UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE UNA RED INTEGRADA PARA UNA EMPRESA BANCARIA

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

PEDRO JOSÉ EDUARDO ESCALANTE TORRES

PROMOCIÓN
2005- I

LIMA – PERÚ
2010

DISEÑO DE UNA RED INTEGRADA PARA UNA EMPRESA BANCARIA

SUMARIO

El presente informe brinda una adecuada y eficiente metodología de diseño de red para la implementación de una red de servicios integrados (datos, telefonía y videoconferencia).

En el primer capítulo se detallan y explican las tecnologías usadas, que son la base teórica para la implementación y operación de los diversos servicios.

En el segundo capítulo se determinan las necesidades de la empresa a nivel de servicios, esto nos sirve para determinar las capacidades a nivel de equipamiento y de enlaces que deben ser proporcionadas para dar un eficiente servicio a los usuarios internos y externos.

En el tercer capítulo se describe la arquitectura y diseño topológico a implementar para cada uno de los servicios y también las descripciones técnicas del equipamiento de telecomunicaciones necesario.

En el cuarto capítulo se definen los costos involucrados en el proyecto, costos de inversión para la habilitación de los servicios y costos de mantenimiento y operación para asegurar la operatividad de cada uno de los servicios.

En el quinto capítulo se dan las conclusiones que han sido obtenidas a lo largo del informe, y se hacen algunas recomendaciones que aseguraran la funcionalidad y permitirá ahorrar costos en los servicios brindados.

Dedico este trabajo a Dios que me ha dado la fortaleza para siempre seguir adelante, a mi familia por su apoyo incondicional y consejos que son una fuente de estimulo y a aquellas personas cuya ayuda ha sido vital para la culminación de este informe.

ÍNDICE

PRÓLOGO

El objetivo de este informe es diseñar una eficiente red de servicios integrados. De esta manera los distintos tráficos de Datos, Telefonía IP y Videoconferencia son encaminados sobre una única red IP, asi se evita tener una infraestructura dedicada por cada uno de los servicios que era lo antiguamente implementado en otras empresas.

La solución implementada permite a la empresa incrementar la productividad, reducir costos de inversión y dar un efectivo mantenimiento a los servicios de voz.

Esta red ofrece el servicio de Internet que es parte del tráfico de datos y para garantizar una alta seguridad de este servicio, se emplean equipos Firewall e IPS, los Firewalls manejan diversas políticas de seguridad para proteger la data interna de cualquier usuario externo y el IPS maneja signaturas que se actualizan cada cierto tiempo para garantizar que se pueda identificar todos los ataques que pudieran generar.

Se ofrece un acceso a extranet, que es una red con la cual se tiene acceso a datos compartidos por otras empresas y cuya información se vuelve muy necesaria y hasta imprescindible, el acceso a este servicio se da por medio de un Firewall debidamente acondicionado que maneja políticas de seguridad y que garantiza los accesos estrictamente necesarios.

La operatividad de todos estos servicios está garantizada por los enlaces de contingencia de esta manera se busca tener los servicios operativos en un 99.9% , así se asegura una alta disponibilidad del negocio.

A lo largo del siguiente informe se va indicando la infraestructura necesaria para una implementación efectiva, estas se ajustan a las necesidades inmediatas y se consideran con un factor de escalabilidad. En todo momento es muy es importante la comunicación con las áreas tanto de sistemas (administradores de servidores, bases de datos, desarrollo, etc.) para que puedan actualizar sobre las nuevas necesidad que puedan surgir y también con las áreas que se encargan de infraestructura física de cada sede (arquitectos, electricistas, mantenimiento).

CAPÍTULO I
MARCO TEÓRICO

1.1 Redes Integradas de Telecomunicaciones

La definición de telecomunicaciones (del prefijo griego tele "distancia", comunicación a distancia) consiste en transmitir un mensaje desde un punto origen hasta otro punto que será el destino, normalmente esta transmisión de información es de forma bidireccional, el termino telecomunicaciones cubre todas las formas de comunicaciones a distancia ya sea radio, televisión, telefonía, transmisión de datos, etc.

Las redes integradas soportan la transmisión y recepción de tráfico de datos, voz y videoconferencia, convergiendo todos estos servicios en una red que tiene la capacidad para procesar estos tipos de tráficos y diferenciarlos unos de otros dándole a cada uno la calidad e importancia que corresponda. Se usa una arquitectura basada en estándares que ofrecen una libre convergencia, nuestra plataforma está basada en la tecnología TCP/IP.

1.1.1 Modelo TCP/IP

Este protocolo fue desarrollado en 1973 por Vinton Cerf, como parte de un proyecto patrocinado por el departamento de defensa de Estados Unidos, empezó conectando redes de servidores de universidades y laboratorios de investigación.

El modelo TCP/IP , recibe este nombre de sus protocolos más importantes las siglas TCP/IP significan Protocolo de Control de Transmisión/Protocolo de Internet, esta tecnología de networking fue desarrollada como un estándar libre, este modelo es influenciado por el modelo OSI que utiliza un enfoque modular de 7 capas, TCP/IP solo utiliza 4 capas las cuales realizan tareas diversas equivalente a las capas del modelo OSI, las principales funciones de las capas del modelo TCP se muestran en la Fig. 1.1:

1.1.2 Capa de Aplicación

En esta capa se establecen las aplicaciones de red y servicios a poder utilizar por el usuario interno. Entre estas aplicaciones se tiene: DNS, FTP, WWW, TELNET, SNMP, etc. como se muestra en la Fig. 1.2.

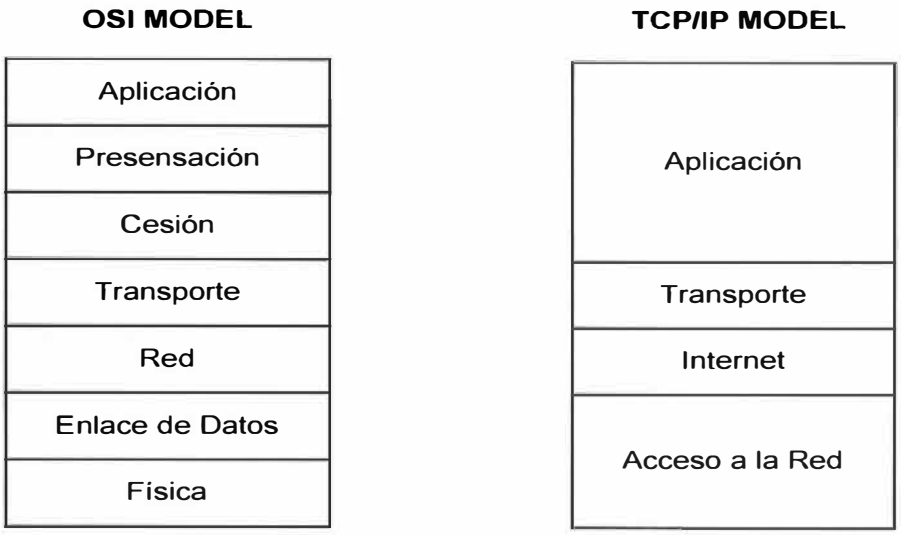


Fig. 1.1 Capas OSI y TCP/IP

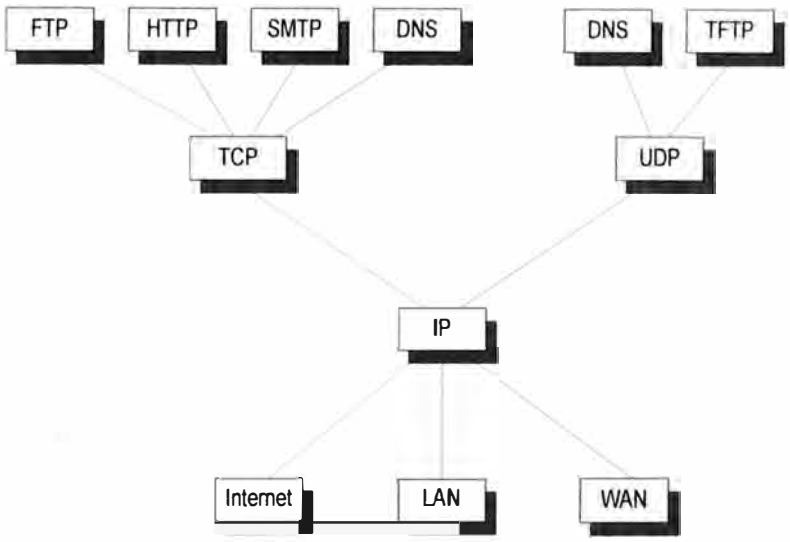


Fig. 1.2 Servicios TCP/IP

1.1.3 Capa de Transporte

Esta capa se encarga de los aspectos de control de flujo, fiabilidad y corrección de errores; forma una conexión lógica entre el equipo transmisor y receptor, en esta capa se encuentran los protocolos TCP y UDP.

Protocolo TCP; El protocolo TCP es orientado a la conexión, ofrece una conexión fiable, establece operaciones de punta a punta, control de flujo y una confiabilidad gracias a los números de secuencia y los acuse de recibo. En esta capa se recibe la información venida desde la capa de aplicación y los divide los paquetes para luego ser enviada a la capa de Internet esta capa se encarga de reensamblar estos mismos paquetes cuando llegan al destino, esta capa también aísla a la capa superior de las tecnologías de red a usar en las capas inferiores.

El Protocolo para el control de la transmisión (TCP) trabaja en un entorno orientado a

conexión, se establece una conexión entre el origen y destino antes de iniciar la transferencia de datos. TCP es responsable de dividir la información en segmentos y reensamblarlos en el destino. reenvía cualquier mensaje que no se haya recibido y re ensambla mensajes a partir de los segmentos recibidos. TCP establece un circuito virtual entre las aplicaciones del usuario final. Algunos de los protocolos que usan TCP:

FTP (Protocolo de transferencia de archivos).

HTTP (Protocolo de transferencia de hipertexto).

SMTP (Protocolo simple de transferencia de correo).

TELNET.

Formato segmento TCP (en la Fig. 1.3 se muestra el formato TCP)

Definiciones de los campos de un segmento TCP:

Puerto origen: El número del puerto que realiza la llamada.

Puerto destino: El número del puerto al que se realiza la llamada.

Número de secuencia: El número para asegurar la secuencia correcta de los datos entrantes.

Número de acuse de recibo: Siguiente octeto TCP esperado.

HLEN: La cantidad de palabras de 32 bits del encabezado.

Reservado: Establecido en cero.

Bits de código: Funciones de control, como configuración y terminación de una sesión.

Ventana: La cantidad de octetos que el emisor está dispuesto a aceptar.

Checksum (suma de comprobación): Suma de comprobación calculada a partir de los campos del encabezado y de los datos.

Indicador de mensaje urgente: Indica el final de la transmisión de datos urgentes.

Opción: Una opción definida actualmente, tamaño máximo del segmento TCP.

Datos: Datos de protocolo de capa superior.

Protocolo UDP; El Protocolo de datagrama de usuario (UDP) no está orientado a conexión, es un protocolo simple que intercambia datagramas entre el origen y destino sin acuse de recibo ni garantía de entrega. El procesamiento de errores y retransmisión debe ser manejado por protocolos de capa superior. El protocolo UDP no usa ventanas ni acuses de recibo de forma que la confiabilidad, en caso sea necesaria, se suministra a través de protocolos de la capa de aplicación. UDP está diseñado para aplicaciones que no requieren ensamblar secuencias de segmentos. Los protocolos que usan UDP incluyen:

TFTP (Protocolo trivial de transferencia de archivos).

SNMP (Protocolo simple de administración de red).

DHCP (Protocolo de configuración dinámica del host).

DNS (Sistema de denominación de dominios).

Formato segmento UDP (en la Fig. 1.4 se muestra el formato UDP.)

Definiciones de los campos de un segmento UDP.

Puerto origen: Número del puerto que realiza la llamada

Puerto destino: Número del puerto al que se realiza la llamada

Longitud: Número de bytes que se incluyen en el encabezado y los datos

Checksum (suma de comprobación): Suma de comprobación calculada a partir de los campos del encabezado y de los datos.

Datos: Datos de protocolo de capa superior

<table>
<tr><th>Bit 0</th><th colspan="2">Bit 15 BIT 16</th><th>BIT 32</th></tr>
<tr><td colspan="2">Puerto Origen (16 Bits)</td><td colspan="2">Puerto Destino (16 Bits)</td></tr>
<tr><td colspan="4">Número de Secuencia (32 Bits)</td></tr>
<tr><td colspan="4">Número de acuse de recibo (32 Bits)</td></tr>
<tr><td>Longitud de encabezado (4 BIT)</td><td>Reservado (6 Bits)</td><td>Bits de código (6 Bits)</td><td>Ventana (16 Bits)</td></tr>
<tr><td colspan="2">Checksum (16 Bits)</td><td colspan="2">Urgente (16 Bits)</td></tr>
<tr><td colspan="4">Opciones (0 - 32 bits)</td></tr>
<tr><td colspan="4">Datos (varia)</td></tr>
</table>

Fig. 1.3 Formato TCP

<table>
<tr><th>Bit 0</th><th>Bit 15 Bit 16</th><th>Bit 32</th></tr>
<tr><td>Puerto Origen (16 Bits)</td><td colspan="2">Puerto Destino (16 Bits)</td></tr>
<tr><td>Longitud (16 Bits)</td><td colspan="2">Checksum (16 Bits)</td></tr>
<tr><td colspan="3">Datos (varia)</td></tr>
</table>

Fig. 1.4 Formato UDP

1.1.4 Capa de Internet

Esta capa encapsula los paquetes venidos de la capa Transporte en datagramas, luego ejecuta algoritmos de enrutamiento con el fin de interconectar distintas redes entre sí, el protocolo que rige esta capa es el Internet IP, protocolos característicos de esta capa son, IP, ICMP e IGMP.

1.1.5 Capa de Acceso a la Red

Define la forma en que los datos son transmitidos a través de la red, incluye los detalles de la capa enlace de datos y física del modelo de referencia OSI; en esta capa se encuentran las tecnologías X.25, Ethernet y otros.

Los estándares del protocolo TCP/IP son abiertos y soportados por todo tipo de sistemas, desarrollados independientemente del hardware de los equipos o sistemas operativos.

TCP/IP funciona en cualquier tipo de medio, no importa si es una red Ethernet, una conexión ADSL o una de fibra óptica. TCP/IP emplea un esquema de direccionamiento público y privado, para el caso de público esta es una única dirección en toda la red, para el caso de direccionamiento privado esta se maneja solo internamente dentro de una empresa.

1.1.6 Encapsulamiento de Datos

Al transmitir los datos, estos cruzan las diversas capas desde la de aplicación hasta la capa de acceso a la red, esta data al pasar por cada capa se le agregara cierta información que es conocida como encabezado, al ser recibida toda la información en el punto destino, estos encabezados son eliminados conforme la data es procesada por cada capa correspondientemente, en la Fig. 1.5 se muestra los encabezados que son agregados durante el encapsulamiento de datos desde la capa de transporte.

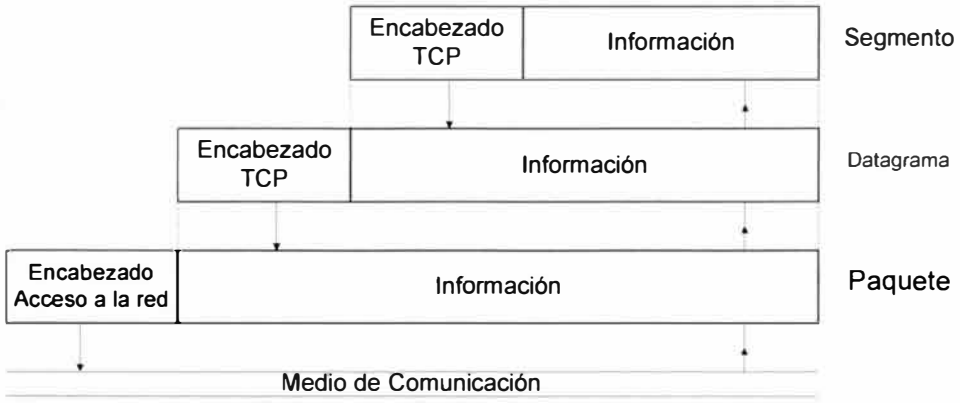


Fig. 1.5 Encapsulamiento Datos.

Se da un ejemplo de un proceso de encapsulamiento:

Tenemos el mensaje "**Programa de Titulación por actualización de conocimientos de la Universidad Nacional de Ingeniería**", como se muestra en la Fig. 1.6.

Programa de Titulacion por actualizacion de conicmientos de la Universidad Nacional de Ingenieria

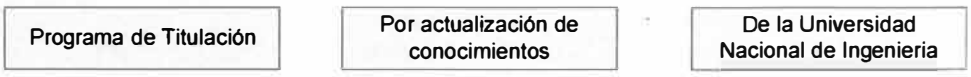


Fig. 1.6 Data a encapsular.

La información recibida en la capa de Transporte TCP es encapsulada colocándole un encabezado TCP en un paquete llamado "Segmento de TCP", como se ve en la Fig. 1.7.

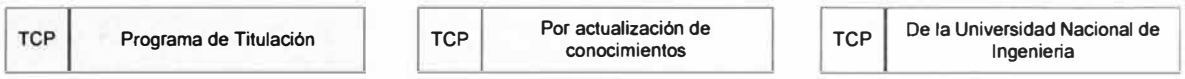


Fig. 1.7 Encapsulamiento en TCP.

La información (Segmento TCP) es entregado a la capa de red IP, esta capa agrega un encabezado IP, a este paquete se le llama Datagrama IP, como se muestra en la Fig. 1.8.

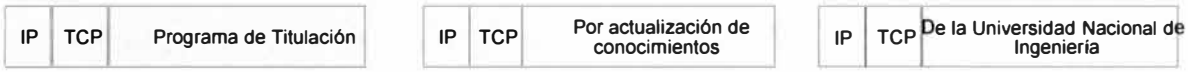


Fig. 1.8 Encapsulamiento en IP.

Finalmente esta información es enviada a la capa de acceso a la red, quien le coloca un encabezado que determina la tecnología con que se encapsula este datagrama, esta determinara que por una red Ethernet pueda enviarse paquetes de diferentes familias de protocolos TCP/IP, DECnet, IPX, etc. Cada uno de estos protocolos tendrá su correspondiente valor para el campo tipo que se encuentra en el encabezado, también en este encabezado el controlador Ethernet calcula la suma de chequeo (cheksum) del paquete completo. En el destino, en esta capa se recalcula el checksum para comprobar que el valor coincide con el original, caso contrario el paquete se desecha. El resultado final sería se muestra en la siguiente, Fig. 1.9:

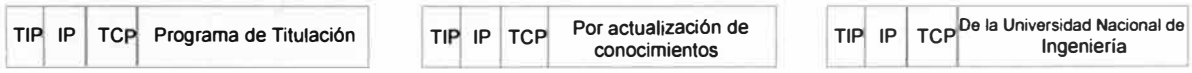


Fig. 1.9 Datos Encapsulados.

Al recibirse en el destino los paquetes, todas las cabeceras se van eliminando en la capa de protocolo que las generó.

En la capa de acceso de red, Ethernet elimina su cabecera al comprobar que el checksum es el correcto luego al verificar en el campo de tipo de código que el datagrama es del tipo IP esta información se pasa a la capa de red IP.

En la capa de red el protocolo IP verifica su cabecera y luego al comprobar en el campo de protocolo (TCP) quita su cabecera correspondiente y se envía a la capa de transporte para que pueda ensamblarse el mensaje original.

1.1.7 Protocolo IP

El protocolo IP es un protocolo de la capa de Internet que permite el desarrollo y envío de datagramas IP a través de un conjunto de redes interconectadas; es un mecanismo sin conexión y no confiable por ello es llamado Best Effor.

El protocolo IP cubre tres aspectos importantes:

Define una unidad básica para el envío de datos en una red, definiendo el formato datagrama IP.

Procesa reglas para que las PCs y Routers procesen paquetes, los descarten o generen mensajes de error.

Se identifica el destinatario teniendo el campo de dirección IP y el campo de máscara de subred.

a) Anatomía del Paquete IP

El paquete IP consta de diversos campos dentro de estos los datos (obtenido de capas superiores) y el encabezado IP, en la Fig. 1.10 se muestran estos encabezados:

Versión: Campo de 4 bits, especifica el formato del encabezado de IP. Si el encabezado es IPv4 este campo tiene el valor de 4 y si es encabezado IPv6. Longitud del encabezado **IP (HLEN)**: Este campo representa la longitud total de toda la información del encabezado, e incluye los dos campos de encabezados de longitud variable.

Tipo de servicio (TOS): Campo de 8 bits, indica el nivel de prioridad o importancia que le ah sido asignada por un protocolo de capa superior.

Longitud total: Campo de 16 bits, indica la longitud total del paquete IP (incluyendo los datos y encabezado).

Identificación: Campo de 16 bits, indica el número secuencial que identifica al datagrama (numero de secuencia).

Señaladores: Campo de 3 bits en el que los dos bits de menor peso controlan la fragmentación. Un bit especifica si el paquete puede fragmentarse, y el otro si el paquete es el último fragmento en una serie de paquetes fragmentados.

Desplazamiento de fragmentos: Campo de 13 bits, usado para ensamblar los fragmentos de datagramas. Este campo permite que el campo anterior termine en un límite de 16 bits.

Tiempo de existencia (TTL): campo que especifica el número de saltos que un paquete puede recorrer, este número disminuye por uno cuando el paquete pasa por un Router y cuando llega a cero el paquete se elimina. Esto evita que los paquetes entren en un loop interminable.

Protocolo: Campo de 8 bits, indica cuál es el protocolo de capa superior, por ejemplo, TCP o UDP.

Checksum del encabezado: campo de 16 bits, garantizar la integridad del encabezado IP.

Fig. 1.10 Paquete IP.

Dirección de origen: campo de 32 bits, especifica la dirección IP del equipo emisor.

Dirección de destino: campo de 32 bits, especifica la dirección IP del equipo receptor.

Opciones: longitud variable permite que IP admita varias opciones, como seguridad.

Relleno: se agregan ceros adicionales a este campo para garantizar que el encabezado IP siempre sea un múltiplo de 32 bits.

Datos: longitud variable hasta un máximo de 64Kb, contiene información de capa superior.

Los campos del encabezado contienen las direcciones origen y destino del paquete y generalmente incluyen la longitud del mensaje. La información para enrutar el mensaje también está incluida en el encabezado de IP, el cual puede ser largo y complejo dependiendo del protocolo de enrutamiento que se utilice.

1.1.8 Direccionamiento IP

La dirección IP opera en la capa de Internet y permite que un equipo pueda localizar a otro dentro de la red.

Una dirección IP es una secuencia de unos y ceros de 32 bits divido en 4 octetos, para que la dirección IP sea más sencilla de manejar se escribe en forma de 4 números decimales (Ej. 192.168.1.2) a cada número decimal se le conoce como un octeto, en la Fig. 1.11 se muestra la conversión de 4 octetos binario a decimal.

Binario : 11000000.10101000.00000001.00001000 y 11000000.10101000.00000001.00001001
Decimal : 192.167.1.8 y 192.168.1.9

Fig. 1.11 Direccionamiento IP.

Para convertir un octeto (byte) que está representado por un número decimal a binario se debe determinar primero la mayor potencia de 2 que pueda caber en el número decimal y así sucesivamente con el resto.

Por ejemplo: 192.168.1.2

192 = 2^7 + 2^6 = 1 1 0 0 0 0 0 0

168 = 2^7 + 2^5 + 2^3 = 1 0 1 0 1 0 0 0

1 = 2^0 = 0 0 0 0 0 0 0 1

2 = 2^1 = 0 0 0 0 0 0 1 0

Cada dirección IP consta de dos partes, una primera parte para identificar la red de donde se conecta el sistema y una segunda para identificar el equipo en particular de esa red. A estas direcciones se les conoce como direcciones jerárquicas porque contiene diferentes niveles, se combina estos dos identificadores en un solo numero este número debe ser único ya que direcciones repetidas no harían posible el enrutamiento. La primera parte identifica la dirección de la red, la segunda la parte del equipo es decir un equipo en particular de la red.

Las direcciones IP se dividen en clases (Clase A, Clase B y Clase C) para definir el tamaño de las redes en la Fig. 1.12 se muestra el rango de direcciones IP por clases.

Las direcciones Clase A, se asignan a redes de mayor tamaño, soportan mas equipos en red.

Las direcciones Clase B, se utilizan para redes de tamaño medio.

Las direcciones Clase C, se usan para redes pequeñas.

Clase de Direccion IP	Bits de Mayor Peso	Primer Intervalo de direccion de octeto	Numero de bits en la direccion de red
Clase A	0	0 - 127	8
Clase B	10	128 - 191	16
Clase C	110	192 - 223	24
Clase D	1110	224 - 239	28

Fig. 1.12 Clases direccionamiento IP.

Cada dirección IP de 32 bits como se vio antes se divide en la parte de red que corresponde a una cantidad de octetos y la parte de host los octetos restantes. En la Fig. 1.13 se muestra la distribución de octetos por campo de red y host. Las direcciones Clase D se utilizan para grupos multicast.

Según el uso de las direcciones IP estas se clasifican en direcciones publicas y direcciones privadas. La agencia de asignación de de números de Internet (IANA) administra la provisión de las direcciones IP públicas para evitar se genere duplicidad, estas direcciones públicas son únicas pero con el rápido crecimiento de Internet las direcciones IP empezaron a escasear por lo que se desarrollaron nuevos esquemas de direccionamiento así como el enrutamiento entre dominios sin clase CIDR y el IPv6. Otra solución al problema de escasez de direcciones públicas es el uso de direcciones IP privadas que no están

conectadas a Internet, para esto se puede usar cualquier dirección de equipo siempre que no se repita dentro de la red privada. Las direcciones privadas son usadas dentro de pequeñas y grandes empresas para comunicar todos sus equipos internos mediante protocolos de enrutamiento de ser necesario .El RFC 1918 asigna 3 bloques de direcciones privadas para uso interno. En estos 3 bloques de direcciones privadas se tiene un intervalo en Clase A, Clase B y Clase C. En la Fig. 1.14 se muestra las direcciones privadas por clase. Es el administrador de red quien se encargara de seleccionar el direccionamiento que estime conveniente cumpliendo con las necesidades de la empresa. La conexión de una red que utiliza direcciones privadas hacia la red externa requiere que las direcciones privadas se conviertan a direcciones públicas o direcciones de extranet. Este proceso de conversión se le conoce como traducción de direcciones de red (NAT). En general, un router es el equipo que se encarga de realizar los Nat que sean necesarios hacia la red externa.

Clase A	Red (8 bits)	Host(24 bits)		
Octetos	1	2	3	4

Clase B	Red(16 bits)		Host(16 bits)	
Octetos	1	2	3	4

Clase C	Red(24 bits)			Host(8 bits)
Octetos	1	2	3	4

Clase D	Host(32 bits)			
Octetos	1	2	3	4

Fig. 1.13 Octetos IP.

Clase	Intervalo de direcciones privadas
A	10.0.0.0 a 10.255.255.255
B	172.16.0.0 a 172.31.255.255
C	192.168.0.0 a 192.168.255.255

Fig. 1.14 Intervalo de Direcciones IP.

1.1.9 Asignación de Dirección IP

Para la asignación de direcciones IP, el administrador de la red puede optar por asignarlas de forma estática o dinámica.

El direccionamiento estático, funciona mejor en redes pequeñas con poca frecuencia de cambios, es fundamental que el administrador de la red lleve un registro de las direcciones

IPs asignadas para evitar conflictos. Para los servidores se recomienda usar direcciones IP estáticas, al igual que las impresoras, equipos de comunicación.

El direccionamiento dinámico, se da por medio del protocolo DHCP que permite que cada equipo pueda obtener una dirección IP en forma dinámica sin que el administrador de la red tenga que configurar manual e individualmente equipo por equipo. Para usar esta forma de direccionamiento se necesita tener un rango de IPs bien definidas y un servidor DHCP que las asigne. Para nuestro caso usaremos este tipo de direccionamiento por manejar una gran cantidad de equipos en red.

1.1.10 Enrutamiento

Se tienen diversos protocolos de enrutamiento que permiten que los equipos ubicados en distintas redes puedan comunicarse entre sí. El protocolo IP es un protocolo no orientado a la conexión lo que significa que no establece ningún circuito de conexión dedicado antes de trasmitir alguna data por lo que es el enrutamiento el mecanismo que hace que la data llegue a su destino. durante la transmisión de información los datos son enviados hacia abajo de capa por capa siguiendo el modelo TCP y es en la capa 2 donde la capa de red encapsula los datos en paquetes lo que se denomina datagramas , el protocolo IP determina la cabecera lo que incluye el direccionamiento y otra información de control que son necesarias para determinar la ruta que seguirá el paquete hasta su destino; se empaquetan todos los datos recibidos de capas superiores, a medida que los paquetes son enviados a través de la red , la información de capa 1 es eliminada y cambiada ,y una vez que se llega a la capa de red este redirige el tráfico hacia su destino final. La determinación de la ruta ocurre a nivel de la capa de red y permite que un router establezca una tabla de enrutamiento seleccionando las mejores rutas hacia las redes a donde se desea llegar.

1.1.11 Protocolo de Enrutamiento interno y externo

Se debe tener claro el concepto de sistema autónomo, este es una red o conjunto de redes bajo una administración en común, los protocolos de enrutamiento interno (RIP, IGRP, EIGRP, OSPF, IS-IS) enrutan datos dentro de un mismo sistema autónomo mientras que los protocolos de enrutamiento externo enrutan redes entre sistemas autónomos diferentes (BGP). En la Fig. 1.15 se muestra los protocolos de enrutamiento interno disponibles.

Como protocolo de enrutamiento interno, se utiliza el protocolo EIGRP este es una versión del protocolo IGRP mejorada que utiliza algunas funciones del protocolo estado de enlace y por la forma de operación es un protocolo de enrutamiento vector distancia avanzado, también se le conoce como un protocolo de enrutamiento hibrido, este protocolo

está diseñado para superar las limitaciones de los protocolos vector distancia (RIP) y también realiza una convergencia más rápida y bajo gasto de ancho de banda.

Como protocolo de enrutamiento externo, se utilizara el protocolo de Gateway fronterizo BGP, este protocolo intercambia información entre sistemas autónomos a la vez que garantiza la selección de la mejor ruta disponible y libres de loops, BGP no usa las métricas usadas por los protocolos de enrutamiento interno, este protocolo toma decisiones de enrutamiento basándose de las políticas en la red.

