, Catalyst3560-12PC)
Calidad de Servicio	Estándar 802.1p CoS y clasificación de campo DSCP se proporcionan, mediante el marcado y reclasificación en función de cada paquete con origen y destino la dirección IP, la fuente y la dirección MAC de destino, o la capa TCP 4 o número de puerto UDP
Seguridad	IEEE 802.1x permite a la seguridad dinámica, basada en puertos, que proporciona autenticación de usuario. IEEE 802.1x con asignación de VLAN permite una asignación de VLAN dinámica para un determinado del usuario, independientemente del lugar donde el usuario está conectado.
Supresión de tormentas de broadcast	Control de broadcast
Protocolo IP	IPV4 – IPV6 (Opcional)
Administración	Sistema de administración via CLI, telnet, http y ssh. Soporte de protocolo SNMP y RMON
Carga y Actualización de Software Base	Administración de software base a través de puerto consola, FTP o TFTP
Manejo de VLANs	Hasta 1024 VLAN y hasta 128 instancias de spanning-tree por switch son compatibles La VLAN de voz simplifica las instalaciones de telefonía, manteniendo el tráfico de voz en un aparte VLAN para facilitar la administración y solución de problemas.

3.3.3 Switch WS-C3750G-12SS (Distribución)

Las características a describir de este switch son: tipo de equipo, espacio, capacidad de conmutación, capacidad de procesamiento, conexión soportada, agregación de enlaces, redundancia totalmente activa, seguridad, tabla de direcciones MAC, supresión de tormentas de broadcast, protocolo IP, calidad de servicio, administración, carga y actualización de software base, enrutamiento IP, manejo de VLANs.

Tabla 3.4 Switch WS-C3750G-12SS de distribución.

Características	Requerimientos Mínimos
Tipo de equipo	Conmutador Multicapa de operación a nivel 2,3 y 4
Espacio	Montable en Rack de 19" (1 RU)
Capacidad de Conmutación (Backplane)	32 Gbps
Capacidad de Procesamiento (Troughput)	38.7 Mbps
Conexión Soportada	Puertos con Autesensing: Half y Full Duplex, AutoMdix
Agregación de enlaces	Agregación de enlaces para configurar grupos troncales
Redundancia totalmente activa	Redundancia en fuente de alimentación
Seguridad	Filtrado de paquetes en capa 2,3 y 4 (basado en puerto, dirección MAC/IP de origen y destino). Protección por contraseñas y administración a nivel usuario. Autenticación confirme al estándar IEEE 802.1X Autenticación local y autenticación Radius
Tabla de Direcciones MAC	Direcciones MAC soportados: - Default Template: 6K - Access Template: 4K - Vlan Template: 12K - Routing Template: 3K
Supresión de tormentas de broadcast	Control de broadcast
Protocolo IP	IPV4 – IPV6 (Opcional)
Calidad de Servicio	ToS/Diffserv IEEE 802.1p COS Cuatro colas de salida por puerto Clasificación de trafico basado en direcciones IP de origen y destino y puertos TCP/UDP Filtrado de paquetes en función de capas 2,3,4
Administración	Sistema de administración via CLI, telnet, http y ssh. Soporte de protocolo SNMP y RMON
Carga y Actualización de Software Base	Administración de software base a través de puerto consola, FTP o TFTP
Enrutamiento IP	Protocolo de enrutamiento: RIP V1, V2 VRRP o Similar
Manejo de VLANs	Estandar IEEE 802.1Q Soporte de 1005 VLANs, 4K VLANs IDs

3.3.4 Switch WS-C2960-24PC-L de acceso

Las características a describir de este switch son: tipo de equipo, espacio, capacidad de procesamiento, conexiones soportadas, puertos, agregación de enlaces, manejo de VLANs, Seguridad, tabla de direcciones MAC, supresión de tormentas de broadcast, protocolo IP, calidad de Servicio, Administración, Carga y Actualización de Software Base, Elementos de Instalación, Estándares soportados.

Tabla 3.5 Switch WS-C2960-24PC-L de acceso

Características	Requerimientos Mínimos
Tipo de equipo	Conmutador Multicapa de operación a nivel 2
Espacio	Montable en Rack de 19" (1 RU)
Capacidad de Procesamiento	10.1Mpps: 48puertos, 6.5 Mpps: 24 puertos
Conexiones soportadas	Puertos con autosensing: Half y Full Duplex; AutoMDIX
Puertos	16Gbps: 48puertos, 16Gbps: 24puertos
Agregación de enlaces	Agregación de enlaces para configurar grupos troncales
Manejo de VLANs	Estándar IEEE 802.1q, soporte de 250 Vlans
Seguridad	Filtrado de paquetes basado en puerto, dirección MAC/IP de origen y destino. Protección por contraseñas y administración a nivel usuario. Autenticación confirme al estándar IEEE 802.1X Autenticación local y autenticación Radius
Tabla de Direcciones MAC	Configurable hasta 8000 direcciones MAC
Supresión de tormentas de broadcast	Control de broadcast
Protocolo IP	IPV4 – IPV6 (Opcional)
Calidad de Servicio	IEEE 802.1p QoS Cuatro colas de salida por puerto
Administración	Sistema de administración via CLI, telnet, http y ssh. Soporte de protocolo SNMP y RMON
Carga y Actualización de Software Base	Administración de software base a través de puerto consola, FTP o TFTP
Elementos de Instalación	Los Equipos incluyen accesorios de fijación en gabinetes y/o rack estándar
Estándares soportados	IEEE 802.3 10Base T IEEE 802.3u, 100Base TX IEEE 802.3ad, 1000Base TX IEEE 802.3x, control de flujo IEEE 802.1d, spanning tree protocol (STP) IEEE 802.1w, Rapid spanning tree protocol IEEE 802.3ad, Link Aggregation Control Protocol (LACP) IEEE 802.1p Priorización IEEE 802.1Q Vlan IEEE 802.1X Autenticación de Usuarios Protocolos: UDP, TFTP, IP, ICMP, TCP, ARP, Telnet, BootP/DHCP, IGMP V1,V2

3.3.5 Resumen de funcionalidades

En esta subsección se resumen las funcionalidades del equipamiento utilizado.

a. Switch WS-C4510R de Core

Permite las redes sin fronteras, proporcionando un alto rendimiento, móvil, segura y experiencias de usuario a través de la conmutación de Capa 2, 3 y 4. Habilita la seguridad, movilidad, rendimiento de las aplicaciones, vídeo y ahorro de energía, por encima de su infraestructura de red.

Apoya la resistencia, la virtualización y la automatización, mejorando aún más la facilidad de uso de la red. Proporciona la escalabilidad y servicios con menor costo total de propiedad y protección de la inversión superior.

Ofrece un alto rendimiento fiable y escalable, con una calidad avanzada dinámica de servicio (QoS) y flexibilidad de configuración para el despliegue de redes sin fronteras.

Integra características de hardware y software para maximizar la disponibilidad de la red, ayudando a asegurar la productividad del personal, rentabilidad y el éxito del cliente.

El diseño de su sistema es centralizado, innovador, flexible y ayuda a garantizar sin problemas la migración a velocidad de cable IPv6 y 10 Gigabit Ethernet (GE).

La compatibilidad hacia adelante y hacia atrás entre generaciones de la serie Cisco Catalyst 4500 se extiende la vida de despliegue, proporcionando protección a la inversión excepcional, al tiempo que reduce el costo total de propiedad.

b. Switch WS-C3560G-24TS de alta disponibilidad

Posee configuración fija, interruptores de nivel empresarial que incluyen IEEE 802.3af y PoE. Es de rápida configuración Ethernet y Gigabit Ethernet.

Posee puertos 10/100/1000 PoE y configuraciones para maximizar la productividad y la protección de la inversión. Permite el despliegue de nuevas aplicaciones tales como telefonía IP, acceso inalámbrico, video vigilancia, la creación de sistemas de gestión.

Los clientes pueden implementar networkwide servicios inteligentes, tales como la calidad de servicio (QoS), limitación de velocidad, listas de control de acceso (ACL), la gestión de multidifusión, y el período de alto rendimiento de enrutamiento, mientras se mantiene la simplicidad de la conmutación de LAN tradicionales.

