UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DE REDES DE DATOS EN TELEFONÍA CELULAR DE 3ra GENERACIÓN

TESIS

QUE PARA OBTENER EL TÍTULO DE:

INGENIERÍA EN COMPUTACIÓN

PRESENTA:

RAÚL GUALITO OLEA

DIRECTOR:

ING. JUAN JOSÉ CARREÓN GRANADOS

2010

AGRADECIMIENTOS:

A mis padres (Salvador y Marnelly), por su incomparable apoyo, cariño y compresión. Por guiarme sobre el camino de la educación.

A mis hermanos (Chavin y Marnelly), por sus comentarios, sugerencias y opiniones. Además de ser excelentes hermanos y amigos son la mejor compañía al vivir bajo el mismo techo.

A Beatriz, por sus consejos, paciencia y opiniones para que me sintiera satisfecho con mi tesis. Además de ser parte fundamental para terminar éste trabajo.

A cada uno de mis profesores, que fueron parte esencial en mi formación profesional y que sin la transmisión de sus conocimientos no habría llegado hasta en donde me encuentro ahora.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad, las redes de comunicación móvil se han ido incrementando gradualmente. Más allá de ser un lujo, como anteriormente se consideraba, su uso cotidiano y su demanda, cada vez más fuerte, ha obligado a las principales empresas productoras de teléfonos a crear una gran cantidad de modelos, marcas y nuevos servicios haciéndolos más atractivos ante el ojo del consumidor.

El uso constante de teléfonos celulares ha provocado que las redes se saturen constantemente, generando considerables problemas en la calidad del servicio. Para brindarle mayor satisfacción y seguridad a todo consumidor, las operadoras de telefonía celular han buscado nuevos mecanismos en infraestructura y tecnología que sean capaces de soportar la cantidad de usuarios existentes y el incremento de los mismos, mantener los enlaces con mayor capacidad y proveer de los servicios adquiridos de manera eficiente.

Aunado a ello, las empresas han implementado nuevas modalidades para conservar sus redes telefónicas, de tal manera que propicie beneficios rentables. Uno de los medios que utilizan para maximizar su economía es el mantenimiento de la infraestructura de red y la re-utilización de equipos, con el fin de invertir menos y recuperar la inversión a corto plazo.

La eficiencia de las comunicaciones depende de múltiples factores, generalmente incluye la confiabilidad del equipo, redundancia en el diseño, disponibilidad de conexiones y mecanismos de protección del diseño del direccionamiento. La capacidad de la red puede tener un mejor rendimiento si las características de software y hardware son aptas para el diseño.

Tomando en consideración la gran labor que requiere mantener y administrar la infraestructura de la tecnología móvil, la presente investigación tiene como principal objetivo explicar la interconexión de los equipos de datos (routers, lan switches) con los equipos de comunicación móvil de tercera generación MSC (Mobile Switching Center) y

MGW (Media Gateway), a partir de un plano geográfico limitado, que va desde la Ciudad de México hasta Guadalajara y Monterrey.

El trabajo está dividido en una serie de capítulos que explican detalladamente, a través de textos, gráficas y cuadros, el proceso de implementación de dicha tecnología. A fin de difundir ésta, cualquier individuo, interesado en el tema, podrá aplicar la misma metodología en el campo de la telefonía celular.

En primera instancia, se revisa la relación de los elementos de red de la operadora móvil con los nuevos dispositivos de red a implementar; es decir, se parte de los nuevos requerimientos de interconexión para mostrar la solución más viable a las necesidades de la operadora móvil.

En el capítulo 2, una vez identificadas las exigencias de la red, se procede a una breve introducción de los equipos de comunicación móvil MSC y MGW, para después, durante el capítulo 3, continuar con el análisis del modelo de tráfico de voz, señalización y gestión. La descripción de éstos últimos es esencial para comprender el potencial y alcance que tiene la red.

Durante el capítulo 4, se describe el funcionamiento y la configuración de los diferentes protocolos y técnicas de ruteo más utilizadas en los mecanismos de protección de voz y paquetes de datos. Más allá de conectarse a una LAN, es necesario integrar las redes con diversos dispositivos, arquitecturas y protocolos.

Finalmente se revisa la estructura de los dispositivos capa tres, como lo son routers y switches, tomando en cuenta el direccionamiento IP, técnicas de ruteo, y todos los elementos necesarios para mantener una red estable, resistente y altamente confiable.

El trabajo pretende mostrar que el éxito de una red de comunicación de datos se encuentra en el diseño y la implementación de la misma. Manteniendo una red escalable, rentable, confiable, estable, los servicios son de alta calidad para los clientes, lo cual genera satisfacción en los mismos y por consiguiente mayor eficacia y eficiencia a las operadoras.

CAPÍTULO 1. Análisis y descripción de requerimientos de la operadora de telefonía móvil

1.1 Entendiendo los requerimientos de la operadora de telefonía móvil

La demanda de usuarios abonados en NEXTEL de México ha crecido a través de los años con lo cual la demanda en la cantidad de servicios es mayor. Las actuales líneas de servicio, comienzan a saturarse y la calidad del servicio a degradarse.

. Las ciudades con cobertura NEXTEL, en la República Mexicana, incluyen: la Ciudad de México, Acapulco, Apizaco, Celaya, Irapuato, Salamanca, Chilpancingo, Córdoba, Cuautla, Cuernavaca, Fresnillo, Guadalajara, Guanajuato, Guasave, Lagos de Moreno, Jalostotitlán, La Paz, La Piedad, León, Los Cabos, Los Mochis, Mazatlán, Monterrey, Morelia, Nuevo Laredo, Orizaba, Pachuca, Puebla, Tulancingo, Querétaro, San Luis Potosí, San Juan de Río, Tijuana, Tlaxcala, Saltillo, Toluca, Veracruz, Hermosillo, Guaymas, Ciudad Obregón, Navojoa, Tepic, Colima, Puerto Vallarta, Cancún, Mérida, Coatzacoalcos, Minatitlán, Campeche, Villahermosa, Durango, Zacatecas, Aguascalientes, Chihuahua, Ciudad Juárez, Torreón, Tepatitlán de Morelos,

Reynosa, Matamoros, Uruapan, Poza Rica, Pátzcuaro, Chetumal, Tampico, Cozumel, San Luis Río Colorado, Mexicali, Magdalena de kino, Estado de México, Santa Ana, Imuris, Nogales, Rosarito, Ensenada, Agua Prieta , Comalcalco y Culiacán.

NEXTEL de México mantiene la comunicación hacia los diversos mercados a través de los principales centros de telecomunicación (llamados MSOs), los cuales se encuentran ubicados en Guadalajara, Monterrey, Estado de México, Tijuana, Ciudad de México, y Chetumal.

De acuerdo a datos oficiales de NEXTEL de México la cantidad de usuarios abonados existentes del 2009 al 2010 se incrementó en 22.4% (Véase figura 1.1.), lo cual provocó un aumento de tráfico entre los principales puntos de comunicación de la República Mexicana (México, Guadalajara, Monterrey, Estado de México).

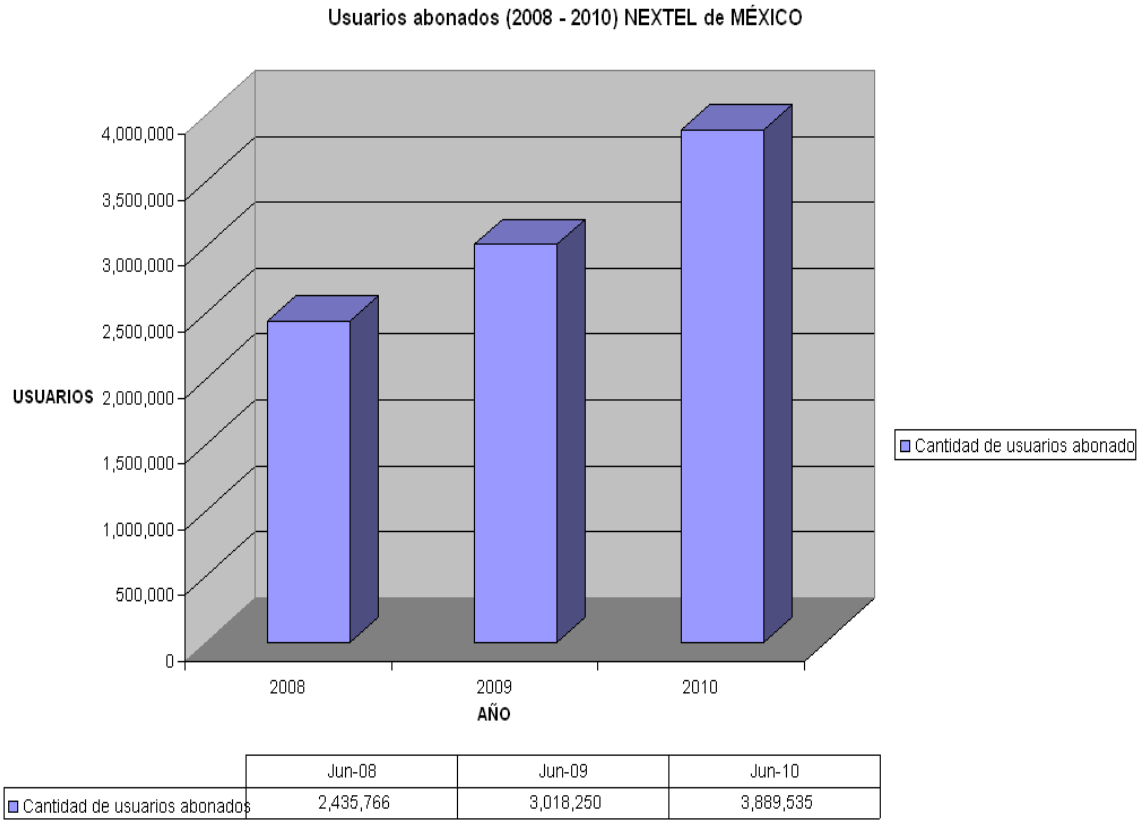

Figura 1.1 Cantidad de usuarios abonados en Nextel de México (2008 – 2010) [1]

[1] *Fuente*: Comunicaciones Nextel de México S.A de C.V.

La actual infraestructura de red de la operadora móvil requiere de conexiones a la red de telefonía pública switcheada (PSTN), ubicada en Guadalajara y Monterrey, con el fin de incrementar su cobertura y servicios. La operadora necesita plataformas y tecnologías que sean capaces de soportar la conexión a la PSTN a través de tecnología TDM (Time Division Multiplexing), y además que el transporte hacia su red interna sea totalmente tecnología IP.

De manera global, los requerimientos son descritos de la siguiente forma:

- ✓ Intercambio de tráfico entre la PSTN (Red de Telefonía Pública Switcheada (TELMEX)) de Guadalajara y Monterrey (sitios principales), con usuarios móviles de la Cd. de México.

- ✓ Intercambio de tráfico entre los MSCs (Mobile Softswitch) que actualmente se encuentran en servicio y un nuevo MSC a integrar con la red actual.