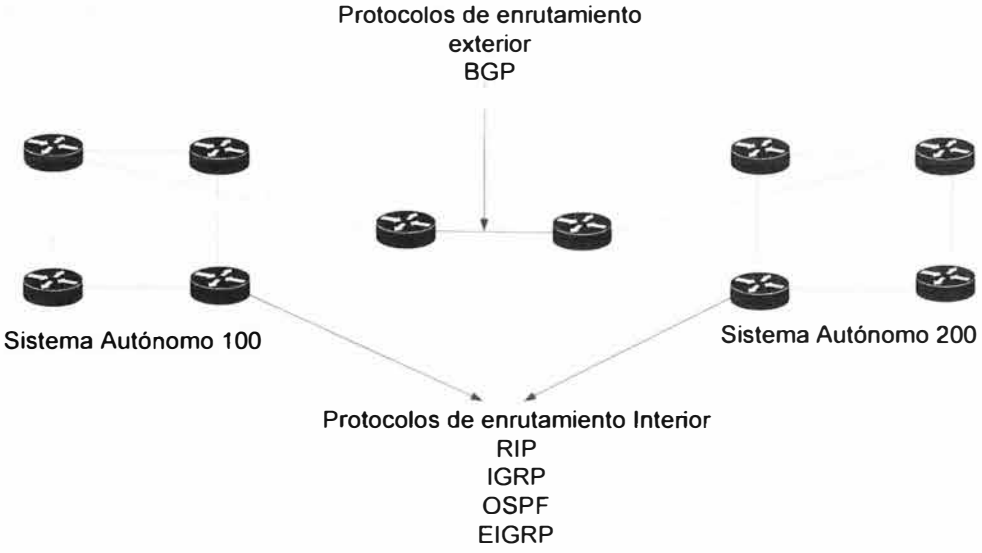


Fig. 1.15 Protocolos de Enrutamiento

1.2 Plataforma Ethernet

Su comienzo fue en 1970 y desde entonces ah evolucionado para satisfacer la creciente demanda de alta velocidad, al aparecer un medio como la fibra óptica Ethernet ah tenido que adaptarse sacando ventaja del ancho de banda que se puede transmitir por este medio. Ethernet es un protocolo sencillo, con capacidad para adecuarse a nuevas tecnologías, confiable y con bajo costo de instalación.

Ethernet comenzó como una tecnología LAN y ha ido evolucionando en nuevas tecnologías como Gigabit Ethernet que se usa ahora en enlaces WAN por el ancho de banda que ofrece. La familia de la tecnología Ethernet incluyen Fast Ethernet y Gigabit Ethernet sus velocidades pueden ser de 10, 100, 1000 o 10000 Mbps, Ethernet emplea señalización banda base la cual utiliza todo el ancho de banda del medio de transmisión. Ethernet usa un sistema de direccionamiento compuesto por direcciones MAC que tienen 48 bits de largo y se expresan en hexadecimales (de estos los primeros seis dígitos identifican al fabricante y los seis dígitos restantes el número de serie de la interfaz), es en la capa de enlace de datos donde se agrega encabezado correspondiente a la MAC y luego

este mensaje es enviado a su destino abriendo rutas de comunicación utilizando la dirección MAC de destino. A medida que estos datos viajan por la red la tarjeta de red de cada dispositivo verifica si su dirección MAC coincide con la dirección MAC destino transportada en la trama de datos y si no coincide descarta la trama , si coincide esta data se pasa a capas superiores

1.2.1 Estructura Ethernet

El paquete Ethernet está compuesto por los campos que se muestran en la Fig. 1.16:
El Preámbulo: es un patrón alternado de unos, se utiliza para la sincronizar los paquetes.
Dirección destino: contiene la dirección MAC destino (unicast, multicast o broadcast).
Dirección de origen: contiene la dirección MAC de origen (generalmente es unicast)
Longitud/Tipo: admite dos usos diferentes. Si el valor es menor a 1536 decimal, 0x600 (hexadecimal), entonces el valor indica la longitud la longitud indica la cantidad de bytes de datos. El valor del tipo especifica el protocolo de capa superior que recibe los datos.
Campos de datos y de relleno: pueden tener cualquier longitud, mientras que el paquete no exceda el tamaño máximo permitido de paquete. La unidad máxima de transmisión (MTU) para Ethernet es de 1500 octetos. Se inserta un relleno no especificado inmediatamente después de los datos del usuario cuando no hay suficientes datos para que la trama cumpla con la longitud mínima especificada. Ethernet requiere que cada trama tenga entre 64 y 1518 octetos de longitud.
FCS: contiene el valor de verificación de CRC de 4 bytes, esto con el fin de verificar si hay paquetes dañados, es creado inicialmente por el equipo emisor y recalculado por el equipo receptor. Si existe un bit dañado en cualquier campo desde la dirección destino hasta el fin del campo de FCS entonces el Cheksum saldrá diferente al original y el paquete se considera dañado.

Ethernet es una tecnología de broadcast de medios compartidos donde el método que se usa para acceder a la red es CSMA/CD que tiene las funciones de transmitir y recibir paquetes de datos, decodificar paquetes de datos y detectar errores en los paquetes. En el método CSMA/CD los dispositivos que deseen transmitir primero deben determinar si el medio está disponible, si el dispositivo determina que la red está ocupada entonces el dispositivo esperara un tiempo aleatorio (determinado por un algoritmo) antes de volver a internar transmitir datos. Se produce una colisión cuando dos dispositivos encuentran la red disponible y transmiten datos por esta. Las colisiones producen una pérdida del ancho

de banda de la red, afecta a todos los dispositivos que intentan conectarse a la red reduciendo así su rendimiento

8	6	6	2	64 a 1500	4
Preambulo	Dirección de destino	Dirección de origen	Tipo	Datos	Secuencia de verificación de paquete

Fig. 1.16 Estructura Ethernet

1.2.2 Conmutación Ethernet

A medida que aumentan los dispositivos conectados al medio físico Ethernet, aumenta la demanda sobre el ancho de banda de este medio por lo que abra mas equipos queriendo transmitir por el mismo medio al mismo tiempo, una solución es agrupar los dispositivos y dividir en segmentos la forma de acceso al medio. Las formas de segmentar el acceso a la red se da por medio del dominio de colisión y el dominio de broadcast.

El dominio de colisión son segmentos de red física, donde las colisiones detienen todas las transmisiones que se puedan hacer en una red un determinado tiempo, este tiempo depende de un algoritmo de postergación. Los equipos como hubs, extienden los dominios de colisión, los switchs y routers dividen los dominios de colisión, los switchs construyen una tabla donde se encuentran las mac aprendidas por puerto, así se sabe porque puerto específicamente transmitir la información según la dirección mac destino, los routers no envían colisiones.

Los dominios de broadcast, se producen cuando se quiere enviar una información y no se conoce el destino, esta información se envía a todos los equipos que son parte del mismo dominio de broadcast, este dominio está conformado por varios dominios de colisión, los routers segmentan los dominios de broadcast.

1.2.3 Flujo de datos

Para explicar del flujo de datos que se trasmiten, se considera el modelo OSI. Hay que tener en cuenta que los datos se encapsulan con una dirección IP de origen y destino en la capa de red y se encapsula con una MAC de destino y origen en la capa 2.

En la capa 3 se hace un filtro correspondiente la IP destino para saber por cual ruta enviar la data, luego en la capa 2 se filtran la tramas basados en la dirección MAC destino, la trama se envía si se dirige a un destino desconocido fuera del dominio de colisión así también se envía si se trata de un broadcast, multicast o unicast, esta trama no se envía si se encuentra al dispositivo destino dentro del mismo dominio del colisión , en la capa 3 se hace un filtrado de IP destino y el paquete solo es enviado si se encuentra esta IP destino. El flujo de datos implica el movimiento de la data a través de las diversas capas, la capa 1

para transmitir en los medios físicos, la capa 2 para la administración de dominios de colisión y la capa 3 para la administración de dominios de broadcast. En la Fig. 1.17 se muestra un ejemplo de este flujo de datos.

1.2.4 Velocidad de Ethernet

Ethernet ah tenido éxito por su simplicidad y por la forma de adaptarse para satisfacer las necesidades cambiantes de los medios. Las modificaciones de Ethernet han resultado en adelantos desde 10Mbps pasando por 100Mbps y llegando sobrepasar 1000Mbps.

Ethernet de 100Mbps, también conocido como Fast Ethernet puede usar un medio de cobre 100Base-TX o un medio de Fibra óptica 100Base-FX, ambos modelos comparten el mismo formato de temporización con respecto al formato de la trama este no cambia. Fast Ethernet utiliza dos pasos para la codificación la primera es una técnica conocida como 4B/5B y la segunda es la codificación de línea correspondientemente si el medio es de cobre o fibra. Fast Ethernet se puede ejecutar a half (donde solo se transmite o recibe información no se puede hacer ambas al mismo tiempo) o full duplex (donde se puede transmitir y recibir información al mismo tiempo se llega a 200Mbps).

Ethernet de 1000Mbps, también conocido como Gigabit Ethernet puede usar un medio de cobre 1000Base T (en cable UTP Cat5 o mejor) o un medio de Fibra óptica 1000Base X, la diferencia de Gigabit Ethernet con Ethernet y Fast Ethernet se encuentra en la capa física, a velocidad altas como en la que se transmite a Gigabit Ethernet se requiere frecuencias cercanas a las limitaciones de ancho de banda que tienen los medios de cobre. Gigabit Ethernet utiliza dos distintos pasos de codificación, la transmisión de datos se realiza de manera eficiente utilizando códigos para representar la corriente binario de bits los datos codificados proporcionan sincronización, uso eficiente del ancho de banda y mejores relaciones de señal/ruido. La codificación que se usa en el medio de fibra es 8B/10B y luego la codificación de línea sin retorno a cero (NRZ), en la Fig. 1.17 se muestra el flujo de datos por los equipos de comunicaciones.

1.3 Procesamiento de Señales

1.3.1 Codificación de la Señal

La codificación busca sincronizar la data que se envía por un medio, dependiendo el tipo del medio físico. Se necesita de un esquema de señalización, la que incluye suficiente información de reloj para asegurar que los circuitos trabajen correctamente, con la señalización se mantiene una tasa de errores baja y se garantiza que la señal pueda sobrevivir por el medio.

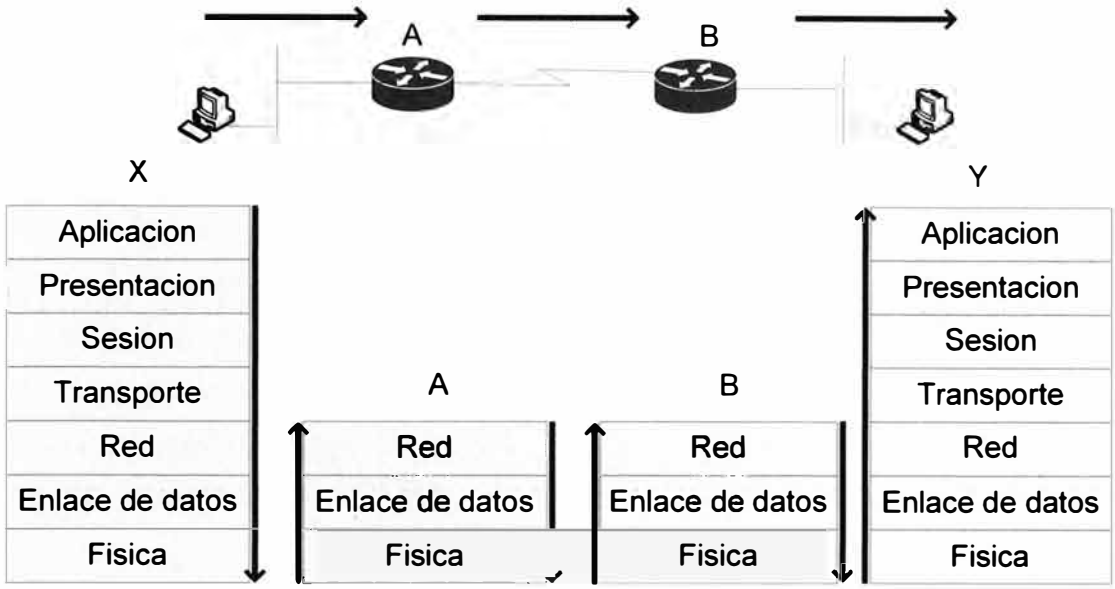


Fig. 1.17 Flujos de Datos

Los métodos de señalización hacen referencia a la forma en que se codifican los datos y el espectro de frecuencia del medio, los métodos de señalización que se usan en la LAN son broadband y baseband.

La señalización broadband, refiere al ancho de banda del medio que es sub dividido por frecuencias y así formar canales, cada uno de estos canales transmite información independiente de los otros.

La señalización baseband, refiere a que solo una señal es transmitida por el medio por lo que utiliza todo el ancho de banda disponible.

Broadband utiliza una tecnología análoga donde MODEM que operan a 4Khz o mas colocan la señal portadora sobre el medio físico de transmisión, broadband es unidireccional por lo que necesita de dos canales para hacerla bidireccional. Los métodos más usados para transmitir en broadband son:

Frecuency Shift Keying (FSK)

Amplitude Modulation Phase Shift Keying (AM PSK)

1.3.2 Tecnología Ethernet

Ethernet utiliza una señalización Baseband con codificación Manchester, en este sistema de codificación se combinan los datos y el reloj en símbolos de bit, cada símbolo de bit se divide en dos partes y la polaridad de la segunda mitad es siempre contraria a la baja, cada bit se envía con una transición de reloj que es utilizada por la estación receptora para

sincronizar todos los datos que son recibidos.

El método de Manchester permite sincronizar al receptor y extraer la data pero a la vez usa el doble de ancho de banda, cada medio de 10Mbps (10 Base-T, 10Base-FL, 10Base5) utiliza una codificación Manchester y utilizan una señalización de línea diferentes.

10BaseT utiliza una señalización de línea física de corriente balanceadas, un hilo lleva entre 0 a 2.5 voltios y el otro de 0 a -2.5. 10BaseFL utiliza una señalización de línea NRZ (No retorno a cero), un pulso de luz indica el nivel alto y la ausencia de luz un nivel bajo.

1.3.3 Tecnología Fast Ethernet

En Fast Ethernet los medios más usados son, 100Base-TX y 100Base-FX; donde Base indica la señalización Baseband , TX que usa dos pares del cable de par trenzado y FX usa Fibra óptica (usa dos hilos de la fibra). Debido a la velocidad en que se transmite en Fast Ethernet 100Mbps y la alta frecuencia en el cable se tiene que la señalización es más compleja que la Ethernet. Dependiendo del medio físico (cobre o Fibra), se va a usar una codificación y señalización diferente:

100Base-TX utilizara una codificación 4B/5B con señalización MLT-3.

100Base-FX utilizara una codificación 4B/5B con señalización NRZI.

El uso de la codificación 4B/5B está definida como código de bloques, esta codificación permite transportar datos de control en cada símbolo representado por un código de 5 bits (estos 5 bits son representados por 4bits), se tiene además un código de relleno que se usa para forzar errores en la señalización.

NRZI, esta señalización utiliza media onda para codificar cada bit.

MLT-3, utiliza un cuarto de onda para codificar cada bit.

Al combinar 4B/5B con señalización NRZI y MLT-3 la señal requiere menor ancho de banda, pero es lo suficientemente robusta para codificar 100Mbps. 100Base-FX al utilizar codificación 4B/5B y señalización NRZI requiere un ancho de banda de 62.5Mhz, ya que la velocidad por la codificación aumenta de 100Mbps a 125Mbps y NRZI utiliza dos bits por ciclo primera mitad. Un cero se define como una señal cuya primera parte es alta y la segunda mitad 100Base-TX al utilizar 4B/5B y señalización MLT-3 requiere un ancho de banda de 31.25Mhz, ya que MLT-3 representa 4 bits por ciclo y requerirá la mitad del ancho de banda de 100Base-FX.

1.3.4 Tecnología Gigabit Ethernet

Esta tecnología tiene como estándar IEEE802.3z para 1000Base-X, especificando una conexión full duplex a 1Gbps e IEEE 802.3ab para 1000Base T que especifica el uso de un

cable de cobre de categoría 5 a más. Las 1000BASE-TX, 1000BASE-SX y 1000BASE-LX utilizan los mismos parámetros de temporización, utilizan un tiempo de bit de 1 nanosegundo (0,000000001 segundos) o 1 mil millonésima parte de un segundo. La trama de Gigabit Ethernet presenta el mismo formato que se utiliza en Ethernet de 10 y 100-Mbps. Para esta tecnología puede usarse como medio de transmisión el cable de cobre trenzado o la fibra óptica, en cable de cobre UTP se usan los 8 hilos de ellos 4 pares de hilo son para transmisión y los otros 4 pares para recepción.

Gigabit Ethernet (1000BASE-X) con base de fibra utiliza en una primera fase la codificación 8B/10B que es similar a la codificación 4B/5B luego en una segunda fase la codificación simple de línea sin retorno a cero (NRZ) de la luz en la fibra óptica. La codificación 8B/10B ofrece una buena detección de error y una sincronización confiable de bits y reloj ambas son la llave para una alta velocidad en la red. En esta codificación 8 bits de data son enviadas como 10bits, los extras 2 bits requieren una señal de transmisión de 1.25 baud por cada bit para transmitir por la red 1Gbps, los extras bits incluyen información de control de transferencia como el paquete de inicio, el paquete final y el identificador. Al recibir el paquete final todos los símbolos son validos si estos contienen cinco 1's y cinco 0's. Caso contrario algún problema debe haber en la transmisión.

Gigabit Ethernet (1000BASE-T) con base en cable par trenzado de cobre de Cat5E a superiores utiliza una codificación de línea 4D-PAM5. La transmisión y recepción de la información se produce en forma bidireccional en ambos sentidos y como es de esperar, esto provoca una colisión permanente en los pares de hilos. La codificación PAM-5, puede alcanzar 2 bits por baudio con una ganancia de 3dB. Esta codificación no ofrece un alto alcance con el uso de la fibra óptica y los dispositivos actuales podrían no soportar esta codificación. La codificación representa los bits con un código de 5 niveles (+2, +1, 0, -1, -2) 4D/PAM5.

En un medio físico UTP se tienen 4 pares de hilo de cobre, en Fast Ethernet 100Base-TX se utiliza un par para transmitir información usando la codificación 4B/5B y otro par es usado detección de colisiones y recibir. 4B/5B es un modelo de codificación que usa 5 bits de la señal para cargar 4 bits de datos, posee 16 valores de datos de los cuales 4 son códigos de control y un código que no se usa.

1.4 Modelos Teóricos

El uso de la tecnología IP para el tráfico de datos, voz y videoconferencia es la llave principal para la transmisión y recepción de estos tipos de tráficos, con esta tecnología se

tiene la posibilidad de establecer niveles de prioridades en el tráfico a transmitir dependiendo de la naturaleza de cada tipo de trafico.

En las mayorías de empresas con más de una sede se establecen conexiones desde el site principal con cada uno de las sucursales, de esta forma se tiene una administración centralizada de todos los servicios, el administrador de red tiene la labor de desarrollar un adecuado dimensionamiento considerando la cantidad y al tipo de tráfico a transmitir. Se tiene como principal objetivo una alta disponibilidad del acceso a la red debido a la importancia del negocio, por ello se establecen sistemas alternos de conexión para en caso de fallas estos permitan a la empresa seguir operando. El acceso a la red Lan es mucho mayor al acceso WAN debido a que en la Lan se manejan tecnologías de mayor velocidad, diversos servidores pueden encontrarse dentro de la Lan (Intranet) y el acceso a estos son distintos a servidores externos (de redes remotas), las redes internas están diseñadas para permitir el acceso por usuarios con privilegios de acceso a la LAN interna de la organización y el acceso es mas rápido comparado al acceso a un server externo, el ancho de banda se define como la cantidad de información que puede fluir a través de una conexión de red en un período dado. El uso de la tecnología Ethernet y los protocolos de comunicaciones usadas en la implementación de servicios de este informe (telefonía IP, videoconferencias y segmentación de datos) son usados por diversas empresas como:

Municipalidades.

Tiendas por departamento.

Supermercados.

Empresas Bancarias.

Por ello este informe se basa en tecnologías que en la práctica se encuentran operando eficientemente en la mayoría de grandes empresas como más de una sede.

Para determinar el ancho de banda a necesitar se debe tener claro los siguientes puntos:

El ancho de banda es finito. En otras palabras, independientemente del medio que se utilice para construir la red, existen límites para la capacidad de la red para transportar información. El ancho de banda está limitado por las leyes de la física y por las tecnologías empleadas para colocar la información en los medios.

El ancho de banda no es gratuito. La red de área local (LAN) tiene la capacidad de brindar un ancho de banda casi ilimitado durante un período extendido de tiempo. Para conexiones por medio de la red de área amplia (WAN), hace falta contratar un eficiente ancho de banda de los proveedores de servicios. En ambos casos, el significado del ancho

de banda, y los cambios en su demanda a través del tiempo, pueden ahorrar importantes sumas de dinero.

El ancho de banda es un factor clave a la hora de analizar el rendimiento de una red, Se debe comprender el fuerte impacto del ancho de banda y la tasa de transferencia en el rendimiento y el diseño de la red. La información fluye en una cadena de bits de un computador a otro en todo el mundo representado enormes cantidades de información que fluyen de ida y de vuelta a través de grandes distancias en segundos, o menos.

La demanda de ancho de banda no para de crecer. No bien se construyen nuevas tecnologías e infraestructuras de red para brindar mayor ancho de banda, se crean nuevas aplicaciones que aprovechan esa mayor capacidad. La entrega de contenidos de medios enriquecidos a través de la red, incluyendo video y audio fluido, requiere muchísima cantidad de ancho de banda. Hoy se instalan comúnmente sistemas telefónicos IP en lugar de los analógicos, se tiene como objetivo el transmitir diversos tipos de tráfico de diferentes prioridades entre las sucursales y proveedores. En la Fig. 1.18 se muestra un ejemplo básico de una empresa con sucursales distribuidos estratégicamente con los cuales se tiene una interconexión permanente y por donde se transmitirá variado tipos de tráfico (datos, telefonía IP, videoconferencia). Es en el site principal donde se concentran los enlaces hacia el exterior y donde principalmente se mantienen los servidores a los cuales se conectaran toda la empresa, centrales telefónicas, servidores de aplicaciones, etc. y es por esta razón la importancia que tiene el enlace redundante para garantizar siempre la operatividad de la red.

Con respecto a la implementación de la solución de telefonía IP, permite a la empresa mejorar la gestión de contactos con los clientes, incrementar la productividad, disminuir el coste operativo y reducir los gastos de telefonía entre sucursales, ya que no suponen un importe adicional al de las comunicaciones de datos. Además, es posible ampliar de forma sencilla el número de conversaciones simultáneas entre sedes, configurar el plan de numeración en función de las necesidades de la empresa y administrar de forma centralizada todo el sistema de telefonía IP.

1.4.1 Protocolo VRRP

Este protocolo es usado en todas las empresas que se menciono antes y permite una contingencia dinámica en caso de fallas con el enlace principal.

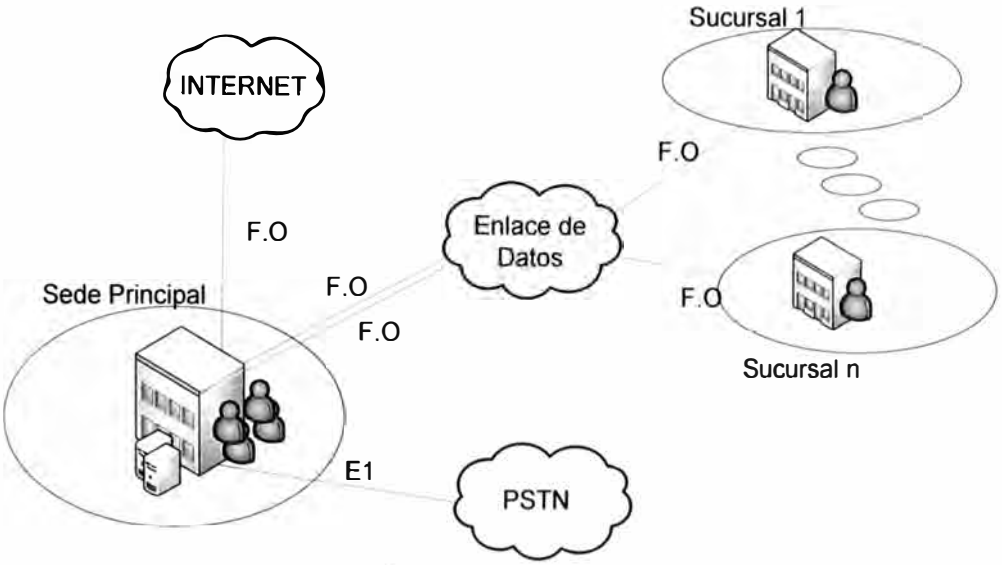


Fig. 1.18 Enlaces de Servicios

Para situaciones en las que se tenga problemas con el equipo de salida principal y se necesite conmutar a otro equipo secundario hasta que se restablezca el principal, se tiene el protocolo VRRP Virtual Router Redundancy Protocol , es un protocolo de redundancia no propietario definido en el RFC 3768 diseñado con el fin de aumentar la disponibilidad del enlace , por medio de este protocolo se tienen dos Routers que proveen el mismo servicio uno será el principal y el segundo estará en standby, cuando el router principal tenga problemas entonces todo el tráfico que llega a este se conmutara al equipo que se encontraba en standby esto hasta que el router principal pueda estar nuevamente activo , los routers deben estar en el mismo segmento de red que los equipo que necesitan acceder a este servicio. El aumento de fiabilidad se consigue mediante el anuncio de una IP virtual como una puerta de enlace por defecto en lugar de la IP de los routers físicos. Los dos routers físicos se configuran representando a la IP virtual, con sólo uno de ellos realizando realmente el enrutamiento. Si el router físico actual que está realizando el enrutamiento falla, el otro router físico negocia para sustituirlo. Se denomina router principal al router físico que realiza realmente el enrutamiento y routers secundario a los que están en espera de que el principal falle.

La principal ventaja obtenida de la utilización del VRRP es una mayor disponibilidad del router por defecto sin necesidad de configurar encaminamiento dinámico o protocolos de descubrimiento de routers en cada equipo final. El VRRP está diseñado para eliminar el punto único de fallo inherente en los entornos configurados con ruta por defecto estática
El protocolo VRRP utiliza los mensajes de anuncio (Advertisements) para indicar que el router que hace de Master se encuentra activo. Estos mensajes se envían a la dirección IP

multicast 224.0.0.18 asignada por la Internet Assigned Numbers Authority (IANA). El número de protocolo IP establecido por la IANA para el VRRP es el 112 (en decimal). Los Advertisements contienen información sobre el router virtual, su prioridad, etc.

Si durante un periodo de tiempo determinado los routers de backup dejan de recibir los mensajes del Master, entonces el router de backup de mayor prioridad pasa a convertirse en el nuevo Master del router virtual.

Por defecto, un equipo de backup que tenga mayor prioridad que el Master actual puede expropiar en sus funciones al mismo y convertirse en el nuevo Master. Este comportamiento asegura que siempre se encuentra como Master el router con mayor prioridad. Sin embargo, si por alguna razón es necesario, se puede deshabilitar administrativamente la expropiación del router virtual.

1.4.2 Protocolo HSRP

El protocolo HSRP es propietario de cisco que provee redundancia en capa 3:

Funcionamiento. Con el fin de minimizar el tráfico de red, sólo los activos y los routers de espera enviar mensajes periódicos HSRP después de que el protocolo ha completado el proceso de elección. Routers adicionales en el grupo HSRP permanecen en el estado LISTEN. Si el router se desactiva, el router standby asume la función de router activo. Si el router en espera o se convierte en el router activo, el otro router es elegido como el router de espera. Cada grupo espera emula un router virtual única (puerta de enlace predeterminada). Para cada grupo, una sola dirección MAC e IP se asignan. Varios grupos de reserva pueden coexistir y se superponen en una LAN y routers individuales pueden participar en varios grupos. En este caso, el router mantiene un estado independiente y temporizadores para cada grupo, supongamos que disponemos de una red que cuenta con dos routers redundantes, RouterA y RouterB. Dichos routers pueden estar en dos posibles estados diferentes: principal (Router A) y secundario (Router B). Ambos routers intercambian mensajes, concretamente del tipo HSRP hello, que le permiten a cada uno conocer el estado del otro. Estos mensajes utilizan la dirección multicast 224.0.0.2 y el puerto UDP 1985.

Si el router principal no envía mensajes de tipo hello al router de secundario dentro de un determinado periodo de tiempo, el router secundario asume que el principal está fuera de servicio (ya sea por razones administrativas o imprevistas, tales como un fallo en dicho router) y se convierte en el router principal. La conversión a router activo consiste en que el router secundario obtiene la dirección virtual que identifica al grupo de routers.

Para determinar cuál es el router principal se establece una prioridad en cada router. La prioridad por defecto es 100. El router de mayor prioridad es el que se establecerá como activo. Hay que tener presente que HSRP no se limita a 2 routers, sino que soporta grupos de routers que trabajen en conjunto de modo que se dispondría de múltiples routers actuando como secundario en situación de espera.

Cuando se pasa del estado secundario al principal el router en espera toma el lugar del router principal, una vez que el temporizador holdtime expira (un equivalente a tres paquetes hello que no vienen desde el router activo, timer hello por defecto definido a 3s y holdtime por defecto definido a 10s). Los tiempos de convergencia dependerán de la configuración de los temporizadores para el grupo y del tiempo de convergencia del protocolo de enrutamiento empleado.

CAPÍTULO II
DETERMINACIÓN DE LAS NECESIDADES

2.1 Descripción de la Empresa

Para una mejor comprensión se define los siguientes términos a usar:

Usuarios: Usuarios internos o trabajadores que pertenecen a la empresa, cuyo propósito es cumplir con las labores asignas en bien de la empresa.

Clientes: Cliente es la persona, empresa u organización que adquiere de forma voluntaria productos o servicios que necesita de una empresa que los provea.

En la actualidad las empresas son cada vez más dependientes de sus redes informáticas y cualquier problema que las deje indisponibles por mínimo que sea, puede llegar a comprometer gravemente las operaciones de dicho centro. En el trabajo del día a día los usuarios necesitan acceder a diversos servicios que son alcanzados mediante las redes de telecomunicaciones.

Los servicios a usar dependiendo del tipo de tráfico son:

Tráfico de datos, se da entre PCs, servidores, impresoras, scanner, equipos de monitoreo, UPS, lectoras, etc.

Tráfico de telefonía IP, se da entre equipos telefónicos y servidores de telefonía, este servicio tiene una alta relevancia para la atención del contac center (que es uno de los más importantes servicios que se da a los clientes) y para establecer comunicación entre todos los usuarios que lo necesiten..

Tráfico de videoconferencia, se da entre los equipos de videoconferencias, usado para reuniones, conferencias, entrevistas, etc.; de esta forma se evitan los viajes, lo que trae un ahorro en tiempo, ahorro en costos y eficiencia, reduce de cierta manera la huella contaminante al ya no viajar en auto.

La empresa bancaria está compuesta por 1 Site Principal, 1 Site Secundario y 5 sucursales ubicadas en zonas estratégicas, en cada una de estas hay usuarios que generan los tráficos antes mencionados.

Site Principal/Secundario, son sedes corporativas y como en toda sede de este tipo se

concentran una gran cantidad de usuarios, quienes conforman diversos grupos de trabajo de funciones diferentes, por ello el tipo de acceso de cada grupo varía según sus necesidades.

Agencia, las agencias estas conformadas por un grupo mucho más reducido de usuarios que conforman un mismo grupo de trabajo.