Está equipado con un robusto conjunto de funciones que brindan escalabilidad y alta disponibilidad a través de enrutamiento IP, así como mejoras de Spanning Tree Protocol para maximizar la disponibilidad de una red de capa 2.

Ofrece características superiores de múltiples capas, QoS granular para ayudar a asegurar que el tráfico de red se clasifica y jerarquizadas, y que la congestión es evitar de la mejor manera posible. La configuración de calidad de servicio se simplifica a través de calidad de servicio automático (Auto QoS), una característica que detecta teléfonos IP de

Cisco y configura automáticamente el switch para la adecuada clasificación y gestión de colas de salida. Esto optimiza la priorización de tráfico y disponibilidad de la red sin el reto de una configuración compleja.

Puede clasificar, reclasificar, la política, marca, cola, y programar los paquetes entrantes, cola y de salida. La clasificación de paquetes permite a los elementos de red discriminar entre los distintos flujos de tráfico y hacer cumplir las políticas sobre la base de Capa 2 y Capa 3.

c. Switch WS-C3750G-12SS de distribución

Facilita el despliegue de aplicaciones convergentes y se adapta al cambio necesidades de negocio de proporcionar flexibilidad de configuración. Soporta la convergencia de la red, y la automatización de los servicios de red inteligentes. Está optimizado para alta densidad Gigabit Ethernet.

Está disponible con la imagen base IP o la imagen de servicios IP. La IP imagen Base incluye la calidad de servicio (QoS), que limita la velocidad, las listas de control de acceso (ACL), enrutamiento estático, Routing Information Protocol (RIP) y el EIGRP. La imagen IP Services proporciona un gran conjunto de características de clase empresarial, incluyendo hardware avanzado basado en IPv6 y routing multicast

d Switch WS-C2960-24PC-L de acceso

Los switches inteligentes Ethernet Catalyst 2960 son una familia de dispositivos autónomos que proveen conectividad a una computadora a velocidades de 100 Mbps y 1 Gbps, y que permite servicios mejorados en la red LAN para empresas grandes, medianas y redes LAN de sedes remotas. También ofrecen seguridad integrada, incluyendo el control de admisión a la red (NAC), avanzado manejo de calidad de servicio (QoS) y soportan enviar servicios inteligentes hasta el extremo de la red.

La serie Catalyst 2960 ofrece:

- Características de inteligencia al extremo de la red, como listas sofisticadas de control de acceso (ACLs) y seguridad avanzada.
- Enlaces trunk de doble propósito para la diversidad de enlaces, permitiendo el uso de enlaces de cobre o fibra. Cada puerto de doble propósito tiene un puerto Ethernet de 10/100/1000 Mbps y un puerto SFP Gigabit, donde solo uno de ellos puede estar activo.
- Control de la red y optimización del ancho de banda usando calidad de servicio avanzado, tasas de límites granulares, listas de control de acceso, y servicios multicast.
- Seguridad de red a través de un amplio rango de métodos de autenticación, tecnologías de encriptación de datos, y control de admisión a la red basada en usuarios.
- Fácil configuración de la red, actualización y resolución de problemas usando el software Cisco Network Assistant.

- Auto configuración para aplicaciones especializadas a través del uso de puertos inteligentes (smartports).

CAPÍTULO IV
CRONOGRAMA Y PRESUPUESTO

En este capítulo se desarrolla la estructura de costos y, la gestión de tiempo del proyecto de ingeniería "Reestructuración de la Plataforma de Red Lan de una Empresa Cervecera".

4.1 Gestión de tiempo

En esta sección se desarrolla: el plan de actividades por fases y el cronograma de tareas. El proyecto tuvo dos componentes:

1) Equipamiento de red

2) Cableado estructurado.- Ejecutado con antelación a la llegada de los equipos de red y de forma totalmente paralela y sin interacción con lo operativo en producción.

4.1.1 Plan de actividades por fases

A continuación se detalla el plan de actividades por fases que se acordó al inicio del proyecto, y al final se indica como se completaron en el tiempo.

a. Fase 1 Configuracion de Equipamiento

Para todos los emplazamientos Ccnstó de la configuración de los switches:

- De alta Disponibilidad
- De distribución
- De borde (acceso)
- De core

b. Fase 2 Despliegue de Equipamiento

Por planta se desplegó:

- Dos switches de alta disponibilidad,
- Dos switches Core
- Dos switches de distribución a las respectivas plantas
- Y los switches de acceso requeridos en cada una.

También se desplegó los switches de acceso para las 51 distribuidoras a nivel nacional

c. Fase 3 Instalación de Equipamiento

Constó de la instalación de:

- El equipamiento en las plantas principales (Lima y provincia)

- El equipamiento en las distribuidoras

d. Fase 4 Afinamiento de configuración de equipamiento

Está constó de:

- El renombramiento de VLANs
- Las pruebas de Conectividad
- Las pruebas de Redundancia

4.1.2 Cronograma

El cronograma de actividades planteado fue de acuerdo a la Tabla 4.1 y al diagrama de Gantt respectivo (Figura 4.1, 4.2 y 4.3). Durante el proceso de implementación de este proyecto se presentaron los siguientes sucesos:

- Contratación de personal técnico temporal, para la configuración de equipos
- Nombramiento de los Administradores de red Lan.
- Coordinación con la proveedora de Wan para realizar trabajos en conjunto de implementación de los equipos de alta disponibilidad y Core

Tabla 4.1 Tareas y tiempos usados

Abastecimiento de Equipos	120 días
Llegada de equipos Cisco (Core, Alta disponibilidad, Distribución)	120 días
Llegada de equipos de Borde	120 días
Fase 1: Configuración de equipamiento	30 días
Configuración de Switches Core	3 días
Configuración de Switches de Distribución	3 días
Configuración de switches de Alta disponibilidad	3 días
Configuración de switches de Borde	21 días
Fase 2: Despliegue de Equipamiento	7 días
Despliegue de equipos (Core, Distribución y Alta Disponibilidad)	3 días
Despliegue de equipos de borde	4 días
Fase 3: Instalación de Equipos	72 días
Instalación de equipos en Plantas	12 días
Instalación en Planta Arequipa	3 días
Instalación en Planta Pucallpa	3 días
Instalación en Planta Cuzco	3 días
Instalación en Planta Lima	3 días
Instalación de Equipos en Distribución	60 días
Instalación en 51 Distribuidoras	60 días
Fase 4: Afinamiento de configuración de equipamiento	4 días
Renombramiento de VLAN	2 días
Revisión de conectividad de equipos	1 día
Pruebas de redundancia	1 día