1) Distribución de enlaces a PSTN.

El requerimiento de diseño está realizado en base a la distribución de E1s por cobertura de área y escenario. El número de E1s a ser soportado está distribuido sobre un total de 3 regiones. Véase tabla 1.1.

Ciudad	Revolución	Guadalajara	Monterrey	Tlalnepantla
Capacidad (E1s). 1ª fase	152	61	81	10
Futura expansión. 2ª fase	50	20	20	10

Tabla 1.1 Distribución de E1s en las distintas regiones [2]

[2] Datos obtenidos de Comunicaciones Nextel de México S.A de C.V.

2) Estrategia de diseño

Con el fin de reducir los gastos de capital (CAPEX), y los gastos operativos (OPEX), de la red de NEXTEL de México, se recomienda introducir la arquitectura de MSCs, la cual se basa en los siguientes principios **:

- ✓ Abundantes características de ruteo y amplia capacidad de manipulación del número de B (número llamado), y el número de A (número que llama).
- ✓ Adaptación de la tecnología IP sobre E1 (IPoE1), con el fin de ahorrar recursos de transmisión.
- ✓ Reutilización de la mayoría de los actuales equipos de red.
- ✓ Los equipos son fáciles de operar y de mantener.
- ✓ Los equipos soportan tecnología 3G y evolución hacia arquitecturas de Mobile Softswitch virtuales.

El diseño cumple totalmente con los estándares 3GPP (3rd Generation Partnership Project) y ETSI (European Telecommunications Standards Institute). Se han realizado pruebas exitosas de interoperabilidad con diferentes proveedores, lo cual asegura la integración de los nuevos equipos a la actual red de NEXTEL.

** La arquitectura de MSCs para telefonía móvil 3G es explicada durante el capítulo 2 del presente trabajo.

1.2 Descripción general del diseño de red a integrar en la operadora de telefonía móvil.

Basados en la arquitectura de MSCs y adaptando los requerimientos de NEXTEL a la misma, la solución más viable es integrar un MSC (Mobile Softswitch) y cuatro MGWs (Media Gateways), los cuales realizarán la función de Tandem y Gateway (*), en conjunto con los MSCs que actualmente se encuentran en producción. En la figura 1.2, se muestra de forma gráfica y general la arquitectura de red a implementar en la operadora móvil NEXTEL.

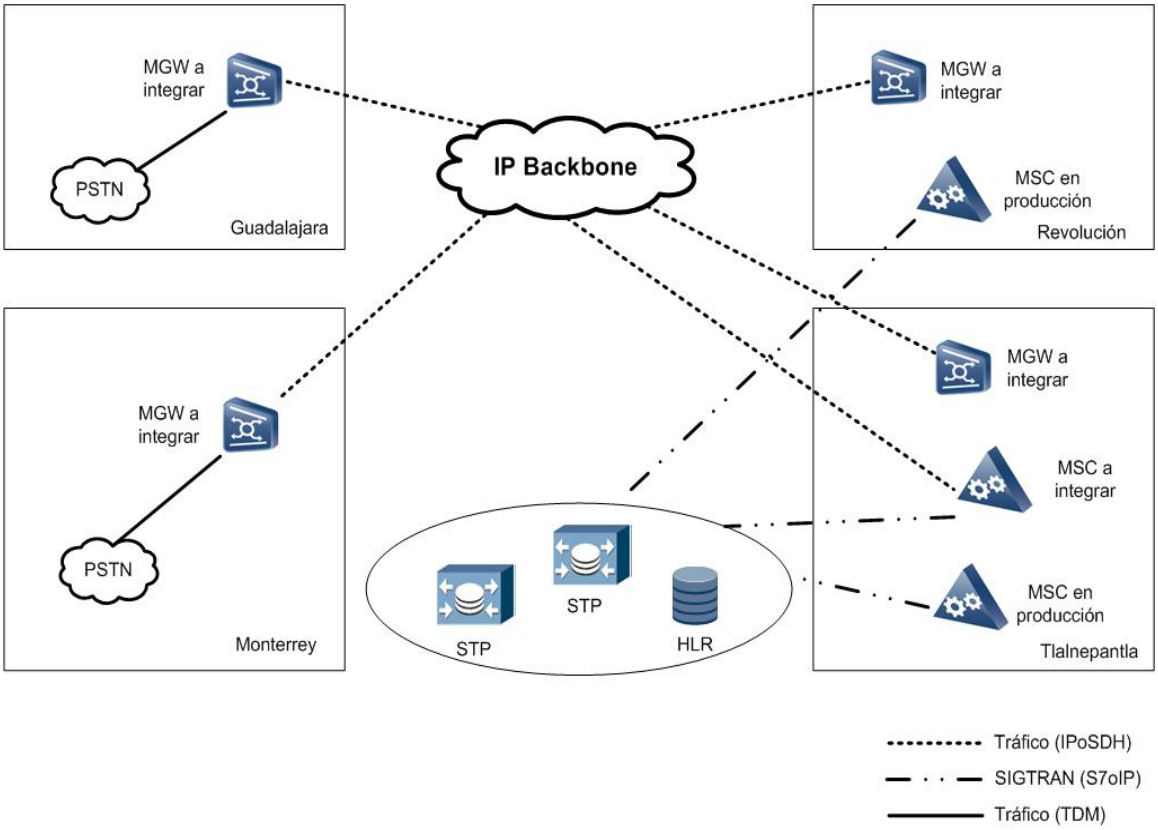

Figura 1.2 Topología de red a implementar [3]

En la solución propuesta, algunos elementos de red son re-utilizados para reducir los CAPEX, incluyendo los medios de transmisión, la red TDM, y la red IP. Es importante recalcar que se utiliza la tecnología IP sobre E1 para ahorrar recursos de transmisión.

[3] Diagrama realizado por el propio autor Raúl Gualito Olea.

Como se muestra en la figura 1.2, el equipo MSC y un MGW se encuentran en el cuarto de telecomunicaciones de Tlalnepantla.

El resto de los MGWs se encuentran en los cuartos de control de sus respectivas ciudades (Monterrey, Guadalajara y Revolución). Los MGWs de los diferentes mercados se conectan con el nuevo MSC, y el nuevo MSC se integra con los MSCs de producción a través de los STPs (Signaling Gateway). El MGW de Monterrey se conecta con la PSTN de Monterrey, y el MGW de Guadalajara se conecta con la PSTN de Guadalajara.

Con el fin de lograr la comunicación entre los distintos mercados se requiere de 2 routers para transporte de tráfico, 2 lan switches para soportar señalización, y 2 lan switches para gestión de los elementos de red (**).

En resumen, la distribución de los equipos es de la siguiente forma:

- 1 MSC en Tlalnepantla.
- 1 MGW en Monterrey.
- 1 MGW en Guadalajara.
- 1 MGW en Revolución.
- 1 MGW en Tlalnepantla.
- 2 routers en sitio Revolución (tráfico).
- 2 Lan switches en sitio Tlalnepantla (señalización).

Se pretende realizar la explicación de lo general a lo particular, por lo que la solución a detalle de cada topología de tráfico (Voz, Señalización y Gestión) se explica durante el capítulo V.

* Las características de la función de Tandem se encuentran explicadas en el capítulo II.
** La solución requiere de alta disponibilidad en las conexiones, de ahí que la cantidad de equipos de datos en cada sitio sea el doble.

CAPÍTULO 2. Introducción a los equipos de comunicación móvil de 3ra. Generación MSC y MGW

Separando el tráfico de voz del tráfico de control, un modelo de red, con la tecnología de MSC, puede utilizar redes de tráfico como IP y TDM. Utilizando el modo de distribución de redes de manera separada, la tecnología de MSCs en conjunto con la tecnología de transmisión de datos provee a los carriers con los siguientes beneficios:

- ✓ Reducción de los costos de operación, improvisando la eficiencia de la transmisión de la red.

- ✓ Protección de la inversión de las operadoras, proveyendo de la evolución de un modelo a otro, protegiendo la base de suscriptores y el incremento de tráfico.

2.1 Introducción a la solución de telefonía móvil utilizando el servidor MSC y MGW

La solución para las operadoras de telefonía móvil o carriers, está basada en los requerimientos de interconexión y características de red de los mismos. La solución provee esquemas de integración de 3G los cuales son fáciles de operar y mantener.

Basados en los requerimientos de construcción de una arquitectura de MSCs para una red telefonía móvil, el MSC está dividido en dos partes: El servidor MSC y el servidor MGW, como se muestra en la figura 2.1.

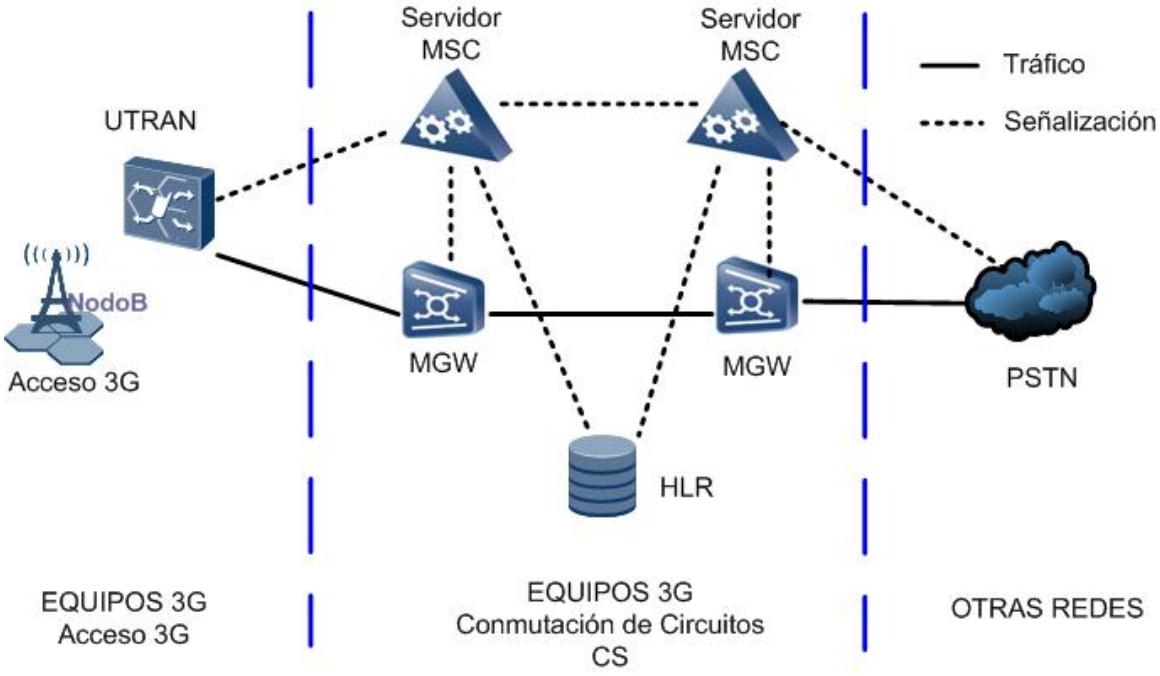

Figura 2.1 Esquema general de conmutación de circuitos en redes de telefonía celular 3G [4]

El servidor MSC se puede conectar a diferentes equipos dependiendo de la solución a implementar, entre ellos se incluye la parte de acceso (UTRAN) y redes de datos para comunicación con otros MSCs, MGWs, STPs.