2.2 Cuantificación de los servicios

Todas las redes de cada sede de ser necesario deben poder interconectarse entre sí sin problemas, esto lo logramos por medio de una adecuada infraestructura de red. Los tráficos de cada servicio se basan en protocolos que permitan ajustar parámetros de calidad de servicio. Es importante tener claro el concepto de calidad de servicio para entender cómo se envían y reciben los distintos tipos de tráficos a través de la WAN.

2.2.1 Concepto de Calidad de Servicio

Desde el punto de vista de la telemática QoS es la capacidad de un elemento de red (bien una aplicación, un servidor, un router, etc.) de asegurar que su tráfico y los requisitos del servicio previamente establecidos puedan ser satisfechos óptimamente en lugar de aumentar el ancho de banda. El uso del acrónimo "oS" es usado como referencia cuando se habla de calidad de servicio, QoS es el término que refiere a calidad de servicio, englobando todos los términos en torno a ella, CoS clase de servicio y ToS tipo de servicio:

a) QoS: CALIDAD DE SERVICIO

Este concepto recoge ciertos parámetros y atributos, reserva ancho banda, retardo extremo a extremo, jitter, tasa de error. Un ejemplo de tecnología que utiliza QoS es UTF DSP.

b) CoS: CLASE DE SERVICIO

La descripción implica, dos procedimientos, en primer lugar la priorización de los distintos tipos de tráfico claramente identificados a través de la red y en segundo lugar la definición de un pequeño número de clases de servicio a las que aplicarla, priorizar es importante en momentos de congestión de la red.

Las aplicaciones que requieren distinguir clases de servicio incluyen tráfico de telefonía IP, vídeo, datos críticos y cualquier otro tráfico sensible al tiempo. No se debe confundir CoS con QoS, a diferencia de QoS, CoS no garantiza ancho de banda o latencia, en cambio permite a los administradores de red solicitar prioridad para el tráfico basándose en la importancia de éste. Existen muchas posibles definiciones de tipos de calidad de servicio, pero la mayoría de las empresas definen las clases de tráfico por tipo de aplicación, tipo de

dispositivo o por tipo de usuario. La tecnología CoS es usado en el estándar IEEE 802.1p, representado en la Fig. 2.1.

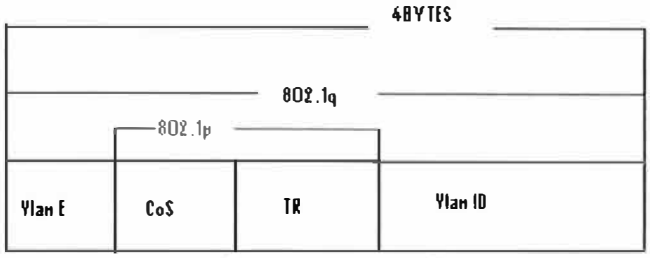


Fig. 2.1 Tecnología CoS

La norma IEEE 802.1p incluye un campo donde especificar la clase de servicio, como se define en tabla N° 2.1 y en la Fig. 2.2 se muestra gráficamente donde aplicar Cos.

TABLA N° 2.1 Valores CoS

Combinación	CoS	Prioridad
111	Network Critical	7
110	Interactive Voice	6
101	Interactive Multimedia	6
100	Streaming Multimedia	4
11	Business Critical	3
10	Standard	2
1	Background	1
0	Best Effort	0

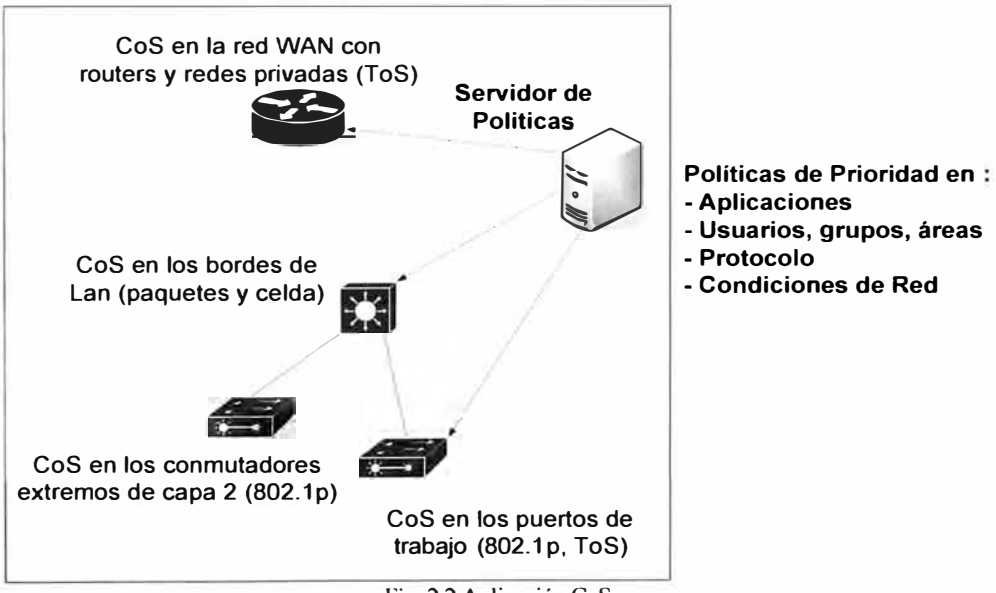


Fig. 2.2 Aplicación CoS

c) ToS: TIPO DE SERVICIO

El tipo de servicio es equivalente a un carril destinado a coches de uso compartido: se reserva ancho de banda con antelación y después se asigna el tráfico que necesite preferencia, como la voz o un CoS con prioridad, de modo que este tráfico pueda utilizar el ancho de banda reservado. ToS no implica, por lo tanto, ningún tipo de garantías. ToS está

incluida como uno de los campos en la tecnología de QoS denominada Diffserv (servicios diferenciados). Es un campo de 8 bits, estando los dos últimos reservados. Con los otros 6 bits restantes es posible obtener 64 combinaciones, de ellas, 48 son utilizadas para direccionar el espacio global y 16 son para uso local. Parte del protocolo IP Versión 4 reserva un campo en el paquete IP para el tipo de servicio (IP TOS). En este campo se pueden especificar los atributos de fiabilidad, capacidad de procesamiento y retardos del servicio, tal y como se ve en la Fig. 2.3:

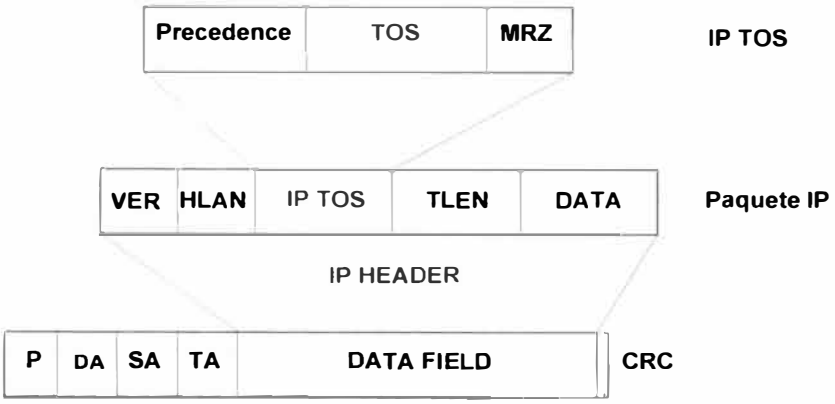


Fig. 2.3 Campo ToS en IPv4

d) Clasificación de QoS

Es posible realizar una clasificación de QoS bajo distintas especificaciones, como se muestra a continuación.

Según la sensibilidad del tráfico:

Teniendo en cuenta la variedad de tráfico existente y los requerimientos de retardo, latencia y ancho de banda para cada tipo, tenemos:

QoS muy sensible al retardo; Un ejemplo de este tipo es para el tráfico de vídeo comprimido, telefonía IP, etc. Para este tipo de tráfico es necesario garantizar la disponibilidad de una determinada cantidad de ancho de banda reservado para y un valor de retardo mínimo que asegure la correcta transmisión del mismo a tiempo real. Para conseguirlo será necesario utilizar mecanismos de prioridad, así como encolar adecuadamente los flujos de datos.

QoS algo sensible al retardo; Como puede ser la emulación de circuito. Al igual que en el caso anterior se garantiza hasta un cierto nivel de ancho de banda, aunque en menor valor. De igual forma, será necesario asignar prioridades para la transmisión de los datos.

QoS muy sensible a pérdidas; Como sucede con el tráfico tradicional. Si se garantiza un nivel de pérdidas de valor cero entonces nunca se descartarán paquetes ni se desbordarán los buffers de almacenamiento del flujo, lo que facilitará el control de transmisión, por otra

parte, esta garantía se hace a nivel de acceso al medio (MAC) o en capas superiores, pero nunca a nivel físico.

QoS nada sensible; Por ejemplo el tráfico de servicios de noticias o tráfico común. La función de este tipo de QoS es usar cualquier oportunidad de transmisión restante y asumir que la capacidad de los buffers posteriores es suficiente para llevarla a cabo, asignándole a este tipo de tráfico la prioridad más baja. A este tipo responden los algoritmos Best Effort o al mejor esfuerzo, utilizado en Internet. En la Fig. 2.4 es posible diferenciar de forma gráfica los tipos de tráfico y sus exigencias de ancho de banda y de sensibilidad a la latencia.

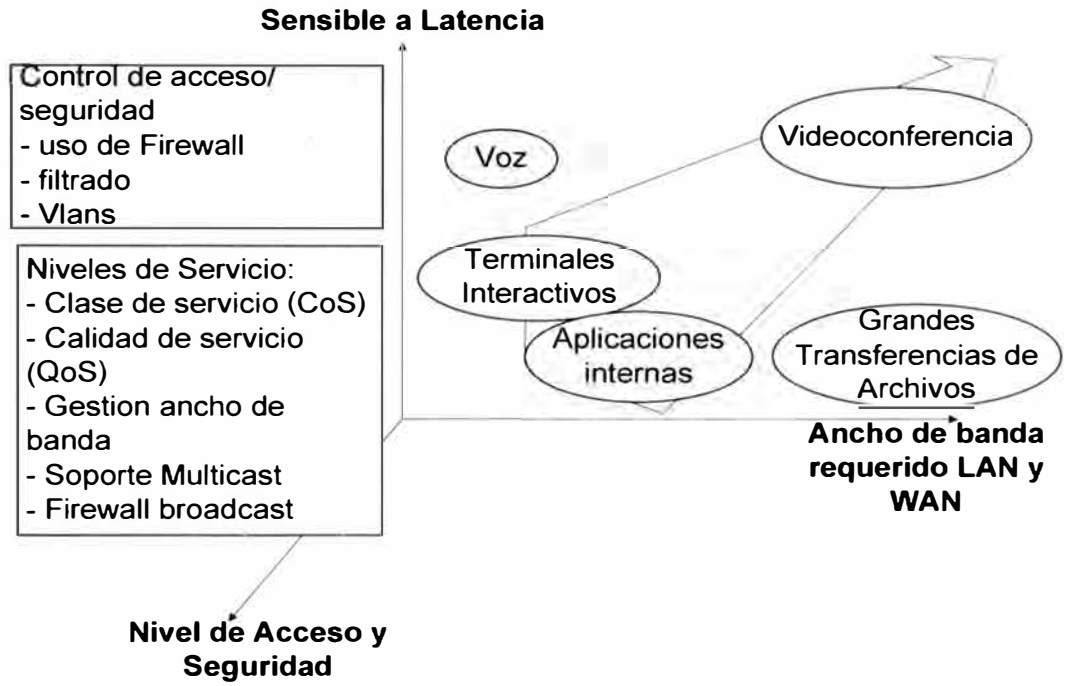


Fig. 2.4 Representación QoS y aplicaciones

Usuarios y administradores demandan niveles de servicio y tiempos de respuesta adecuados para aplicaciones críticas

Según quién solicite el nivel de calidad de servicio:

Teniendo en cuenta que la petición de QoS puede ser realizada por el usuario final o por los routers, nos encontramos con:

QoS IMPLÍCITA; En este tipo el router asigna automáticamente los niveles de calidad servicio en función del criterio especificado por el administrador de la red, según el tipo de aplicación, protocolo o dirección de origen. Hoy en día todos los routers, ofrecen este tipo de QoS. El proceso es el siguiente:

Estaciones finales: Las estaciones finales son los que transmiten los paquetes.

Router: Le llegan los paquetes, realiza un estudio de los datos entrantes y los prioriza, según la prioridad asignada por el administrador de red. Estos datos vuelven a ser transmitidos hacia el siguiente router, donde se repite el proceso.

QoS EXPLÍCITA; Este tipo de QoS permite al usuario o aplicación solicitar directamente un determinado nivel de servicio que han de respetar los routers.

Estaciones finales: En este caso las estaciones finales transmiten una petición RSVP, si ésta es aceptada, los paquetes son transmitidos.

Router: Los datos entrantes son priorizados de acuerdo a instrucciones del nodo de destino, pasando al próximo router, donde se repetirá el proceso.

Según las garantías:

Se tiene en cuenta la reserva de recursos de red para proporcionar los servicios.

QoS GARANTIZADA / Hard QoS; También conocida como "hard QoS" la calidad de servicio garantizada es en la que se reserva recursos de la red para garantizar el tráfico determinado, consiguiendo así unos niveles máximos de garantías para este tráfico.

QoS NO GARANTIZADA / Lack of QoS; El tráfico es transmitido por la red sin garantías ni reservas de recursos de la red. Es el tipo de QoS correspondiente a los servicios Best Effort (Mejor servicio).

QoS SERVICIOS DIFERENCIADOS/ Soft QoS; También conocida como "soft QoS" es el punto medio entre los dos tipos anteriores. Para este tipo se realiza una diferenciación de tráfico, siendo tratados algunos mejor que el resto. Es el utilizado, por DiffServ.

Según el lugar de aplicación:

Es posible aplicar calidad de servicio en los extremos y en los bordes de la red, tenemos:

QoS EXTREMO A EXTREMO (end-to-end); Es la aplicación de las políticas de calidad de servicio entre los equipos extremos de la red. Con este tipo de QoS, los equipos de comunicación intermedios tienen la función de observar la marca de los paquetes (en el caso de 802.1p), sin tener que calcular la clase de servicio de cada paquete reducido.

QoS BORDE A BORDE (edge-to-edge); Es la aplicación de las políticas de calidad de servicio entre dos puntos cualesquiera de la red. Por Ej.dos routers extremos.

Esto tiene varias ventajas: en primer lugar no se requiere constante intervención del administrador de la red, se tiene separada el área de infraestructura de la red del grupo de administrador de servidores, son menos los dispositivos que tienen que ser manejados para la obtención de la QoS. Además, la accesibilidad por parte de un usuario cualquiera de la red o de un hacker para cambiar las especificaciones de QoS es mucho menor.

A este tipo también se le conoce como calidad de servicio relativa.

e) Tráfico de red

Es dependiente del tipo de aplicación que por ella circulan, de esta manera podríamos establecer una diferenciación del tráfico.

Según el tipo de aplicación tendremos:

Tráfico habitual, multimedia, multicast, broadcast, tiempo real, etc.

Según la sensibilidad al retardo tendremos:

Tráfico algo sensible al retardo. Ejemplos son los procesos de transacción on-line, la entrada de datos remota y algunos protocolos como SNA. Este tipo de aplicaciones requieren retardos de un segundo o, incluso, menos. Retardos mayores supondrían hacer esperar a los usuarios por la contestación a sus mensajes antes de que puedan continuar trabajando, disminuyendo así la productividad de los negocios.

Tráfico muy sensible al retardo. El tráfico en tiempo real es de este tipo, tal y como las conversaciones vocales, telefonía IP, la videoconferencia y multimedia en tiempo real. Todos ellos requieren un retraso de tránsito muy pequeño (típicamente menos de una décima de segundo en un sentido, incluyendo el procesamiento en las estaciones finales) y un nivel de variación (jitter) mínimo.

Tráfico muy sensible a las pérdidas. Ej. Datos tradicionales.

Tráfico nada sensible. Ej. Servicios de noticias.

Para cada uno de estos tipos de tráfico establecemos un tipo de QoS según la clasificación realizada en el apartado anterior y, en consecuencia, la asignación de un nivel de prioridad

2.2.2 Tráfico de datos

El tráfico de datos, se divide en tres tipos CoS1, CoS2 y CoS3, este trafico se dan entre todas las sedes de la empresa, hacia Internet y con proveedores externos dependiendo del servicio a requerir, los tráficos se procesan aplicando políticas de seguridad y el acceso se realizara desde cualquier PC en la red, estas se comunican con los servidores que se encuentran en los site principal y/o secundario.

El acceso hacia Internet se hace por medio de dos enlaces (trabajan en modo Activo/Activo), instalados en los site principal y secundario, cada enlace tiene un propósito diferente y en caso de problemas con el enlace principal, el secundario asume toda la carga manteniendo la misma forma de operación que se tiene.

El acceso hacia la extranet se hace por medio de dos enlaces contratados para este fin, instalados en los site principal y secundario, estos enlaces trabajan en modo activo/standby,

el acceso normal se da por el enlace principal ubicado en el site principal y en caso de problemas por el enlace secundario ubicado en el site secundario, el propósito de este enlace es conectar con otros empresas con el fin de hacer consultas de datos, usando los servicios que ellos ofrecen.

2.2.3 Tráfico de Telefonía

El servicio de telefonía IP funciona en la misma infraestructura de la red de datos, esta es una de las principales ventajas que se tiene con esta tecnología comparada a la telefonía convencional, ya que no es necesario realizar cableado dedicado por cada punto de telefonía como se hace con las líneas convencionales. La voz es transmitida en forma de paquetes de datos, es digitalizada y transformada en datos que luego es transmitida empleando el protocolo IP, de los principales puntos de importancia de esta tecnología son:
La facilidad y eficiencia en la transmisión de voz.
Reducción de costos.
Equipos de comunicaciones (rotures, switches) que trabajan también con datos.
Mejor administración de llamadas.

Al interconectar la red IP con la red PSTN se utilizara un equipo router gateway, entre las funciones de este equipo se encuentran la codificación vocal, señalización DTMF, supresión de eco, generación de conexiones RTP, este equipo se encargara de hacer el traductor entre la red de telefonía publica conmutada y la red IP. El enlace se hace por líneas primarias (PRI E1) provistas por un operador PSTN, cada línea telefónica E1 entrega hasta 30 canales de voz, a los cuales se les puede asociar una cierta cantidad de números telefónicos directos. A diferencia de las líneas fijas convencionales, los 30 canales de voz son compartidos dinámicamente entre todos los números asignados, facilitando el manejo de grandes volúmenes de tráfico telefónico. Se tiene contratados 2 troncales E1 PRI, para realizar y recibir llamadas desde el exterior, la distribución de estas troncales E1:
1 E1 → Contac Center
1 E1 → Resto

PRI (Interfaz de Tasa Primaria) es un estándar de telecomunicaciones utilizados en la Red Digital de Servicios Integrados o RDSI, para la ejecución de múltiples DS0 de voz y transmisiones de datos entre dos ubicaciones físicas, es una línea RDSI para fines industriales (el sistema E1 es popular en toda Europa y Australia). Compuesto por 30 canales B + 1 canal D, lo que equivale a una tasa de bits de 2.048 Mbit. . El canal B se utiliza para la transmisión de datos, incluidos los de voz, el canal D es para señalización y

control (interfaz de tasa primaria hace uso del protocolo Q.931 sobre el canal D).

Para la operación de este servicio se tiene un cluster de servidores Callmanager que administran y monitorean a todos los equipos telefónicos conectados a la red.

El tráfico que generan los equipos de telefonía debe manejarse con la mayor prioridad (CoS5) por ser sensible a los retardos, se reserva un específico ancho de banda en la WAN para las llamadas entre anexos ubicados en diferentes sedes.

2.2.4 Tráfico de Videoconferencia

El tráfico se realiza entre los equipos de videoconferencia instalados en los site principal y secundario, este tipo de tráfico se maneja como datos críticos (CoS5) debido al sensible comportamiento que tiene con respecto al retardo de la misma forma que el tráfico telefónico, por ello se asegura el ancho de banda necesario en la WAN y no tener inconvenientes en el funcionamiento de este servicio.

2.2.5 Tráfico de Internet

La necesidad del uso de Internet se ah vuelto vital, debido a toda la información en línea a la que es compartida y con los accesos necesarios se puede acceder sin problemas. Se tienen dos enlaces, principal y secundario ubicados respectivamente en los site principal y secundario que trabajan en modo Activo/Activo, cada una proporcionada por operadores diferentes, Telmex y Telefónica respectivamente. Para este servicio al tenerse dos enlaces, por el primero se dará acceso a un grupo determinado de usuarios que tendrá permitido los sitios web necesarios para cumplir con su labor diaria y por el segundo enlace se da acceso al resto de usuarios que necesitan otros tipos de accesos. Se divide el acceso en grupos para poder tener un mejor control de los sitios web que son visitados.

2.2.6 Tráfico de Extranet

Por medio de este enlace se tendrá acceso a información que es compartida con empresas externas, la restricción de este enlace se hace de entrada y salida, internamente un grupo especifico de usuarios podrá acceder a este enlace por las labores que realiza y desde el exterior solo podrán ingresar a ciertos servicios acordados previamente, por ello hay equipos de seguridad que mediante diversas políticas restringen en tráfico entrante y saliente.

Se tienen dos enlaces para este servicio, principal y secundario que trabajan en modo Activo/Standby, el acceso es siempre por el enlace principal ubicado en el cite principal, pero en caso de problemas con este enlace se activa el segundo enlace en el site secundario que opera con las mismas políticas de seguridad que el primero (las políticas son replicadas

en ambos equipos) y que normalmente se encuentra en estado standby. Estos enlaces son provistos por Telefónica de Perú.

2.3 Determinación del tráfico a usar

2.3.1 Servicio de Datos

Dentro del Tráfico correspondiente a los servicios de datos, se encuentran los generados entre PCs, servidores, impresoras, equipos de comunicaciones, scanner, etc.

Se realiza un estudio detallado de los tráficos críticos e indispensables y dependiendo de la importancia de estos se les dará la prioridad que corresponda. En las sedes corporativas (site principal y secundario) se encuentra un gran número de usuarios distribuidos en todos los pisos, cada usuario tiene asignado una PC con acceso a la red. La distribución en los sites se muestra en las tablas N° 2.2 y 2.3:

TABLA N° 2.2 Distribución de usuarios por piso Site

Piso	Usuarios	PCS
Piso 1	60	60
Piso 2	60	60
Piso 3	60	60
Piso 4	60	60
Piso 5	60	60

Por agencia:

TABLA N° 2.3 Distribución de usuarios por piso Agencia

Piso	Usuarios	PCS
Piso 1	15	15

Cada usuario en agencia necesita un promedio de 90kbps (según pruebas) para poder efectuar consultas y/o otras actividades por las que necesite acceder a los servidores y solo un estimado de 55% (debido al tipo de función que realizan) de usuarios se conectara a la vez al site principal.

Tráfico Datos por Agencia = 15 x 55% x 90kbps = 742.5Kbps

De este tráfico se considera que el 60% podrá llegar a ser datos críticos:

Máximo datos críticos = 742.5kbps x 60% = 445.5kbps Datos Críticos

Datos no críticos = 742.5kbps – 445.5kbps = 297Kbps Datos No críticos

Tráfico Datos de las 5 Agencias = 5 x 742.5kbps = 3712.5kbps

No todas las agencias se conectan al mismo tiempo, por ello se considera que un 70% de este tráfico debe garantizarse con el site principal.

Tráfico de Datos a garantizar = 3712.5kbps x 70% = 2598.75kbps

Tráfico de Datos Críticos a garantizar = 2598.75kbps x 60% = 1559.25kbps

Tráfico de Datos No Críticos a garantizar = 2598.75kbps – 1559.25kbps = 1039.5kbps

Cada usuario en el site secundario, necesita un promedio de 120kbps (según prueba) de acceso hacia el site principal donde se encuentran los servidores y solo un estimado de 30% de usuarios se conectara a la vez.

Tráfico de datos site Secundario = 300 x 30% x 120kbps = 10800kbps

De este tráfico se considera que el 60% podrá llegar a ser datos críticos:

Máximo Datos Críticos = 10800kbps x 60% = 6480kbps datos Críticos

Con esto se garantiza que en caso de saturación del enlace los datos críticos tendrán prioridad para ocupar el 60% del enlace.

Datos No Críticos = 10800kbps – 6480kbps = 4320kbps

En resumen el tráfico de datos críticos y no críticos del enlace principal y secundario se calcula considerando lo que es consumido por todas las agencias. En la tabla N° 2.4 se observa el resumen de los anchos de banda necesaria para acceso de datos.

Datos críticos: 6480kbps + 1559.25kbps = 8039.25kbps

Datos no críticos: 4320kbps + 1039.5kbps = 5359.5Kbps

TABLA N° 2.4 Ancho de banda CoS2 y CoS1 por sede

Sede	Pisos	Cantidad Sedes	Usuarios	PCS	Ancho de Banda Datos Críticos	Ancho de Banda Datos No Críticos	Ancho de Banda Total
Site Corporativo	5	2	300	300	8039.25kbps	5359.5kbps	13398.75kbps
Agencia	1	5	15	15	445.5kbps	297Kbps	742.5Kbps

El consumo de la red es a demanda, en caso que el tráfico de datos críticos no sea mucho, la reserva que se tenga será usada por el resto de tráfico.

2.3.2 Servicio de Telefonía IP

El tráfico telefónico es muy variante, durante el día existen horas de tráfico intenso mientras que en otras apenas se tiene tráfico, la solución de telefonía tiene la capacidad de soportar el tráfico pico producido por causas extraordinarias. Para establecer la intensidad del tráfico a soportar se considera el periodo de tiempo de 60 minutos consecutivos de mayor volumen de tráfico. Como unidad de tráfico se tiene el Erlang que es la intensidad de tráfico de un canal o un grupo de canales en el que el tiempo de observación coincide con el tiempo total de ocupación, entendiendo por tal la suma de los tiempos de ocupación parciales del canal o canales que se consideren.

Siendo toc el tiempo de ocupación total en hora pico:

T, el tiempo de observación

n, el número de canales

$$A = \frac{\sum_{i=0}^{n} (toc)i}{T} \quad (2.1)$$

a) Dimensionamiento Troncales E1

Para el área de Contac Center se espera una atención en hora pico de 400 llamadas , de acuerdo al área de servicios al usuario se espera también una atención promedio por llamada de 80s, la probabilidad de encontrar el sistema ocupado en hora pico debe ser como máximo de 1%.

$$A = \frac{400 llamadas x 80s}{3600s} = 8.88 \text{ Erlang}$$

Se tiene A= 8.88 Erlang

Con un tráfico de 8.88 Erlang y una probabilidad de pérdida de 1% correspondería 17 canales, pero debido a que el proveedor de las troncales solo puede facilitarlas en grupo de 15 , se contrata una troncal E1 de 30 canales (con esta cantidad se cubrirá las expectativas). En la tabla N` 2.5, se muestra la tabla erlang de donde se obtuvo los canales a necesitar.

TABLA Nº 2.5 Tabla Erlang

n	Probabilidad de pérdida (E)										n
	0.007	**0.008**	**0.009**	**0.01**	**0.02**	**0.03**	**0.05**	**0.1**	**0.2**	**0.4**	
1	.00705	.00806	.00908	.01010	.02041	.03093	.05263	.11111	.25000	.66667	**1**
2	.12600	.13532	.14416	.15259	.22347	.28155	.38132	.59543	1.0000	2.0000	**2**
3	.39664	.41757	.43711	.45549	.60221	.71513	.89940	1.2708	1.9299	3.4798	**3**
4	.77729	.81029	.84085	.86942	1.0923	1.2589	1.5246	2.0454	2.9452	5.0210	**4**
5	1.2362	1.2810	1.3223	1.3608	1.6571	1.8752	2.2185	2.8811	4.0104	6.5955	**5**
6	1.7531	1.8093	1.8610	1.9090	2.2759	2.5431	2.9603	3.7584	5.1086	8.1907	**6**
7	2.3149	2.3820	2.4437	2.5009	2.9354	3.2497	3.7378	4.6662	6.2302	9.7998	**7**
8	2.9125	2.9902	3.0615	3.1276	3.6271	3.9865	4.5430	5.5971	7.3692	11.419	**8**
9	3.5395	3.6274	3.7080	**3.7825**	4.3447	4.7479	5.3702	6.5464	8.5217	13.045	**9**
10	4.1911	4.2889	4.3784	4.4612	5.0840	5.5294	6.2157	7.5106	9.6850	14.677	**10**
11	4.8637	4.9709	5.0691	**5.1599**	5.8415	6.3280	7.0764	8.4871	10.857	16.314	**11**
12	5.5543	5.6708	5.7774	5.8760	6.6147	7.1410	7.9501	9.4740	12.036	17.954	**12**
13	6.2607	6.3863	6.5011	6.6072	7.4015	7.9667	8.8349	10.470	13.222	19.598	**13**
14	6.9811	7.1155	7.2382	7.3517	8.2003	8.8035	9.7295	11.473	14.413	21.243	**14**
15	7.7139	7.8568	7.9874	8.1080	9.0096	9.6500	10.633	12.484	15.608	22.891	**15**
16	8.4579	8.6092	8.7474	8.8750	9.8284	10.505	11.544	13.500	16.807	24.541	**16**

17	9.2119	9.3714	9.5171	**9.6516**	10.656	11.368	12.461	14.522	18.010	26.192	**17**
18	9.9751	10.143	10.296	10.437	11.491	12.238	13.385	15.548	19.216	27.844	**18**
19	10.747	10.922	11.082	11.230	12.333	13.115	14.315	16.579	20.424	29.498	**19**
20	11.526	11.709	11.876	12.031	13.182	13.997	15.249	17.613	21.635	31.152	**20**
21	12.312	12.503	12.677	12.838	14.036	14.885	16.189	18.651	22.848	32.808	**21**
22	13.105	13.303	13.484	13.651	14.896	15.778	17.132	19.692	24.064	34.464	**22**
23	13.904	14.110	14.297	14.470	15.761	16.675	18.080	20.737	25.281	36.121	**23**
24	14.709	14.922	15.116	15.295	16.631	17.577	19.031	21.784	26.499	37.779	**24**

Para el resto del banco, se espera una recepción en hora pico de 200 llamadas, se espera también una atención promedio por llamada de 90s, la probabilidad de encontrar el sistema ocupado en hora pico debe ser como máximo de 1%, con respecto a la salida de llamadas se espera en hora pico 150 llamadas para dar un eficiente servicio al usuario interno se espera una probabilidad de pérdida de 1%.

$$A = \frac{200 llamadas x 90s}{3600s} = 5 \text{ Erlang}$$

Se tiene A = 5Erlang (Para la recepción de llamadas)

$$A = \frac{150 llamadas x 90s}{3600s} = 3.75 \text{ Erlang}$$

Se tiene A= 3.75 Erlang (Para la salida de llamadas)

Con un tráfico de 5 Erlang se necesitan 11 Canales.

Con un tráfico de 3.75 Erlang se necesitan 9 Canales.