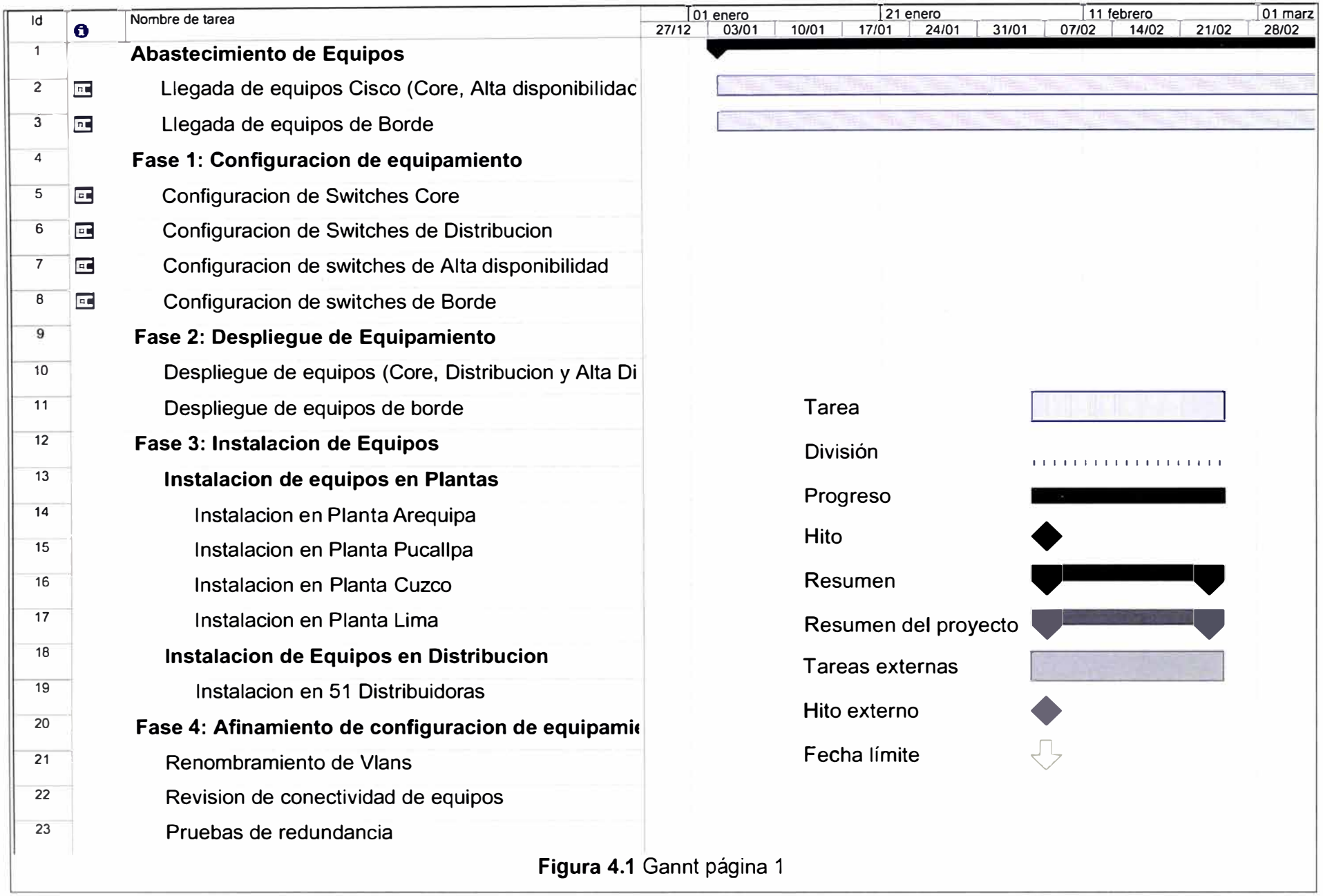

Figura 4.1 Gannt página 1

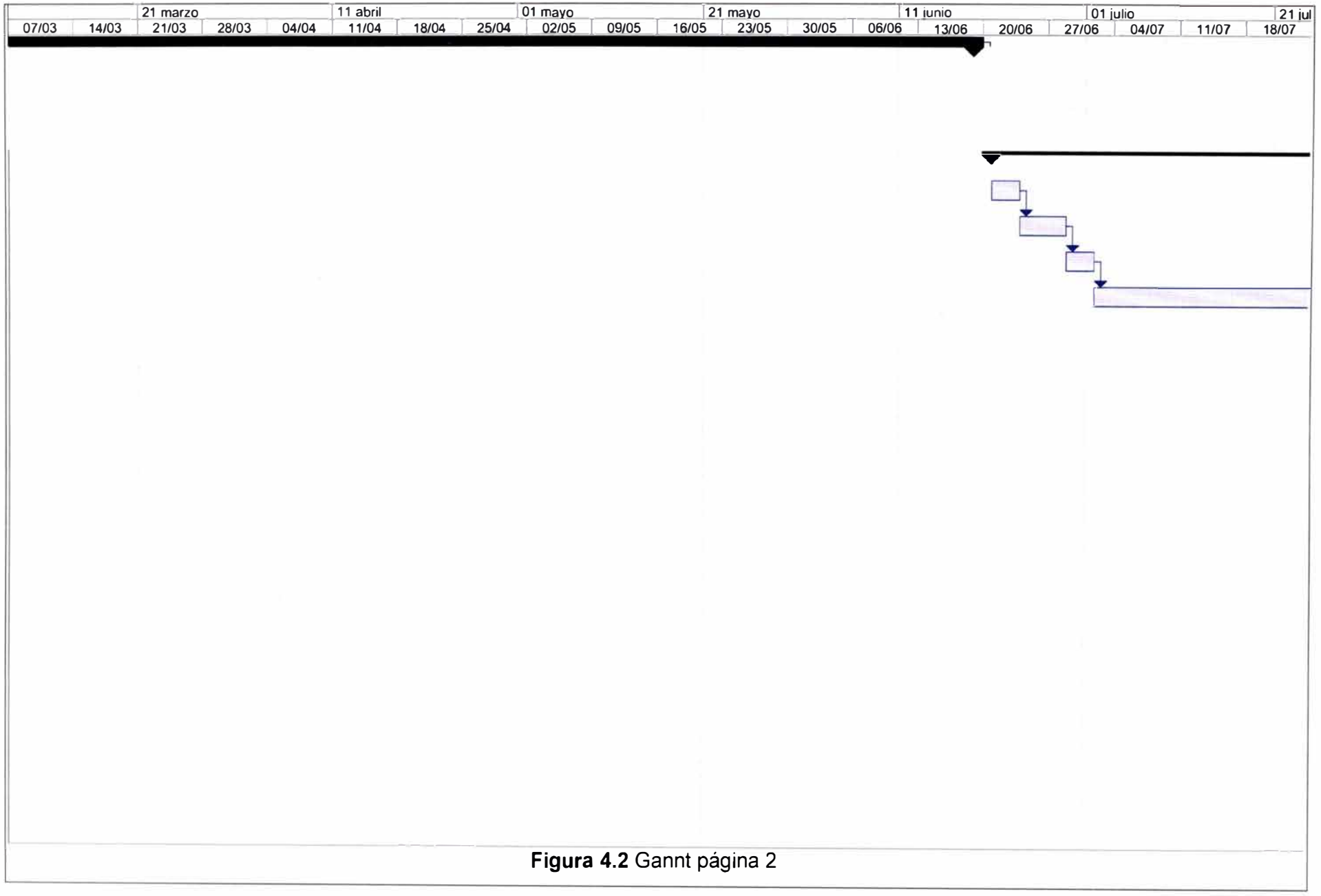

Figura 4.2 Gannt página 2

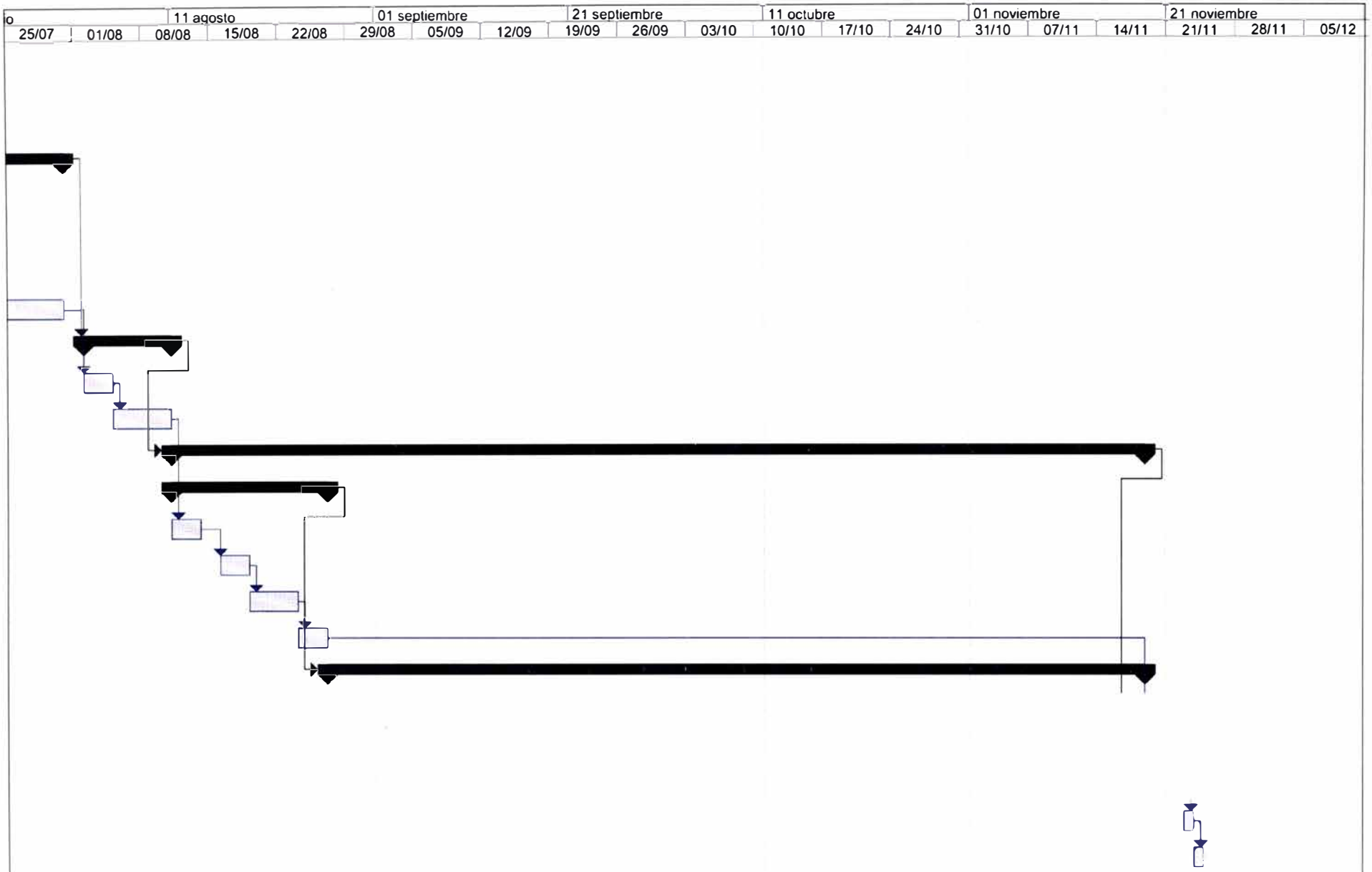

Figura 4.2 Gannt página 2

4.2 Relación de equipamiento y costos

En las Tablas 4.2, 4.3, 4.4 y 4.6, se muestran el listado de equipos. Los precios están en dólares americanos.

Tabla 4.2 Presupuesto de switches core

Producto	Descripción	Cant	Unidad	Total
WS-C4510R	Catalyst C4510R	8	22,990.00	183,920.00
CAB-CONSOLE-RJ45	Console Cable 6ft with RJ45 and DB9F	8	30.00	240.00
CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	16	-	-
CON-SNTP-C4510R	SMARTNET 24X7X4 Cat C4510R Enhanced Multilayer Img	8	3,215.00	25,720.00
GLC-SX-MM=	GE SFP, LC connector SX transceiver	128	500.00	64,000.00
PWR-RPS2300	Cisco Redundant Power System 2300 and Blower,No Power Supply	8	1,200.00	9,600.00
C3K-PWR-750WAC	Catalyst 4500-R power supply	16	1,990.00	31,840.00
CAB-16AWG-AC	AC Power cord, 16AWG	16	-	-
CAB-RPS2300	RPS 2300 Cable for Devices other than E-Series Switches	8	-	-
CON-SNTP-RPS2300	SMARTNET 24X7X4 PWR-RPS2300	8	388.00	3,104.00
				$318,424.00

Tabla 4.3 Presupuesto de switches de alta disponibilidad

Producto	Descripción	cant	Unidad	Total
WS-C3560G-24TS-E	Catalyst 3560 24 10/100/1000T + 4 SFP + IPS Image	8	8,790.00	70,320.00
CAB-CONSOLE-RJ45	Console Cable 6ft with RJ45 and DB9F	8	30.00	240.00
CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	8	-	-
CON-SNTP-3560GTE	SMARTNET 24X7X4 Cat 3560 24 10/100/1000T + 4 SFP En	8	1,268.00	10,144.00
GLC-SX-MM=	GE SFP, LC connector SX transceiver	32	500.00	16,000.00
				$96,704.00

Tabla 4.4 Switches de distribución

Producto	Descripción	Cant	Unidad	Total
WS-C3750G-12S-E	Catalyst 3750 12 SFP + IPS Image	8	11,990.00	95,920.00
CAB-CONSOLE-RJ45	Console Cable 6ft with RJ45 and DB9F	8	30.00	240.00
CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	16	-	-
CON-SNTP-3750G12E	SMARTNET 24X7X4 Cat 3750 12 SFP Enhanced Multilayer Img	16	2,215.00	35,440.00
GLC-SX-MM=	GE SFP, LC connector SX transceiver	128	500.00	64,000.00
PWR-RPS2300	Cisco Redundant Power System 2300 and Blower,No Power Supply	8	1,200.00	9,600.00