[4] Diagrama reproducido de Huawei Technologies Co, Ltd., "*Mobile Softswitch Center documentation V100R007*", Shenzhen CHINA, Networking Application & Product Orientation.

.El servidor MSC realiza, en general, el siguiente control de funciones de:

- Administración de datos del suscriptor.
- Procesamiento de señalización.
- Procesamiento de llamada.
- Administración de seguridad.

Como se muestra en la figura 2.1, el servidor MGW es el punto de comunicación entre la PSTN y el MSC. El MGW realiza, en general, las siguientes funciones:

- Administración de paquetes de voz.
- Codificación / Descodificación de señales digitales.
- Cancelación de ecos.
- Administración de paquetes de control.

Manteniendo el tráfico de voz separado del tráfico de control, el MSC puede ser configurado de una de las siguientes formas:

- Servidor Virtual VMSC.
- Servidor con funciones de gateway GMSC.
- Servidor con funciones de tandem TMSC.

Servidor virtual MSC (VMSC).

EL MSC soporta diferentes clases de protocolos, incluyendo H.248, BICC, SIP, CAP, RANAP, MAP, ISUP, TUP y BSSAP. Cuando el MSC es conectado con la parte de acceso (UTRAN, BSS) y con el MGW se dice que el MSC se encuentra configurado de forma virtual (VMSC).

En la tabla 2.1, se muestra el significado de las diferentes clases de protocolos que soporta el MSC.

Protocolo	Nombre Completo
BICC	Bearer Independent Call Control Protocol. Protocolo de Control Independiente de tráfico de Voz.
CAP	CAMEL Application Part. Aplicación CAMEL.
BSSAP	Base Station Subsystem Application Part. Aplicación de Subsistema de Estaciones Base.
RANAP	Radio Access Network Application Part. Aplicación de Acceso de Radio de Red.
MAP	Mobile Application Part. Aplicación Móvil.
ISUP	Integrated Services Digital Network User Part. Servicios Integrados-Digitales de Usuarios de Red.
SIP	Session Initiation Protocol Protocolo de Inicio de Sesiones

Tabla 2.1 Lista de Protocolos

Servidor con funciones de gateway GMSC.

Se dice que el MSC realiza las funciones de gateway cuando puede intercambiar información de señalización con las siguientes redes:

- PSTN (Red de Telefonía Pública Conmutada).
- Red Fija.
- Otras PLMN (Red móvil Terrestre Pública)

Cuando el servidor MSC es configurado como gateway, realiza las siguientes funciones.

- Sirve como oficina móvil entre distintas redes.
- Analiza el ruteo entre las redes.
- Implementa la conexión de las llamadas y el acuerdo entre las redes.

Servidor con funciones de tandem TMSC.

Como una oficina de Tandem, el servidor MSC realiza las siguientes funciones:

- Análisis de ruteo de llamadas.
- Convergencia de llamadas en intra-redes.

Cuando el MSC es configurado como Tandem (TMSC) provee una gran cantidad de troncales TDM (E1s) y de canales IP.

2.2 Características y funciones del servidor MSC

El MSC (Mobile Softswitch Center) es un servidor encargado de proporcionar el control, procesamiento y gestión de una o varias llamadas de telefonía celular. Es el dispositivo capaz de controlar la administración de los servicios de voz y datos basados en IP o TDM. El MSC es el núcleo y cerebro de una red de comunicación móvil, ya que sobre él se encuentra la decisión de entregar una llamada de manera exitosa a otros dispositivos o redes de comunicación móvil.

A continuación se listan algunas de las características más importantes del servidor MSC:

1) Interconexión con los elementos existentes de la red la operadora móvil.

El diseño de redes móviles cumple con los estándares de 3GPP y ETSI. Pruebas de interoperabilidad con diferentes proveedores han sido totalmente probadas, lo que asegura una buena integración con los equipos que se encuentran actualmente en producción (NORTEL, CISCO, TELLABS, TEKELEC).

2) Alta capacidad de integración.

El sistema MSC provee una avanzada tecnología en hardware, alta capacidad de integración, y capacidad para futura expansión.

- Las tarjetas utilizan circuitos de integración avanzados como ASIC, PLD, FPGA, lo cual simplifica la carga de trabajo del MSC, y mejora la integración del sistema.
- Cuando el MSC utiliza el tipo de tarjeta 750C, el MSC, en configuración completa, soporta hasta 3.2 millones de suscriptores (configurado como VMSC), y 900,000 circuitos de voz TDM (configurado como TMSC).
- El MSC en configuración completa, requiere de tres gabinetes. La carga de poder del MSC es cerca de 8.5 kW.

3) Análisis de Números.

El MSC provee la función de análisis de números, la cual tiene varias aplicaciones:

1) Soportar y recibir y almacenar hasta 32 dígitos.

2) Soportar el análisis de números de hasta 32 dígitos.

3) Soportar 4096 códigos GT (Global Title).

4) Soportar la función de pre-análisis de números para llamadas entrantes y llamadas salientes.

5) Soportar discriminación de números de llamadas entrantes.

6) Soportar la restricción de mínima cantidad de dígitos y máxima cantidad de dígitos.

7) Soportar la manipulación de dígitos (número de A, número de B, números roaming).

4) Diseño de hardware.

Todas las tarjetas manejan el esquema de alta disponibilidad, respaldos Activo/Stand by, y carga compartida.

Existen avanzadas técnicas de detección y aislamiento de fallas, lo cual mejora el sistema de mantenimiento, y asegura que los servicios no sean afectados cuando un nodo simple presenta fallas.

5) Sistema de Billing.

El servidor que almacena los archivos de cobro, también llamados CDRs, es el servidor de Billing, que para el sistema MSC es llamado servidor iGWB. EL iGWB utiliza un sistema doble de respaldo en caliente y arreglo de disco duro RAID5, con lo cual se habilita la función de doble backup de la base de datos y unidades de almacenamiento.

2.3 Características y funciones del servidor MGW

El MGW (Media Gateway, por sus siglas en inglés) es el servidor capaz de habilitar, procesar y convertir la conexión de servicios de voz entre diferentes redes de comunicación. El MGW puede ayudar a las operadoras de telefonía móvil o carriers, a construir redes de comunicación rentables, con bajo costo y altamente escalables.

EL MGW es capaz de interactuar con el MSC para soportar diferentes servicios de red, como son los Servicios de Valor Agregado (VAS). Los nuevos servicios, pueden ser introducidos de forma fácil y rápida, debido a la arquitectura de red que mantiene de forma separada con el MSC.

El MGW provee las siguientes funciones básicas:

- Soporta los siguientes codecs de voz: G.711A/G.711μ/G.723.1/G.726/G.729.
- Asegura la calidad del tráfico voz, aplicando los siguientes tipos de tecnología:
    - Canceladores de eco (EC).
    - detección de actividad de voz (VAD).
    - Generación de ruido confortable (CNG).
    - detección de paquetes de voz perdidos. (PLC).
- Cuenta con la capacidad de almacenar diferentes tipos de tonos. Colección y envío de dígitos.
- función de sistemas embebidos para gateways de señalización, adaptación y re-envío de señalización de TDM (Time Division Multiplexing) a IP (Internet Protocol), con lo cual reduce la complejidad de la red.
- Capacidad de doble respaldo con MSC. Cuando el MGW se encuentra conectado a un MSC maestro y un MSC de respaldo, el MGW cuenta con la capacidad de conmutar automáticamente al MGW de respaldo sin interrumpir los servicios de red.

- Funciona como MGW virtual, varios MGWs pueden estar conectados al mismo tiempo al servidor MSC, cada uno trabajando con funciones lógicas de manera independiente.
- El diseño de las tarjetas de datos permite que el ancho de banda de voz sea compartido entre sus puertos, lo que permite soportar enlaces de hasta 2 Gigabytes.

CAPÍTULO 3. Análisis de modelos de tráfico

Una parte muy importante en el diseño de red de comunicación móvil es considerar los modelos de tráfico de voz, control y gestión.

Con base en los modelos de tráfico se puede dimensionar la cantidad de componentes de comunicación móvil, puertos y links a utilizar durante el desarrollo del proyecto. Durante el desarrollo de los mismos se toman en cuenta diferentes aspectos como son: Ancho de paquetes IP, convergencia de puertos de una interfaz que se encuentra adjunta a una o varias tarjetas, habilidad de las troncales entre puertos, tipo de puertos a utilizar, mecanismos de calidad de voz, cantidad de llamadas entrantes y salientes, cantidad de canales de voz a soportar, tipo de códec de voz. En el presente capítulo se estudian los modelos de tráfico necesarios para el diseño de una red de telefonía celular de tercera generación.

3.1 Análisis del modelo de tráfico de voz

En una red IP, para asegurar la calidad del servicio de voz, es necesario considerar los siguientes parámetros: retardos (delays), proporción de los paquetes perdidos, y variaciones de los retardos (jitters).

La calidad de los servicios de voz en una red IP, se encuentra definida en la tabla 3.1:

DATOS	Retardos (ms)	Proporción de paquetes perdidos	Variación del retardo (ms)
Voz	<50 (Recomendado) <400 (Máximo)	≤1%	≤1
Señalización	≤100	≤0.1% (Considerando horas pico)	≤10

Tabla 3.1 Parámetros de Calidad de Servicio de Voz en IP [5]

La calidad del servicio de una red IP, dependiendo del códec a utilizar, es diferente. El operador móvil puede obtener diferente coeficiente de compresión de voz de acuerdo al tipo de códec a utilizar, para éste caso en específico la operadora requiere de utilizar el códec G729b con muestreo de 20 ms, el cual es un mecanismo de compresión de datos de voz que cuenta con las características mostradas en la tabla 3.2.

Proporción del intervalo de muestreo de compresión de voz (ms)	Estimado de proporción de tráfico IP a comprimir (%)	Factor de compresión de voz, proporcionado por el MGW.	Calidad del servicio de voz
729 10ms	70.40	42.24	Con distorsión
729 20ms	**39.20**	**23.52**	Buena
729 30ms	28.80	17.28	Excelente

Tabla 3.2 Características de códec G729 [5]

[5] Huawei Technologies Co, Ltd., "*Mobile Softswitch Center documentation V100R007*", Shenzhen CHINA, VoIP Planning & Codec Configuration.

De la tabla 3.2 se puede concluir que a mayor tiempo de muestreo menor factor de compresión pero mayor calidad en el servicio de voz, y a menor tiempo de muestreo mayor factor de compresión pero menor calidad de servicio de voz.