En la tabla N`2.5, se muestra la tabla erlang de donde se obtuvieron los canales a necesitar. En total se necesitaran 20 Canales en hora pico, con este dato se puede dimensionar la cantidad de troncales a contratar, se tiene un E1 (30 canales) casi en su totalidad por ello para futuro crecimiento.

En total se tiene 1 troncal E1 para Contac Center y 1 troncal E1 para el resto de usuarios (llamadas entrantes y salidas). En la tabla Nº 2.6 se tiene el resumen de las troncales E1

TABLA Nº 2.6 Troncales E1 por sede

Sede	Cantidad de sedes	Pisos	Usuarios	PCS	Cantidad de Teléfonos	Troncales E1
Site Corporativo	2	5	300	320	250	2
Agencia	5	1	15	15	8	0

b) Dimensionamiento WAN

Para determinar el dimensionamiento del enlace WAN, se espera en hora pico 400 llamadas con el site principal (que es donde se encuentran la mayoría de usuarios) estas llamadas correspondes a todas llamadas salientes ya sea por la PSTN o hacia otro site y/o

agencias, también las llamadas que son recibidas, se espera una atención promedio de 120s, la posibilidad de encontrar el sistema ocupado debe ser como máximo 0.01%.

A = 13.3 Erlang

Con un tráfico de 13.3 Erlang se necesitan 29 canales, en la tabla. Nº 2.7, se muestra la tabla erlang de donde se obtuvo los canales a necesitar. Cada canal con la telefonía IP implementada consumirá 32kbps, se necesitan 29 x 32 = 928 kbps. Para cubrir futuras necesidades y poder contener todas las llamadas en hora pico se decide contratar un ancho de banda e 1.2 Mbps solo para telefonía tanto en el site principal y secundario.

Para las agencias, se espera que en hora pico realicen 30 llamadas con el cite principal, se espera una atención promedio de 60 segundos por llamada, la posibilidad de encontrar el sistema ocupado debe ser como máximo 0.01%.

A = 0.5 Erlang

Con un tráfico de 0.5 Erlang se necesitan 6 canales. Cada canal con la telefonía IP implementada consumirá 32kbps, se necesitan 6 x 32 = 192 KPSS .Se contra 192 KPSS para el enlace WAN de las 5 agencias. Este tráfico se da en Cosa debido a la prioridad que se le debe de dar. En la tabla Nº 2.8 se muestra el resumen de ancho de banda en Cosa a usar por sede.

TABLA Nº 2.7 Tabla Erlang

n	Probabilidad de pérdida (E)										n
	0.00001	**0.00005**	**0.0001**	**0.0005**	**0.001**	**0.002**	**0.003**	**0.004**	**0.005**	**0.006**	
1	.00001	.00005	.00010	.00050	.00100	.00200	.00301	.00402	.00503	.00604	**1**
2	.00448	.01005	.01425	.03213	.04576	.06534	.08064	.09373	.10540	.11608	**2**
3	.03980	.06849	.08683	.15170	.19384	.24872	.28851	.32099	.34900	.37395	**3**
4	.12855	.19554	.23471	.36236	.43927	.53503	.60209	.65568	.70120	.74124	**4**
5	.27584	.38851	.45195	.64857	.76212	.89986	.99446	1.0692	1.1320	1.1870	**5**
6	.47596	.63923	.72826	.99567	1.1459	1.3252	1.4468	1.5421	1.6218	1.6912	**6**
7	.72378	.93919	1.0541	1.3922	1.5786	1.7984	1.9463	2.0614	2.1575	2.2408	**7**
8	1.0133	1.2816	1.4219	1.8298	2.0513	2.3106	2.4837	2.6181	2.7299	2.8266	**8**
9	1.3391	1.6595	1.8256	2.3016	2.5575	2.8549	3.0526	3.2057	3.3326	3.4422	**9**
10	1.6970	2.0689	2.2601	2.8028	3.0920	3.4265	3.6480	3.8190	3.9607	4.0829	**10**
11	2.0849	2.5059	2.7216	3.3294	3.6511	4.0215	4.2661	4.4545	4.6104	4.7447	**11**
12	2.4958	2.9671	3.2072	3.8781	4.2314	4.6368	4.9038	5.1092	5.2789	5.4250	**12**
13	2.9294	3.4500	3.7136	4.4465	4.8306	5.2700	5.5588	5.7807	5.9638	6.1214	**13**
14	3.3834	3.9523	4.2388	5.0324	5.4464	5.9190	6.2291	6.4670	6.6632	6.8320	**14**
15	3.8559	4.4721	4.7812	5.6339	6.0772	6.5822	6.9130	7.1665	7.3755	7.5552	**15**
16	4.3453	5.0079	5.3390	6.2496	6.7215	7.2582	7.6091	7.8780	8.0995	8.2898	**16**
17	4.8502	5.5583	5.9110	6.8782	7.3781	7.9457	8.3164	8.6003	8.8340	9.0347	**17**
18	5.3693	6.1220	6.4959	7.5186	8.0459	8.6437	9.0339	9.3324	9.5780	9.7889	**18**
19	5.9016	6.6980	7.0927	8.1698	8.7239	9.3515	9.7606	10.073	10.331	10.552	**19**
20	6.4460	7.2854	7.7005	8.8310	9.4115	10.068	10.496	10.823	11.092	11.322	**20**

21	7.0017	7.8834	8.3186	9.5014	10.108	10.793	11.239	11.580	11.860	12.100	**21**
22	7.5680	8.4926	8.9462	10.180	10.812	11.525	11.989	12.344	12.635	12.885	**22**
23	8.1443	9.1095	9.5826	10.868	11.524	12.265	12.746	13.114	13.416	13.676	**23**
24	8.7298	9.7351	10.227	11.562	12.243	13.011	13.510	13.891	14.204	14.472	**24**
25	9.3240	10.369	10.880	12.264	12.969	13.763	14.279	14.673	14.997	15.274	**25**
26	9.9265	11.010	11.540	12.972	13.701	14.522	15.054	15.461	15.795	16.081	**26**
27	10.537	11.659	12.207	13.686	14.439	15.285	15.835	16.254	16.598	16.893	**27**
28	11.154	12.314	12.880	14.406	15.182	16.054	16.620	17.051	17.406	17.709	**28**
29	11.779	12.976	13.560	15.132	15.930	16.828	17.410	17.853	18.218	18.530	**29**
30	12.417	13.644	14.246	15.863	16.684	17.606	18.204	18.660	19.034	19.355	**30**

TABLA N° 2.8 Ancho de banda Cosa a necesitar para telefonía

Sede	Cantidad de sedes	Pisos	Usuarios	PCS	Cantidad de Teléfonos	Ancho de Banda Cosa
Cite Corporativo	2	5	300	300	250	1,2 Mbps
Agencia	5	1	15	15	8	192Kbps

2.3.3 Servicio de Videoconferencia

El tráfico de video depende del momento de uso, esta solo transmite y recibe Tráfico con el otro dispositivo de videoconferencia (hay uno por cite, principal y secundario), debido a que el Tráfico de este sistema siempre es 384kbps, se solicita esta cantidad para el enlace WAN del cite principal y secundario, este tráfico corresponde al tipo de Tráfico Cosa debido a la prioridad que se le debe de dar. En la tabla N° 2.9 se muestra el resumen de ancho de banda necesario para videoconferencia.

TABLA N° 2.9 Ancho de banda CoS5 a necesitar para videoconferencia.

Sede	Cantidad de sedes	Pisos	Usuarios	PCS	Ancho de Banda CoS5
Site Corporativo	2	5	300	300	384kbps
Agencia	5	1	15	15	-

2.3.4 Servicio de Internet

El tráfico hacia Internet no es constante, se necesita acceder a este enlace debido a las páginas de consultas que son necesarias, la cantidad de usuarios que en un momento determinado se conecten a Internet es muy variable por ello uso de este enlace varia según la hora de conexión, se tienen dos accesos a Internet y dependiendo el tipo de acceso que tena el usuario podrá acceder por un determinado enlace.

Se define usar 4Mbps en cada enlace de Internet ya que es muy complejo medir las conexiones que hay en hora pico, y no todas corresponden necesariamente al plano laboral, por ello teniendo una salida de 4Mbps (donde se garantice el 100% de ancho de banda), se tiene como consigna ir midiendo el consumo de este enlace y de ser necesario hacer un upgrade con el feedback realizado. En la siguiente tabla se muestra el resumen de ancho de banda necesario inicialmente para acceso a Internet por sede.

TABLA Nº 2.10 Ancho de banda para Internet

Sede	Cantidad de sedes	Pisos	Usuarios	PCS	Ancho de Banda Internet
Site Corporativo	2	5	300	300	4 Mbps
Agencia	5	1	15	15	-

2.3.5 Servicio de Extranet

Al haber información que se necesita compartir entre empresas, se establece un enlace dedicado para todas estas consultas, el acceso se hace desde un grupo especifico de usuarios ubicados en los site y agencias. Se establece inicialmente un enlace de 3Mbps por acuerdo con la empresa que realiza la conexión con las otras entidades y como se menciono antes habrá un enlace de este tipo en el site Principal y Secundario. En la tabla Nº 2.11 se muestra el resumen del ancho de banda necesario para extranet.

TABLA Nº 2.11 Ancho de banda para Extranet

Sede	**Cantidad de sedes**	**Pisos**	**Usuarios**	**PCS**	**Ancho de Banda Extranet**
Site Corporativo	2	5	300	300	3 Mbps
Agencia	5	1	15	15	-

La tabla Nº 2.12 muestra el resumen de todo el ancho de banda y troncales E1 necesarias.

TABLA Nº 2.12 Ancho de banda y troncales E1

Sede	**Cantidad de sedes**	**Pisos**	**Usuarios**	**PCS**	**Cantidad de Teléfonos**	**Ancho de Banda Datos Críticos Cos2**	**Ancho de Banda Datos No Críticos CoS1**	**Ancho de Banda CoS5**	**Ancho de Banda Total**	**Troncales E1**
Site Corporativo	2	5	300	300	250	8039.25kbps	5359.5kbps	1280Kbps	14679.75 kbps	2
Agencia	5	1	15	15	8	445.5kbps	297Kbps	192Kbps	934.5kbps	0

CAPÍTULO III
INGENIERÍA DEL PROYECTO

3.1 Arquitectura de la red

La arquitectura necesaria de servicios e interconexiones se muestra en la siguiente figura:

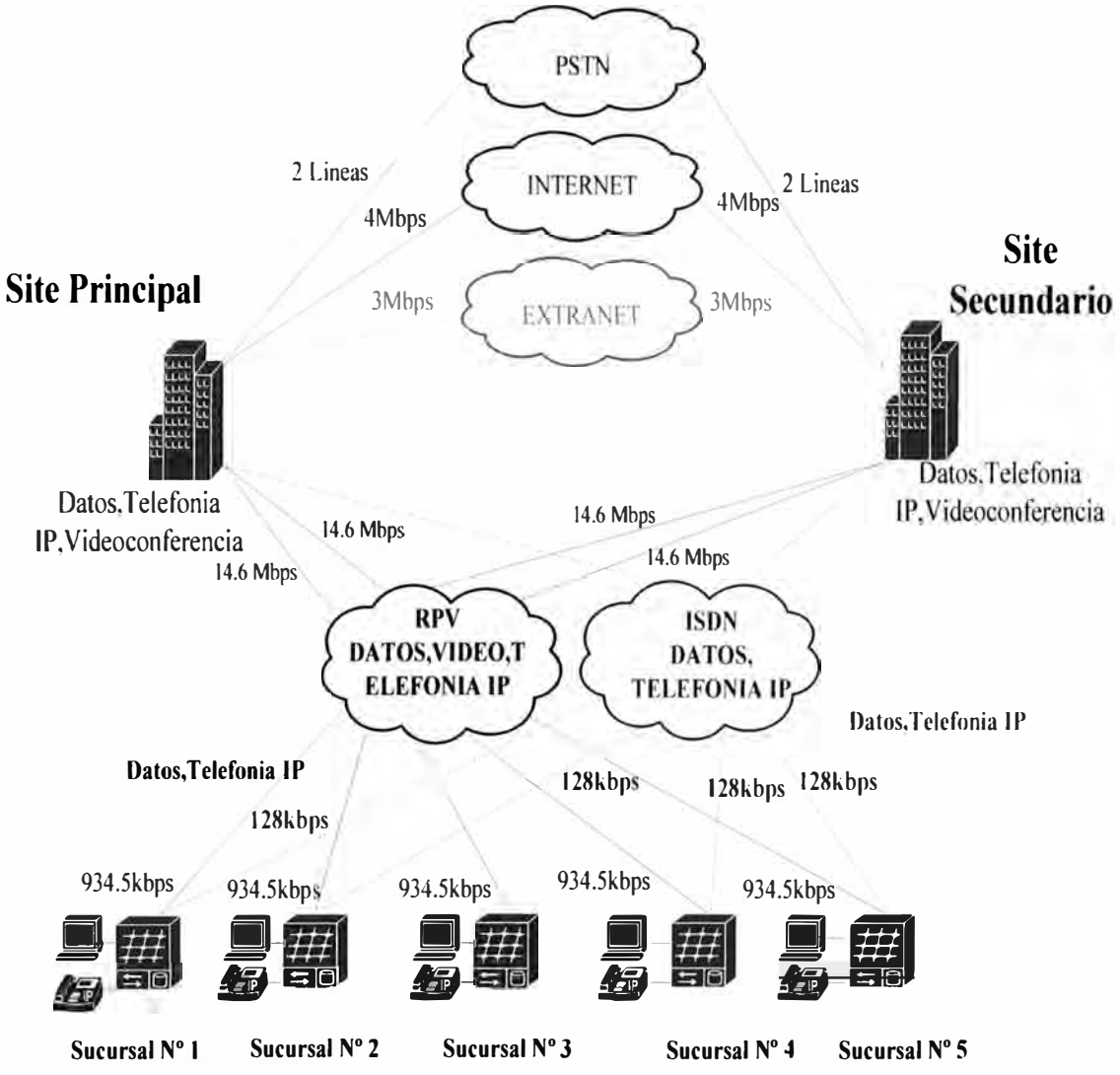


Fig. 3.1 Distribución de los enlaces de servicios

La arquitectura necesaria para todos los servicios de datos, telefonía y video se muestra en la Fig. 3.2 (dentro del site principal y secundario).

La interconexión de los cuartos de comunicaciones distribuidos en los pisos 1, 2, 4 y 5 con el data center se muestra en la Fig. 3.3.

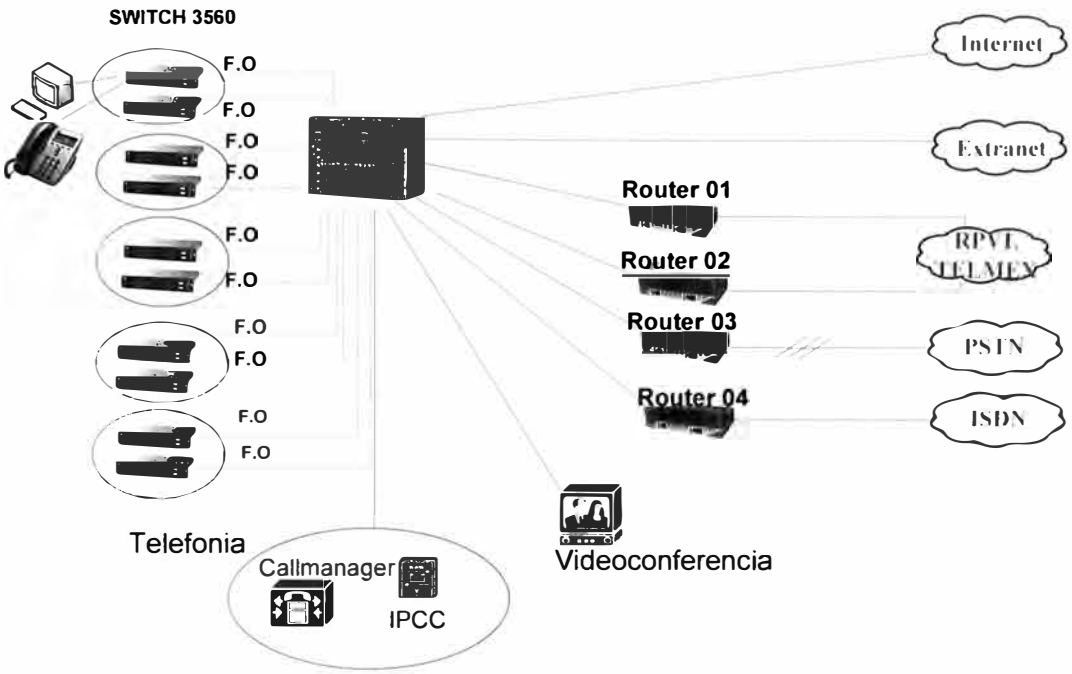


Fig. 3.2 Distribución de redes internas

La interconexión de los cuartos de comunicaciones distribuidos en los pisos 1, 2, 4 y 5 con el data center se muestra en la Fig. 3.3:

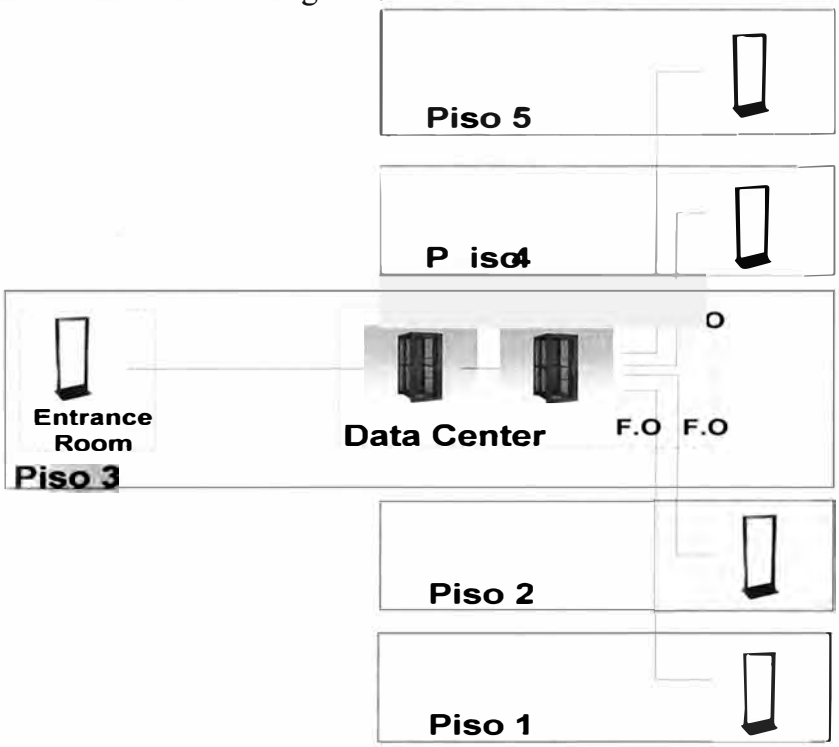


Fig. 3.3 Interconexión de Cuartos de Comunicaciones y Datacenter (Site Principal/Secundario)

La red LAN soporta los servicios de Datos, Telefonía, Video, acceso a Internet y Extranet; se emplea una topología en estrella, donde todos los servicios conmutan a un equipo principal "SWITCH CORE" y dependiendo del servicio o Tráfico cursado el switch core enrutara el Tráfico a los equipos "routers" correspondientes para que puedan llegar a su destino.

3.1.1 Diseño red LAN

Se diseña la red LAN considerando los siguientes objetivos y metas:

Funcionalidad: La red debe suministrar conectividad de usuario a usuario y de usuario a aplicación con una velocidad y confiabilidad razonable, permitiendo cumplir con las necesidades laborales.

Escalabilidad: La red debe poder aumentar de tamaño sin que se produzcan cambios importantes en el diseño general.

Adaptabilidad: La red debe diseñarse teniendo en cuenta futuras tecnologías. La red no debería incluir elementos que limiten la implementación de nuevas tecnologías.

Facilidad de administración: La red debe estar diseñada para facilitar su monitoreo y administración, con el objeto de asegurar una estabilidad de funcionamiento constante.

Se busca siempre la forma de maximizar el ancho de banda y el rendimiento de la red LAN, para lograrlo se tiene en cuenta las siguientes consideraciones de diseño:

Función y ubicación de los servidores.

Los dominios de colisión.

Segmentación de la red

Los dominios de broadcast

Función y ubicación de los servidores, los servidores los dividimos en servidores empresariales o servidores de grupo de trabajo. Un servidor empresarial ofrece servicios que son usados por todos los usuarios como DNS, MAIL, Active Directory entre otros. Un servidor de grupo de trabajo ofrece servicios restringidos para un conjunto de usuarios como ftp, archivos compartidos, procesamiento de texto. Los servidores de grupo de trabajo se encuentran cercanos a los usuarios que acceden a las aplicaciones de estos servidores así el Tráfico da menos saltos hasta llegar a su destino.

Dominios de colisión, los nodos Ethernet utilizan CSMA/CD, cada nodo debe disputar con otros para acceder al medio compartido o al dominio de colisión. Si dos equipos transmiten al mismo tiempo, se produce una colisión y cuando se produce esta la trama transmitida se elimina, luego se envía una señal broadcast a todos los otros equipos de red los equipos esperan un período de tiempo al azar y luego vuelven a enviar los datos. Las colisiones excesivas pueden reducir el ancho de banda disponible de un segmento de red a 35 – 40% del ancho de banda disponible.

Segmentación de la red, la segmentación se realiza cuando un sólo dominio de colisión se divide en dominios de colisión más pequeños. Los dominios de colisión más pequeños

reducen la cantidad de colisiones en un segmento LAN y permiten una mayor utilización el ancho de banda. Los dispositivos de la Capa 2 como por ejemplo bridges y switches pueden segmentar la red LAN. Los routers pueden lograr esto a nivel de la Capa 3.

Los dominios de broadcast, se produce un broadcast cuando el control de acceso al medio destino (MAC) se configura en FF-FF-FF-FF-FF-FF, este dominio se refiere al conjunto de dispositivos que reciben una trama de datos de broadcast desde cualquier dispositivo dentro de este conjunto. Todos los equipos que reciben una trama de datos de broadcast deben procesarla, este proceso consume los recursos y el ancho de banda disponible del equipo de cómputo. Los routers reducen el tamaño del dominio de colisión y el tamaño del dominio de broadcast en la Capa 3.

El diseño de la red interna lo dividimos en 3 capas, tomando como referencia el modelo OSI, de esta forma se aísla o divide las funciones que cada capa debe realizar para que en conjunto puedan trabajar de forma efectiva.

a) Diseño Capa 1

El cableado LAN se basa en la tecnología Fast Ethernet. Fast Ethernet es la tecnología Ethernet que se ha actualizado de 10 Mbps a 100 Mbps y tiene la capacidad de utilizar la funcionalidad full-duplex. Fast Ethernet utiliza la topología de bus lógica y el método CSMA/CD para direcciones MAC. Los temas de diseño en la Capa 1 incluyen el tipo y estructura de cableado que se debe utilizar (normalmente cable de cobre o fibra óptica), esto también incluye el estándar TIA/EIA-568-A para los esquemas de cableado. Los tipos de medios de la Capa 1 incluyen el par trenzado no blindado (UTP) o el par trenzado blindado (STP) Categoría 5, 5e o 6 10/100BASE-TX y el cable de fibra óptica 100BaseFX.

En el diseño de cableado se utiliza cable de fibra óptica en el backbone y conductos verticales, el cable UTP Categoría 6a se utilizara en los tendidos horizontales. Estos sistemas se implementan según estándares de la industria bien definidos como la especificación TIA/EIA-568-A. El estándar TIA/EIA-568-A especifica que cada dispositivo conectado a la red debe estar conectado a una ubicación central a través de cableado horizontal, esto se aplica si todos los equipos que necesitan acceso a la red y se encuentran dentro de un límite de distancia de 100 metros (328 pies) para el UTP Ethernet Categoría 6a.

b) Diseño capa 2

El propósito de los dispositivos de la Capa 2 en la red es conmutar tramas basadas en sus direcciones MAC destino, ofrecer detección de errores y reducir la congestión en la red.

Los más comunes son los switchs LAN. estos determinan el tamaño de los dominios de colisión.

Otra característica importante de un switch LAN es la forma en que puede asignar ancho de banda por puerto. Esto permite ofrecer más ancho de banda para el cableado vertical, los uplinks y los servidores, este tipo de conmutación se conoce como conmutación asimétrica. La conmutación asimétrica proporciona conexiones de conmutación entre puertos con distinto ancho de banda por ejemplo, una combinación de puertos de 10 Mbps y de 100 Mbps. La conmutación simétrica ofrece conexiones conmutadas entre puertos de ancho de banda similar.

c) Diseño capa 3

Los dispositivos de la Capa 3 posibilitan la creación de segmentos LAN únicos tanto lógica y física, permiten la comunicación entre segmentos basados en las direcciones IP. El enrutamiento de Capa 3 determina el flujo de tráfico entre los segmentos de red física exclusivos basados en direcciones IP destino. El router a diferencia del switch no envía broadcasts basados en LAN, tales como las peticiones ARP.

3.1.2 Segmentación de la Lan

Se realiza un diseño jerárquico:

La capa de acceso proporciona a los usuarios de grupos de trabajo acceso a la red.

La capa de distribución brinda conectividad basada en políticas.

La capa núcleo o CORE proporciona transporte óptimo entre sitios. A la capa core también la denominamos backbone.

Estas capas se definen para ayudar a lograr un diseño de red exitoso y pueden existir físicamente sin embargo no es un requisito.

La capa de acceso, es el punto de entrada para las estaciones de trabajo a la red. el dispositivo utilizado en esta capa es un switch administrable. Si una estación de trabajo o un servidor se conectan directamente a un puerto de switch, entonces el ancho de banda completo de puerto del switch se encontrara disponible para el equipo conectado, las funciones de la capa de acceso también incluyen el filtrado y la micro segmentación de la capa MAC. El filtrado de la capa MAC permite a los switches dirigir las tramas sólo hacia el puerto de switch que se encuentra conectado al dispositivo destino. El switch crea pequeños segmentos de Capa 2 denominados micro segmentos.

La capa de Distribución, esta capa segmenta las redes en dominios de broadcast, se pueden aplicar políticas y listas de control de acceso para filtrar paquetes. Esta capa aísla

los problemas de red para los grupos de trabajo en los cuales se producen, también evita que estos problemas afecten la capa core. Las funciones de esta capa son:

Unificación de las conexiones del armario de cableado

Definición de dominio de broadcast/multicast.

Enrutamiento VLAN.

Seguridad.

La capa de core, es un backbone de conmutación de alta velocidad, se utilizan switches de capa 3 y por medio de este se tiene una administración centralizada de toda la red.

3.1.3 Definición de Topología

Se denomina topología a la forma de interconexión entre PCS, impresoras, servidores y otros dispositivos IP. El modelo elegido es un factor fundamental que va a determinar el rendimiento y la funcionalidad de la red. La topología idónea va a depender de diferentes factores, entre los principales, el número de máquinas a interconectar, el tipo de acceso al medio físico necesario y distribución de usuarios. Podemos distinguir tres diferentes topologías a considerar:

La topología física, que es la disposición real de las máquinas, dispositivos de red y cableado (los medios) en la red.

La topología lógica, que es la forma en que las máquinas se comunican a través del medio físico. En este caso se utilizara la topología lógica de broadcast (Ethernet).

La topología de broadcast simplemente significa que cada PC envía sus datos hacia todos las demás PCs del mismo medio de red. Los equipos no siguen ningún orden para utilizar la red, sino que cada máquina accede a la red para transmitir datos en el momento en que lo necesita. En nuestro caso particular se escogió la topología en estrella debido a su facilidad de administración y de mejor control para administración.

a) Acceso a red de datos, telefonía IP y video

Topología Física - Topología en estrella

La topología en estrella tiene un nodo central de donde se irradian los enlaces hacia los demás nodos. La función del nodo central la realiza el switch CORE, este analiza las direcciones destinos de los paquetes y según esta información reenvía los paquetes a los equipos que corresponda. En la Fig. 3.4 se observa un modelo de topología en estrella. La desventaja principal de esta topología es que si el nodo central falla, toda la red perdería conexión por ello el nodo central debe tener un adecuado mantenimiento y monitoreo.

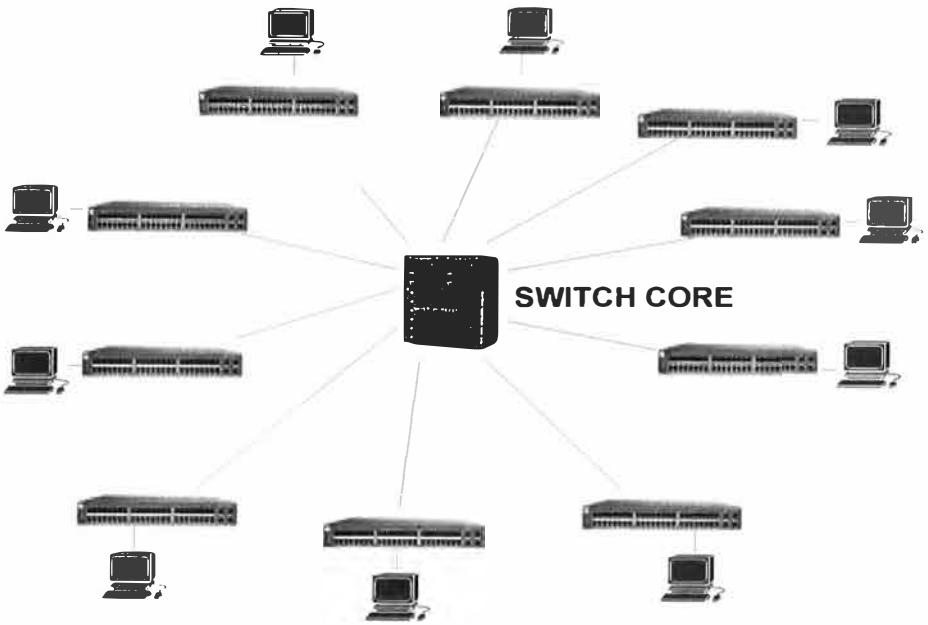


Fig. 3.4 Topología Estrella

Topología Lógica

Lógicamente las redes se dividirán en sub- redes por medio de Vlans, estas son creadas en la capa de CORE, y distribuidas a lo lago de la backbone hasta llegar a los switchs de acceso, cada puerto de los switchs de acceso pertenecerá a una especifica vlan dependiendo del propósito que tendrá el dispositivo que se conecte. La tabla N° 3.1 muestra los segmentos de red del site principal, secundario y agencias con sus respectivas Vlans.