C3K-PWR-750WAC	Catalyst 3750-E / 3560-E 750WAC power supply	16	1,990.00	31,840.00
CAB-16AWG-AC	AC Power cord, 16AWG	16	-	-
CAB-RPS2300	RPS 2300 Cable for Devices other than E-Series Switches	8	-	-
CON-SNTP-RPS2300	SMARTNET 24X7X4 PWR-RPS2300	8	388.00	3,104.00
				240,144.00

Tabla 4.5 Switches de Acceso

Producto	Descripción	Cant	Unidad	Total
WS-C2960-24PC-L	Catalyst 2960 24 10/100 PoE + 2 T/SFP LAN Base Image	164	2,495.00	409,180.00
CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	164	-	-
CAB-CONSOLE-RJ45	Console Cable 6ft with RJ45 and DB9F	164	30.00	4,920.00
CON-SNTP-C29602PC	SMARTNET 24X7X4 Cat2960 24 10/100 PoE-2T/SFP LAN Bse Im	164	316.00	51,824.00
GLC-SX-MM=	GE SFP, LC connector SX transceiver	328	500.00	164,000.00
				629,924.00

Al sumar los totales de las tablas anteriores, se obtiene un costo de 1' 285, 196 USD sólo en equipos de comunicación LAN.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. La reestructuración de la red LAN de la empresa cervecera, una vez completada todas las etapas de despliegue y pruebas, por más de un año de funcionamiento a demostrado un gran desempeño.
2. La nueva plataforma proporcionada ha demostrado ser óptima para el uso de telefonía IP y periféricos, los cuales vienen siendo implementados paulatinamente a través de otro proyecto. La red ha respondido eficientemente no habiéndose presentado inconvenientes hasta la fecha.
3. Se ha logrado con la nueva plataforma reducir el número de fallas y el tiempo de resolución, esto debido a la robustez de la plataforma y su redundancia a nivel LAN con respecto a las plantas.
4. La seguridad de la red se ha mejorado a nivel usuario, ya que ahora se posee administración remota de los equipos de comunicación para mayor control de los puertos de usuario.

Recomendaciones

1. Se recomienda que anualmente se realice un estudio de los incidentes y desempeño de la red, a fin de obtener información necesaria para un posible escalamiento a mediano plazo.
2. Se recomienda realizar mantenimiento preventivo de los equipos de comunicaciones cada cuatro meses, lo cual implica tiempos de respuesta de redundancia, actualización de los IOS de cada equipo de comunicación, así cómo limpieza de los equipos.