Tomando en cuenta los datos anteriores, el ancho de banda de tráfico para cada sitio, se encuentra calculado en base al número de E1's a conectar, y al factor de compresión de voz del MGW. A continuación se muestra la formula utilizada para calcular el ancho de banda de tráfico de voz:

Ancho de banda de tráfico de voz IP = No. de E1´s * No. de canales de voz por E1 * factor de compresión de voz del MGW

En la tabla 3.3, se muestra el ancho de banda de tráfico de voz IP para cada ciudad, considerando la primera fase del proyecto (**):

Ciudad	Total de E1s para voz	Ancho de Banda G729 (AB)
Guadalajara	61	AB(kbps)= 61x 30=1830x23.52= 43041 kbps proporción de compresión= 1830x64=117120/43041= 2.72
Monterrey	81	AB(kbps)=81x30=2430x23.52= 57153 kbps
Tlalnepantla	10	AB(kbps)=10x30=300x23.52= 7056 kbps
Revolución	152	AB(kbps)=152x30=4560x23.52= 107252kbps

Tabla 3.3 Ancho de Banda de voz por ciudad, primera fase

** Por definición un E1 consta de 32 divisiones (time slots) de 64 kbps cada una, de las cuales 30 divisiones o time slots son ocupados para transmitir voz y 2 son ocupados para señalización y control de la llamada. Por lo cual el número de canales disponibles para transmitir voz en un E1 es 30.

En la tabla 3.4, se muestra el ancho de banda de tráfico de voz IP para cada ciudad, considerando la segunda fase del proyecto.

Ciudad	Total de E1s para voz	Ancho de Banda G729 (AB)
Guadalajara	20	AB(kbps)= 20x 30=600x23.52= 14112 kbps proporción de compresión= 600x64=38400/14112= 2.72
Monterrey	20	AB(kbps)=20x30=600x23.52= 14112 kbps
Tlalnepantla	10	AB(kbps)=10x30=300x23.52= 7056 kbps
Revolución	50	AB(kbps)=50x30=1500x23.52= 35280 kbps

Tabla 3.4 Ancho de Banda de voz por ciudad, segunda fase

En la tabla 3.5, se muestra el total de ancho de banda de tráfico de voz IP para cada ciudad, considerando ambas fases del proyecto.

Ciudad	Total de E1s para voz	Ancho de Banda G729 (AB)
Guadalajara	81	AB(kbps)= 81x 30=2430x23.52= **57154 kbps** proporción de compresión= 2430x64=155520/57154= 2.72
Monterrey	101	AB(kbps)=101x30=3030x23.52= **71266 kbps**
Tlalnepantla	20	AB(kbps)=20x30=600x23.52= **14112 kbps**
Revolución	202	AB(kbps)=202x30=6060x23.52= **142531 kbps**

Tabla 3.5 Total de Ancho de Banda de voz por ciudad

Es necesario contar con enlaces y equipos capaces de soportar el ancho de banda especificado en la tabla 3.5, debido a que es parte esencial para mantener la red en estado funcional y sin problemas.

3.2 Revisión del modelo de tráfico de señalización

El tráfico de señalización es considerado de forma importante en el diseño de la red debido a que la señalización se encarga de realizar el control de la llamada y la comunicación entre el MSC y el MGW. En comparación con el ancho de banda de voz, la señalización es muy pequeña, ya que solo se ocupa en el momento en que se realiza el disparo de solicitud y terminación de una llamada en el MSC.

Como se explicó en la sección 3.1, un E1 consta de 32 time slots de 64 kbps de ancho de banda en cada time slot, de los cuales dos de ellos son reservados para fines de señalización.

El ancho de banda de señalización, se encuentra calculado en base a la siguiente formula:

Ancho de banda de señalización IP = No. de E1´s * No. de canales de señalización por E1 * Ancho de Banda de un time slot de un E1 (64).

Considerando el total de E1s a implementar, la tabla 3.6 muestra el total de ancho de banda de señalización, para mantener comunicados los diferentes mercados:

Ciudad	Total de E1s para voz	Ancho de Banda (AB)
Guadalajara	81	AB = 81 x 2 x 64 = **10368 kbps**
Monterrey	101	AB =101 x 2 x 64 = **12928 kbps**
Revolución	262	AB = 262 x 2 x 64 = **33536 kbps**

Tabla 3.6 Total de Ancho de Banda de señalización por ciudad

3.3 Revisión del modelo de tráfico de gestión

En una red IP, es importante mantener la gestión de cada uno de los equipos con el fin de realizar rutinas de operación y mantenimiento a los mismos. Esto es, si se requiere de alguna operación o cambio de configuración en los equipos, ya sea router, lan switch, MSC o MGW, poder realizarla, a través de la red, sin necesidad de acudir de manera presencial al equipo.

El ancho de banda para la gestión de los equipos, es un dato que se encuentra en las especificaciones de los mismos. En la tabla 3.7 se muestran los datos más utilizados;

Equipo	Ancho de Banda (AB)
MGW	AB = 64 kbps a 128 kbps.
MSC	AB =64 kbps a 128 kbps.
Router	AB = 64 kbps
LAN switches	AB = 64 kbps

Tabla 3.7 Total de Ancho de Banda de gestión por equipo [6, 7]

[6] Huawei Technologies Co, Ltd., "*Mobile Softswitch, Universal Media Gateway Center documentation V100R007*", Shenzhen CHINA, Operation and maintaining data.

[7] Huawei Technologies Co, Ltd., "*Quidway NE40 Engine, router*", Shenzhen CHINA, System Capacity.

CAPÍTULO 4. Mecanismos de protección de voz y datos en dispositivos de red capa tres

4.1 Introducción a VLANs y troncales 802.1 Q

Una red tradicional Ethernet es una red de broadcast, donde todos los hosts se encuentran en el mismo dominio de broadcast, y se conectan con otro dominio a través de hubs y switches. El hub es un dispositivo de capa física sin la función de switcheo, entonces los paquetes recibidos son reenviados a todos los puertos. El switch es un dispositivo de capas el cual puede re-enviar paquetes de acuerdo a la dirección MAC del paquete. Cuando el switch recibe un paquete de broadcast o un paquete desconocido de unicast en donde la dirección MAC no está incluida en la tabla de direcciones MAC del switch, se re-enviará el paquete a todos los puertos, excepto por el puerto por donde se recibió el paquete. En éste caso, un host en la red recibe muchos paquetes, en donde el destino no es él mismo. Entonces, recursos de ancho de banda son utilizados, causando serios problemas de seguridad.

Un camino tradicional de aislar dominios de broadcast es utilizar routers. Sin embargo, los routers no son económicos y, proveen pocos puertos, entonces no pueden realizar el subneteo para éste caso en particular.

La tecnología VLAN fue desarrollada para switches, con el fin de controlar los broadcasts en una LAN.

Creando VLANs en una red LAN, puedes dividir la LAN en múltiples LANs lógicas, las cuáles tendrán un dominio de broadcast propio. Hosts en la misma VLAN se comunican con otros hosts, como si ellos estuvieran en la LAN. Sin embargo, hosts que se encuentran en diferentes VLANs no pueden comunicarse directamente. La figura 4.1 ilustra la implementación de una VLAN.

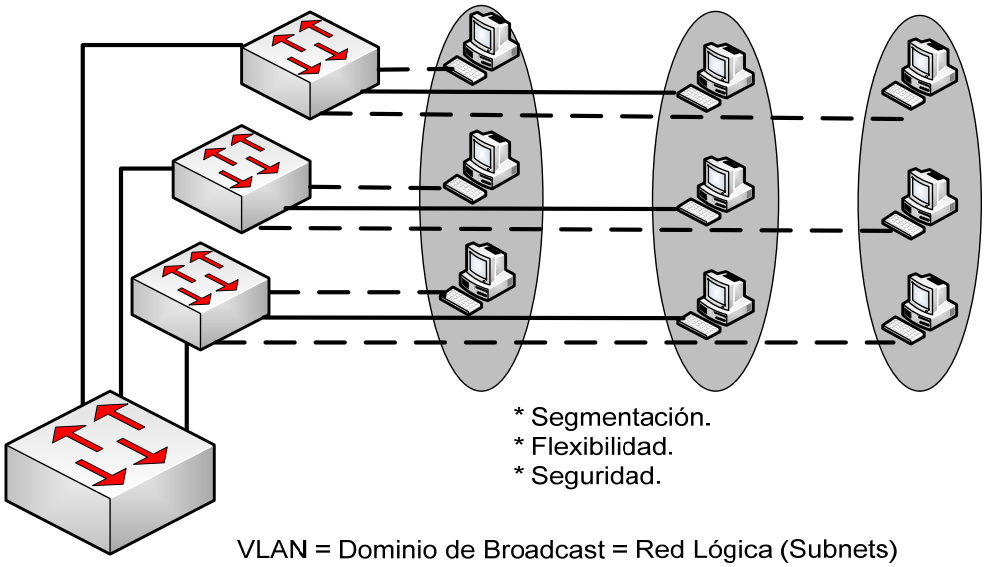

Figura 4.1 Introducción a VLANs [8]

[8] Diagrama reproducido de CISCO Systems Inc. "*Interconnecting Cisco Networking Devices Part 2*", San Jose USA, Implementing VLANs, 2007.

Una VLAN puede abarcar múltiples switches, o routers. Esto, habilita a los hosts que se encuentran en la VLAN a pertenecer a diferentes segmentos de red.

Comparado con una red tradicional Ethernet, una VLAN tiene las siguientes ventajas:

- Los broadcasts se encuentran limitados a las VLANs. Esto, proporciona un decremento en la utilización de ancho de banda y mejora el rendimiento de la red.
- La seguridad de la red es mejorada. La VLAN no se puede comunicar con otra VLAN directamente. Esto es, un host en una VLAN no puede acceder a los recursos en otra VLAN, de forma directa, a menos que routers o switches capa 3 sean ocupados.
- La configuración de la red es reducida. VLANs pueden ser utilizadas para un grupo específico de hosts. Cuando la posición física del host cambia dentro de un rango de la VLAN, no es necesario cambiar la configuración de red del host.

4.1.1 Principios de VLAN

VLAN tags en los paquetes son necesarios en el switch para identificar paquetes de diferentes VLANs. Un dispositivo capa 3 (router), puede identificar el ligado de la capa de encapsulación de datos, entonces se puede agregar el campo de VLAN tag dentro de la capa de encapsulación de datos, sí es necesario. La figura 4.2 muestra la configuración de diferentes VLANs en diferentes switches capa 3.