TABLA N° 3.1 Direccionamiento IP

Site Principal	Vlan	IP
Red Servidores	10	10 100 0 0 /24
Red Datos 1	100	10 100 4 0 /22
Red Datos 2	200	10 100 8 0 /22
Red Telefonía	300	10 100 12 0 /22
Red Video	350	10 100 16 4 /29
Site Secundario	**Vlan**	**IP**
Red Servidores	20	10 100 0 0 /24
Red Datos 1	110	10 100 4 0 /22
Red Datos 2	210	10 100 8 0 /22
Red Telefonía	310	10 100 12 0 /22
Red Video	360	10 100 16 4 /29

	Datos					Telefonia			
Agencia 1	10	200	0	16	/27	10	210	0	16
Agencia 2	10	200	0	32	/27	10	210	0	32
Agencia 3	10	200	0	48	/27	10	210	0	48
Agencia 4	10	200	0	64	/27	10	210	0	64
Agencia 5	10	200	0	80	/27	10	210	0	80

La red Lan soporta los servicios de Datos, Telefonía y Videoconferencia conviviendo en una sola infraestructura de red, estas redes son desplegadas y enrutadas entre sí según se requiera.

La red de Datos, tienen un exclusivo segmento de red y así darles un nivel de seguridad aplicando diversas políticas de acceso). Para que se interconecten todas las redes de todas las sedes, se tienen routers de borde que establecen los enlaces RPV provisto por Telmex Perú (Red Privada Virtual de Multiservicios), estos router realizan el marcado del Tráfico saliente aplicando calidad de servicio, con ello el Tráfico es diferenciado en la WAN, se contrata un determinado ancho de banda y este será divido por tipos de tráfico. La Fig. 3.5 muestra la topología de interconexión de datos entre site principal y agencia.

La red de Telefonía, está compuesta por teléfonos IPs de modelos 7975G, 7911G, 2 servidores de Telefonía (Callmanager) que conforman un cluster de telefonía (donde cada servidor tiene la capacidad de administrar hasta 7500 teléfonos), equipos Gateway y un servidor IVR para contac center. El cluster de telefonía está compuesto por dos o más servidores que comparten la misma base de datos y trabajan juntos para dar soporte al grupo de dispositivos de teléfonos IP, en nuestro caso tenemos dos servidores un Publisher y un Suscriber, de esta forma aseguramos un 99.99 % de operatividad del sistema telefónico. El cluster de estos servidores realiza dos importantes funciones:

Elimina el punto de falla que sería tener solo un Server.

Permite que múltiples dispositivos trabajen juntos en el procesamiento de llamadas.

Cada uno de los servidores se encontrara en diferentes sedes para de esta forma tener una contingencia en caso de que se tenga problemas en el site principal. Estos equipos generan reportes de llamadas y llevaran un eficiente control de llamadas. Se tiene un server de Contac Center IPCC, que administra todos los audios que son escuchados por los clientes externos y usuarios internos, provee una solución integral automática de distribución de llamadas, interactiva respuesta de voz e integración con la telefonía (IVR). Las llamadas recepcionadas por estos IVRs son derivadas a un grupo de personas especializadas en dar la información y soporte necesario.

Se tiene como operador de hacia la PSTN a la empresa **Telefónica del Perú**, se tienen contratadas 2 líneas troncales E1 (cada una con capacidad de 30 canales) distribuidas así:

Una troncal E1 se usa para las llamadas salientes y entrantes correspondientes de los sites principal/secundario y agencias (se hace un balance según se requiera) y una troncal E1 es solo para las llamadas salientes y entrantes del Contac Center. La Fig. 3.6 muestra la

topología de troncales E1 a necesitar por site.

Para las llamadas celulares salientes, se tiene un Gateway Celular (ITS), por medio de este equipo se enrutaran las llamadas salientes a celular a los 3 mayores operadores de telefonía celular existentes en el país, se tienen 10 chips para llamadas a Claro, Movistar y Nextel. Con cada grupos de chips se tiene una bolsa de minutos y de esta forma se realiza un ahorro en los costos de llamadas. La Fig. 3.7 muestra la topología de gateway celular.

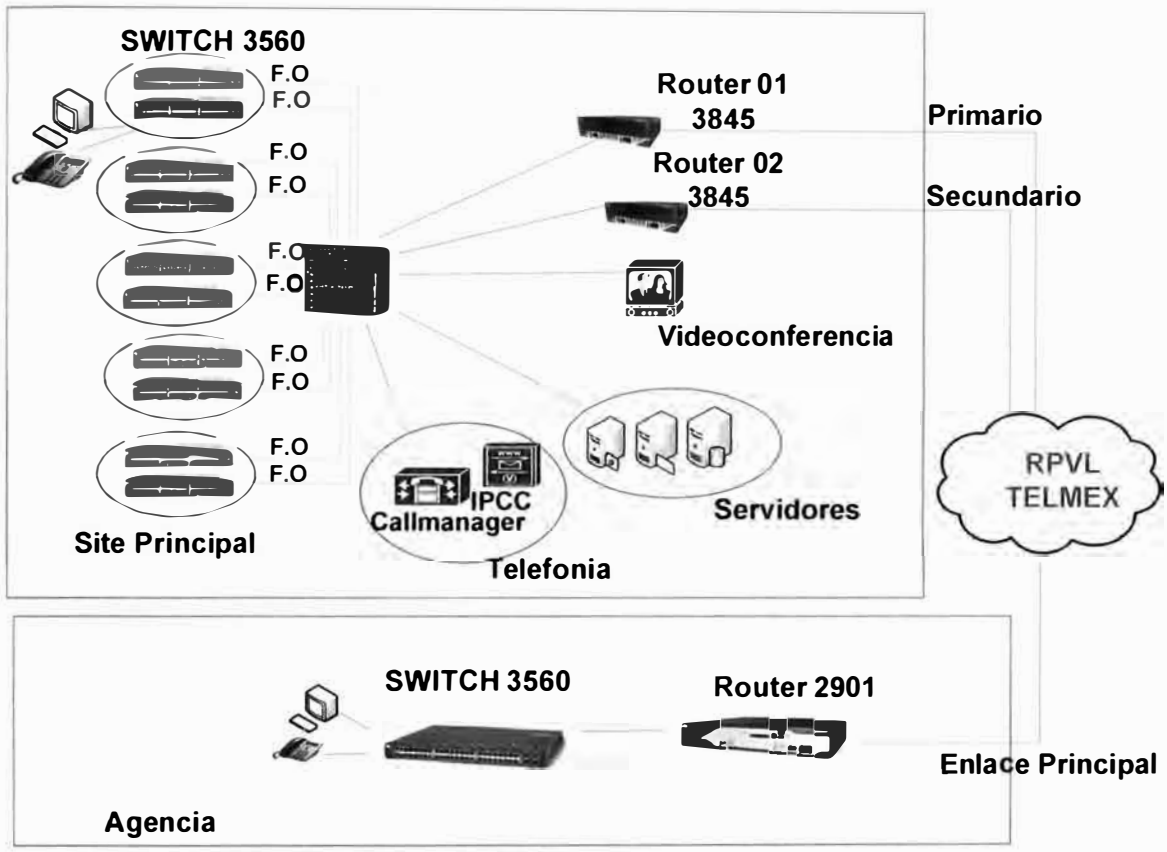


Fig. 3.5 Enlace con sede externa

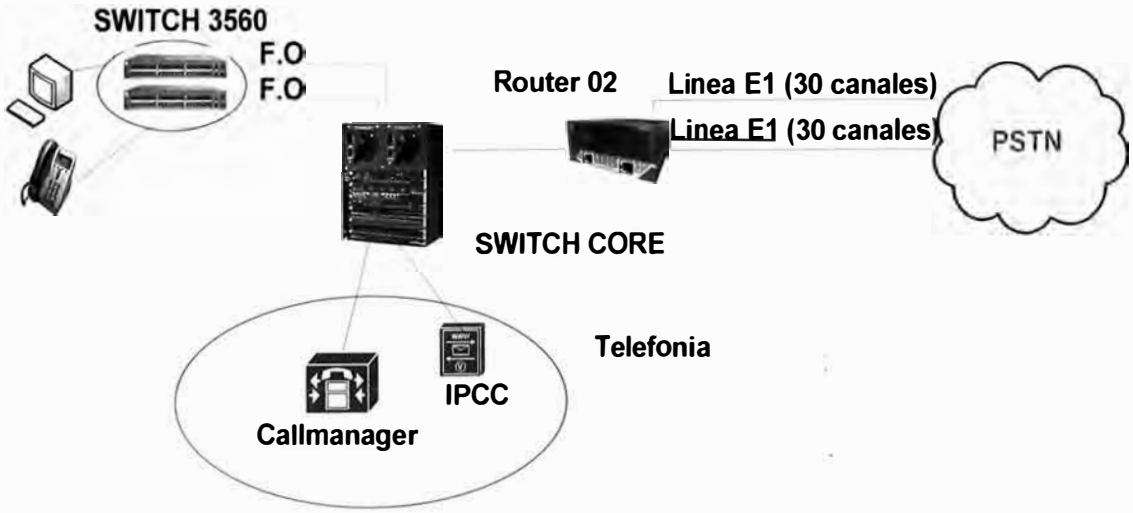


Fig. 3.6 Topología de Telefonía

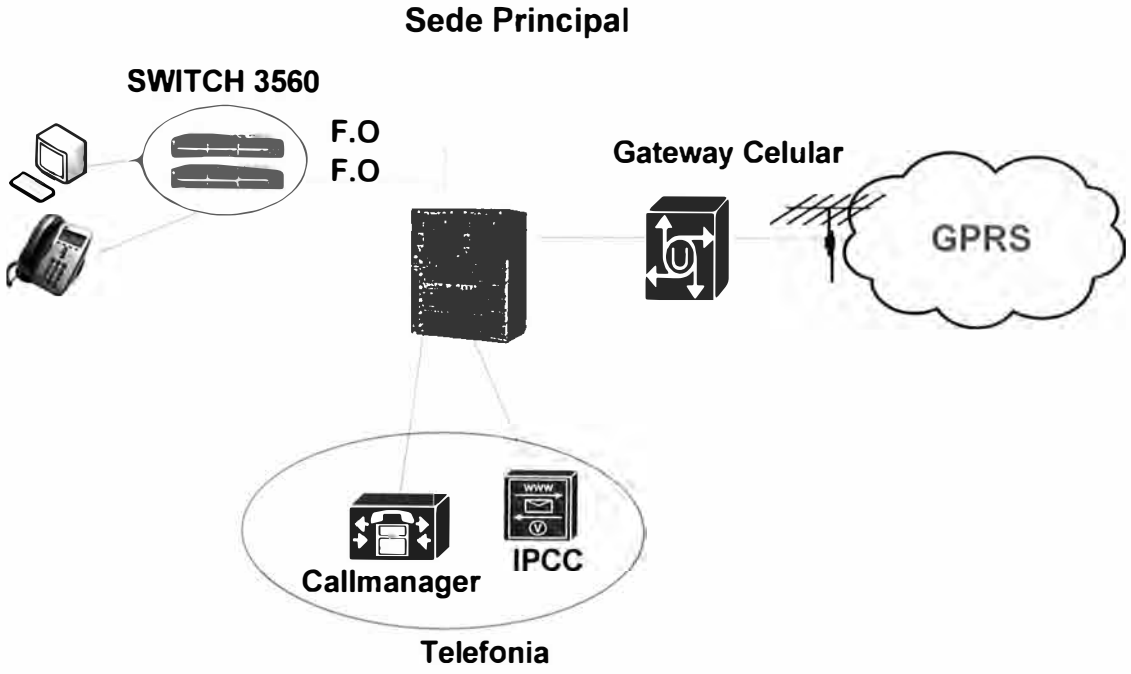


Fig. 3.7 Topología Telefónica Gateway Celular

b) Acceso a Internet

El enlace hacia la red de Internet se realiza por medio de dos proveedores, tenemos a **Telmex Perú** como proveedor del enlace principal y a **Telefónica del Perú** como proveedor del enlace backup o secundario.

Topología Física

Para el acceso a Internet se tiene una topología en estrella donde el equipo principal es el switch CORE, este switch esta ubicado en cada site principal y secundario este tendrá una conexión hacia a un Firewall ASA 5540, este equipo protegerá a la red interna de accesos no autorizados desde Internet y los accesos hacia este, luego del Firewall por la interface failover/stateful se conecta nuevamente al switch core con el propósito de enviar el tráfico failover - stateful (este tráfico es fundamental para que ambos equipos puedan medir sus estados de activo o standby y saber cuáles son las conexiones establecidas en cualquier momento), este tráfico es enviado hacia el otro site donde se encuentra el otro Firewall por medio de la nube RPV, finalmente desde cada Firewall hay una conexión hacia un segmento del switch core que comunicara directamente hacia los equipos IPS que son el primer nivel de seguridad para el acceso desde Internet. Se requieren de servidores DNS, Proxy, Mail y Web Sense (para restringir páginas Web), con los cuales se trabajara la conexión de salida.

Topología Lógica - Modo de Trabajo Activo-Activo

Los Firewall trabajan en el modelo failover activo/activo, este modelo está sólo

disponible a aplicaciones de seguridad en múltiple contextos, para nuestro caso usaremos dos, contexto 1 y contexto 2.

En modo failover Activo/Activo, ambos Firewall (ASA de la marca CISCO), tendrán los dos contextos pero solo uno estará activo y el otro en standby por Firewall, cada contexto manejara un tráfico diferente, en el ASA01 se encuentra activo el contexto1 y el contexto2 en standby.

En caso que uno de los equipos ASA (Ej. ASA01) falle, el otro equipo ASA (ASA02) asumirá todo el trabajo. Las siguientes tablas muestran los contextos a manejar por cada Firewall.

Tabla Nº 3.2 Contexto por ASA

	Contexto 1	Contexto 2
ASA01	Activo	Stanby
ASA02	Standby	Activo

Manejo por contexto

Tabla Nº 3.3 Interfaces a usar por ASA

Contexto 1

Tráfico de entrada :Interface	Tráfico de Salida :Interface
Navegación(Vlan 100) : G0/1.1	Outside Navegación(Vlan770) : G0/0.1

Contexto 2

Tráfico de entrada :Interface	Tráfico de Salida :Interface
Servicios (Vlan 200) : G0/2.1	Outside Servicios (Vlan 880) : G0/0.2

ASA01

El equipo ASA01 manejara el contexto1 en modo activo, este contexto manejara el tráfico que corresponde a Navegación , el tráfico llegara al contexto 1 por medio de la interface G0/1 (subinterface G0/1.1) como Vlan 100 y luego de aplicarse las políticas de seguridad respectivas, este tráfico saldrá transformado como Vlan 770 y enviado por medio de un enlace trunk hacia el switch CORE SW4506-SW, luego el tráfico será enviado hacia un equipo IPS (Intrusión Prevention System) que aplicara políticas de seguridad por medio de signaturas actualizadas y finalmente el tráfico es enviado al router de borde correspondiente al servicio que provee Telmex Perú.

A la interface G0/2 (subinterface G0/2.1) se le asigna la Vlan 210, esta se encuentra en modo pasivo hasta que la misma deje de estar en activo en el otro ASA. Este equipo se encuentra en el site principal.

ASA02

El equipo ASA02 manejara el contexto 2 en modo activo, este contexto manejara el tráfico que corresponde a servicios especiales (por este contexto se accederán a páginas web y servicios de otras empresas), este tráfico llegara al contexto 2 por medio de la interface G0/2 (subinterface G0/2.2) como Vlan 200 y luego de aplicarse las políticas de seguridad respectivas, este tráfico saldrá transformado como Vlan 880 y enviado por medio de un enlace trunk hacia el switch CORE SW4506-SW, luego el Tráfico será enviado hacia un equipo IPS que aplicara políticas de seguridad por medio se signaturas actualizadas y finalmente el tráfico es enviado al router de borde correspondiente al servicio que provee Telefónica del Perú.

A la interface G0/1(subinterface G0/1.2) se le asigna la Vlan 110 esta se encuentra en modo pasivo hasta que la misma deje de estar en activo en el otro ASA. Este equipo se encuentra en el site secundario. La Fig. 3.9 muestra la topología de Internet en modo activo/activo y la tabla Nº 3.4 el ancho de banda por enlace.

TABLA Nº 3.4 Enlace de Internet

Enlace	Sitio	Descripción	Ancho de Banda	Proveedor
Internet	Site Principal	Internet Principal	4Mbps	TELMEX
Internet	Site Secundario	Internet Secundario	4Mbps	Telefónica

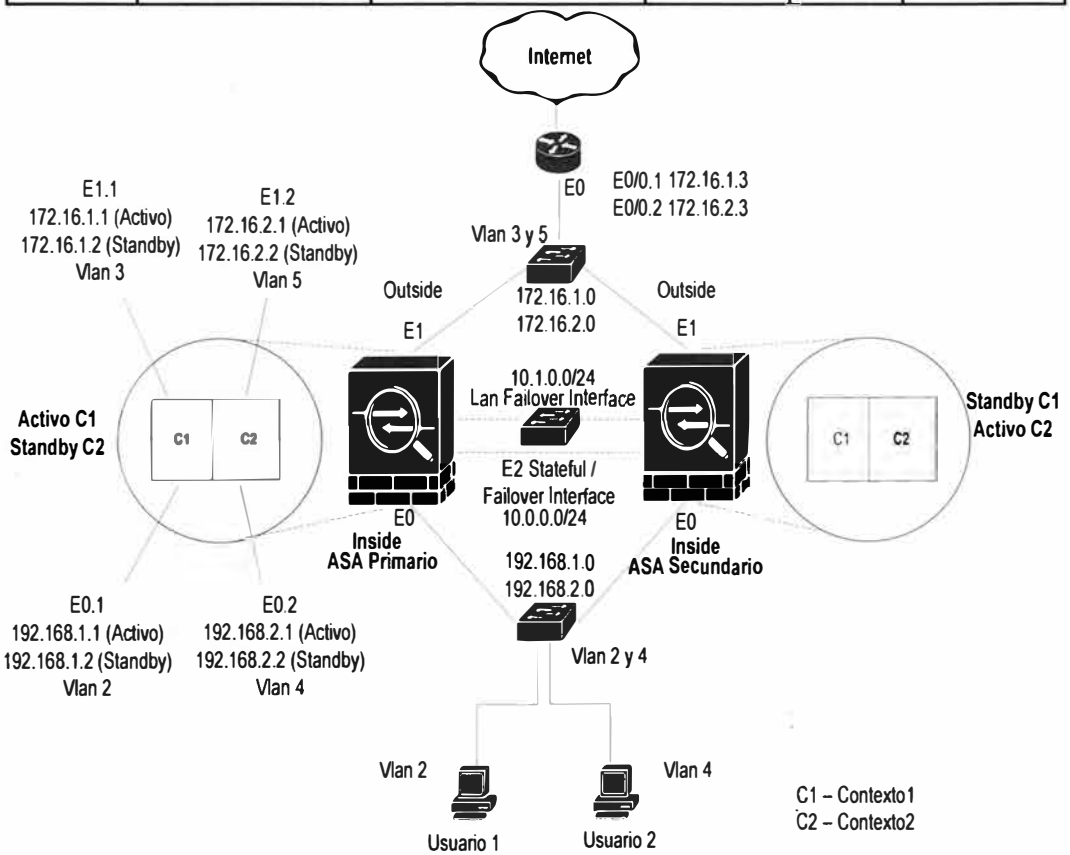
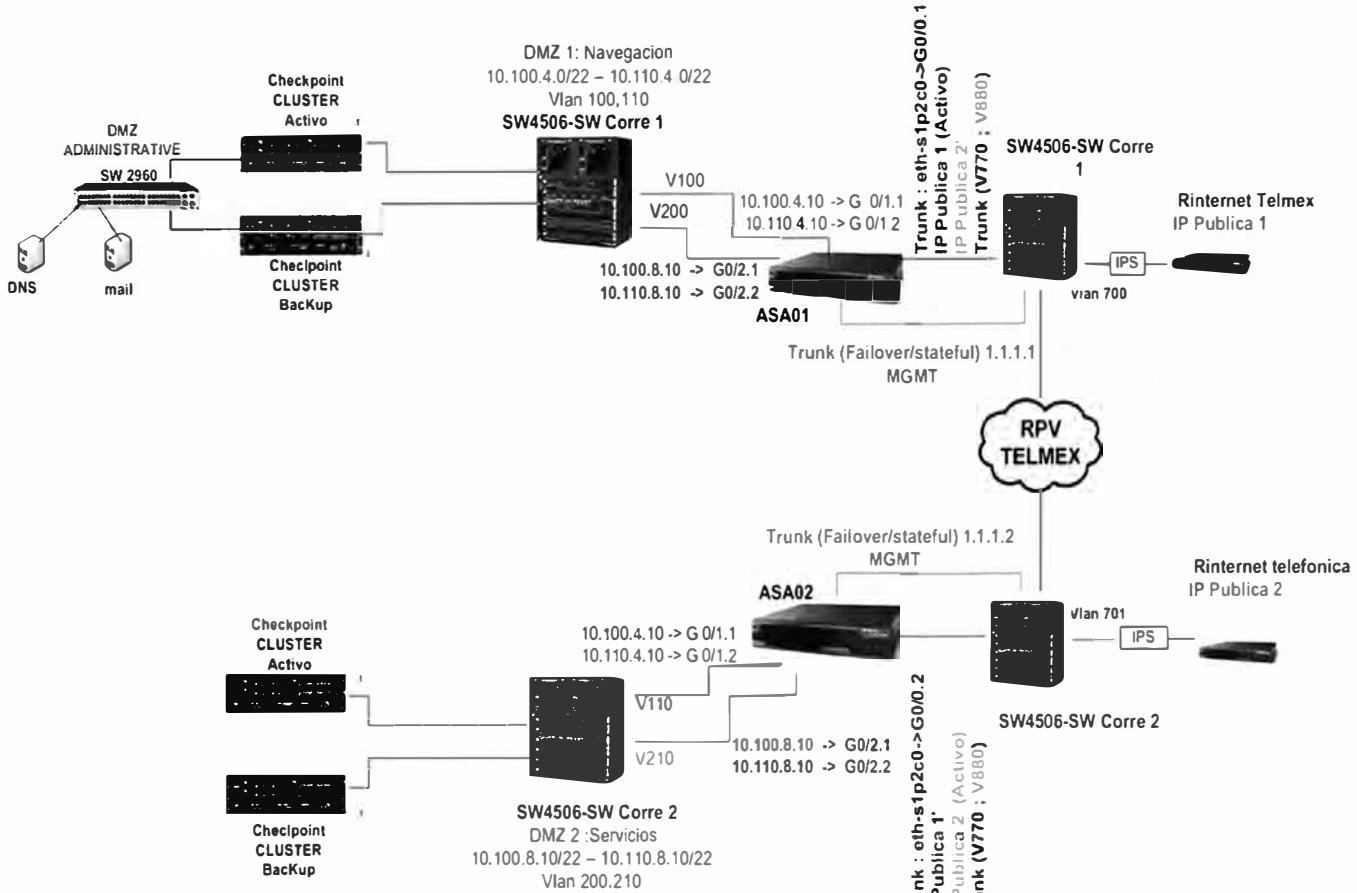


Fig. 3.8 Topología lógica Activo/Activo



LEYENDA

	ASA01	ASA02
Navegacion (Principal)	Vlan 100 CTX1 (activo) : G0/1.1	Vlan 110 CTX1 (pasivo) : G0/1.2
Servicios (Principal)	Vlan 200 CTX2 (activo) : G0/2.1	Vlan 210 CTX2 (pasiivo) : G0/2.2
Navegacion (Secundario)	Vlan 110 CTX1 (activo) : G0/1.2	Vlan 110 CTX1 (pasivo) : G0/1.1
Servicios (Secundario)	Vlan 210 CTX2 (activo) : G0/2.2	Vlan 210 CTX2 (pasiivo) : G0/2.1
Outside Navegacion	Vlan: 770 CTX1 (activo) : G0/0.1	Vlan: 770 CTX1 (pasivo) : G0/0.2
Outside Servicios	Vlan: 880 CTX2 (pasivo) : G0/0.1	Vlan: 880 CTX2 (activo) : G0/0.2

Fig. 3.9 Topología Internet

c) Acceso a Extranet

Se tiene la necesidad de tener comunicación constante con proveedores, empresas del mismo rubro, etc.; debido a la importancia de validar datos o intercambiar información.

Topología Física

Debe haber un Firewall con las políticas adecuadas para proteger a la red del banco de la red de proveedores externos, para nuestro caso usaremos un cluster de equipos checkpoint de la marca Nokia que trabajara en modo activo/standby. La misma topología debe de tenerse en el site secundario donde también habrá un segundo enlace con terceros que se usara como contingencia del enlace principal.

Topología Lógica

Se trabajara con la topología Activo/StandBy, esto quiere decir que en el enlace principal a la red de proveedores habrán dos Firewall con la misma configuraciones solo que uno de los dos estará activo y el otro en standby. La Fig. 3.10 muestra la topología de acceso a extranet.

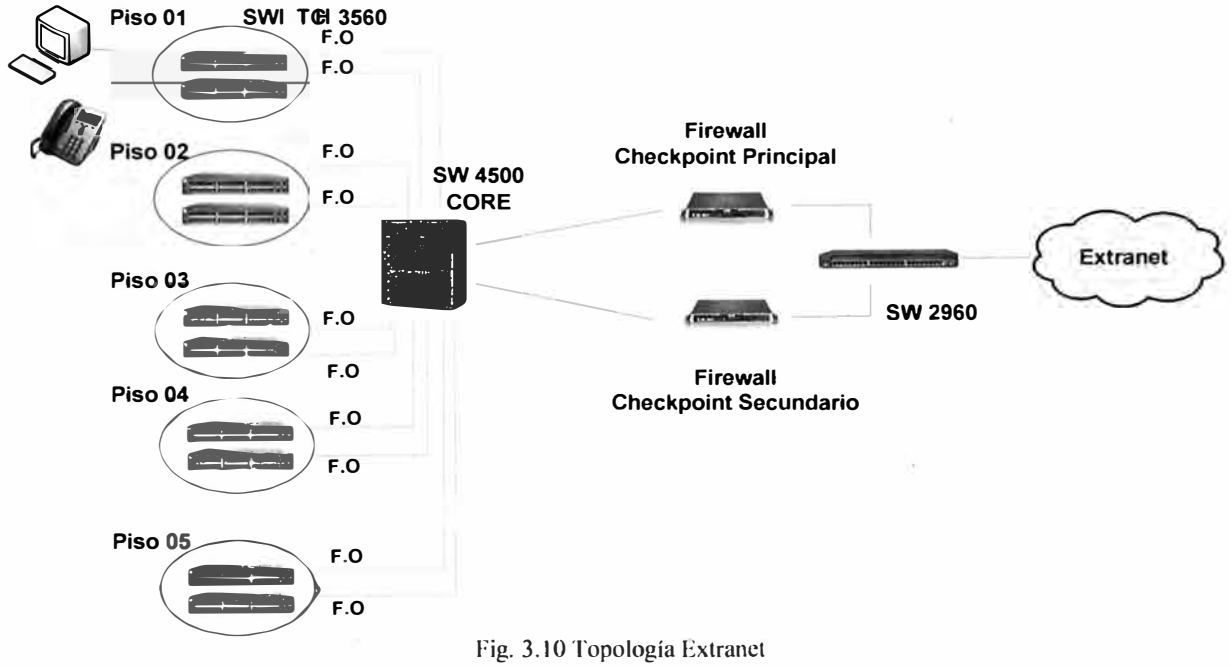


Fig. 3.10 Topología Extranet

Habrán en dos cluster, uno se encontrara en el site principal y el segundo en el site secundario, en caso que se tenga problemas con el enlace del site principal, el tráfico hacia extranet será enrutado al segundo cluster de esta forma no se perderá conexión con este enlace.

3.1.4 Contingencia de Servicios

Un aspecto muy importante a considerar es la necesidad de tener enlaces de contingencia, estos mantendrán los servicios operativos, permitiendo que el banco continúe

con su negocio. Con este concepto se tiene una alta disponibilidad de los servicios más importantes y necesarios para la operación del banco:

a) Contingencia red de Datos, Telefonía IP y Videoconferencia

La contingencia se da teniendo un segundo router de borde RPV (backup) en el site principal y secundario (que es donde se encuentran los servidores que ofrecen estos servicios), por el router principal se hace el enrutamiento del tráfico hacia el exterior mientras que el router backup permanece en standby, pero en caso de falla del router principal el router backup asumirá automáticamente toda la carga hasta que el principal se restablezca. Ambos equipos tendrá la misma configuración y la forma de conmutar de un equipo al otro será automatica usando el protocolo de CISCO HSRP (**Hot Standby Router Protocol**) que es una versión propietaria de CISCO de VRRP, se crea un cluster formado por el router principal y el router secundario.

Para este router backup se tiene un enlace con Telmex (el cual debe venir de oun nodo diferente que el principal) de la misma cantidad de ancho de banda que el principal, el tráfico se encuentra diferenciado por calidad de servicio de la misma manera que el principal. De esta manera se asegura una constante comunicación entre las sedes corporativas y con las agencias en caso de fallas en el enlace principal.

Se tiene una conexión vía la red ISDN provisto por Telefónica del Perú, esto servirá para que las agencias que también tienen una conexión ISDN de contingencia puedan comunicarse con el site principal donde se encuentran los servidores y conexiones con otras instituciones en caso que el enlace principal dentro de la misma agencia fallara, al ser la conexión ISDN limitada por agencia a 128Kbps (2 canales B y 1 canal de señalización D - BRI) , solo se permitirá el tráfico estrictamente necesario para el negocio ya que de otra forma el enlace se saturaría de inmediato. La Fig. 3.11 muestra las contingencias de datos y telefonía IP que proporciona el site principal/secundario. En caso hubiera un problema general con todo el site principal, las otras sedes se podrán conectar al site secundario donde se encontraría servidores backup.

b) Contingencia en Telefonía IP

Para la contingencia del enlace de telefonía, aparte de las tres líneas E1 principales que se tienen en el site principal , se tienen 3 líneas E1 adicionales. en el site secundario como contingencia, cada una de estas troncales tiene una numeración diferente, el proveedor de estas líneas es Telefónica del Perú y con ellos se tiene establecido que en caso de fallas con la línea principal se redirecciones las llamadas hacia las líneas de contingencia que

corresponda, de esta forma el cliente externo seguirá llamando al número corporativo conocido luego cuando la línea principal se restablezca se retira el desvió y se vuelve a activar las líneas E1 primarias. La Fig. 3.12 muestra la contingencia de telefonía externa.