ANEXO A
PLANTILLA SWITCH WS-C4510R (CORE)

```
smlllpeli7sof01#sh run
Building configuration...

Current configuration : 26333 bytes
! (Equipo carga su configuracion actual)
! Last configuration change at 10:53:56 PERU Fri Dec 24 2010 by lzamora
! NVRAM config last updated at 10:53:57 PERU Fri Dec 24 2010 by jgonzala
!
version 12.2
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service compress-config
!(Nombre de equipo)
hostname smlllpeli7sof01
! (booteando el IOS)
boot-start-marker
boot system bootflash:/cat4500-entservicesk9-mz.122-40.SG.bin
boot system bootflash:/cat4500-entservicesk9-mz.122-31.SGA1.bin
boot system slot0:/cat4500-entservicesk9-mz.122-31.SGA1.bin
boot-end-marker
! (Configuracion de password de consola)
no logging console
enable secret 7 $1$jRsg$16fMWBkyJHcFAMikUnpW8/
enable password 7 1441325F08107A3B0B
! (Configuracion de password de usuarios)
username lzamorac privilege 15 password 7 0341094F1F27674761
username jgonzala privilege 15 password 7 0553164A710F7B5B1A
aaa new-model
aaa authentication login backacs group tacacs+ local
aaa authorization exec backacs group tacacs+ local
aaa authorization commands 15 backacs group tacacs+ local
aaa accounting exec backacs start-stop group tacacs+
aaa accounting commands 15 backacs start-stop group tacacs+
!
aaa session-id common
clock timezone PERU -5
hw-module uplink select tengigabitethernet
qos (Configuracion de QoS)
qos dbl
qos map dscp 24 25 26 27 28 29 30 31 to tx-queue 4
qos map dscp 32 33 34 35 36 37 38 39 to tx-queue 4
qos map cos 5 to dscp 46
!
ip dhcp excluded-address 10.165.124.1
ip dhcp excluded-address 10.165.124.2
ip dhcp excluded-address 10.165.124.3
! (Configuracion de dhcp, quien asigna la IP a usuario)
ip dhcp pool DHCP-SIATE-HH
   network 10.165.124.0 255.255.255.0
   domain-name latam.americas.GCN.local
   dns-server 10.165.104.2 10.165.104.4
```

```
   default-router 10.165.124.1
   lease 0 5
!
ip subnet-zero
!
power redundancy-mode redundant
port-channel load-balance src-dst-port
!
!
! (Configuracion de spannoing tree)
spanning-tree mode rapid-pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree vlan 2 priority 0
spanning-tree vlan 4-10 priority 4096
!
redundancy
 mode sso
 main-cpu
  auto-sync standard
!
vlan internal allocation policy ascending
!
class-map match-all VOICE
  match access-group 100
!
!
policy-map VOIP
  class VOICE
   set precedence 5
policy-map autoqos-voip-policy
  class class-default
    dbl
!
!
interface Loopback0
 no ip address
!
interface Port-channel1
 interface Port-channel1
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 logging event link-status
 logging event trunk-status
 flowcontrol receive on
! (Configuracion de Puerto TenGig)
interface TenGigabitEthernet1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode on
!
interface TenGigabitEthernet1/2
 Shutdown
```

```
! (Configuracion de Puerto Gig)
interface GigabitEthernet1/1
switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
 no ip address
 logging event link-status
 logging event trunk-status
!
interface GigabitEthernet1/2
Shutdown
!
interface GigabitEthernet1/3
Shutdown
!
interface GigabitEthernet1/4
 Shutdown
!
interface GigabitEthernet1/5
 Shutdown
!
interface GigabitEthernet1/6
 Shutdown
!
interface GigabitEthernet1/7
 Shutdown
!
interface GigabitEthernet1/8
 Shutdown
!
interface GigabitEthernet1/9
 Shutdown
!
interface GigabitEthernet1/10
 Shutdown
!
interface GigabitEthernet1/11
 Shutdown
!
interface GigabitEthernet1/12
 Shutdown
! (Configuracion de Puerto TenGig)
interface TenGigabitEthernet2/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode on
!
interface TenGigabitEthernet2/2
 Shutdown
!
interface Vlan1
 no ip address
!
```

```
interface Vlan2 (Creacion de Vlan)
 description Vlan Usuarios
 ip address 10.165.7.254 255.255.248.0
 ip helper-address 10.165.104.12
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 standby 1 ip 10.165.0.1
 standby 1 timers 1 3
 standby 1 priority 150
 standby 1 preempt
 standby 1 track GigabitEthernet5/3 20
!
interface Vlan5
 description Vlan Managment
 ip address 10.165.103.3 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 standby 1 ip 10.165.103.1
 standby 1 timers 1 3
 standby 1 priority 140
 standby 1 preempt
!
interface Vlan6
 description Vlan Usuarios-Volvo
 ip address 10.165.112.3 255.255.248.0
 ip helper-address 10.165.104.12
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 standby 1 ip 10.165.112.1
 standby 1 timers 1 3
 standby 1 priority 140
 standby 1 preempt
!
interface Vlan9
 description Vlan Videocamaras
 ip address 10.165.126.3 255.255.255.128
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 standby 1 ip 10.165.126.1
 standby 1 timers 2 5
 standby 1 priority 150
 standby 1 preempt
!
interface Vlan10
 description Vlan Videoconferencia
 ip address 10.165.126.131 255.255.255.128
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 standby 1 ip 10.165.126.129
```

```
 standby 1 timers 2 5
 standby 1 priority 200
 standby 1 preempt
!
interface Vlan124
 description Vlan HH-SI ATE
 ip address 10.165.124.2 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 standby 1 ip 10.165.124.1
 standby 1 timers 1 3
 standby 1 priority 150
 standby 1 preempt
! (Configuracion de Protocolo Eigrp3)
router eigrp 3
 network 10.165.72.0 0.0.0.127
 network 10.165.77.20 0.0.0.3
 network 10.165.77.28 0.0.0.3
 network 10.165.77.32 0.0.0.3
 network 10.165.77.40 0.0.0.3
 network 10.165.77.68 0.0.0.3
 no auto-summary
! (Configuracion de Rutas estaticas)
ip classless
ip route 10.18.50.0 255.255.255.248 10.17.10.2
ip route 10.18.50.0 255.255.255.248 10.17.20.2
ip route 10.165.100.140 255.255.255.255 10.165.103.3
ip route 10.165.140.0 255.255.255.128 10.165.103.3
ip route 10.165.140.128 255.255.255.128 10.165.103.3
ip route 10.165.12.0 255.255.255.0 10.165.77.42
ip route 10.165.100.140 255.255.255.255 10.165.103.190
ip route 10.165.140.0 255.255.255.128 10.165.103.190
ip route 10.165.140.128 255.255.255.128 10.165.103.190
ip route 172.16.2.0 255.255.255.252 192.168.1.50
ip route 192.168.10.0 255.255.255.0 192.168.1.50
no ip http server
no ip http secure-server
ip tacacs source-interface Vlan5
!
!
ip prefix-list vlan124 seq 5 permit 10.165.124.0/24
!
ip prefix-list vlan2 seq 5 permit 10.165.0.0/21
!
ip prefix-list vlan5 seq 5 permit 10.165.103.0/24
!
ip prefix-list vlan6 seq 5 permit 10.165.112.0/21
!
ip prefix-list vlan7 seq 5 permit 10.165.120.0/22
!
logging trap debugging
logging 10.165.103.253
!
```

```
! (Configuracion de Access-list)
access-list 90 permit 10.165.103.253
access-list 91 permit 10.165.119.249
access-list 91 permit 10.165.119.250
access-list 91 permit 10.165.119.251
access-list 91 permit 10.165.103.249
access-list 91 permit 10.165.103.250
access-list 91 permit 10.165.103.251
access-list 91 permit 10.165.103.253
access-list 91 permit 10.165.7.249
access-list 91 permit 10.165.7.250
access-list 91 permit 10.165.7.251
!
route-map LANBACKUS permit 20
 match ip address prefix-list vlan2
 set metric 200 10 255 1 1500
!
route-map LANBACKUS permit 60
 match ip address prefix-list vlan6 vlan5 vlan8
 set metric 100 10 255 1 1500
!
!
snmp-server group BKTEL v3 auth notify
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFF0F
snmp-server community r53m4ld RO
snmp-server community w5rm1lt3 RW
snmp-server trap-source Vlan5
snmp-server location CORE_SECUNDARIO_ATE
snmp-server contact British Telecommunications plc.
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps flash insertion removal
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps envmon fan shutdown supply temperature
snmp-server enable traps config
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vlan-membership
snmp-server host 10.165.103.253 version 3 auth backusgmd
snmp-server host 199.80.46.57 r53m4ld
snmp-server host 199.80.48.112 r53m4ld
tacacs-server host 10.165.103.254
tacacs-server directed-request
tacacs-server key 7 0402292D3B046017
radius-server source-ports 1645-1646
!
control-plane
!
banner motd ^C
```

```
   #  #  ##  ##### #  # # #  # ####  ##
   #  # # #  #  # ## # # ## # # #  # ##
   #  # #  # #  # # # # # # # #    ##
   # ## # ###### ##### # # # # # # # # ###  ##
   ## ## #  # # #  #  ## # #  ## #  #
   #  # #  # #  # #  # # #  # ####  ##
```

You are trying to enter in a private system. Only authorized users will accede to the system. Any nonauthorized attempt is prohibited and will be registered. The authorized users accept the policies and norms of the company. The use of the system is monitoring and it will be generated legal measures corresponding.