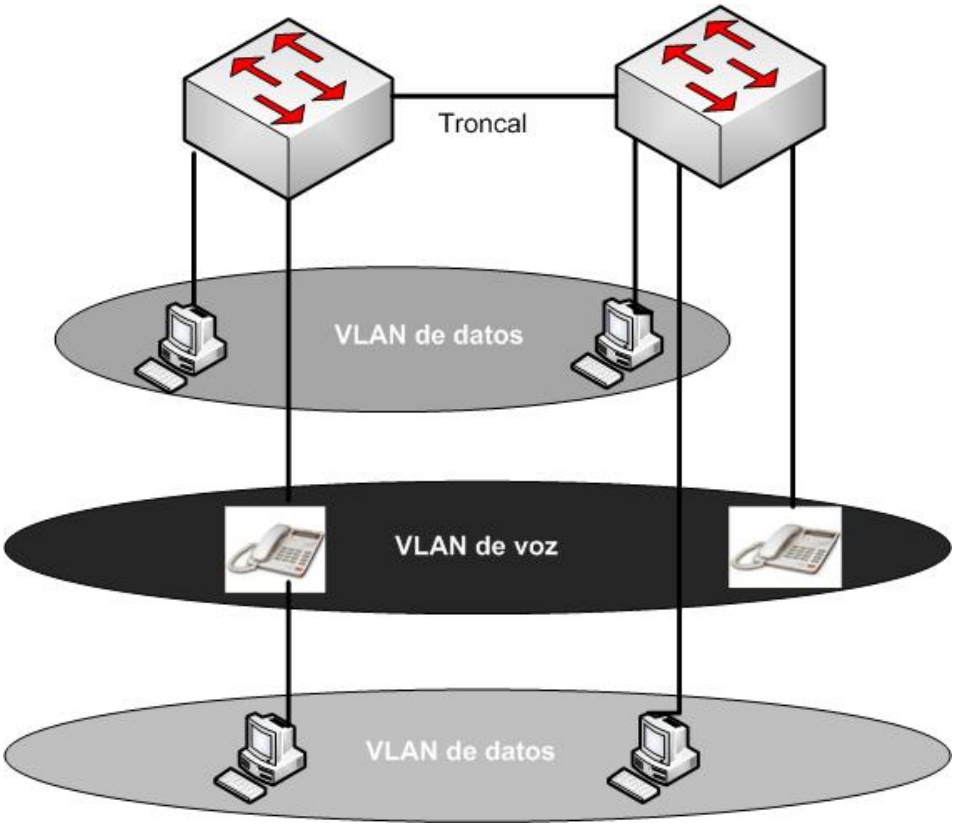

Figura 4.2 Operación de una VLAN [9]

[9] Diagrama reproducido de CISCO Systems Inc. "*Interconnecting Cisco Networking Devices Part 2*", USA, VLAN Operation, 2007.

4.1.2 Modos de una VLAN

Se pueden configurar puertos que pertenezcan a una VLAN con diferentes modos, los cuales determinan a qué VLAN pertenecen. Los puertos pertenecientes al switch pueden pertenecer a uno de los siguientes modos de VLAN:

- **VLAN estática:** Un administrador configura de manera estática la asignación de los puertos de una VLAN.
- **VLAN dinámica:** Los switches soportan la asignación de VLANs de manera dinámica utilizando un Servidor de Políticas de Administración de VLANs (VMPS, por sus siglas en inglés). El VMPS contiene una base de datos que mapea la dirección MAC con la asignación de la VLAN. Cuando un paquete de datos llega a un puerto dinámico en un switch, el switch busca en el servidor VMPS la VLAN a la cual fue asignado el puerto, en base a la dirección MAC fuente del paquete de datos de entrada. Un puerto dinámico puede pertenecer, única y exclusivamente, a una VLAN en un tiempo. Varias computadoras pueden ser asignadas a varios puertos dinámicos, siempre y cuando todas las computadoras pertenezcan a la misma VLAN.
- **VLAN de Voz:** Un puerto asignado a una VLAN de voz es un puerto de acceso, que se encuentra conectado a un teléfono IP, configurado para utilizar una VLAN para voz y otra VLAN para tráfico de datos, en donde el tráfico de datos es recibido por un dispositivo adjunto al teléfono. La figura 4.3 muestra los modos de una VLAN.

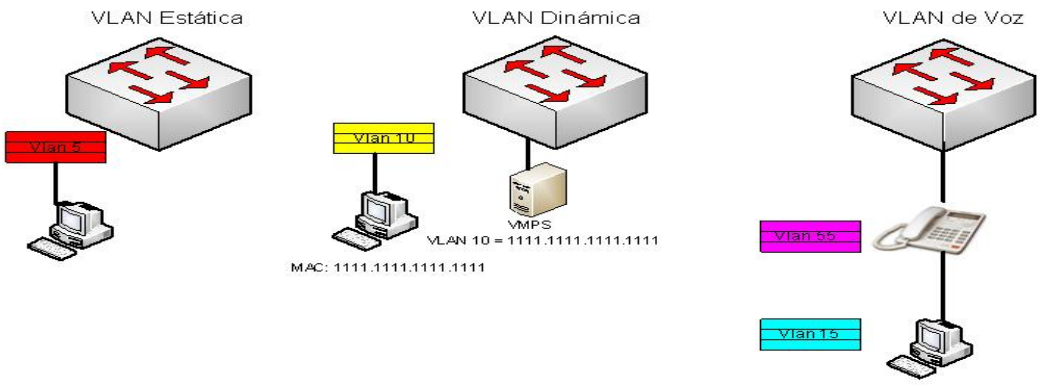

Figura 4.3 Modos de una VLAN [10]

[10] Diagrama reproducido de CISCO Systems Inc. "*Interconnecting Cisco Networking Devices Part 2*", USA, VLAN Modes, 2007.

4.1.3 Troncales con protocolo 802.1 Q

Una troncal es una conexión punto a punto entre una o más interfases de switches ethernet o dispositivos de red como routers. Las troncales ethernet cargan con el tráfico de múltiples VLANs y permiten extender las VLANs a través de diferentes redes. Los switches soportan el protocolo IEEE 802.1Q para interfases fast ethernet y giga ethernet.

Las interfases de troncales ethernet soportan diferentes modos de troncales. Se puede configurar una interfaz como modo troncal y modo no troncal, o tener una negociación troncal con una interfaz de algún otro switch o vecina.

Cada puerto con protocolo 802.1Q es asignado a una troncal. Todos los puertos en modo troncal se encuentran en una VLAN nativa. A cada puerto 802.1Q le es asignado un identificador que está basado en la VLAN nativa (VID, VLAN ID) del puerto (la VLAN por default es la VLAN 1). Todos los paquetes de datos, que no se encuentran con identificador de VLAN, son asignados a la VLAN por default (VLAN 1), el cual es especificado en el parámetro VID. La figura 4.4 ilustra la conexión entre switches a través de troncales 802.1 Q.

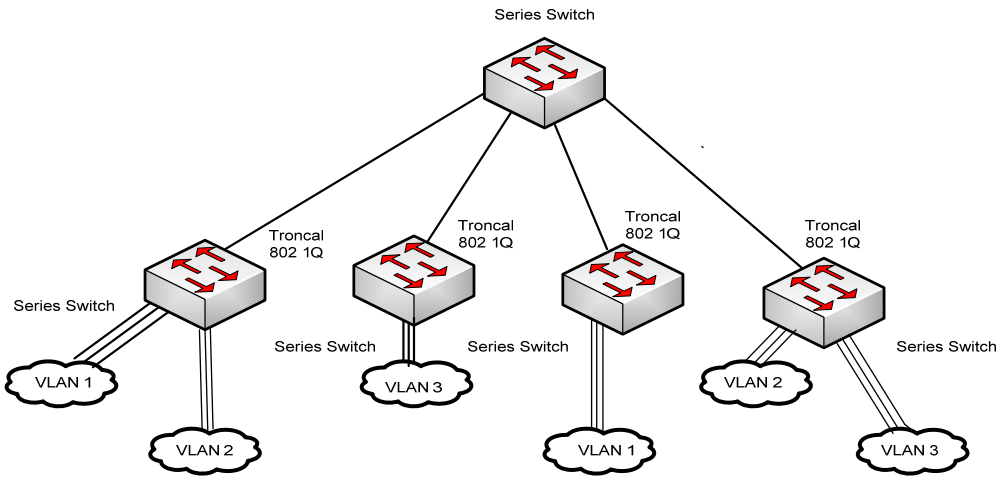

Figura 4.4 Troncales 802.1 Q [11]

[11] Diagrama reproducido de "InterVLAN Routing and ISL/802.1Q Trunking", {en línea}, dirección URL: http://www.cisco.com/en/US/tech/tk389/tk815/technologies_configuration_example09186a00800949fd.shtml {consulta: Diciembre 2009}.

4.1.4 Tramas 802.1Q

802.1Q IEEE utiliza un mecanismo interno de identificación de VLANs (tagging), el cual inserta cuatro bytes dentro de la trama ethernet original entre la dirección MAC fuente y el tipo y ancho de trama. Debido a que 802.1Q altera la trama, el dispositivo en donde se genero la troncal reconfigura la trama checando la secuencia (FCS), sobre la trama modificada.

Es responsabilidad del switch ethernet mirar sobre el campo de cuatro bytes, y determinar dónde entregar la trama. Una parte diminuta del campo de cuatro bytes, 3 bits para ser exactos, son utilizados para especificar la prioridad de la trama. Los detalles de esta pequeña parte son especificados en el estándar IEEE 802.1p. La cabeza de la trama 802.1Q contiene el campo 802.1p, por lo cual se debe de contar con la trama 802.1Q para poder tener la trama 802.1p.

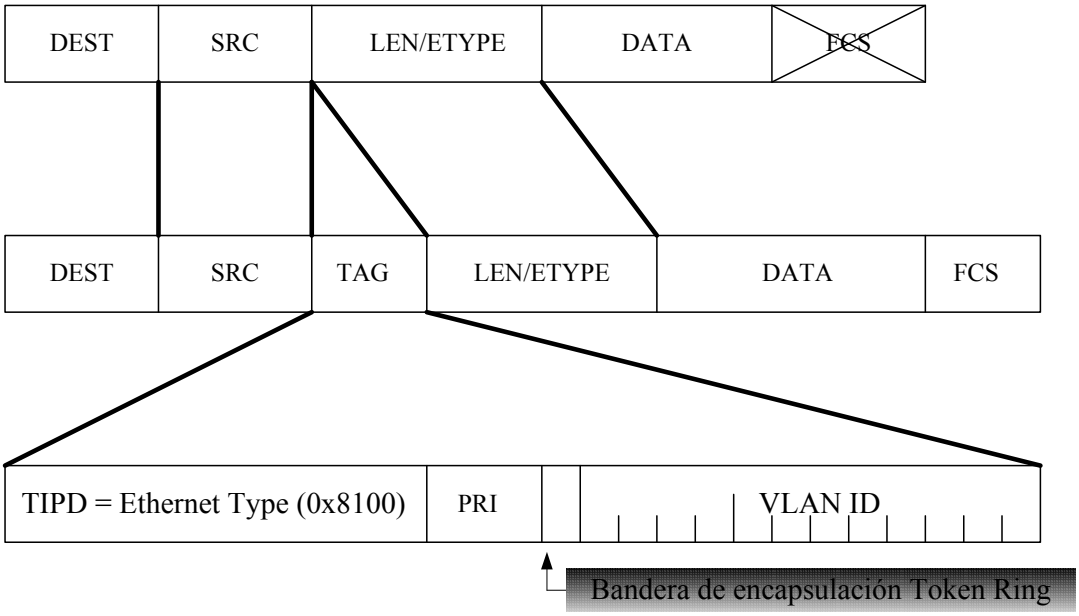

Figura 4.5 Trama 802.1Q [12]

[12] Diagrama reproducido de "*IEEE 802.1Q Frame Format*", {en línea}, dirección URL: http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094665.shtml,{consulta: Mayo 2010}.