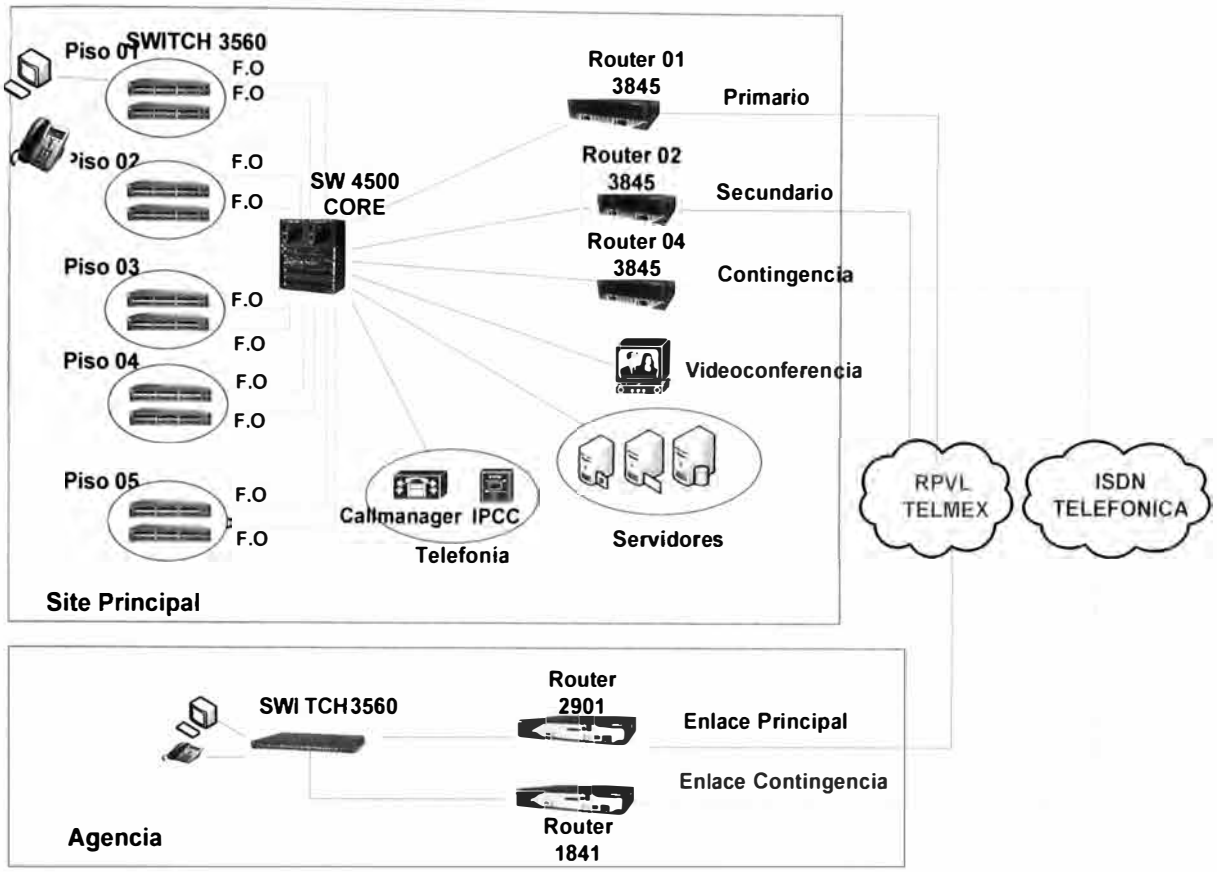


Fig. 3.11 Contingencia Datos

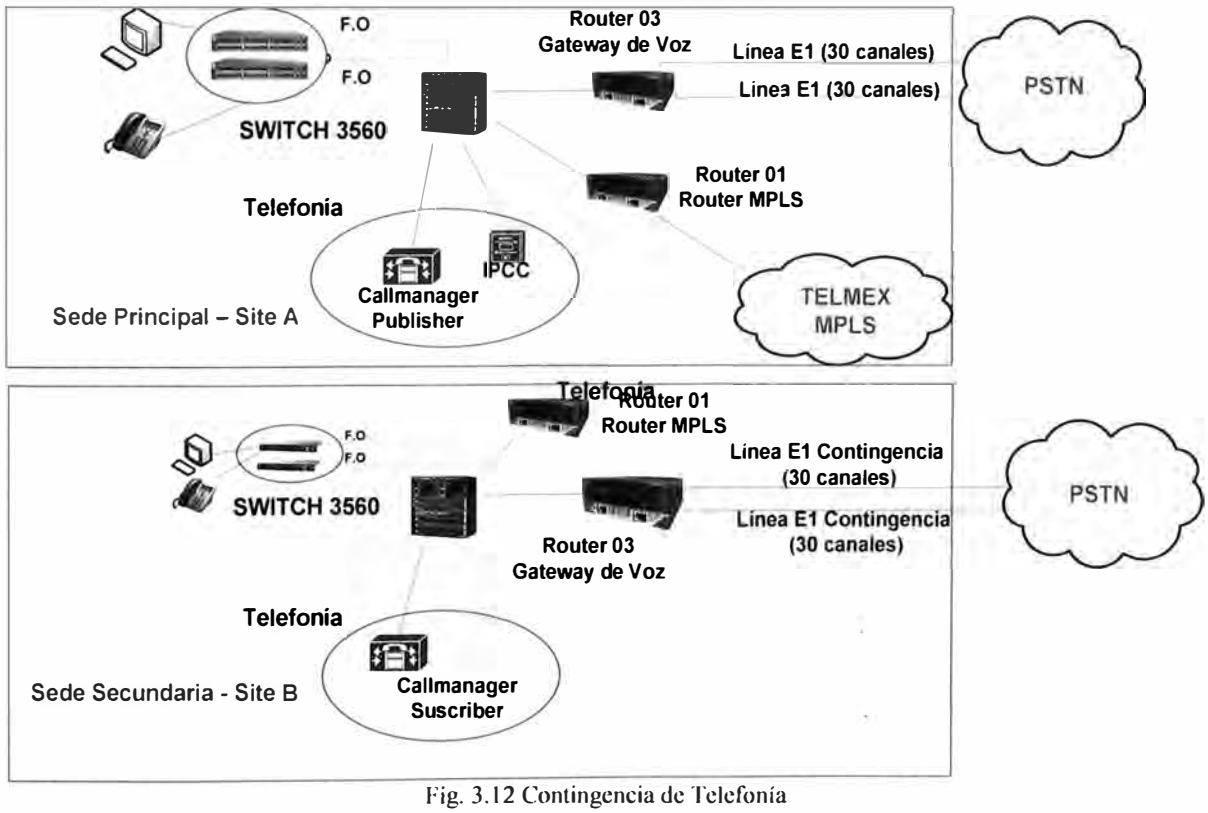


Fig. 3.12 Contingencia de Telefonía

c) Contingencia en Agencia

Para la contingencia de enlace en las agencias, se tendrá una línea ISDN, a la cual se puede acceder por medio de un router, este router estará conectado en la LAN de la agencia, se usa el protocolo HSRP para que el tráfico conmute del enlace principal al enlace de contingencia automáticamente cuando se detecte fallas con el enlace principal, cuando el enlace principal cae, entonces el protocolo HSRP identifica este problema y hace la conmutación automática hacia el router de contingencia , en este router se aplican políticas para garantizar que solo el tráfico estrictamente necesario sea el que se transmita por este enlace, luego cuando el enlace principal es restablecido el protocolo HSRP identifica el estado del enlace y conmuta nuevamente hacia el enlace principal y todo la comunicación se restablece. La Fig. 3.13 muestra la contingencia de enlace en agencia.

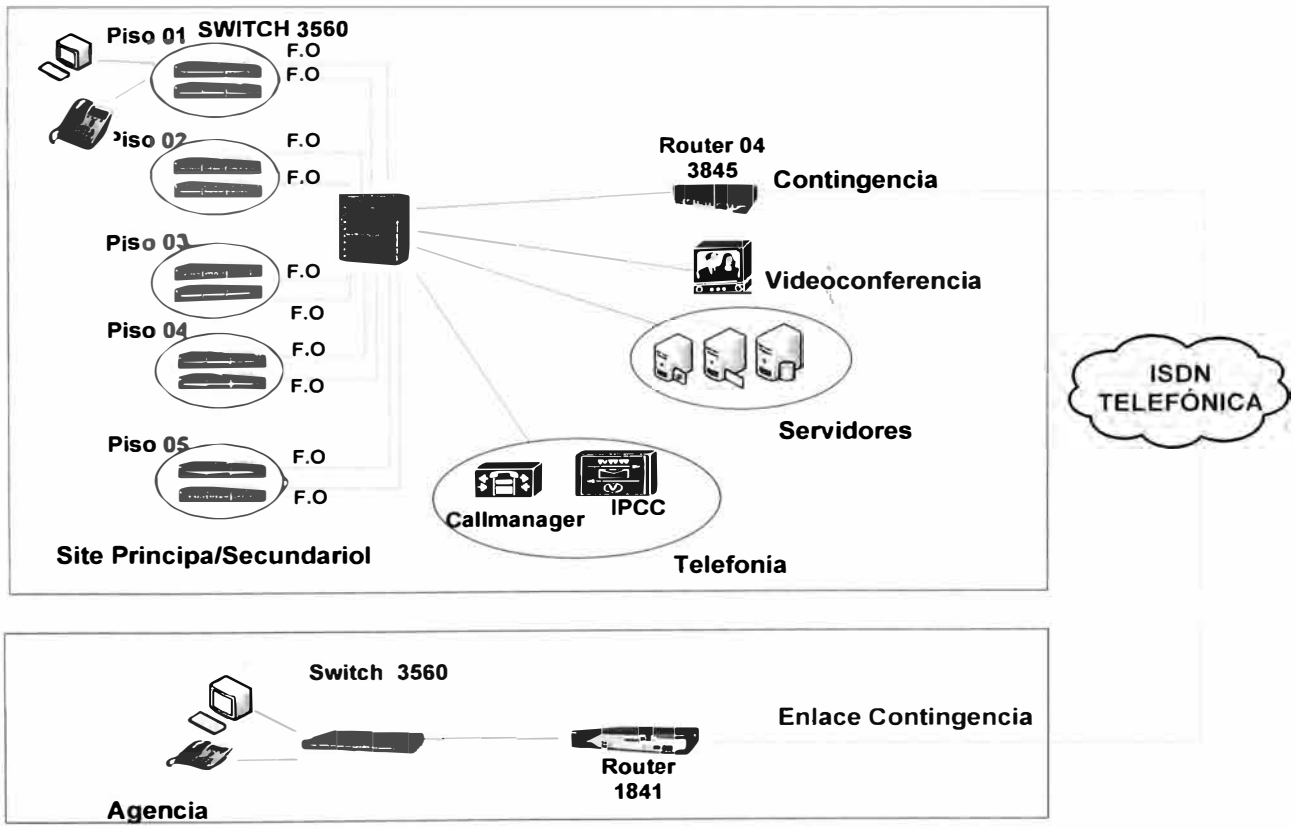


Fig. 3.13 Contingencia en Agencia

3.2 Determinación del equipamiento necesario

Se determina el equipamiento a usar, agrupándolos por servicios y la sede donde se encuentren, empezaremos con el site principal en la cual se encuentran concentrados los servicios de Datos, Telefonía IP, Videoconferencia, Internet, Extranet.

Para los servicios de Datos, se necesitan de los equipos que se muestran en la tabla N°3.5

, estos son los necesarios en el site principal y secundario:

TABLA N° 3.5 Equipamiento de datos, telefonía y video site principal y secundario

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca	UR
1	2	Roture RPV	3845	Site Principal/Secundario	CISCO	2
2	2	Roture Contingencia de RPV	3845	Site Principal/Secundario	CISCO	2
3	2	Router ISDN	3845	Site Principal/Secundario	CISCO	2
4	1	Tarjeta E1 ISDN	VWIC2-1MFT-T1/E1	Site Principal/Secundario	CISCO	-
5	2	Switch CORE	4500	Site Principal/Secundario	CISCO	10
6	2	Módulos 24 puertos puertos GBIC - MTRJ	WS-X4124-FX-MT	Site Principal/Secundario	CISCO	-
7	20	Switch Catalyst 3560-48PS	3560	Site Principal/Secundario	CISCO	1
8	20	Módulos SFP puertos Gbic	MTRJ	Site Principal/Secundario	CISCO	-

La tabla N° 3.6 muestra los equipos a necesitar por Agencia:

Tabla N° 3.6 Equipamiento datos y telefonía por Agencia

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca	UR
1	5	Roture RPV	2901	Agencias	CISCO	1
2	5	Roture Contingencia ISDN	1751	Agencias	CISCO	
3	5	Tarjetas BRI	WIC-1B-S/T-V3	Agencias	CISCO	-
4	5	Switch Catalyst 3560-48PS	3560	Agencias	CISCO	1

Para los servicios de Telefonía IP y Contac Center, se necesitara de equipos que se muestran en la tabla N° 3.7 en Site Principal y Site Secundario:

Tabla N° 3.7 Equipamiento Telefonía IP site principal y secundario

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca	UR
1	2	Roture Gateway de voz (ios 12,3 11T)	3845	Site Principal/Secundario	CISCO	1
2	4	Tarjetas E1(2 puertos C/U)	VWIC-2MFT-E1	Site Principal/Secundario	CISCO	-
3	4	PVDM 48-Channel Fax/Voice DSP Module	PVDM2-48	Site Principal/Secundario	CISCO	-
4	2	Servidor Callmanager 7.1	MCS7816I4-K9-CMC2	Site Principal/Secundario	CISCO	1
5	500	Teléfonos IP	7911G	Site Principal/Secundario	CISCO	-
6	20	Teléfonos IP	7975G	Site Principal/Secundario	CISCO	-

La tabla N° 3.8 muestra los equipos de telefonía a necesitar en el site principal:

Tabla N° 3.8 Equipamiento Telefonía IP site principal

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca	UR
1	1	Gateway Celular	CGW-P ISDN PR	Site Principal/Secundario	ITS TELEC	-
2	1	Servidor UCCX 5.0 callcenter	MCS-7816-H3-CCX1	Site Principal/Secundario	CISCO	-

La tabla N° 3.9 muestra los equipos de telefonía a necesitar en las 5 agencias:

Tabla Nº 3.9 Equipamiento Telefonía IP agencia

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca	UR
3	30	Teléfonos IP	7911	Agencias	CISCO	-

Para el servicio de Video, se necesitara de los equipos de la siguiente tabla, en Site Principal y Site Secundario:

Tabla Nº 3.10 Equipamiento videoconferencia site principal y secundario

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca	UR
1	2	Tandberg Edge videoconferencia	Edge 95/85/75XP	Site Principal/Secundario	Tandberg	-
2	2	videoconferencia Televisor 37'	37'	Site Principal/Secundario	LG	-

Para el servicio de Internet, se necesitara de los siguientes servidores que van a tener una conexión hacia Internet y pueden ser consultados desde el exterior.

Solo se están considerando los equipos necesarios por parte de comunicaciones, adicional a estos se necesitaran:

Servidores DNS: Para la resolución de nombres de dominios.

Servidor Mail: Para que pueda darse el servicio de correo electrónico.

Servidor WEB: Para accesos a la Web de la empresa.

Servidor de servicios: Para realizar operaciones en Línea u otros servicios ofrecidos al público.

Se necesitara de los equipos de comunicaciones de la tabla Nº 3.11 en el site principal y secundario.

Tabla Nº 3.11 Equipamiento Internet

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca	UR
1	2	Firewall Activo/Activo	ASA 5540	Site Principal/Secundario	CISCO	1
2	4	Firewall Activo/Standby	Checkpoint	Site Principal/Secundario	NOKIA	1
3	2	Intrusión Prevention System	4200	Site Principal/Secundario	CISCO	1
4	2	Para cluster Checkpoint	2960	Site Principal/Secundario	CISCO	1

Para el servicio de extranet, se necesitara de los equipos de la tabla Nº 3.12 en Site Principal y Site Secundario:

Tabla Nº 3.12 Equipamiento Extranet

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca	UR
1	4	Firewall Activo/Standby	Checkpoint	Site Principal/Secundario	NOKIA	
2	2	switch extranet	2960	Site Principal/Secundario	CISCO	1

3.3 Especificaciones técnicas

Los equipos a usar para toda esta infraestructura son:

Routers, dispositivo de capa de Internet que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red.

Switch, dispositivo de red que filtra, reenvía o inunda tramas basándose en la dirección destino de cada trama

Servidores de Telefonía, dispositivo que administra la solución de telefonía IP (Callmanager), para llamadas a celular salientes se tiene un gateway celular y para contac center un servidor IPCC.

Teléfonos IP, equipos telefónicos que funcionan con la tecnología IP.

Equipos videoconferencia, dispositivo que envía imágenes y audio en tiempo real hacia otro equipo destino.

Firewall e IPS, equipos que administran políticas de seguridad para proteger a la red interna de accesos no autorizados.

Las características técnicas de todos estos equipos por modelos se encuentran en el anexo A, debido a la amplitud de información encontrada se desarrolla en este anexo.

3.4 Infraestructura necesaria

Para poder brindar los servicios de datos, telefonía IP, videoconferencias, Internet, etc.; se necesita tener una infraestructura de cableado estructurado que cumpla con las normas establecidas como la Norma ANSI/TIA/EIA 568-B, la cual define estándares para establecer el cableado estructurado para sites comerciales y sites de campus. en esta se definen los tipos de cables, distancias, conectores, requisitos de instalación, métodos de testeo de la estructura, brindando una guía para la planificación e instalación de los sistemas de cableado, siguiendo este estándar se garantiza un nivel de vida del cableado mayor a 10 años.

3.4.1 Área de trabajo

Este está conformado por el espacio físico donde se ubica el usuario, PC, Teléfono IP, Fax, impresoras, scanner, entre otros.

Por cada estación de trabajo, se debe de instalar dos conectores de red uno destino para datos y la otra para telefonía IP (los ductos deben de tener la capacidad de poder llevar dos puntos de red por área de trabajo). Luego desde estos puntos de red se debe conectar por medio de un cable de red de 3m aprox. hacia el equipo final que puede ser una PC.

Teléfono IP, etc.

El cable de red debe terminar en ambos extremos en conectores RJ45 bajo la norma T568A o T568B, además estos cables deben ser certificados para poder garantizar una larga operación. Los puntos de red necesarios por las estaciones de trabajos, impresoras, scanner, etc. Las siguientes tablas muestran los accesorios a necesitar.

En site Principal y Cite Secundario:

Tabla N° 3.13 Equipamiento área de trabajo

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca
1	640	Fachee ate (Datos-Voz) Fig. 3.14	Estación de trabajo	Cite Principal/Secundario	Panduit

Por las 5 Agencias:

Tabla N° 3.14 Equipamiento área de trabajo

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca
1	100	FacePlate (Datos-Voz) Fig. 3.14	Estación de trabajo	Agencias	Panduit

Fig. 3.14 Face Plate (Datos-Voz)

La cantidad necesaria de estos cables Cat6a se muestran en las siguientes tablas.

En Site Principal y Site Secundario:

Tabla N° 3.15 Cables de red

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca
1	700	Cables de Red 2,1mts	Cat 6a	Estación de trabajo	Panduit
2	700	Cables de Red 1,5mts	Cat 6a	Patch Panel	Panduit

Por las 5 Agencias

Tabla N° 3.16 Cables de red

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca
1	100	Cables de Red 2,1mts	Cat 6a	Estación de trabajo	Panduit
2	125	Cables de Red 1,5mts	Cat 6a	Patch Panel	Panduit

3.4.2 Cableado Horizontal

La infraestructura está conformado por un cableado horizontal, el cual corresponde al cableado desde el área de trabajo del usuario o donde se encuentra el equipo a conectar hasta el cuarto de comunicaciones donde se encuentran los equipos de comunicaciones, el

cable de red a usar según la norma ANSI/TIA/EIA – 568-A, es el cable UTP de par trenzado de categoría 6a (avanzado opera en frecuencias de hasta 550MHz y pueden llegar a proveer transferencias de 10GBit/s mitiga los efectos de diafonía y crosstalk) debe tener un máximo de 90 metros. Estos cables terminaran en regletas o patch panels (de 24, 48, 72 y 96 puertos), ubicadas en los rack de comunicaciones y en el área del usuario en conectores jack RJ45, la fig. 3.15 muestra la instalación de un patch panel y la 3.16 como se interconecta la estación de trabajo hasta el patch panel.

Fig. 3.15 Patch Panel
Fuente: American Tech Suply

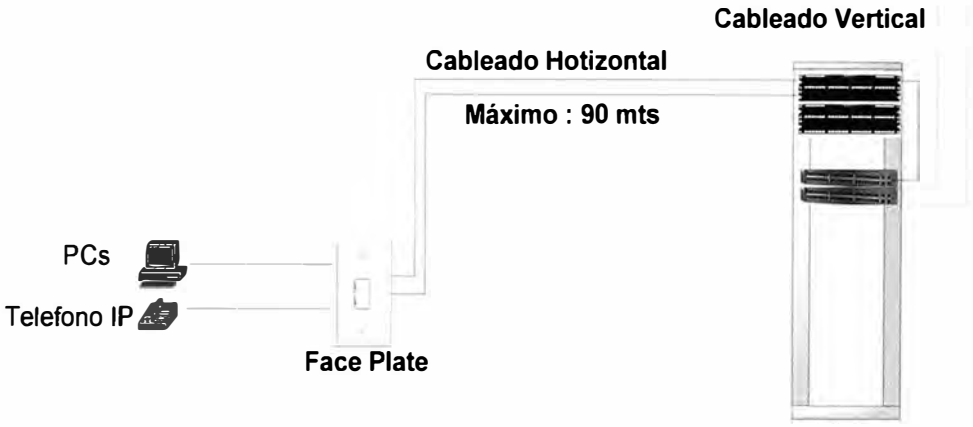


Fig. 3.16 Cableado Horizontal

3.4.3 Cableado Vertical

Este cableado también conocido como backbone comunica los cuartos de comunicaciones de los sites principal y secundario con el data center (hay un cuarto de comunicaciones por piso) para este cableado se tiene la opción de usar Fibra Óptica Multimodo o Monomodo, se decide usar fibra óptica debido a la gran velocidad que este medio de transmisión ofrece, con este medio de transmisión y recepción los equipos de comunicaciones podrán intercambiar información con una muy alta velocidad. Por ser más económico y por que la distancia que se cubrirá no es mucha se opta a usar F.O Multimodo (se recomienda esta a distancias menores de 1 kilómetro). Para que los equipos de comunicaciones puedan conectarse por medio de F.O deben usarse unos adaptadores especiales en los switchs, son conocidos como módulos SFP Gbic, usaremos 1 Gbic MTRJ

que se instala en el switch de acceso, luego por un jumper CAB-MTRJ-SC-MM, se conecta el switch de acceso al de cada cuarto de comunicaciones con el patch panel de FO ubicado en el rack de cada piso (puertos SC MM),en estos patch panel de F.O se encuentran reflejados las conexiones de todos los switchs de acceso, de este patch panel por medio de otro jumper CAB-MTRJ-SC-MM una vez en el data center se conecta hacia el switch CORE (puerto MTRJ), de esta forma se tienen conectados los switch de acceso con el switch CORE. La tabla N° 3.17 muestra los jumpers de F.O a necesitar.

Tabla N° 3.17 Jumpers F.O

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca
1	20	Jumper F.O(PATCH PANEL - SWITCH ACCESO) 1mts	MTRJ - SC	Site Principal/Secundario Piso2	OPTRONICS
2	20	Jumper F.O (PATCH PANEL - SWITCH CORE) 2mts	MTRJ - SC	Site Principal/Secundario Piso2	OPTRONICS

3.4.4 Data Center y Cuarto de Comunicaciones

El datacenter es el centro de procesamiento, almacenamiento y enrutamiento de la red, contiene los sistemas de cómputo y equipos de misión critica para el negocio, los sistemas incluidos dentro de un data center y cuarto de comunicaciones son las siguientes:

Infraestructura de cableado.

Monitoreo y sistemas de gestión de infraestructura.

Piso elevado.

Sistema de control.

Seguridad informática.

Sistemas de detección y extinción de incendios.

Control de acceso.

Sistema de refrigeración.

Sistema de potencia UPS, baterías y generadores.

Los objetivos del Data Center, son:

Transmitir/recibir datos eficiente y rápidamente.

Transmitir/recibir datos confiablemente y proporcionar acceso a los mismos.

Proveer aplicaciones de misión critica.

Se tienen como base estándares internacionales para la implementación del Data Center:

ANSI/TIA 942: Telecommunications Infrastructure Standard (Standard Americano).

ANSI/NECA/BICSI-002: Complementario a la TIA 942.

EN 50173-S: Tecnología de la información / Data Centers (Standard Europeo).

ISO/IEC Draft 24764: Tecnología de la Información.

El objetivo de estos estándares es:

Guiar en la planeación y construcción.

Especificar los requisitos mínimos de cumplimiento.

Durante el proceso de diseño se siguieron las siguientes etapas:

Estimar los requisitos de espacio, potencia, refrigeración (se analizan las expectativas de crecimiento al considerar estos parámetros).

Proveer los requerimientos de espacio, potencia, refrigeración, seguridad, carga de piso. puesta a tierra, protección eléctrica, etc.

Coordinar los planes preliminares de distribución de espacio con los arquitectos a cargo.

Crear un plan de distribución de los equipos en el piso y proveer los requerimientos para los ductos de comunicaciones.

Obtener un plan actualizado con los ductos, equipos eléctricos y mecánico agregado al plan de distribución del piso a plena carga.

Diseñar el cableado con base en los equipos a instalar en las diferentes áreas.

En nuestro diseño seguimos el estándar americano ANSI/TIA 942 (todos los estándares son similares se opta por este diseño por su comprobada funcionalidad y experiencia).

a) Entrance Room (ER)

Este es el cuarto de entrada para los proveedores de servicios (Telmex, Telefónica) donde se instalan los enlaces de RPV, Internet, Extranet y otros equipos a los cuales deba tener acceso el proveedor, esta área se encuentra fuera del cuarto de telecomunicaciones para evitar que el proveedor pueda tocar cualquier otro equipo que no le competa, esta área se interconecta con el cuarto de telecomunicaciones por medio de cableado horizontal.

b) Main Distribution Area (MDA)

Es el cuarto de telecomunicaciones donde se encuentran los equipos de comunicaciones Routers, Switchs, PBX, Servidores, etc.

Hay muchos aspectos a analizarse al momentos de diseñar los cuartos de comunicaciones y data centers, estos se pueden encontrar en el estándar.

Dentro de estos se tienen ; altura de rack , carga sobre el piso, iluminación, dimensionamiento de puertas , espacios, accesos, temperatura, puesta a tierra, distribución de rack y gabinetes, cableado horizontal, cableado vertical, piso elevado, aire acondicionado, redundancia

Con respecto a la redundancia, según el estándar americano se tienen 4 niveles por tipo de data center estos niveles son conocidos como Tires, el que corresponde al data center

implementado es el nivel III y cumple los requisitos que se exigen en este nivel que son contar con múltiples rutas de distribución, potencia y refrigeración. El data center en este nivel puede realizar actividades planificadas sin interrumpir la operación (mantenimiento preventivo, adición o retiro de componentes, test de componentes y sistemas), cuenta con la capacidad suficiente para soportar la carga mientras se realiza el mantenimiento. Y tiene la capacidad para en un futuro llegar a ser TIER IV. El ER y MDA conformarían nuestro data center y la conexión entre ellos será por cableado horizontal.

c) Cuartos de Comunicaciones

Los cuartos de comunicaciones son las habitaciones debidamente acondicionadas en las agencias y pisos de las sedes principal/secundaria, donde se encontraran todos los equipos de comunicaciones, switch, routers, servidores, UPS, estos equipos son alojados dentro de RACKS. Las consideraciones para el diseño de los cuarto de comunicaciones es más simple que para los data centers, pero hay normas que deben ser las mismas, como el no estar cerca de los baños (para evitar cualquier posibilidad de inundación). En estos cuartos también se encuentran tableros eléctricos que controlan el abastecimiento de energía de todos los equipos de comunicaciones instalados.

Por cada cuarto hay un sistema de aire acondicionado, estos son empotrados a la pared y para el caso de los Data Center por el falso piso, con un sistema de control y monitoreo dentro del cuarto de comunicaciones. En la tabla N° 3.18 se tienen los equipos de aire acondicionado a necesitar.

Tabla N° 3.18 Aire Acondicionado

Ítem	Cantidad	Descripción	Ubicación
1	2	Aire Acondicionado CRAC	Site Principal/Secundario por falso piso
1	13	Aire Acondicionado	Cuartos Comunicaciones Empotrado en pared

Los Gabinetes y Rack a usar, según las características que deben cumplir de almacenamiento de equipos, se encuentran en la siguiente tabla N° 3.19:

Tabla N° 3.19 Gabinetes y Rachas

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca	UR
1	4	Rack Gabinete	S722C122B	Site Principal/Secundario Piso3	Panduit	45
2	5	Rack Pedestal	CMR19X84NU	Site Principal Piso1, 2, 4 y 5	Panduit	45
3	5	Rack Pedestal	CMR19X84NU	Site Secundario Piso1, 2, 4 y 5	Panduit	45
4	5	Rack Pedestal	CMR19X84NU	Agencias Cuarto Comunica.	Panduit	45
					Total Gabinete	4
					Toral Rack	15

Fig. 3.18 Rack Gabinete (36UR)
Fuente www.panduit.com

Fig. 3.19 Rack Pedestal (36 UR)
Fuente www.panduit.com.

Los gabinetes ubicados en los site principal/secundario llevan instalados patch panels de F.O (que son puntos de acceso desde el MDA (Data Center) hacia los cuartos de comunicaciones donde se encuentran los racks) estos patch panels son de puertos SC por lo que los jumpers a usar tienen este tipo de conector en uno de sus extremos. Se necesitaran los siguientes patch panels de FO que se muestran en las Tablas N° 3.20 y 3.21.

Para data center en site principal y secundario (Piso 3).

Tabla N° 3.20 Patch Panels F.O

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca	UR
1	2	Rack Mount Fiber	FMT1	Site Principal/Secundario/Agencias	Panduit	1
2	32	SC Duplex Adapter Module	Duplex Adapter Modules	Site Principal/Secundario/Agencias	Panduit	-

Para Cuartos de Comunicaciones en Site Principal y Secundario (Piso 1, 2, 4 y 5).

Tabla N° 3.21Patch Panels F.O

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca	UR
1	8	Rack Mount Fiber	FMT1	Site Principal/Secundario/Agencias	Panduit	1
2	16	SC Duplex Adapter Module	Duplex Adapter Modules	Site Principal/Secundario/Agencias	Panduit	-

Cada site posee 5 pisos y en cada piso hay 60 usuarios, para poder soportar esta cantidad de usuarios se necesitan patch panels RJ45 (contienen los reflejos de los puntos de red de las áreas de trabajo), estos se ubicaran en los cuartos de comunicaciones de todos los pisos, también habrá uno en el cuarto ER para que conecte los equipos de los proveedores con los equipos de la empresa (cada patch es de 48 puertos RJ45).

Cada Agencia posee un piso y en el habrá como máximo 15 usuarios, por ello el patch panel a usar es solo es de 32 puertos, con ello se tienen puertos suficientes para satisfacer las necesidades de la agencia y futuras expansiones. Se necesitaran los siguientes Patch Panels.

En Site Principal y Site Secundario (Data Center y Cuartos de Comunicaciones).

Tabla Nº 3.22 Patch Panels cobre

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca	UR
1	22	Patch Panel - 48 puertos	DP48688TGY	Site Principal/Secundario/Agencias	Panduit	2
2	10	Capacity Horizontal Cable Managers	NM2	Site Principal/Secundario/Agencias	Panduit	2

Por Agencia:

Tabla Nº 3.23 Patch Panels cobre

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca	UR
1	5	Patch Panel - 48 puertos	DP48688TGY	Agencia	Panduit	2
2	5	Capacity Horizontal Cable Managers	NM2	Agencia	Panduit	2

Los Data Centers y Cuartos de comunicaciones debe reunir ciertas características como:

Temperatura: esta debe ser monitorea permanentemente, lo que conlleva a usar aire acondicionado, debiendo encontrarse entre 18° - 24° con humedad relativa de 30% - 55%

Dimensiones: debe tener una altitud como mínima de 2.4m entre el falso techo y suelo

Energía: Se tienen equipos que proveerán la energía a los equipos de comunicaciones debidamente acondicionados, estos son un transformador de aislamiento y un UPS.