Esta intentando ingresar en un sistema privado. Solo usuarios autorizados podran acceder al sistema. Cualquier intento no autorizado esta prohibido y sera registrado. Los usuarios autorizados aceptan las politicas y normas de la empresa. El uso del sistema es monitoreado y generara medidas legales correspondientes.

```
^C
line con 0
 exec-timeout 5 0
 password 7 11501C0B441E192C2972
 authorization commands 15 backcs
 authorization exec backacs
 accounting commands 15 backacs
 accounting exec backacs
 logging synchronous
 login authentication backacs
 stopbits 1
line vty 0 4
 access-class 91 in
 exec-timeout 2 0
 password 7 144E17055F08380B0970
 authorization commands 15 backacs
 authorization exec backacs
 accounting commands 15 backacs
 accounting exec backacs
 logging synchronous
 login authentication backacs
 transport input telnet ssh
!
ntp clock-period 17208442
ntp server 10.165.103.252
end

smlllpeli7sof01#       exit
Connection to 10.165.103.3 closed.
```

ANEXO B
PLANTILLA SWITCH WS-C3560G-24TS (ALTA DISPONIBILIDAD)

```
Current configuration : 14457 bytes
!
! Last configuration change at 11:43:26 PERU Fri Dec 24 2010 by jgonzala
! NVRAM config last updated at 11:43:28 PERU Fri Dec 24 2010 by jgonzala
!
version 12.2
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
! (Configuracion de nombre de equipo)
hostname smlllpeli7sof59
!
boot-start-marker
boot-end-marker
!
logging buffered 32000
no logging console
! (Configuracion de password de consola)
enable secret 7 $1$ZetX$ccQ68sRRtfVHSpolvbBdl0
enable password 7 091A6E5D1D11470224
! (Configuracion de Password de Usuario)
username lzamorac privilege 15 password 7 041E594216090A4526
username jgonzala privilege 15 password 7 0553164A710F7B5B1A
aaa new-model
!
!
aaa group server tacacs+ TACGROUP
 server 10.165.103.254
 ip tacacs source-interface Vlan86
!
aaa authentication login backacs group TACGROUP local
aaa authorization exec backacs group TACGROUP local
aaa authorization commands 15 backacs group TACGROUP local
aaa accounting exec backacs start-stop group TACGROUP
aaa accounting commands 15 backacs start-stop group TACGROUP
!


aaa session-id common
clock timezone PERU -5
system mtu routing 1500
vtp domain BACKUS
vtp mode transparent
ip subnet-zero
no ip source-route
ip routing
no ip domain-lookup
ip domain-name Backus
!

!
crypto pki trustpoint TP-self-signed-3882668928
 enrollment selfsigned
```

```
 subject-name cn=IOS-Self-Signed-Certificate-3882668928
 revocation-check none
 rsakeypair TP-self-signed-3882668928
!

! (Configuracion de Spanning tree)
spanning-tree mode rapid-pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 86
!
ip tftp source-interface Vlan86
ip ssh time-out 60
ip ssh authentication-retries 2
ip ssh version 2
!
!
!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
 logging event trunk-status
 load-interval 30
! (Configuracion de Puerto Gig)
interface GigabitEthernet0/1
 description -- A ROUTER PE-ATE-R03 --
 switchport access vlan 86
 switchport mode access
 switchport nonegotiate
 load-interval 30
 speed 100
 duplex full
 no mdix auto
! (Configuracion de Puerto Gig)
interface GigabitEthernet0/2
 description -- Conexion Switch CORE 1 --
 no switchport
 ip address 10.165.77.17 255.255.255.252
 ip hello-interval eigrp 3 1
 ip hold-time eigrp 3 2
 load-interval 30
! (Configuracion de Puerto Gig)
interface GigabitEthernet0/3
 description -- A FIREWALL INTERNAL 1 --
 switchport access vlan 86
 switchport mode access
 switchport nonegotiate
 load-interval 30
 no mdix auto
```

```
 no cdp enable
!
interface GigabitEthernet0/4
 shutdown
!
interface GigabitEthernet0/5
 shutdown
!
interface GigabitEthernet0/6
 shutdown
!
interface GigabitEthernet0/7
 shutdown
!
interface GigabitEthernet0/8
 shutdown
!
interface GigabitEthernet0/9
 shutdown
!
interface GigabitEthernet0/10
 shutdown
!
interface GigabitEthernet0/11
 shutdown
!
interface GigabitEthernet0/12
 shutdown
!
interface GigabitEthernet0/13
 shutdown
!
interface GigabitEthernet0/14
 shutdown
!
interface GigabitEthernet0/15
 shutdown
!
interface GigabitEthernet0/16
 shutdown
!
interface GigabitEthernet0/17
 shutdown
!
interface GigabitEthernet0/18
 shutdown
!
interface GigabitEthernet0/19
 shutdown
!
interface GigabitEthernet0/20
 shutdown
!
interface GigabitEthernet0/21
```

```
 shutdown
!
interface GigabitEthernet0/22
 shutdown
!
interface GigabitEthernet0/23
 shutdown
!
interface GigabitEthernet0/24
 shutdown
! (Configuracion de Puerto Gig)
interface GigabitEthernet0/25
 description -- Conexion Switch CORE 1 --
 no switchport
 ip address 10.165.77.17 255.255.255.252
 ip hello-interval eigrp 3 1
 ip hold-time eigrp 3 2
 load-interval 30
! (Configuracion de Puerto Gig)
interface GigabitEthernet0/26
 description -- Conexion Switch CORE 2 --
 no switchport
 ip address 10.165.77.21 255.255.255.252
 ip hello-interval eigrp 3 1
 ip hold-time eigrp 3 2
 load-interval 30
! (Configuracion de Puerto Gig)
interface GigabitEthernet0/27
 description -- Conexion Switch WC-3560G-24TS_SECUNDARIO --
 switchport access vlan 86
 switchport mode access
 switchport nonegotiate
 logging event trunk-status
!
interface GigabitEthernet0/28
 shutdown
!
interface Vlan1
 no ip address
! (Creacion de Vlan)
interface Vlan10
 ip address 10.165.77.13 255.255.255.240
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 standby 1 ip 10.165.77.14
 standby 1 timers 1 3
 standby 1 priority 150
 standby 1 preempt
!
! (Configuracion de Protocolo EIGRP)
router eigrp 3
 redistribute connected route-map NETBACKUS
```

```
 redistribute static metric 2000 10 255 1 1500
 no auto-summary
 network 10.165.77.16 0.0.0.3
 network 10.165.77.20 0.0.0.3
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.165.77.1
no ip http server
no ip http secure-server
!
!
ip prefix-list vlan86 seq 1 permit 10.165.77.0/28
logging trap debugging
logging 10.165.103.253
! (Creacion de access list)
access-list 90 permit 10.165.103.253
access-list 91 permit 10.165.119.249
access-list 91 permit 10.165.119.250
access-list 91 permit 10.165.119.251
access-list 91 permit 10.165.103.249
access-list 91 permit 10.165.103.250
access-list 91 permit 10.165.103.251
access-list 91 permit 10.165.7.249
access-list 91 permit 10.165.7.250
access-list 91 permit 10.165.7.251
route-map NETBACKUS permit 10
 match ip address prefix-list vlan86
 set metric 200 10 255 1 1500
!
snmp-server user w5rm1lt3 w5rm1lt3 v1
snmp-server user w5rm1lt3 w5rm1lt3 v2c
snmp-server group BKTEL v3 auth
snmp-server group backusgmd v3 auth notify
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFF7F
snmp-server community r53m4ld RO
snmp-server community w5rm1lt3 RW
snmp-server user w5rm1lt3 w5rm1lt3 v1
snmp-server user w5rm1lt3 w5rm1lt3 v2c
snmp-server trap-source Vlan86
snmp-server location ATE_Central_Telef_1
snmp-server contact British Telecommunications plc.
snmp-server system-shutdown
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps cluster
snmp-server enable traps entity
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
```

```
snmp-server enable traps vlan-membership
snmp-server host 10.165.103.253 version 3 auth backusgmd
snmp-server host 199.80.46.57 r53m4ld
snmp-server host 199.80.48.112 r53m4ld
tacacs-server host 10.165.103.254
tacacs-server directed-request
tacacs-server key 7 135C35393F292873
!
control-plane
!
banner motd ^C



    #  #  ##  ##### #  # # #  # ####  ##
    #  # # #  #  # ## # # ## # #  # ##
    #  # #  # #  # # # # # # # #    ##
    # ## # ###### ##### # # # # # # # ### ##
    ## ## #  # #  # #  ## # #  ## #  #
    #  # #  # #  # #  # # #  # ####  ##


  ------------------------------------------------------------------

  You are trying to enter in a private system. Only authorized users
  will accede to the system. Any nonauthorized attempt is prohibited
  and will be registered. The authorized users accept the policies
  and norms of the company. The use of the system is monitoring and
  it will be generated legal measures corresponding.

  ------------------------------------------------------------------

  Esta intentando ingresar en un sistema privado. Solo usuarios
  autorizados podran acceder al sistema. Cualquier intento no
  autorizado esta prohibido y sera registrado. Los usuarios
  autorizados aceptan las politicas y normas de la empresa. El
  uso del sistema es monitoreado y generara medidas legales
  correspondientes.

  ------------------------------------------------------------------


^C
!
line con 0
 exec-timeout 5 0
 password 7 04020E085C2D5E6E2441
 authorization commands 15 backacs
 authorization exec backacs
 accounting commands 15 backacs
 accounting exec backacs
 logging synchronous
 login authentication backacs
```

```
 stop-character 36
line vty 0 4
 access-class 91 in
 exec-timeout 30 0
 password 7 04020E085C2D5E6E2441
 authorization commands 15 backacs
 authorization exec backacs
 accounting commands 15 backacs
 accounting exec backacs
 login authentication backacs
 transport input telnet ssh
line vty 5 15
 transport input none
!
ntp clock-period 36030616
ntp server 10.165.103.252
end
```