Como se muestra en la figura 4.5, el campo de VLAN tag contiene 4 sub-campos, incluyendo TPID, prioridad, CFI, y VLAN ID:

El campo de VLAN ID (Identificador de VLAN), identifica la VLAN a la cual deberá de ser entregado el paquete. Cuando el switch recibe un paquete con no VLAN tag, encapsulará dicho paquete, con la VLAN por default asignada al paquete en el puerto de entrada, y el paquete será enviado a la VLAN por default que le fue asignada en el puerto de entrada.

4.1.5 VLANs Nativas 802.1 Q

Una troncal 802.1 Q, y sus puertos troncales asociados contienen un valor nativo de VLAN. 802.1 Q no realiza el tag de la tramas para las VLANs nativas. Sin embargo, como se observa en la figura 4.6, estaciones ordinarias pueden leer tramas nativas no taggeadas, pero no pueden leer cualquier trama con tráfico taggeado.

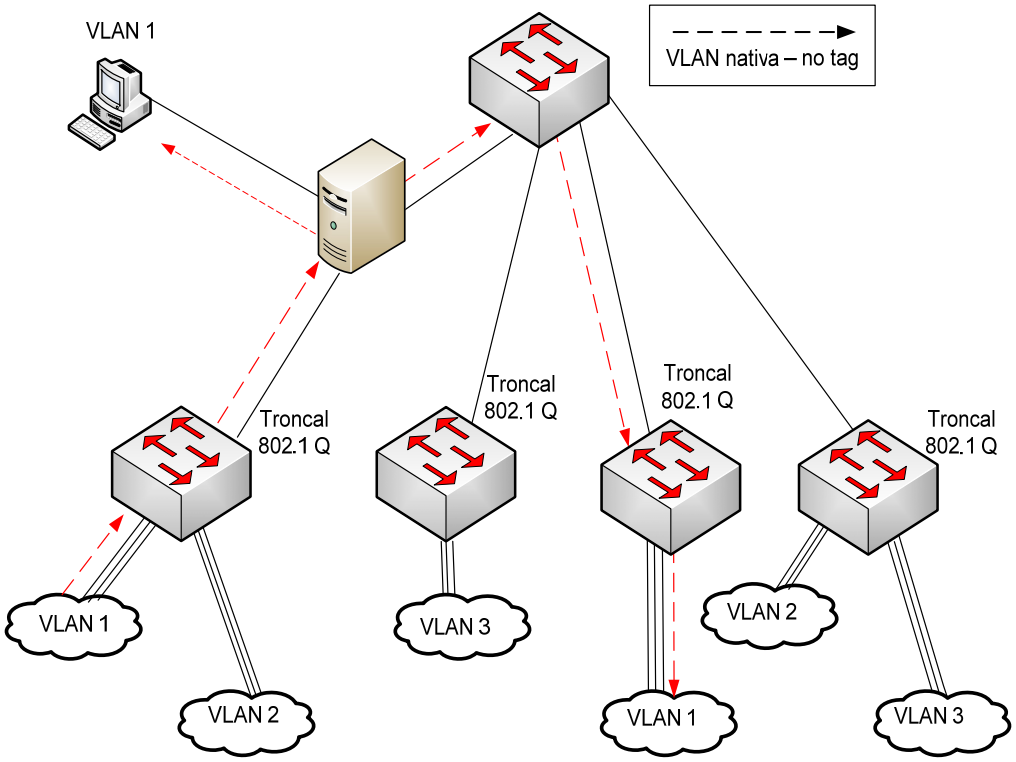

Figura 4.6 VLANs Nativas [13]

[13] Diagrama reproducido de "*802.1Q native VLANs*", {en línea}, dirección URL: http://www.cisco.com/en/US/tech/tk389/tk689/nativevlan_example09186a0080094784.shtml,{consulta: Abril 2010}.

4.1.6 Configuración de troncales 802.1Q

CONFIGURANDO TRONCALES 802.1Q

<SwitchX> system-view

Acceso a modo de configuración

[SwicthX] interface ethernet [*No de interfaz]*

Acceso a inteface en donde se realizará el trunk

[SwicthX] portswitch mode [*access* | *dynamic* | *trunk*]

Tipo de modo de acceso de la interface

[SwicthX] port trunk allow-pass vlan [*No. De VLAN*]

Configuración de VLANs que podrán pasar por el puerto troncal

[SwicthX] portswitch trunk encapsulation [dot1q |]

Troncal con tipo de encapsulamiento dot1.q

VERIFICANDO TRONCALES 802.1Q

<SwitchX> system-view

Acceso a modo de configuración

[SwicthX] display interface ethernet [*No de interfaz] [portswicth* | *trunk]*

Despliegue de información de interface troncal

4.1.7 Protocolo de troncales VLAN (VTP)

VTP (VLAN trunking protocol, por sus siglas en inglés), es un protocolo de mensajes capa 2, que mantiene la consistencia de la configuración de las VLANs administrando el agregado, borrado y cambio de nombres de las VLANs a través de la red. VTP minimiza las inconsistencias de configuración de VLANs que pueden causar problemas, como es el duplicado de los nombres de las VLANs o especificaciones incorrectas en el tipo de VLAN.

Un dominio de VTP es uno o varios switches interconectados, los cuales comparten el mismo ambiente de VTP. Se puede configurar un switch para estar solamente en un dominio de VTP.

Por default, los switches ethernet (CISCO) se encuentran en un estado no administrado de dominios hasta que reciban un anuncio de un dominio sobre una conexión troncal, o hasta que se configure un ambiente administrado de dominio. Las configuraciones realizadas sobre un servidor VTP son propagadas a través de las conexiones troncales hacia todos los switches conectados en la red. Véase figura 4.7.

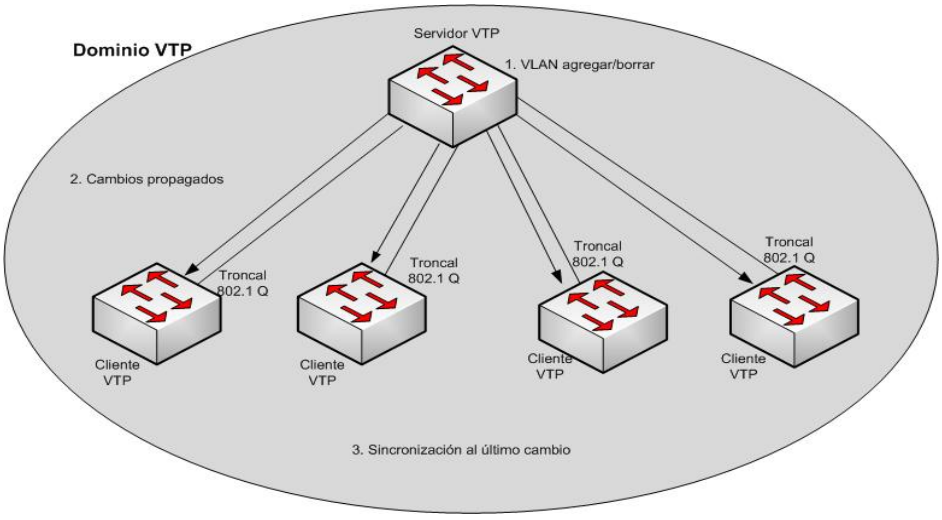

Figura 4.7 Protocolo de troncales VTP [14]

[14] Diagrama reproducido de "*VLAN trunking protocol*", {en línea}, dirección URL: http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml {consulta: Diciembre 2009}.

4.1.8 Modos de troncales de VLAN (VTP)

El protocolo VTP opera en los siguientes modos: servidor, transparente, o cliente. Se pueden completar diferentes tareas dependiendo del modo de operación de VTP. Las características de los diferentes modos se encuentran a continuación:

- ***Servidor:*** El modo por default de un switch es servidor, sin embargo las VLANs no serán propagadas sobre la red, hasta que sea especificado o aprendido el nombre de dominio. Cuando se realiza un cambio en la configuración de una VLAN sobre un servidor VTP, el cambio es propagado a todos los switches del dominio VTP. Los mensajes VTP son transmitidos sobre todas las conexiones troncales.
- ***Transparente***: Cuando se realiza un cambio sobre la configuración de una VLAN en modo transparente, los cambios tienen efecto solamente sobre el switch local y no se propagan a otros switches del dominio VTP. El modo transparente de VTP re-envía anuncios de VTP que recibe dentro de un dominio.
- ***Cliente:*** No se pueden realizar cambios sobre la configuración de la VLAN cuando un switch se encuentra en modo cliente; sin embargo, el cliente de VTP puede enviar cualquier VLAN que se encuentre en su base de datos hacia otro switch VTP. Avisos de VTP se encuentran también son re-enviados en éste modo.

En la figura 4.8 se muestra en forma gráfica las características de los diferentes modos de troncal de VLAN.

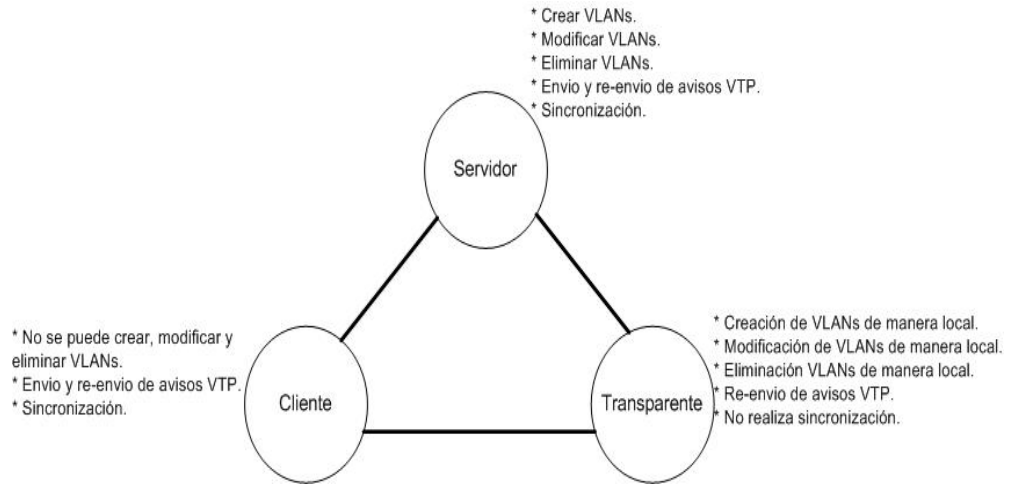

Figura 4.8 Modos de VTP [15]

[15] Diagrama realizado por el propio autor Raúl Gualito Olea.