Luminarias: Se usan lámparas fluorescentes de 32W, estas son frágiles, requieren una electrónica especial para el rápido encendido.

El UPS, de las siglas ininterrumpible Power Suplí (suministro de energía ininterrumpidle) es un equipo que tiene la función de entregar una mejor calidad de energía a los equipos que usen de él, en nuestro caso los equipos de comunicaciones. Eso lo realiza filtrando las subidas y bajas de tensión, eliminando los armónicos y por medio de sus baterías abastecerán por un determinado tiempo (tiempo de autonomía) de energía a los equipos de comunicación mientras se resuelve el problema con el suministro de energía comercial. La capacidad de este equipo debe ser mayor a la suma de la potencia que consumen todos los equipos que usen de esta fuente, para nuestro caso vamos a usar **Liebert NX de 40 - 120kVA (On-Line UPS) y** para agencias. Este UPS funciona en conjunto con un banco de baterías, las que según el estándar que seguimos deberá durar entre 5 – 30 minutos, en nuestro caso 30 min. a máxima carga, este debe ser el tiempo suficiente para conmutar a otro tipo de fuente

Transformador de aislamiento: Este equipo permite aumentar y disminuir la energía eléctrica en un circuito de corriente alterna manteniendo la frecuencia. Su propósito es dar protección de ruidos.

3.4.5 Puesta a Tierra

Con un adecuado diseño de puesta tierra las corrientes eléctricas y voltajes pasajeros son dirigidas hacia tierra compuesta por una masa neutra donde son dispersados sin retorno, de esta forma se podrá dar una mayor vida a los equipos , protegiéndolos de fenómenos eléctricos transitorios que pueden ingresar a los sistemas eléctricos en fracciones de segundos (nanosegundos) , para esta implementación se sigue el estándar de sistemas de puesta atierra para redes de telecomunicaciones ANSI/TIA/EIA-607. Finalidad principal de la puesta a tierra:

Obtener una baja resistencia eléctrica para derivar a tierra Fenómenos Eléctricos Transitorios (FETs.), corrientes de falla estática y parásita; así como ruido eléctrico y de radio frecuencia.

Mantener los potenciales producidos por las corrientes de falla dentro de los límites de seguridad.

Hacer que el equipamiento de protección sea más sensible y permita una rápida derivación de las corrientes defectuosas a tierra.

La habilitación de las puestas en tierra en los site principal/secundario y agencias, se realiza conjuntamente con el proveedor encargado y especializado de acondicionar el sistema eléctrico.

En resumen se necesitaran los siguientes equipos de comunicaciones.

Tabla N° 3.24 Equipos Comunicaciones

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca	UR
1	7	Router	3845	Site Principal/Secundario	CISCO	2
2	1	Tarjeta E1 ISDN	VWIC2-1MFT-T1/E1	Site Principal/Secundario	CISCO	-
3	2	Switch CORE	4500	Site Principal/Secundario	CISCO	10
4	2	Módulos 24 puertos puertos GBIC - MTRJ	WS-X4124-FX-MT	Site Principal/Secundario	CISCO	-
5	25	Switch Catalyst 3560-48PS	3560	Site Principal/Secundario/Agencia	CISCO	1
6	20	Módulos SFP Puertos Gbic	MTRJ	Site Principal/Secundario	CISCO	-
7	5	Router RPV	2901	Agencias	CISCO	1
8	5	Router Contingencia ISDN	1751	Agencia	CISCO	
9	5	Tarjetas BRI enlace ISDN	WIC-1B-S/T-V3	Agencia	CISCO	-
10	4	Tarjetas E1 (2 puertos C/U)	VWIC-2MFT-E1	Site Principal/Secundario	CISCO	-
11	4	PVDM 48-Channel Fax/Voice DSP Module	PVDM2-48	Site Principal/Secundario	CISCO	-
12	2	Servidor Callmanager 7.1	MCS7816I4-K9-CMC2	Site Principal/Secundario	CISCO	1
13	530	Teléfonos IP	7911G	Site Principal/Secundario/Agencias	CISCO	-

14	15	Teléfonos IP	7975G	Site Principal/Secundario	CISCO	-
15	1	Roture Gateway Celular	CGW-P ISDN PRI	Site Principal/Secundario	ITS TELECOM	
16	1	Servidor UCCX 5.0	MCS-7816-H3-CCX1	Site Principal	CISCO	-
17	2	Videoconferencia Tandberg Edge	Edge 95/85/75XP	Site Principal/Secundario	Tandberg	-
18	2	Tv videoconferencia 37'	37'	Site Principal/Secundario	LG	-
19	2	Firewall Activo/Activo	ASA 5540	Site Principal/Secundario	CISCO	1
20	8	Firewall Activo/Standby	Checkpoint IP 290	Site Principal/Secundario	NOKIA	
21	2	IPS Intrusion Prevention System	4200	Site Principal/Secundario	CISCO	1
22	4	Switch cluster Checkpoint	2960	Site Principal/Secundario	CISCO	1

Gabinetes y Rack.

Tabla Nº 3.25 Racks y Gabinetes

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca	UR
1	4	Rack Gabinete	S722C122B	Site Principal/Secundario	Panduit	45
2	15	Rack Pedestal	CMR19X84NU	Site Principal/secundario/Agencia	Panduit	45

Accesorios y Cableado.

Tabla Nº 3.26 cableado y accesorios

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca	UR
1	27	Patch Panel - 48 puertos	DP48688TGY	Site Principal/Secundario/Agencia	Panduit	2
2	15	Capacity Horizontal Cable Managers	NM2	Site Principal/Secundario/Agencia	Panduit	2
3	10	Rack Mount Fiber	FMT1	Site Principal/Secundario	Panduit	1
4	48	SC Duplex Adapter Module	Duplex Adapter Modules	Site Principal/Secundario	Panduit	-

Tabla Nº 3.27cabkeado y accesorios

Ítem	Cantidad	Descripción	Modelo	Ubicación	Marca	UR
1	20	Jumper F.O(PATCH PANEL - SWITCH ACCESO) - 1mts	MTRJ - SC	Site Principal/Secundário (Data Center)	Panduit	-
2	20	Jumper F.O (PATCH PANEL - SWITCH CORE) – 2mts	MTRJ - SC	Site Principal/Secundario (Cuartos Comunicaciones)	Panduit	-
3	660	FacePlate (Datos-Voz)	Estación de trabajo	Site Principal/Secundario/Agencia	Panduit	-
4	800	Cables de Red – 2.1mts	Cat 6	Site Principal/Secundario/Agencia	Panduit	-
5	825	Cables de Red – 1.5mts	Cat 6	Site Principal/Secundario/Agencia	Panduit	-

CAPÍTULO IV
COSTO DEL PROYECTO

4.1 Costos de Inversión

La inversión constituye un punto sumamente importante al momento de determinar las tecnologías y equipamiento a usar, este costo se efectúa una única vez al momento de adquirir los servicios o equipos que serán empleados para satisfacer las necesidades de la empresa, en el caso de los equipos una vez adquiridos estos son transformados en tangibles del banco. Los equipos a considerar deben reunir ciertas características como:

Ajustarse a las necesidades económicas del banco.

Cumplir con los requisitos técnicos necesarios para soportar todos los servicios a brindar.

Tener la capacidad de soportar mejoras en los servicios que proveen.

Ser adaptables a nuevas tecnologías.

Tener una garantía hasta por 4 años.

Surge el concepto de CAPEX (**Capital Expenditures**), que es el gasto que realiza la empresa para adquirir bienes capitales con la intención de mantener o aumentar su producción de prestación de servicios para los usuarios internos y clientes. Los equipos adquiridos tienen una vida útil por lo que los costos de estos se van devaluando con el tiempo transcurrido y el uso que tengan, para nuestro caso se considera 4 años como tiempo de depreciación para los equipos de comunicaciones y luego de este tiempo se evita hacer cualquier contrato de mantenimiento o soporte ya que se considera que termino la vida útil de los mismos y lo que se busca es reemplazarlos por equipos nuevos de mayor capacidad o tecnología y se ajusten a las necesidades que se tendrán en ese momento.

En las siguientes tablas se tienen los costos de los equipos de comunicaciones, enlaces de servicios, cableados, accesorios y otros gastos que surgen durante la implementación de este proyecto.

Los costos de equipos de comunicación para los servicios de datos, telefonía IP, videoconferencia, Internet y Extranet, se muestran en la tabla Nº 4.1

Tabla Nº 4.1 Costos equipos comunicaciones

Ítem	Cantidad	Descripción	Precio Unitario $ (sin IGV)	Precio Total $ (sin IGV)
1	7	Router 3845	11.050,00	77.350,00
2	1	Tarjeta E1 ISDN VWIC2-1MFT-T1/E1	1.700,00	1.700,00
3	2	Switch CORE 4500	25.058,00	50.116,00
4	2	Módulos 24 puertos GBIC – MTRJ WS-X4124-FX-MT	8.495,75	16.991,50
5	25	Switch Catalyst 3560-48PS	8.070,75	201.768,75
6	20	Módulos SFP Puertos Gbic MTRJ	425,00	8.500,00
7	5	Router RPV 2901	1.695,75	8.478,75
8	5	Router Contingencia ISDN 1751	1.780,75	8.903,75
9	5	Tarjetas BRI para enlace ISDN WIC-1B-S/T-V3	3.570,00	17.850,00
10	4	Tarjetas E1 (2 puertos C/U) VWIC-2MFT-E1	1.700,00	6.800,00
11	4	PVDM 48-Channel Fax/Voice DSP Module PVDM2-48	2.040,00	8.160,00
12	2	Servidor Callmanager 7.1 MCS781614-K9-CMC2	8.495,00	16.990,00
13	530	Teléfonos IP - 7911G	225,00	119.250,00
14	15	Teléfonos IP - 7975G	599,25	8.988,75
15	1	Gateway Celular ITS CGW-P ISDN PRI	5.300,00	5.300,00
16	1	Servidor UCCX 5.0 MCS-7816-H3-CCX1	3.400,00	3.400,00
17	2	Equipo Videoconferencia Edge 95/85/75XP	17.000,00	34.000,00
18	2	Tv para las videoconferencia 37'	1.445,00	2.890,00
19	2	Firewall Activo/Activo ASA 5540	14.445,75	28.891,50
20	8	Firewall Active/Standby Checkpoint IPS 2900	11.419,50	91.356,00
21	2	Intrusion Prevention System 4200	10.195,75	20.391,50
22	4	Switch Para cluster Checkpoint 2960	1.295,00	5.180,00
Total				743.256,50

Costos de Rack y Gabinetes, se muestra en la tabla Nº 4.2:

Tabla Nº 4.2 Costos racks y gabinetes

Ítem	Cantidad	Descripción	Precio Unitario $ (sin IGV)	Precio Total $ (sin IGV)
1	4	Rack Gabinete S722C122B	700,00	2.800,00
2	15	Rack Pedestal CMR19X84NU	150,00	2.250,00
Total				5.050,00

Costos Cables y Accesorios, se muestra en la tablaNº 4.3 y 4.4:

Tabla Nº 4.3 Cables y accesorios

Ítem	Cantidad	Descripción	Precio Unitario $ (sin IGV)	Precio Total $ (sin IGV)
1	27	Patch Panel - 48 puertos DP48688TGY	578,00	15.606,00
2	15	Capacity Horizontal Cable Managers NM2	50,00	750,00
3	10	Rack Mount Fiber FMT1	100,00	1.000,00
4	48	SC Duplex Adapter Module Duplex Adapter Modules	25,00	1.200,00
Total				18.556,00

Tabla Nº 4.4Cables y accesorios

Ítem	Cantidad	Descripción	Precio Unitario $ (sin IGV)	Precio Total $ (sin IGV)
1	20	Jumper F.O(patch panel –switch acceso) MTRJ - SC 1mts	60,00	1.200,00
2	20	Jumper F.O(patch panel –switch acceso) MTRJ - SC 2 mts	65,00	1.300,00
3	660	FacePlate (Datos-Voz)	12,00	7.920,00
4	800	Cables de Red Cat 6 - 2.1mts	11,00	8.800,00
5	825	Cables de Red Cat 6 - 1.5mts	9,00	7.425,00
Total				26.645,00

Costos Otros:

Estos costos involucran la instalación de un sistema de energía (UPS, Baterías, Transformador de aislamiento), aire acondicionado y otros que surgen en el proyecto, se muestra en la tabla Nº 4.5:

Tabla Nº 4.5 Costos otros

Ítem	Cantidad	Descripción	Costo Otros por sede $ (sin IGV)	Costo Total $ (sin IGV)
1	2	Site Principal/Secundario	30.000,00	60.000,00
2	5	Agencia	9.000,00	45.000,00
3	-	Otros	1.000,00	10.000,00
Total				115.000,00

Los costos por implementación de los enlaces, se encuentran en las siguientes tablas.

Enlace RPV Site principal, secundario y Agencias:

Costo por Instalación, se muestra en la tabla Nº 4.6.

Tabla Nº 4.6 Costos de instalación

Ítem	Cantidad	Descripción	Costo por sede $ (Sin IGV)	Costo Total $ (Sin IGV)
1	2	Ancho de Banda Cos2 8039,25kbps - CoS1 5359,5kbps - CoS5 1280Kbps (site principal y secundario)	650,00	1.300,00
2	5	Ancho de Banda Cos2 162kbps - CoS1 108kbps - CoS5 192 (agencias)	650,00	3.250,00
Total				4.550,00

Troncales E1 Site principal y secundario:

Costo por Instalación, se muestra en la tabla Nº 4.7.

Tabla Nº 4.7Costos de instalación

Ítem	Cantidad	Descripción	Costo por sede $ (Sin IGV)	Costo Total $ (Sin IGV)
1	2	Site Principal/Secundario 2 Troncales E1	800,00	1.600,00
Total				1.600,00

Enlace Internet:

Costo por Instalación, se muestra en la tabla N° 4.8.

Tabla N° 4.8 Costos de instalación

Ítem	Cantidad	Descripción	Costo por sede $ (Sin IGV)	Costo Total $ (Sin IGV)
1	2	Enlace Internet 4Mbps (site principal y secundario)	612,00	612,00
Total				612,00

Enlace Extranet:

Costo por Instalación, se muestra en la tabla N° 4.9.

Tabla N° 4.9 costos de instalación

Ítem	Cantidad	Descripción	Costo por sede $ (Sin IGV)	Costo Total $ (Sin IGV)
1	2	Enlace extranet 3Mbps (site principal y secundario)	650,00	1.300,00
Total				1.300,00

Costos por cableado:

Costo por Instalación, se muestra en la tabla N° 4.10 y 4.11.

Tabla N° 4.10 costo de instalación de cableado

Ítem	Cantidad	Descripción	Costo por Punto$ (Sin IGV)	Costo Total $ (Sin IGV)
1	640	Instalación Site Principal/Secundario cableado certificado Cat6a	25,00	16.000,00
2	100	Instalación Agencia cableado certificado Cat6a	25,00	2.500,00
Total				18.900,00

Tabla N° 4.11 costo de instalación de cableado

Ítem	Cantidad	Descripción	Costo por sede $ (Sin IGV)	Costo Total $ (Sin IGV)
1	16	Instalación Site Principal/Secundario cableado de F.O Multimodo	700,00	1.400,00
Total				1.400,00

Costos Totales CAPEX, se muestra en la tabla N° 4.12:

Tabla N° 4.12 costo totales

	CAPEX $ (Sin IGV)
Total	1.147.509,00

4.2 Costos de operación y mantenimiento (OPEX)

Una vez completados los costos por inversión o CAPEX, se tiene el costo de operación que es el costo en curso para que un sistema pueda funcionar y mantenerse en operación; Dentro de este costo se encuentra los pagos mensuales por los servicios de RPV, extranet, Internet, telefonía (el costo de la telefonía varía según el mes de facturación ya que se

factura según las llamadas que se realizan a los diferentes destino para esto lo optimo es contratar una bolsa de minutos que se ajusta a las necesidades de la empresa y ofrezcan tarifas competitivas para llamar a los destinos preferentes) y el pago a los especialistas de telecomunicaciones.

Todos los servicios son administrados por un grupo de especialistas que deben ser de la carrera Ingeniería en Telecomunicaciones o de una otra a fin, ellos se encargan de realizar las labores de soporte, mantenimiento, monitoreo, administración y optimización de la red. Entre sus principales funciones están:

Administrar los equipos de comunicaciones como routers, switchs, servidores de Telefonía, IPCC, DHCP, equipos de videoconferencia, Gateway de telefonía celular, entre otros

Administrar y monitorear los enlaces locales RPV entre las diversas sedes, Internet y Extranet.

Administrar la red backbone y Lan de cada site y agencia.

Administrar y monitorear los Firewall del enlace a Internet, añadir, eliminar y modificar políticas de seguridad según corresponda.

Administrar y monitorear los Firewall de enlaces con terceros (Extranet), añadir, eliminar y modificar políticas de seguridad según corresponda.

Coordinar con los proveedores respectivos el mantenimiento de los enlaces por lo menos una vez al año.

Coordinar con los proveedores respectivos la solución de problemas que se presenten en la red o servicios, darles seguimiento a estos problemas y reportarlos mediante informes.

Realizar respaldos de los equipos de comunicaciones, Firewalls y pruebas de continuidad de negocio cada cierto tiempo.

Realizar upgrade según correspondan, de acuerdo a la expansión de la empresa y las nuevas necesidades.

Proponer proyectos de optimización de la red tanto en tecnología como económicamente.

Se tienen contratos de mantenimiento con los proveedores de los equipos y enlaces de comunicaciones, de esta forma se tiene un respaldo para solucionar fallas complejas o realizar las consultas pertinentes.

Los costos mensuales de los enlaces, se muestran en las siguientes tablas.

Enlace RPV Site/Principal y Agencias, se muestra en la tabla Nº 4.13

Tabla N° 4.13 costo mantenimiento

Ítem	Cantidad	Descripción	Costo por sede $ (Sin IGV)	Costo Total $(Sin IGV)
1	2	Ancho de Banda Cos2 8039,25kbps - CoS1 5359,5kbps - CoS5 1536Kbps	1.051,35	2.102,70
2	5	Ancho de Banda Cos2 162kbps - CoS1 108kbps - CoS5 192Kbps	291,15	1.455,75
Total				3.558,45

Líneas Telefónicas Troncales E1 (involucra el alquiler y el consumo promedio por las troncales E1 hacia la PSTN este consumo varia mes a mes pero se toma una referencia), se muestra en la tabla N° 4.14.

Tabla N° 4.14 costo mantenimiento

Ítem	Cantidad	Descripción	Costo por sede $ (Sin IGV)	Costo Total $ (Sin IGV)
1	2	Site Principal/Secundario 3 Troncales E1	45,00	90,00
2	1	Consumo promedio por llamadas por los 3 troncales E1	5.000,00	4.000,00
Total				4.090,00

Enlace Internet, se muestra en la tabla N° 4.15.

Tabla N° 4.15 costo mantenimiento

Ítem	Cantidad	Descripción	Costo por sede $ (Sin IGV)	Costo Total $ (Sin IGV)
1	2	Enlace Internet 4Mbps	1.250,00	2.500,00
Total				2.500,00

Enlace Extranet, se muestra en la tabla N° 4.16.

Tabla N° 4.16 costo mantenimiento

Ítem	Cantidad	Descripción	Costo por sede $ (Sin IGV)	Costo Total $ (Sin IGV)
1	2	Enlace extranet 3Mbps	360,00	720,00
Total				720,00

Costos por soporte de proveedores, se muestra en la tabla N° 4.17.

Tabla N° 4.17 costo mantenimiento

Ítem	Cantidad	Descripción	Costo por sede $ (Sin IGV)	Costo Total $ (Sin IGV)
1	1	Soporte en Equipos y enlaces	500,00	500,00
Total				500,00

Costos por especialistas encargados de administrar toda la infraestructura, se muestra en la tabla N° 4.18

Tabla N° 4.18 costos otros

Ítem	Cantidad	Descripción	Costo por especialista $ (Sin IGV)	Costo Total $ (Sin IGV)
1	2	Especialistas	3.000,00	6.000,00
Total				6.000,00

Costos Otros (Energía, mantenimiento UPS, aire acondicionado y otros), se muestra en la tabla Nº 4.19.

Tabla Nº 4.19 costos otros

Ítem	Cantidad	Descripción	Costo por sede $ (Sin IGV)	Costo Total $ (Sin IGV)
1	1	Costos Otros	3.500,35	3.500,35
Total				3.500,35

Costos Totales OPEX

Tabla Nº 4.20 costo totales de mantenimiento

	OPEX
Total	21.868,80

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Del siguiente informe se concluye:

1. La solución propuesta se basa en la implementación de enlaces de datos, telefonía y videoconferencia con sus respectivos enlaces de contingencia, con esta solución los usuarios tienen un eficiente acceso a los servicios que les son imprescindibles para realizar sus labores cotidianas, se provee un continuo acceso a los servicios por medio de los enlaces de contingencia dándole un 99.9% de operatividad sobre la red. Se tiene una gestión sencilla y centralizada ya que la tecnología predominante es la IP y se tiene una conexión Ethernet de alta velocidad, esta solución es muy eficiente para la empresa bancaria que requiere de una red de alta velocidad de servicios centralizados de datos, telefonía y video de alta capacidad, de eficiente gestión y con altos niveles de seguridad.
2. El uso de la tecnología IP en este proyecto es fundamental ya que permite manejar niveles de calidad de servicio en los diversos tráficos para el caso de la telefonía IP, le añade muchos beneficios como movilidad ya que estos equipos pueden funcionar en cualquier punto de red que se conecten. Los costos de implementación de esta tecnología son menores que la telefonía convencional (ya que no se necesita cablear por cada punto donde se conecte el teléfono o re cablear si se cambia de sitio) y los beneficios mayores. El uso de esta tecnología representa una solución viable por lo comentado y por los siguientes beneficios en general:

   Rentabilidad: Se saca el máximo beneficio de la velocidad, calidad de servicio con que se puede manejar todo el tráfico con esta tecnología mejorando así la eficiencia de la empresa.

   Ahorro: Solo se necesita un solo tendido de cableado para que por este puedan transmitirse todos los tráficos necesarios (datos, telefonía, video). A diferencia que la telefonía convencional que necesita un cableado exclusivo por línea analógica, la administración era más tediosa y no se tenía una fácil movilidad de estos equipos.

   Flexibilidad: Esta tecnología es parte de la capa 3 del modelo TCP/IP, por lo que trabaja con los protocolos de capa superiores encapsulándolos por medio de una dirección IP.

   Gestión: Con esta tecnología se tiene una eficiente administración de los servicios ya que la base con que funcionan es la misma.

3. El uso de la tecnología Ethernet , es dominante en la LAN es en esta tecnología se origina y terminan todos los tráficos que son necesitados por los servicios instalados, se aceptan variaciones en el medios, anchos de banda y demás variaciones en las capas 1 y 2 , pero se mantiene un solo formato de trama. El uso de esta tecnología representa los siguientes beneficios:

   Sencillez: Su implementación, administración y mantenimiento es mucho más sencilla que Token Ring y FFDI.

   Capacidad para incorporar nuevas tecnologías: Ya que esta tecnología Ethernet ah ido evolucionando de inicialmente 10Mbps llegando ahora a poder manejar 10Gbps y aun se tienen versiones más rápidas en desarrollo.

   Confiabilidad: A diferencia de Token Ring si un nodo fallara en Ethernet no se deshabilita toda la red, ya que con Ethernet se tiene otra forma de interconectar los nodos.

   Bajo costo de instalación y actualización: A diferencia de Token Ring y FFDI los equipos y el tipo de cableado para Ethernet son más económicos.
4. Esta implementación es una alternativa viable económicamente ya que con la inversión que se haga en implementar esta solución, la empresa poder abrir 2 sedes principales con 5 agencias para atención al público en general, y así poder realizar todos los negocios propios de la empresa. A la vez no se requiere más costos en administración de cada uno de los servicios por separado ya que todos estos se encuentran centralizados y se basan en la misma tecnología.

Recomendaciones

1. Durante la implementación de cada uno de los servicios se deben de realizar pruebas de stress, acceso y funcionalidad para de esta forma confirmar que se tienen los servicios conformes a las necesidades.
2. Debe ser un compromiso que cada 6 meses se haga pruebas de los enlaces de contingencia y de ser necesarios actualizarlos según los requerimientos y necesidades que vayan surgiendo.
3. Se deben de tener contratos con los proveedores tanto de los servicios y equipamiento de comunicaciones donde se comprometan a dar una respuesta rápida y eficiente en caso de fallas o problemas. Esto se logra definiendo claramente los SLA en los contratos.
4. Se debe de realizar por lo menos 2 veces al año un estudio sobre la capacidad y necesidades que se tendrán para los siguientes 6 meses ya sea necesidad de más equipos o de upgrades a enlaces para de esta forma asegurar la normal operación de la empresa. Este estudio también debe incluir la búsqueda de medios para reducir los costos por servicio en el caso de la telefonía buscar bolsas de minutos que se amolden a las necesidades actuales, con costos por minutos competitivos.
5. Se deben de monitorear constantemente los enlaces para asegurar que no se presenten anomalías que puedan perjudicar el performance de la red, como un monitoreo continuo de aplicaciones que pasan por la WAN. Un monitoreo de la estabilidad de los

enlaces se puede lograr por medio de aplicativos de monitoreo (por Ej. ciscoworks, hpopenview) que monitorean constantemente estos enlaces y se alarman cuando presentan problemas.

6. Se deben tener una coordinación constante con el área se seguridad tecnológica para identificar anomalías que puedan pueden ser ocasionadas por virus en la red o intentos de accesos no permitidos.

ANEXO A
DATASHEETS DE EQUIPOS DE COMUNICACIONES

Datasheets de equipos de comunicaciones

Router 3845

Las características de este modelo pueden encontrarse en la siguiente dirección Web http://www.cisco.com/en/US/prod/collateral/routers/ps5855/product_data_sheet0900aecd8016a8e8.html

Cisco 3800 Series Features	Cisco 3845/3845-NOVPN
Network-module slots: These slots can accommodate a standard network module, enhanced network module (NME), enhanced extended network module (NME-X), and high-density extension module (EVM-HD). The NME-X, when available, will have a wider form factor than the NME. You can combine two side-by-side NME slots to accommodate one double-wide network module (NMD) or when available, a double-wide enhanced extended network module (NME-XD).	• NM • NME • NME-X • NMD • NME-XD • EVM-HD
Maximum number of network modules, NMEs, and NME-Xs supported	4
Maximum number of NMD/NME-XDs supported	2
Maximum number of EVM-HDs supported	2
Number of HWIC slots (These HWIC slots also support VICs, VWICs, and WICs.)	4
Number of fixed LAN ports (fixed RJ-45 port for 10/100/1000 connectivity)	2 Gigabit Ethernet (10/100/1000)
Number of fixed Small Form-Factor Pluggable (SFP) ports (for SFP Gigabit Ethernet connectivity)	1
Number of AIM slots (for optional AIMs for offloading compute-intensive features)	2
Number of PVDM slots (for optional PVDM2s)	4
Number of USB 1.1 ports (for future use with USB flash memory, security tokens for secure Cisco IOS Software configuration distribution, and off-platform storage of VPN credentials)	2
Embedded VPN (hardware-based VPN encryption acceleration)	Yes*
Number of console ports (up to 115.2 kbps)	1

Number of auxiliary ports (up to 115.2 kbps)	1
Memory: External Compact Flash and internal double-data-rate (DDR) synchronous dynamic RAM (SDRAM) with ECC**	• Default: 64-MB Compact Flash; 256-MB DDR SDRAM • Maximum: 512-MB Compact Flash; 1-GB DDR SDRAM

Especificaciones técnicas del modelo:

Cisco 3800 Series Features	**Cisco 3845/3845-NOVPN**
Dimensions (H x W x D)	• 5.25 x 17.25 x 16 in. • 3RU
Weight (minimum)	35 lb
Rack-mounting	Yes, 19- and 23-in. options
Wall-mounting	No
AC input voltage	100-240 VAC, autoranging
AC input frequency	47-63 Hz
AC input current	• 4A (110V) • 2A (230V) • Startup current 50A maximum (one cycle)
AC IP input current	• 8A (110V) • 4A (230V) • Startup current 50A maximum (one cycle)
DC input voltage	24-60 VDC, autoranging positive or negative
DC input current	• 18A (24V) • 7A (60V) • Startup current 50A<10 ms
Output	• AC or DC power supply: • 300W for system • AC IP power supply: • 300W for system • 360W for IP Phones (-48V)
Redundant power supply (RPS)	Internal AC, AC IP, or DC RPS
Recommended RPS unit	--
Typical power dissipation (no modules)	79W (269 BTU/hr)

AC without IP phone support	435W (1485 BTU/hr)
AC with IP phone support: System only	555W (1890 BTU/hr)
AC with IP phone support: IP phones	360W (1128 BTU/hr)
DC	460W (1570 BTU/hr)
Operating temperature	32 to 104°F (0 to 40°C)
Nonoperating temperature	-40 to 158°F (-40 to 70°C)
Relative humidity (noncondensing)	5-85% noncondensing
Maximum operating temperature at altitude	40°C at sea level 40°C at 6,000 ft (1,800m) 30°C at 13,000 ft (4,000m) 27.2°C at 15,000 ft (4,600m) Note: Derate 1.4°C per 1,000 ft above 6,000 ft
Noise level (minimum)	56 dBa typical, 58 dBa maximum
Safety	• UL 60950 • CAN/CSA C22.2 No. 60950 • EN 60950 • AS/NZS 60950
EMC	• 47 CFR, Part 15 • ICES-003 Class A • EN55022 Class A • CISPR22 Class A • AS/NZS 3548 Class A • VCCI V-3 • EN 300386 • EN 61000
Telcom	• 47 CFR, Part 68 • TIA/EIA/IS-968 • CS-03 • RTTE Directive

Router 2901

Las características del modelo pueden encontrarse en la siguiente dirección web http://www.cisco.com/en/US/prod/collateral/routers/ps10537/data_sheet_c78_553896.html

	Cisco 2901
Embedded hardware-based cryptography acceleration (IPSec + SSL)	Yes

Cisco Unified SRST Sessions	35
Cisco Unified CCME Sessions	35
Total onboard WAN 10/100/1000 Ports	2
RJ-45-based ports	2
SFP-based ports (use of SFP port disables the corresponding RJ-45 port)	0
Service Module slots	0
Double-wide Service Module slots (use of a double-wide slot will occupy all single-wide service module slots in a 2900)	0
EHWIC slots	4
Double-wide EHWIC slots (use of a double-wide EHWIC slot will consume two EHWIC slots)	2
ISM slots	1
Onboard DSP (PVDM) slots	2
Memory DDR2 ECC DRAM - Default	512 MB
Memory (DDR2 ECC DRAM) - Maximum	2 GB
Compact Flash (external) - Default	slot 0: 256 MB slot 1: none
Compact Flash (external) - Maximum	slot 0: 4 GB slot 1: 4 GB
External USB 2.0 flash memory slots (Type A)	2
USB Console port (Type B) (up to 115.2 kbps)	1
Serial console port	1
Serial auxiliary port	1
Power-supply options	AC and PoE
RPS support (External)	No
AC input voltage	100 to 240 VAC auto ranging