ANEXO C
PLANTILLA SWITCH WS-C3750G-12SS (DISTRIBUCIÓN)

```
=~=~=~=~=~=~=~=~=~=~=~=    PuTTY    log    2011.01.24    15:05:59
=~=~=~=~=~=~=~=~=~=~=~=

smlllpeli2sof01#sho run
Building configuration...

Current configuration : 8180 bytes
! (Ccargando configuracion)
! Last configuration change at 15:50:39 PERU Fri Jan 14 2011 by izamorac
! NVRAM config last updated at 15:50:40 PERU Fri Jan 14 2011 by lzamorac
!
version 12.2
!
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
! (Configuracion de Nombre de equipo)
hostname smlllpeli2sof01
!
boot-start-marker
boot-end-marker
!
logging buffered 32000
no logging console
!
! (Configuracion de password de consola)
enable secret 5 $1$0O5/$UGL..7Bx1gPrDWjhWE8gt0
enable password 7 055D265B25581E1936
!
! (Configuracion de password de usuario)
username lzamorac privilege 15 password 7 04180E5228604D1B40
username jgonzala privilege 15 password 7 094013115D1C52461B
aaa new-model
!
!
aaa authentication login backacs group tacacs+ local
aaa authorization exec backacs group tacacs+ local
aaa authorization commands 15 backacs group tacacs+ local
aaa accounting exec backacs start-stop group tacacs+
aaa accounting commands 15 backacs start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PERU -5
switch 1 provision ws-c3750g-12s
system mtu routing 1500
ip subnet-zero
no ip source-route
 ip routing
ip domain-name Backus
```

```
!
! (Configuracion de spanning tree)
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
!
vlan internal allocation policy ascending
!
ip tftp source-interface Vlan2
ip ssh time-out 60
ip ssh authentication-retries 2
ip ssh version 2
!
class-map match-all VOICE
 match access-group 100
!
!
policy-map VOIP
 class VOICE
  set precedence 5
!
!
!
! (Configuracion de interface Gig)
interface GigabitEthernet1/0/1
 description -- CORE 1 --
 no switchport
 ip address 10.165.77.42 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 mls qos trust ip-precedence
 service-policy input VOIP
!
! (Configuracion de interface Gig)
interface GigabitEthernet1/0/2
switchport access vlan 2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
 mls qos trust ip-precedence
!
! (Configuracion de interface Gig)
interface GigabitEthernet1/0/3
 switchport access vlan 2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
 mls qos trust ip-precedence
!
! (Configuracion de interface Gig)
interface GigabitEthernet1/0/4
 switchport access vlan 2
```

```
 switchport mode trunk
 switchport nonegotiate
 mls qos trust ip-precedence
!
! (Configuracion de interface Gig)
interface GigabitEthernet1/0/5
 switchport access vlan 2
 switchport mode trunk
 switchport nonegotiate
 mls qos trust ip-precedence
!
interface GigabitEthernet1/0/6
 Shutdown
 !
interface GigabitEthernet1/0/7
 Shutdown
!
interface GigabitEthernet1/0/8
 Shutdown
!
interface GigabitEthernet1/0/9
 Shutdown
!
interface GigabitEthernet1/0/10
  Shutdown
!
interface GigabitEthernet1/0/11
 Shutdown
!
interface GigabitEthernet1/0/12
 Shutdown
!
! (Creacion de vlan 2)
interface Vlan2
 description Vlan Usuarios
 ip address 10.165.7.254 255.255.248.0
 ip helper-address 10.165.104.12
 no ip redirects
 no ip unreachables
 no ip proxy-arp
!
no ip http server
no ip http secure-server
!
!
logging trap debugging
logging 10.165.103.253
!
! (creación de Access list)
access-list 90 permit 10.165.103.253
access-list 91 permit 10.165.119.249
access-list 91 permit 10.165.119.250
access-list 91 permit 10.165.119.251
access-list 91 permit 10.165.103.249
```

```
access-list 91 permit 10.165.103.250
access-list 91 permit 10.165.103.251
access-list 91 permit 10.165.103.253
access-list 91 permit 10.165.7.249
access-list 91 permit 10.165.7.250
access-list 91 permit 10.165.7.251
access-list 91 permit 199.80.46.57
access-list 91 permit 10.165.12.110
access-list 91 permit 199.80.48.112
access-list 91 permit 199.80.46.0 0.0.0.255
access-list 91 permit 199.80.48.0 0.0.0.255
access-list 91 permit 199.80.49.0 0.0.0.255
access-list 91 permit 194.102.25.0 0.0.0.255
access-list 91 permit 194.102.26.0 0.0.0.255
access-list 100 permit udp any any range 16384 32767
access-list 100 permit tcp any any eq 1720
access-list 100 permit tcp any eq 1720 any
access-list 100 permit ip host 10.165.12.13 host 10.165.103.145
access-list 100 permit ip any host 10.165.103.145
access-list 100 permit ip any host 10.165.12.13
snmp-server user w5rm1lt3 w5rm1lt3 v1
snmp-server user w5rm1lt3 w5rm1lt3 v2c
snmp-server group BKTEL v3 auth
snmp-server group backusgmd v3 auth notify
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFF7F
snmp-server community r53m4ld RO
snmp-server community w5rm1lt3 RW
snmp-server user w5rm1lt3 w5rm1lt3 v1
snmp-server user w5rm1lt3 w5rm1lt3 v2c
snmp-server trap-source Vlan1
snmp-server location ATE_Sistemas_TR77
snmp-server contact British Telecommunications plc.
snmp-server system-shutdown
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps cluster
snmp-server enable traps entity
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps license
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx root-inconsistency loop-inconsistency
snmp-server enable traps syslog
snmp-server enable traps vlan-membership
snmp-server host 10.165.103.253 version 3 auth backusgmd
snmp-server host 199.80.46.57 r53m4ld
snmp-server host 199.80.48.112 r53m4ld
tacacs-server host 10.165.103.254
tacacs-server directed-request
tacacs-server key 7 135C35393F292873
```

```
!
control-plane
!
banner motd ^C
     #  #  ##  #####  #  # # #  # ####  ##
     #  # # #  #  # ##  # # ##  # #  #  ##
     #  # #  # #  # # # # # ## # #    ##
     # ## ###### #####  # ## # # # # # ###  ##
     ## ## #  # #  #  #  ## # #  ## #  #
     #  # #  # #  # #  # # #  # ####  ##

  ____________________________________________________________________
  You are trying to enter in a private system. Only authorized users
  will accede to the system. Any nonauthorized attempt is prohibited
  and will be registered. The authorized users accept the policies
  and norms of the company. The use of the system is monitoring and
  it will be generated legal measures corresponding.

  ____________________________________________________________________
   Esta intentando ingresar en un sistema privado. Solo usuarios
   autorizados podran acceder al sistema. Cualquier intento no
   autorizado esta prohibido y sera registrado. Los usuarios
   autorizados aceptan las politicas y normas de la empresa. El
   uso del sistema es monitoreado y generara medidas legales
   correspondientes.

  ____________________________________________________________________
^C
!
line con 0
 exec-timeout 5 0
 password 7 135C121C5800160A067C
 authorization commands 15 backacs
 authorization exec backacs
 accounting commands 15 backacs
 accounting exec backacs
 login authentication backacs
line vty 0 4
 access-class 91 in
 exec-timeout 2 0
 password 7 005D1608575719262279
 authorization commands 15 backacs
 authorization exec backacs
 accounting commands 15 backacs
 accounting exec backacs
 login authentication backacs
 transport input telnet ssh
 line vty 5 15
 transport input none
!
ntp clock-period 36030638
ntp server 10.165.103.252
end

smlllpeli2sof01#
```