4.1.9 Operación de troncales VLAN (VTP)

Los avisos de VTP son enviados a través del dominio de administración. Los avisos de VTP son enviados cada 5 minutos o cada vez que existe un cambio en la configuración de las VLANs. Los avisos son transmitidos sobre la VLAN de default (VLAN 1) utilizando una trama de multicast. Un número de revisión es incluido en cada aviso de VTP. Un número de revisión mayor indica que la información de la VLAN anunciada es más reciente que la información almacenada.

Uno de los componentes más críticos de VTP, es la configuración de los números de revisión. Como se observa en la figura 4.9, cada vez que un servidor VTP modifica la información de una VLAN, el servidor VTP incrementa la configuración del número de revisión en uno. El servidor entonces envía un aviso de VTP con la nueva configuración. Sí el número de revisión anunciado es mayor al número de revisión almacenado en los otros switches del dominio de VTP, los swicthes sobre-escriben la configuración de la VLAN con la nueva información almacenada. La configuración del número de revisión en un switch configurado en modo transparente es cero.

El switch que recibe el anuncio VTP debe revisar varios parámetros antes de incorporar la información recibida de la VLAN. Primero, el nombre de dominio de administración y la contraseña debe de coincidir con el configurado en el switch. Siguiente, si la configuración del número de revisión indica que el mensaje fue creado después de la configuración en uso, el switch incorpora la VLAN anunciada.

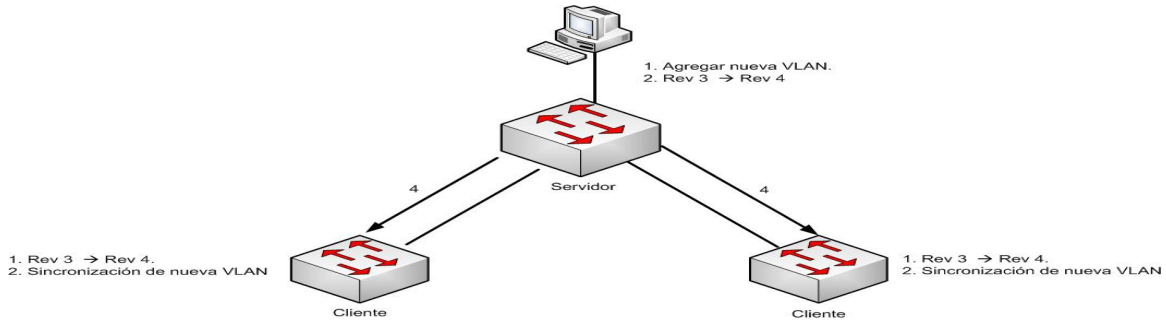

Figura 4.9 Operación de VTP [16]

[16] Diagrama reproducido de CISCO Systems Inc. "*Interconnecting Cisco Networking Devices Part 2*", USA, VTP Operation, 2007.

4.1.10 Creación y verificación de VLAN

Antes de crear VLANs, se debe decidir si se utilizará el protocolo VTP con el fin de mantener la configuración global de las VLANs de la red.

El número máximo de VLANs es dependiente de cada switch. Los switches pueden soportar hasta 250 VLANs definidas por el usuario.

Los swicthes contienen una configuración por default en donde varias VLANs son preconfiguradas para soportar diferentes tipos de tráfico y protocolos. La VLAN por default es la VLAN 1. Ciertos protocolos propietarios de CISCO como CDP y anuncios VTP son enviados sobre la VLAN 1.

Para establecer una comunicación de manera remota con el switch, el switch deberá tener una dirección IP. La dirección IP deberá de estar en la VLAN de administración, la VLAN 1. Si el protocolo VTP es configurado, antes de poder crear una VLAN, el switch deberá de ser configurado en modo servidor VTP o modo transparente.

Para agregar una VLAN a la base de datos de las VLANs de un switch, es necesario asignar un nombre y número a la VLAN. Normalmente el rango de VLANs es entre 1 – 1001. El rango entre 1002 – 1005 se encuentra reservado para Token Ring y VLANs FDDI. Si el switch se encuentra en modo VTP transparente o servidor, se puede agregar, modificar y remover configuraciones de las VLANs 2-1001. (Las VLANs 1, 1002 -1005 son automáticamente creadas y no pueden ser removidas.)

CREANDO VLANs

<SwitchX> system-view
Acceso a modo de configuración
[SwicthX] vlan [No. de VLAN]
Agregar una VLAN
[vlan(No. VLAN)] description [*descripción de la VLAN*]
Descripción ó nombre la VLAN
[SwicthX] interface vlan-interface [*No. De VLAN*]
Configuración de VLANs con características de capa 3
[int vlan-if] ip address [*dirección ip*] [*máscara*]
Configuración de IP sobre la VLAN
[SwitchX] display vlan [brief | *vlan-id* | *all* | *vlan name*]
Despliegue de características de VLAN configuradas.

4.1.11 Asignación de puertos del switch a una VLAN

Después de crear una VLAN, se puede manualmente asignar un puerto o un número de puertos a la VLAN. Un puerto puede pertenecer a solo una VLAN en un tiempo. Cuando se asigna un puerto a una VLAN, utilizando éste método, es conocido como puerto de acceso estático.

En la mayoría de los switches, se puede configurar la asignación de puerto de la VLAN desde el modo de interfaz de configuración utilizando el comando **portswitch access** o **switchport access.** Utiliza el comando **vlan** *vlan-number*, para configurar acceso estático. Utiliza la opción ***dynamic*** para mantener la VLAN controlada y asignada por un VMPS. Una vez configuradas las VLANs se puede desplegar la información de las mismas de manera global ó individual con el comando **show vlan all** ó **display vlan all**, como se muestra en la figura 4.10.

ASIGNANDO PUERTOS A VLAN

<SwitchX> system-view

Acceso a modo de configuración

[SwicthX] interface ethernet x/x/x

Acceso a interface ethernet

[int ethe x/x/x] portswitch access [*vlan vlan#* | *dynamic*]

Puerto de acceso asignado a una VLAN

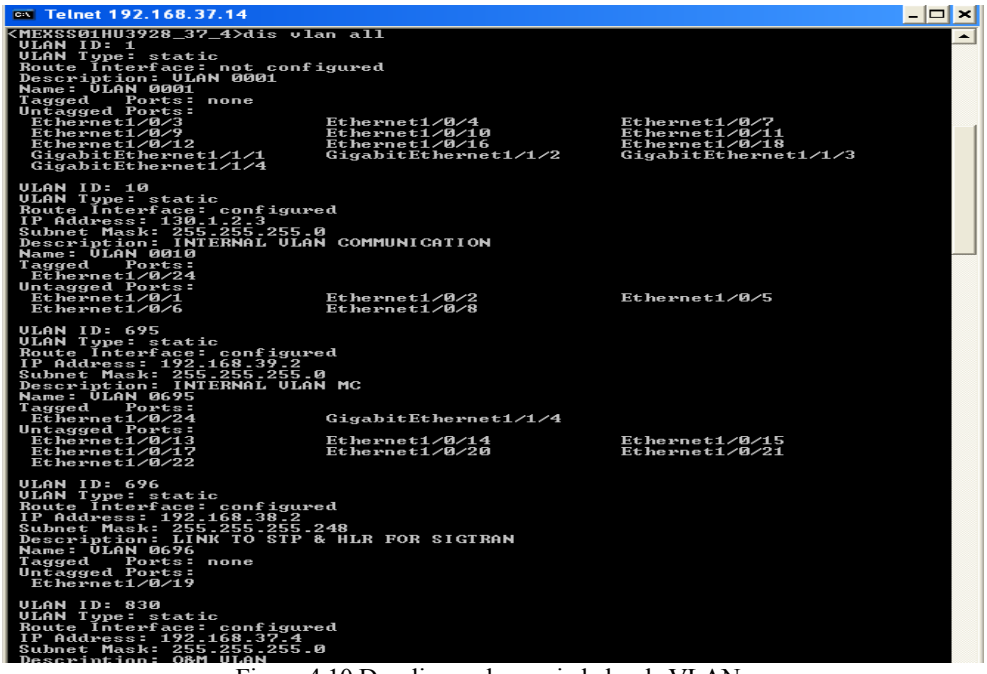

Figura 4.10 Despliegue de propiedades de VLANs

4.2 Mejorando el rendimiento de redes IP con el protocolo STP (Spanning Tree Protocol)

La mayoría de las redes complejas incluyen dispositivos redundantes para evitar fallas en puntos únicos. Aunque las topologías redundantes eliminan algunos problemas, puede introducir algunos otros. El protocolo de Spanning Tree (STP) es un protocolo de administración de capa 2 que provee trayectorias redundantes, además de prevenir loops no deseados en una red completamente switcheada.

Algunos de los problemas que pueden ocurrir con links y dispositivos redundantes en una red switcheada son los siguientes:

- Lluvia de broadcast: Si no se cuenta con un proceso de evitar loops en operación, cada switch inunda de broadcast hacia todos los puertos del switch (excepto al mismo) de manera interminable.
- Transmisiones Múltiples de Datagramas: Múltiples copias de datagramas pueden ser entregadas a estaciones destino. La mayoría de los protocolos esperan, solamente, recibir una única copia del datagrama de cada transmisión. Múltiples copias del mismo datagrama pueden causar errores no recuperables.
- Inestabilidad en la base de datos MAC: Se puede tener instabilidad en la base de datos de las direcciones MAC por recibir copias del mismo datagrama a través de diferentes puertos. El re-envío de datos puede causar problemas cuando el switch consume los recursos que son copiados con inestabilidad en la tabla de las direcciones MAC. Véase figura 4.11.

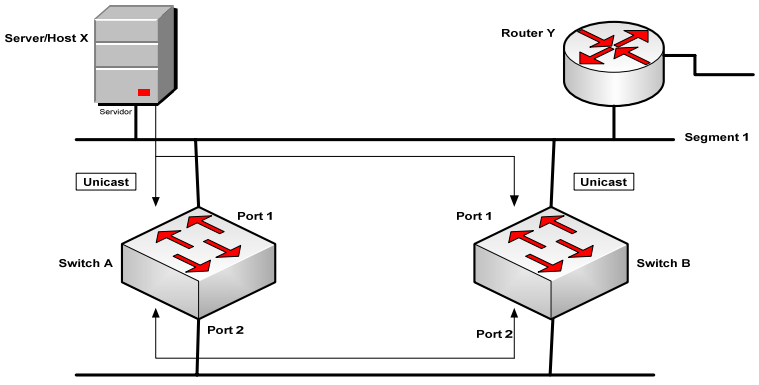

Figura 4.11 Inestabilidad en base de datos MAC [17]

[17] Diagrama reproducido de "*Understanding Spanning Tree Protocol*", {en línea}, dirección URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/sw_ntman/cwsimain/cwsi2/cwsiug2/vlan2/stpapp.htm {consulta: Enero 2010}.

4.2.1 Resolviendo problemas de loops con protocolo STP

STP provee la resolución de loops, administrando las trayectorias físicas de los segmentos de red. STP permite la redundancia por trayectorias físicas mientras prevee efectos no deseables de loops activos en la red. STP es un estándar 802.1D definido por el comité de la IEEE.