AC input frequency	47 to 63 Hz
AC input current range AC power supply (maximum)	1.5 to 0.6A
AC input surge current	<50A
Typical Power (no modules) (Watts)	40
Maximum Power with AC power supply (Watts)	150
Maximum Power with PoE power supply (platform only) (Watts)	175
Maximum end-point PoE power available from PoE power supply (Watts)	130
Maximum end-point PoE power capacity with PoE Boost (Watts)	N/A
Dimensions (H x W x D)	1.75 x 17.25 x 17.3 in. (44.5 x 438.2 x 439.4 mm)
Rack height	1RU (rack unit)
Rack-mount 19in. (48.3 cm) EIA	included
Rack Mount 23in. (58.4 cm) EIA	optional
Wall-mount (refer to installation guide for approved orientation)	Yes
Weight with AC power supply (no modules)	13.4 lb (6.1 kg)
Weight with AC PoE power supply (no modules)	14.3 lb (6.5 kg)
Typical weight fully configured	16 lb (7.3 kg)
Airflow	Front to side
Optional Airflow Kit	N/A
Temperature: 5,906 feet (1,800) maximum altitude	32 to 104°F (0 to 40°C)
Temperature: 9,843 feet (3,000m) maximum altitude	32 to 77°F (0 to 25°C)
Temperature: 13,123 feet (4,000m) maximum altitude	N/A
Temperature: Short-term (per NEBS) 5906 feet (1,800m) maximum altitude	N/A
Altitude	10,000 ft (3,000m)
Relative humidity	10 to 85%

Short-term (per NEBS) humidity	N/A
Acoustic: Sound pressure (typical/maximum)	41/53 dBA
Acoustic: Sound power (typical/maximum)	49/61 dBA
Temperature	-40 to 158°F (-40 to 70°C)
Relative humidity	5 to 95%
Altitude	15,000 ft (4,570m)
Safety	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1
EMC	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1
Telecom	TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3 RTTE Directive

Router 1841

Las características del modelo pueden encontrarse en la siguiente dirección web http://www.cisco.com/en/US/prod/collateral/routers/ps10537/data_sheet_c78_553896.html

Cisco 1800 Series	**Cisco 1841**
Target Applications	Secure data
Chassis	

Form Factor	Desktop, 1-rack-unit (1RU) height (4.75 cm high with rubber feet)
Chassis	Metal
Wall-Mountable	Yes
Rack-Mountable	Yes (Optional Rackmount kit: ACS-1841-RM-19=)
Dimensions (W x D)	• 13.5 x 10.8 in. (34.3 x 27.4 cm) • Height without rubber feet: 1.73 in. (4.39 cm) • Height with rubber feet: 1.87 in. (4.75 cm)
Weight	• Maximum: 6.2 lb (2.8 kg); with interface cards and modules • Minimum: 6.0 lb (2.7 kg) (no interface cards and modules)
Architecture	
DRAM	Synchronous dual in-line memory module (DIMM) DRAM
DRAM Capacity	• Default: 128 MB • Maximum: 384 MB
Flash Memory	External compact Flash
Flash Memory Capacity	• Default: 32 MB • Maximum: 128 MB
Modular Slots-Total	Two
Modular Slots for WAN Access	Two
Modular Slots for HWICs	Two
Modular Slots for Voice Support	None-The Cisco 1841 does not support voice
Analog and Digital Voice Support	No
VoIP Support	Voice-over-IP (VoIP) pass-through only
Onboard Ethernet Ports	Two 10/100
Onboard USB Ports	One (1.1)
Console Port	One-up to 115.2 kbps
Auxiliary Port	One-up to 115.2 kbps
Onboard AIM Slots	One (internal)
Packet-Voice-DSP-Module (PVDM) Slots on Motherboard	None-The Cisco 1841 does not support voice
Integrated Hardware-based Encryption on Motherboard	Yes

Encryption Support in Software and Hardware by Default	DES, 3DES, AES 128, AES 192, AES 256
Power Supply Specifications	
Internal Power Supply	Yes
Redundant Power Supply	No
DC Power Support	No
AC Input Voltage	100 to 240 VAC
Frequency	50 to 60 Hz
AC Input Current	1.5A maximum
Output Power	50W (maximum)
System Power Dissipation	
	153 BTU/hr
Software Support	
First Cisco IOS Software Release	12.3(8)T
Cisco IOS Software default Image, Release	IP BASE, 12.4(15)T
Environmental	
Operating Temperature	32 to 104°F (0 to 40°C)
Operating Humidity	10 to 85% noncondensing operating; 5 to 95% noncondensing, nonoperating
Nonoperating Temperature	-4 to 149°F (-25 to 65°C)
Operating Altitude	10,000 feet (3000 meters) @ 77°F (25°C)
Noise Level	Normal operating temperature: • <78° F/26°C: 34 dBA • >78°F/26°C through <104°F/40°C: 37 dBA • >104°F/40°C: 42 dBA
Regulatory Compliance	
Safety	• UL60950-1 • CAN/CSA 60950-1 • AS 3260 • EN60950-1
EMI	• EN 55022, 1998, class A • CISPR22, 1997, class A • CFR47, Part 15, Subpart B, 1995, class A

	• EN61000-3-2 Harmonic Current Emission (only for equipment >75W but <16A) • EN61000-3-3 Voltage Fluctuation and Flicker (only for equipment ≤16A)
Immunity	• CISPR24, 1997 ITE-Immunity characteristics, Limits and methods of measurement • EN 55024,1998 ITE-Immunity characteristics, Limits and methods of measurement • EN50082-1, 1997 Electromagnetic compatibility-Generic immunity standard, Part 1 • EN 300 386, 1997 Telecommunications network equipment EMC requirements • The requirements are covered by the following standards: • IEC 61000-4-2:1995 Immunity to Electrostatic Discharges • IEC 61000-4-3:1995 Immunity to Radio Frequency Electromagnetic Fields • IEC 61000-4-4:1995 Immunity to Electrical Fast Transients • IEC 61000-4-5:1995 Immunity to Power Line Transients (Surges) • IEC 61000-4-6:1996 Immunity to Radio Frequency Induced Conducted Disturbances • IEC 61000-4-11:1995 Immunity to Voltage Dips, Voltage Variations, and Short Voltage Interruptions
Network Homologation	• USA-TIA-968-A, T1.TRQ.6-2001 • Canada-CS-03 • European Union-RTTE Directive 5/99 • Argentina-CTR 21 • Australia-AS/ACIF S002, S003, S016, S031, 3043 • Brazil-225-540-788, CTR3, 225-100-717 Edition 3, NET 001/92 1990 • China-ITU-G.992.1, ITU-G.992.1, ITU-G.991.2, CTR3, ITU I.431 1993 • Hong Kong-HKTA 2033, HKTA 2033, HKTA 2014, HKTA 2017 Issue 3 2003, HKTA 2011 Issue 1, HKTA 2011 Issue 2, HKTA 2013 Issue 1 • India-I_DCA_18_02_Jun_99-199, S/ISN-01/02 Issue 1999 S/ISN-02 1 1998, IR/PRI-01/02 Issue 1 1998, S/INT-2W/02 MAY 2001, S/INT-2W/02 MAY 2001 • Israel-U.S. approval accepted • Japan-Technical condition (DoC acceptance in process) • Korea-U.S. approval accepted • Mexico-U.S. approval accepted • New Zealand-PTC 270/272, CTR 3, ACA 016 Revision 4 1997, PTC 200 • Singapore-IDA TS ADSL1 Issue 1, IDA TS ADSL 2, IDA TS HDSL, IDA TS ISDN 1 Issue 1 1999, IDA TS ISDN 3 Issue 1 1999, IDA TS PSTN 1 Issue 4, IDA TS PSTN 1 Issue 4, IDA TS PSTN 1 Issue 4 • South Africa-U.S. approval accepted • Taiwan-U.S. approval accepted

SWITCH 4500

Las características del modelo pueden encontrarse en la siguiente dirección web http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps4324/product_data_sheet0900aecd801792b1.html

Feature	**Cisco Catalyst WS-C4507R-E Chassis**

Total Number of Slots	7
Line Card Slots	5
Supervisor Engine Slots	2**
Dedicated Supervisor Engine Slot Numbers	3 and 4
Supervisor Engine Redundancy	Yes (Supervisor II-Plus, II-Plus-10GE, IV, V, V-10GE, 6-E, 6L-E)
Supervisor Engines Supported	Supervisor 6-E Supervisor 6L-E Supervisor V-10GE Supervisor V Supervisor IV Supervisor II-Plus-10GE Supervisor II-Plus
Bandwidth per Line Card Slot Using Supervisor 6-E	Up to 24 Gbps on all slots
Number of Power Supply Bays	2
AC Input Power	Yes
DC Input Power	Yes
Integrated Power over Ethernet	Yes
Minimum Number of Power Supplies	1
Power Supplies Supported	• 1000W AC • 1400W AC • 1300W ACV • 2800W ACV • 4200W ACV • 6000W ACV • 1400W DC (triple input) • 1400W-DC-P • External AC power shelf
Number of Fan-Tray Bays	1
Location of 19-inch Rack Mount	Front
Location of 23-inch Rack Mount	Front (option)

SWITCH 2960

Las características del modelo pueden encontrarse en la siguiente dirección web

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/product_data_sheet0900aecd80322c0c.html

	Specification
Performance	• 16 Gbps switching fabric (Catalyst 2960PD-8TT-L , Catalyst 2960-8TC-L, Catalyst 2960-24TT-L, Catalyst 2960-24TC-L, Catalyst 2960-24LT-L, Catalyst 2960-24PC-L, Catalyst 2960-48PST-L, Catalyst 2960-48TT-L, Catalyst 2960-48TC-L) • 32 Gbps switching fabric (Catalyst 2960G-8TC-L, Catalyst 2960G-) • Forwarding rate based on 64-byte packets: • Catalyst 2960-24TT-L: 6.5 Mpps • Catalyst 2960-24TC-L: 6.5 Mpps • Catalyst 2960-24LT-L: 6.5 Mpps • Catalyst 2960-24PC-L : 6.5 Mpps • Catalyst 2960G-24TC-L: 35.7 Mpps • 64 MB DRAM • 32 MB flash memory • Configurable up to 8000 MAC addresses • Configurable up to 255 IGMP groups • Configurable maximum transmission unit (MTU) of up to 9000 bytes, with a maximum Ethernet frame size of 9018 bytes (Jumbo frames) for bridging on Gigabit Ethernet ports, and up to 1998 bytes for bridging of Multiprotocol Label Switching (MPLS) tagged frames on both 10/100 and 10/100/1000 ports
Connectors and Cabling	• 10BASE-T ports: RJ-45 connectors, 2-pair Category 3, 4, or 5 unshielded twisted-pair (UTP) cabling • 100BASE-TX ports: RJ-45 connectors, 2-pair Category 5 UTP cabling • 1000BASE-T ports: RJ-45 connectors, 4-pair Category 5 UTP cabling • 1000BASE-T SFP-based ports: RJ-45 connectors, 4-pair Category 5 UTP cabling • 1000BASE-SX, -LX/LH, -ZX, -BX and CWDM SFP-based ports: LC fiber connectors (single/multimode fiber) • 100BASE-LX, -BX, -FX: LC fiber connectors (single/multimode fiber).
Power Connectors	• Customers can provide power to a switch by using either the internal power supply or the Cisco RPS 675. The connectors are located at the back of the switch. Note: The Catalyst 2960-8TC-L and Catalyst 2960G-8TC-L do not have RPS ports. • Internal-Power-Supply Connector • The internal power supply is an autoranging unit. • The internal power supply supports input voltages between 100 and 240VAC. • Use the supplied AC power cord to connect the AC power connector to an AC power outlet. • Cisco RPS Connector • The connector offers connection for an optional Cisco RPS 2300 that uses AC input and supplies DC output to the switch. • The connector offers a 2300W redundant power system that supports up to six external network devices and provides power to two failed devices at a time. • The connector automatically senses when the internal power supply of a connected device fails and provides power to the failed device, preventing loss of network traffic. • Only the Cisco RPS 2300 (model PWR-RPS2300) should be attached to the redundant-power-system receptacle.

Indicators	• Per-port status: Link integrity, disabled, activity, speed, full-duplex • System status: System, RPS, link status, link duplex, link speed
Dimensions (H x W x D)	• Cisco Catalyst 2960-24TT-L: 1.73 x 17.5 x 9.3 in. (4.4 x 44.5 x 23.6 cm) • Cisco Catalyst 2960-24TC-L: 1.73 x 17.5 x 9.3 in. (4.4 x 44.5 x 23.6 cm) • Cisco Catalyst 2960-24LT-L: 1.73 x 17.5 x 13 in. (4.4 x 44.5 x 33.2 cm) • Cisco Catalyst 2960-24PC-L : 1.73 x 17.5 x 13 in. (4.4 x 44.5 x 33.2 cm)) • Cisco Catalyst 2960G-24TC-L: 1.73 x 17.5 x 12.9 in. (4.4 x 44.5 x 32.8 cm)
Weight	• Cisco Catalyst 2960PD-8TT-L: 3 lb (1.4 kg) • Cisco Catalyst 2960-8TC-L: 3 lb (1.4 kg) • Cisco Catalyst 2960-24TT-L: 8 lb (3.6 kg) • Cisco Catalyst 2960-24TC-L: 8 lb (3.6 kg) • Cisco Catalyst 2960-24LT-L : 10 lb (4.5 kg) • Cisco Catalyst 2960-24PC-L : 12 lb (5.4 kg) • Cisco Catalyst 2960G-24TC-L: 10 lb (4.5 kg)
Environmental Ranges	Normal Operating Conditions: • -5°C to +45°C, up to 5,000 feet (1500 m) • -5°C to +40°C, up to 10,000 feet (3000 m) • -5°C to +35°C, up to 13,000 feet (4000 m) Short-Term* Exceptional Operating Conditions: • -5°C to +55°C, at sea level • -5°C to +50°C, up to 5,000 feet (1500 m) • -5°C to +45°C, up to 10,000 feet (3000 m) • -5'C to +40'C, up to 13,000 feet (4000 m) * Not more than following in one year period: 96 consecutive hours, or 360 hours total, or 15 occurrences
Acoustic Noise	• ISO 7779: Bystander position operating to an ambient temperature of 25°C • Cisco Catalyst 2960-24TT-L: 40 dBa • Cisco Catalyst 2960-24TC-L: 40 dBa • Cisco Catalyst 2960-24LT-L : 48 dBa • Cisco Catalyst 2960-24PC-L : 48 dBa • Cisco Catalyst 2960G-24TC-L: 41 dBa
Mean Time Between Failure (MTBF)	• Cisco Catalyst 2960-24TT-L: 407,707 hrs • Cisco Catalyst 2960-24TC-L: 402,926 hrs • Cisco Catalyst 2960-24LT-L : 311,781 hrs • Cisco Catalyst 2960-24PC-L : 243,277 hrs • Cisco Catalyst 2960G-24TC-L: 313,828 hrs
AC Input Voltage and Current	• DC input, 48 VDC, 0.3A (Cisco Catalyst 2960PD-8TT-L), • (For AC input, use PWR-A= sold separately) • 100-240VAC (autoranging), 0.5-0.25A, 50-60 Hz (Cisco Catalyst 2960-8TC-L) • 100-240VAC (autoranging), 0.8-0.4A, 50-60 Hz (Cisco Catalyst 2960G-8TC-L) • 100-240 VAC (autoranging), 3.0-1.5A, 50-60 Hz (Cisco Catalyst 2960-24LT-L) • 100-240 VAC (autoranging) 8.0-4.0A, 50-60 Hz (Cisco Catalyst 2960-24PC-L) • 100-240VAC (autoranging), 1.3-0.8A, 50-60 Hz (Cisco Catalyst 2960-24TT-L and Catalyst 2960-24TC-L and Catalyst 2960-48TT-L and Catalyst 2960-48TC-L) • 100-240VAC (autoranging), 3.0-1.5A, 50-60 Hz (Cisco Catalyst 2960G-24TC-L and Catalyst 2960G-48TC-L)

Power Rating	• Cisco Catalyst 2960-24TT-L: 0.05kVA • Cisco Catalyst 2960-24TC-L: 0.05kVA • Cisco Catalyst 2960-24LT-L : 0.175 kVA • Cisco Catalyst 2960-24PC-L : 0.470 kVA • Cisco Catalyst 2960G-24TC-L: 0.075kVA
DC Input Voltages (RPS Input)	• (No RPS input for Cisco Catalyst 2960PD-8TT-L , Catalyst 2960-8TC-L and Catalyst 2960G-8TC-L) • Cisco Catalyst 2960-24TT-L: +12V at 5A • Cisco Catalyst 2960-24TC-L: +12V at 5A • Cisco Catalyst 2960-24LT-L : +12V at 8.3A, -48V at 2.7A • Cisco Catalyst 2960-24PC-L : +12V at 11.25A, -48V at 7.8A • Cisco Catalyst 2960G-24TC-L: +12V at 10.5A

SWITCH 3560

Las características del modelo pueden encontrarse en la siguiente dirección web http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5528/product_data_sheet09186a00801f3d7d.html"

Description	**Specification**
Performance	• 32 Gbps forwarding bandwidth • Forwarding rate based on 64-byte packets: • 13.1 Mpps (Cisco Catalyst 3560-48TS and Catalyst 3560-48PS); • 128 MB DRAM • 32 MB Flash memory (Cisco Catalyst 3560G-24TS, Catalyst 3560G-24PS, Catalyst 3560G-48TS, Catalyst 3560G-48PS, Catalyst 3560-24TS, Catalyst 3560-48TS, and Catalyst 3560-8PC); • 16-MB Flash memory (Cisco Catalyst 3560-48PS and Catalyst 3560-24PS) • Configurable up to 12,000 MAC addresses • Configurable up to 11,000 unicast routes • Configurable up to 1000 IGMP groups and multicast routes • Configurable maximum transmission unit (MTU) of up to 9000 bytes, with a maximum Ethernet frame size of 9018 bytes (Jumbo frames), for bridging on Gigabit Ethernet ports, and up to 1546 bytes for bridging of Multiprotocol Label Switching (MPLS) tagged frames on 10/100 ports
Connectors and Cabling	• 10BASE-T ports: RJ-45 connectors, two-pair Category 3, 4, or 5 unshielded twisted-pair (UTP) cabling • 10BASE-T PoE ports: RJ-45 connectors, two-pair Category 3, 4, or 5 UTP cabling power pins 1,2 (negative) and 3,6 (positive) • 100BASE-TX ports: RJ-45 connectors, two-pair Category 5 UTP cabling • 100BASE-TX PoE ports: RJ-45 connectors, two-pair Category 5 UTP cabling, power on pins 1,2 (negative) and 3,6 (positive) • 1000BASE-T ports: RJ-45 connectors, four-pair Category 5 UTP cabling • 1000BASE-T SFP-based ports: RJ-45 connectors, four-pair Category 5 UTP cabling • 1000BASE-SX, -LX/LH, -ZX, and CWDM SFP-based ports: LC fiber connectors (single/multimode fiber) • Cisco Catalyst 3560 SFP Interconnect Cable: two-pair shielded cabling, 50 cm • Management console port: RJ-45-to-DB-9 cable for PC connections; for terminal connections, use RJ-45-to-DB-25 female data-terminal-equipment (DTE) adaptor (can be ordered separately from Cisco; part number ACS-DSBUASYN=)

Power Connectors	• Customers can provide power to a switch by using either the internal power supply or the Cisco RPS 2300. The connectors are located at the back of the switch. Note: The Cisco Catalyst 3560-8PC and Catalyst 3560-12PC do not have an RPS port. • Internal-Power-Supply Connector • The internal power supply is an autoranging unit. • The internal power supply supports input voltages between 100 and 240 VAC. • Use the supplied AC power cord to connect the AC power connector to an AC power outlet. • Cisco RPS Connector • The connector offers connection for an optional Cisco RPS 2300 that uses AC input and supplies DC output to the switch. • The connector supports up to six external network devices and provides power to two failed devices at a time. • The connector automatically senses when the internal power supply of a connected device fails and provides power to the failed device, preventing loss of network traffic. • Only the Cisco RPS 2300 (model PWR-RPS2300) should be attached to the redundant-power-supply receptacle.
Indicators	• Per-port status LEDs: Link integrity, disabled, activity, speed, full-duplex indications, PoE applied, PoE error, and PoE disabled indications • System-status LEDs: System, RPS, link status, link duplex, link speed, and PoE indications
Dimensions (H x W x D)	• Cisco Catalyst 3560-48PS: 1.73 x 17.5 x 14.9 in. (4.4 x 44.5 x 37.8 cm) • Cisco Catalyst 3560G-48PS: 1.73 x 17.5 x 16.1 in. (4.4 x 44.5 x 40.9 cm)
Weight	• Cisco Catalyst 3560-48PS: 13.2 lb (6.0 kg) • Cisco Catalyst 3560G-48PS: 15.5 lb (7.0 kg)
Environmental Ranges	• Operating temperature: 32 to 113°F (0 to 45°C) • Storage temperature: -13 to 158°F (-25 to 70°C) • Operating relative humidity: 10 to 85% (noncondensing) • Operating altitude: Up to 10,000 ft (3049m) • Storage altitude: Up to 15,000 ft (4573m)
Acoustic Noise	• ISO 7779: Bystander position operating to an ambient temperature of 25°C • Cisco Catalyst 3560-48PS: 42 dBa • Cisco Catalyst 3560G-48PS: 52-58 dBa
Mean Time Between Failure (MTBF)	• Cisco Catalyst 3560-48PS: 173,500 hours • Cisco Catalyst 3560G-48PS: 147,000 hours

ASA 5540

Las características del modelo pueden encontrarse en la siguiente dirección web http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html

	Cisco ASA 5540

	
Users/Nodes	Unlimited
Firewall Throughput	Up to 650 Mbps
Maximum Firewall and IPS Throughput	• Up to 500 Mbps with AIP-SSM-20 • Up to 650 Mbps with AIP-SSM-40
3DES/AES VPN Throughput	Up to 325 Mbps
IPsec VPN Peers	5000
SSL VPN Peers* Included/ Maximum)	2/2500
Concurrent Connections	400,000
New Connections/ Second	25,000
Integrated Network Ports	4 Gigabit Ethernet, 1 Fast Ethernet
Virtual Interfaces (VLANs)	200
Security Contexts (Included/ Maximum)*	2/50
High Availability	Active/Active and Active/ Standby
Expansion Slot	1, SSM
User-Accessible Flash Slot	1
USB 2.0 Ports	2
Serial Ports	2 RJ-45, console and auxiliary
Rack-Mountable	Yes
Wall-Mountable	Not Available
Security Lock Slot (for Physical Security)	Not Available

Memory	1 GB

Minimum System Flash	64 MB
System Bus	Multibus architecture

Temperature	32 to 104°F (0 to 40°C)
Relative humidity	5 to 95 percent noncondensing
Altitude	Designed and tested for: 0 to 9840 ft (3000 m). Agency approved for: 2000 m
Shock	1.14 m/sec (45 in./sec) 1/2 sine input
Vibration	0.41 Grms2 (3 to 500 Hz) random input
Acoustic noise	60 dBa max

IPS 4200

Las características del modelo pueden encontrarse en la siguiente dirección web http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/ps9157/product_data_sheet09186a008014873c_ps4077_Products_Data_Sheet.html

	Cisco IPS 4260
	
Performance: Media-rich	2 Gbps
Performance: Transactional	1 Gbps
Standard monitoring interface	10/100/1000BASE-TX
Standard command and control interface	10/100/1000BASE-TX
Optional monitoring interfaces	• Four 10/100/1000BASE-TX (up to 9 monitoring interfaces) • Two 1000BASE-SX (up to 4 fiber monitoring interfaces)
Redundant power supply	Optional
Automated hardware fail- open	Yes*
Form factor	Two rack units
Height	3.45 in. (87.6 mm)
Width	17.14 in. (435.3 mm)
Depth	20 in. (508 mm)

Weight	40 lb (18.14 kg) (when fully loaded)
Rack-mountable	Yes
Auto-switching	100 to 240 VAC
Frequency	47 to 63 Hz, single-phase
Operating current	8.9A (100 VAC), 4.5A (200 VAC)
Operating temperature	10 to 35°C (50 to 95°F)
Nonoperating temperature	-40 to 70°C (-104 to 158°F)
Operating relative humidity	10 to 85% (noncondensing)
Nonoperating relative humidity	5 to 95% (noncondensing)
Heat dissipation @ full power	648 Btu/hr

Servidor de Telefonía Callmanager V7.0 y UCCX 5.0

Las características del modelo pueden encontrarse en la siguiente dirección web

Callmanager:

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps556/data_sheet_c78-485333.html

UCCX:

http://www.cisco.com/en/US/prod/collateral/voicesw/custcosw/ps5693/ps1846/product_data_sheet0900aecd805e1d54.html

Firewall Checkpoint IP395

Las características del modelo pueden encontrarse en la siguiente dirección web http://www.checkpoint.com/products/softwareblades/advanced-networking.html

Feature	Details
Supported Internet Protocols	IPv4 RFC 791
	ICMP RFC 792
	ARP RFC 826
	ICMP Router Discovery (server) RFC 1256
	Router Discovery v6 (ICMP v6) RFC 2466 *
	CIDR RFC 1519
	Static Routes
	Multicast Tunnels *

	IPv6 Core RFCs *
	VRRPv2 RFC 3768 *
	VRRPv3 (IPv6) draft-ietf-vrrp-ipv6-spec-08.txt *
	Requirements for IPv4 Routers RFC 1812
	Quality of Service *
	RFC 2474 (general diffserv PHB information)
	RFC 3246 (EF behavior description)
	RFC 2597 (AF behavior description)
	Bootp/DHCP Relay RFCs 951, 2131
	Route Aggregation and Redistribution
	Unnumbered Interfaces
	Link Negotiation IEEE 802.3ad
	Flow Control IEEE 802.3x
	Private (RFC 1918) and Public IP Routing
	VLAN 802.1Q Transparent mode
Dynamic Routing Protocols	RIP RFC 1058
	RIP Version 2 (with authentication) RFC 1723
	RIPng (IPv6) RFC 2080 *
	OSPFv2 RFC 2328
	OSPF NSSA RFC 3101 *
	OSPFv3 (IPv6) RFC 2740 *
	BGP4 RFCs 1771, 1963, 1966, 1997, 2918
	BGP4++ RFC 2545, 2858 (unicast IPv6) *
Multicast Protocols*	IGMPv2 RFC 2236
	IGMPv3 RFC 3376 *
	PIM-SM RFC 4601
	PIM-SSM RFC 4601 *
	PIM-DM RFC 3973
	PIM-DM State Refresh draft-ietf-pim-refresh-02.txt *
	DVMRP (multicast) RFC 1075 *
QOS	

Minimum Bandwidth Allocation	Weighted Fair Queuing (WFQ) algorithm. Guarantees can be set for a group of connections in aggregate, or on a per-connection basis.
Weighted Priorities	Allocates bandwidth according to relative merit as defined by business requirements
Bandwidth Limits	Sets bandwidth restrictions for non-critical network applications.
Low Latency Queuing (LLQ)	Reduce delay for latency-sensitive traffic
Integrated Differentiated Services (DiffServ)	Enables Service Providers to offer end-to-end QoS for VPN and unencrypted traffic on IP WANs
ISP Redundancy	
Multiple modes	Load Sharing or Primary/Backup
Server Load Balancing/Connect Control	
Server Load Balancing	Distributes network traffic among a number of servers. Supports various load-balancing methods and server availability check
Load Balancing Algorithms	Server Load, Round Trip, Round Robin, Random and Domain

Gateway Celular

Las características del modelo pueden encontrarse en la siguiente dirección web http://www.its-tel.com/index.php?Itemid=96&option=com_zoo&view=item&category_id=3&item_id=16CGW-P ISDN PRI Cellular Gateway

System

Intelligent Routing- Return up to 1,500 mobile calls directly to the calling DDI (Direct Dial-In).

Least Cost Routing (LCR) -Up to 20 tables

Number portability support

Full Device Control- Local & remote configuration

Maintenance alarms

CDR-log for up to 3,500 records

Incoming & Outgoing Calls Control

19" rack mounting

Prepaid capability

Cellular

4 SIM per cellular channel

Up to 16 cellular cards

Up to 128 SIMs per system

Supports: CDMA, GSM, UMTS*

PRI

Dialing Mode Support (Overlap/ En Block)

PRI grouping

E1/T1

Hardware Specification

Indicator: Led

Dimensions (H*W*D):

133*443*290mm

5.24/17/6*11.42"

Weight: 6.5Kg/ 14.33 Lbs

Operating temperature: 0oC-45oC / 32oF-113oF

Relative humidity: 5-95%

Installation: 19" rack, 3U

Antennas

Directional- 7.5db , Omni- 2.5 db

BIBLIOGRAFIA

1. ANSI/TIA/EIA-942. "Telecommunications Infrastructure Standard for Data Centers" TIA. 2005
2. ANSI/TIA/EIA-568-B. "Commercial Building Telecommunications Cabling Standard" TIA. 2001
3. RAAP "Modelo TCP/IP"
   RAAP - http://www.raap.org.pe/docs/RAAP2_Modelo_tcpip.pdf, 2007
4. CISCO "Cisco Certified Network Associate",
   Cisco networking academy -Version 3.1, 2007
5. IESPANA "Capítulo 2 Calidad de Servicio"
   URL: http://qos.iespana.es/capítulo2.htm, 2008
6. "Tráfico de colas",
   URL: http://usuarios.multimania.es/redestelco/eval2/ejercicio.html, 2009
7. "PROTOCOLO DE CONTROL DE TRANSMISIÓN",
   URL: http://www.rfc-es.org/rfc/rfc0793-es.txt
8. "PROTOCOLO TCP/IP"
   URL:http://www.terra.es/personal/jjfbaigo/manu_net/tcp/tcpip.htm
9. AMP "Data Center Basics Standards & Cabling Design",
   Tyco Electronics, 2009
10. UNAM "Planeación Internet"
    URL:http://www.ingenieria.unam.mx/~jkuri/Apunt_Planeacion_internet/TEMAVI.4.pdf, 2008
11. CISCO "Products & Services"
    URL: www.cisco.com, 2010
12. Panduit "Products Overview",
    URL: http://www.panduit.com/Products/ProductOverviews/index.htm, 2010
13. WIKIPEDIA "Capital expenditure",
    URL: http://en.wikipedia.org/wiki/Capital_expenditure, 2009
14. World Lingo "Capital expenditure"
    URL: http://www.worldlingo.com/ma/enwiki/es/Capital_expenditure
15. "Concepto de inversión y costo operativo",
    URL:http://www.ingenieria.unam.mx/~jkuri/Apunt_Planeacion_internet/TEMAVI.4