ANEXO D
PLANTILLA SWITCH WS-C2960-24PC-L (ACCESOS)

```
!
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption

(creación de Vlan)
********** vlan x*********************
!
interface vlan 1
ip addres 10.165.26.23 255.255.255.0
no ip proxy-arp
no ip directed-broadcast
no shut
!
ip default-gateway 10.165.26.1

! (creación de Hostname de equipo)
hostname XXXXXXXXX
! (creación de Password de usuario)
username oguzmanm privilege 15 password Jlo$z&45
username rvinello privilege 15 password Vh$p17a%
! (creación de Password de consola)
enable secret 9atp1uL8
enable password 6@4dt0pO
!
no service tcp-small-servers
no service udp-small-servers
no ip finger
no service finger
no ip http server
no ip http secure-server
no ip source-route
ip domain-name Backus
clock timezone PERU -5
no ip domain-lookup
logging buffered 32000 debugging
no logging console
aaa new-model
aaa authentication login backacs group tacacs+ local
aaa authorization exec backacs group tacacs+ local
aaa authorization commands 15 backacs group tacacs+ local
aaa accounting exec backacs start-stop group tacacs+
aaa accounting commands 15 backacs start-stop group tacacs+
logging trap debugging
logging 10.165.103.253
! (creación de Access list)
access-list 90 permit 10.165.103.253
access-list 91 permit host 10.165.7.251
access-list 91 permit host 10.165.7.250
access-list 91 permit host 10.165.7.249
access-list 91 permit host 10.165.103.253
access-list 91 permit host 10.165.103.251
```

```
access-list 91 permit host 10.165.103.250
access-list 91 permit host 10.165.103.249
access-list 91 permit host 10.165.119.251
access-list 91 permit host 10.165.119.250
access-list 91 permit host 10.165.119.249
snmp-server contact Administrador Switches
snmp-server location SJuan
snmp-server system-shutdown
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps cluster
snmp-server enable traps entity
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vlan-membership
tacacs-server host 10.165.103.254
tacacs-server directed-request
tacacs-server key 9BKTEL9
!
!
banner motd /



    #  #  ##  #####  #  # # #  # ####  ##
    #  # # #  #  # ##  # # ##  # #  # ##
    #  # #  # #  # # # # # # # # #    ##
    # ## # ###### #####  # ## # # # ## # ###  ##
    ## ## #  # # #  #  ## # #  ## #  #
    #  # #  # #  # #  # # #  # ####  ##


 You are trying to enter in a private system. Only authorized users
 will accede to the system. Any nonauthorized attempt is prohibited
 and will be registered. The authorized users accept the policies
 and norms of the company. The use of the system is monitoring and
 it will be generated legal measures corresponding.


  Esta intentando ingresar en un sistema privado. Solo usuarios
  autorizados podran acceder al sistema. Cualquier intento no
  autorizado esta prohibido y sera registrado. Los usuarios
  autorizados aceptan las politicas y normas de la empresa. El
  uso del sistema es monitoreado y generara medidas legales
  correspondientes.
```

```
 /
!
 line con 0
 exec-timeout 5
 password 9en3lr@M8
 authorization commands 15 backacs
 authorization exec backacs
 accounting commands 15 backacs
 accounting exec backacs
 login authentication backacs

!
 line vty 0 4
 exec-timeout 2
 password 9en3lr@M8
 authorization commands 15 backacs
 authorization exec backacs
 accounting commands 15 backacs
 accounting exec backacs
 login authentication backacs

 !
 line vty 5 15
 transport input none

!
 ntp server 10.165.103.252

!
end
```

(Configuracion de SSH)

```
********** SSH **********
!
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
ip ssh version 2
!
! (creación de Interfases)
interface range f0/1 - 24
switchport host
 no shutdown
!
```

ANEXO E
GLOSARIO DE TÉRMINOS

ACL	Listas de Control de Acceso
ARP	Address Resolution Protocol
Core	Núcleo
CRC	Comprobación cíclica de redundancia
DHCP	Dynamic Host Configuration Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
FCS	Secuencia de verificación de trama
HSRP	Hot Standby Router Protocol
Hub	Concentradores
IP	Internet Protocol
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos
IOS	Internetwok Operating System
LLC	Logical Link Control
LAN	Red de área local
MAC	Medium Access Control
NAC	Control de admisión a la red
NIC	Tarjeta de interfaz de red
OTDR	Reflectómetro óptico de dominio de tiempo
PDU	Unidad de Data de Protocolo
PoE	Power over Ethernet
QoS	Calidad de servicio.
SC	Conector Lucent
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Punta Recta
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TIA	Asociación de las Industrias de las Telecomunicaciones
UTP	Cableado de par trenzado no blindado
VLAN	Redes virtuales
WAN	Wide Area Network
XMPP	Extensible Messaging and Presence Protocol

BIBLIOGRAFÍA

[1] William Stallings, "Data and Computer Communications", Macmillan USA, 7th Edition.

[2] Cisco, "CCNP Cisco Certified Network Professional", modulo 3 Multilayer switching, version 3.0

[3] Balaji Sivasubramanian, et al, "Analyzing the Cisco Enterprise Campus Architecture",

[4] Cisco Catalyst 4500 Series Chassis. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps4324/product_data_sheet0900aecd801792b1.pdf

[5] Cisco Catalyst 3560 Series Switches Data Sheet. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5528/product_data_sheet09186a00801f3d7d.pdf

[6] Cisco Catalyst 3750 Data Sheet. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5023/product_data_sheet0900aecd80371991.pdf

[7] Cisco Catalyst 2960-S and 2960 Series Switches with LAN Base Software. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/product_data_sheet0900aecd80322c0c.pdf