STP comprende las siguientes características:

- STP forza a ciertos puertos a un estado de stand by para que no re-envíen o inunden de datagramas los switches (Véase figura 4.12). El efecto global, es que existirá una única trayectoria para cada segmento de red activo en cualquier tiempo.
- Sí existe un problema de conectividad sobre cualquiera de los segmentos dentro de una red, STP re-establece la conectividad automáticamente activando la trayectoria de respaldo.

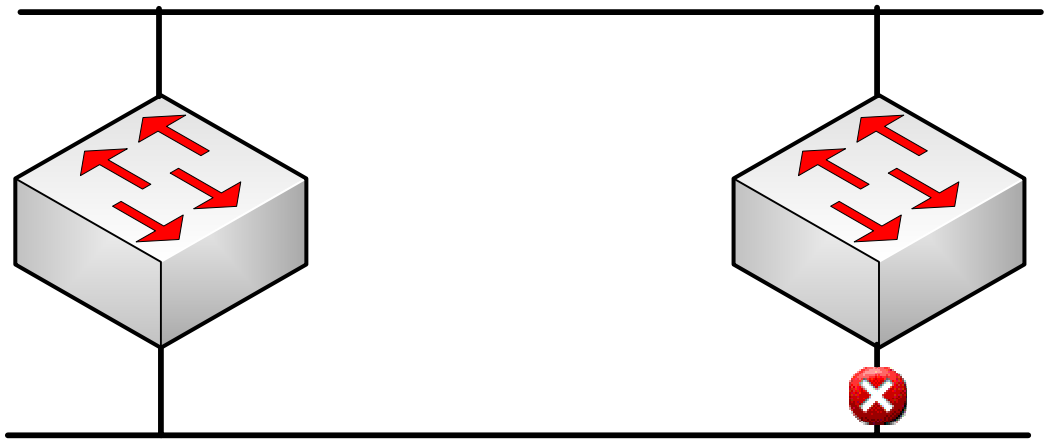

Figura 4.12 Resolución de loops con STP [18]

[18] Diagrama realizado por el propio autor Raúl Gualito Olea.

4.2.2 Operación de Spanning-Tree

STP realiza 3 pasos para proveer una topología libre de loops lógicos:

1. **Selección de un swicth que actuará como puente principal o raíz:** STP tiene un proceso para seleccionar un switch raíz. Solamente un swicth puede actuar como principal en una red. Sobre el equipo principal, todos los puertos son puertos designados. Los puertos designados se encuentran, normalmente, en estado de re-envío de paquetes. En estado de re-envío, un puerto puede enviar y recibir paquetes de tráfico. En la figura 4.13, el switch X es seleccionado como el puente principal.

2. **Selección de puertos raíz sobre el o los switches que actuarán como puentes no raíz:** STP establece un puerto raíz sobre cada switch con puente no raíz. El puerto raíz, es el puerto con la trayectoria de menor costo de un switch con puente de respaldo. Los puertos raíz se encuentran normalmente en estado de re-envío de paquetes. El costo de la trayectoria de STP es un costo acumulado calculado sobre el ancho de Banda. En la figura 4.13, la trayectoria con el menor costo al puente principal desde el switch Y, es a través del link fast ethernet 100BASE-T.

3. **Selección de puerto designado sobre cada segmento:** Sobre cada segmento, STP establece un puerto designado. El puerto designado es seleccionado sobre el puente que tienen la trayectoria de menor costo hacia el puente principal. Los puertos designados se encuentran normalmente en estado de re-envío de paquetes. En la figura 4.13, los puertos designados para ambos segmentos están sobre el puente raíz, por que el puente raíz está directamente conectado a ambos segmentos. El puerto ethernet 10BASE-T en el switch Y es un puerto no designado por que existe solamente un puerto designado por segmento. Los puertos no designados se encuentran normalmente en estado de bloqueo, para que lógicamente rompan el loop lógico de la topología. Cuando un puerto se encuentra en estado de bloqueo, los paquetes de tráfico no son re-enviados, pero pueden recibir tráfico.

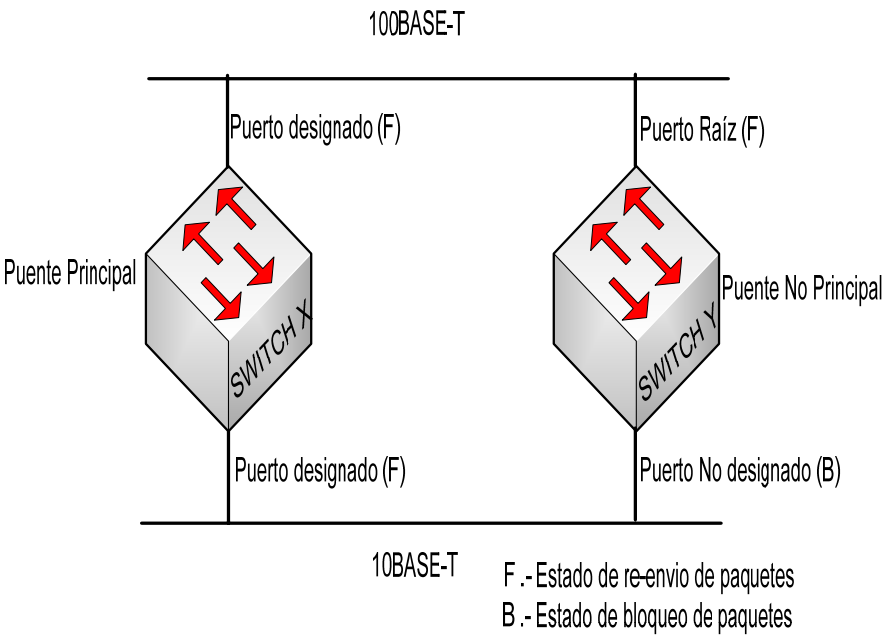

Figura 4.13 Funcionamiento de STP [19]

[19] Diagrama reproducido de CISCO Systems Inc. "*Interconnecting Cisco Networking Devices Part 2*", San Jose USA, Spanning Tree Protocol, 2007.

4.2.3 Selección de puente principal o raíz en protocolo STP

Los switches que tienen configurados el algoritmo de Spanning-tree intercambian mensajes de configuración con otros switches y puentes en intervalos regulares (cada 2 segundos por default). Los switches realizan el intercambio de éste tipo de mensajes mediante un datagrama de multicast llamado protocolo de puente para datos (BPDU, Bridge Protocol Data Unit). Una información contenida dentro del paquete BPDU es el ID del puente (BID, bridge ID).

El protocolo STP asigna un único valor de BID a los switches. El BID está compuesto por una prioridad (2 bytes) y la dirección MAC (6 bytes). La prioridad por default, de acuerdo a IEEE 802.1 D, es 32,768 (1000 0000 00000 0000 en binario, o 0x8000 en formato hexadecimal), el cuál es el valor medio. El swicth con el puente principal es el puente con el menor BID.

En la figura 4.14, ambos switches tiene la misma prioridad. El swicth con la dirección MAC menor es el switch con el puente principal.

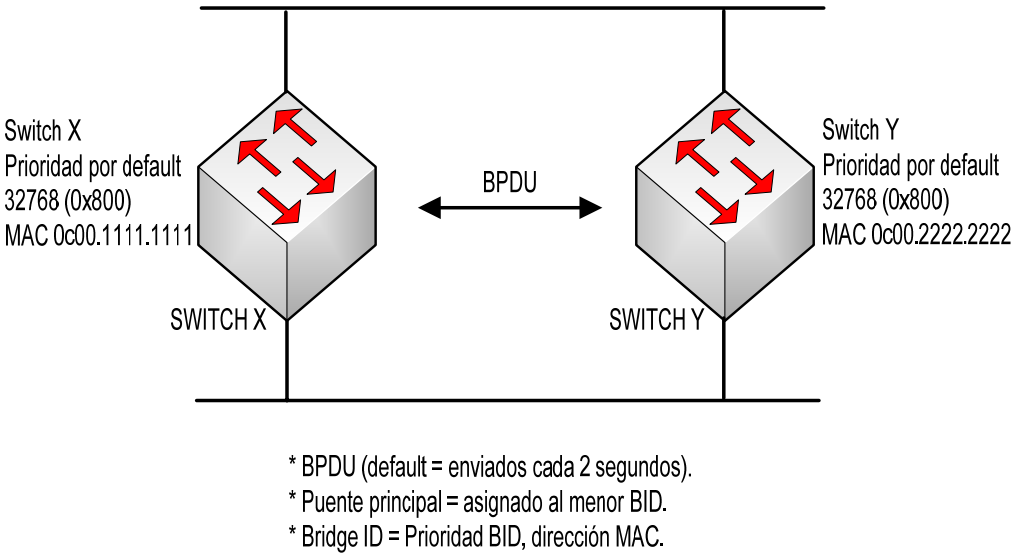

Figura 4.14 Selección de puente principal o raíz [20]

[20] Diagrama reproducido de "*CCNP study guide, SYBEX*", Wade Edwards & Terry Jack, San Francisco, Switching & Spanning Tree Protocol, 2008.

4.2.4 Estados de puertos en el protocolo Spanning-tree

Existen cinco estados por los que un punto puede pasar al utilizar en protocolo STP:

- Bloqueo.
- Escuchar.
- Aprender.
- Re-enviar.
- Deshabilitar.

Cuando STP es habilitado, cada puente principal en la red va a través del estado de bloqueo y transitorio al estado de escuchar y aprender. Sí el protocolo es correctamente configurado, los puertos alcanzan su estado de bloqueo y re-envío de paquetes. Los puertos de re-envío proveen la trayectoria de menor costo al puente raíz. Durante un cambio de topología, un puerto temporalmente implementa el estado de escuchar y aprender.

Todos los puertos puentes, inicialmente inician en estado de bloqueo, mientras esperan por los paquetes BPDU. Cuando los swictches se encuentran en proceso de boot, funciona como sí fueran el puente principal y entran en estado transitorio de listening. Una ausencia de BPDUs por cierto periodo de tiempo es llamado edad máxima (max_age, por sus siglas en inglés), los cuáles tienen un tiempo por default de 20 segundos. Sí un puerto se encuentra en estado de bloqueo y no recibe ninguna BPDU dentro de la edad máxima, las transiciones del puente comienzan del estado de bloqueo al estado de escuchar. Cuando un puerto se encuentra en estado transitorio de escuchar, es habilitado para enviar y recibir BPDUs, y determinar la topología activa. En éste punto, el switch no permite el paso de tráfico de paquetes. Durante el estado de escuchar, el puente realiza 3 pasos:

- Selecciona el puente principal o raíz.
- Selecciona los puertos raíces sobre los puentes no principales.
- Selecciona los puertos designados sobre cada segmento.

El tiempo que toma a cada puerto pasar del estado transitorio de escuchar a aprender o de escuchar a re-enviar paquetes es llamado retraso de re-envío (forward delay). El retraso de re-envío tiene un tiempo de default de 15 segundos.

El estado de aprender reduce la cantidad de inundaciones en los puertos, requeridas

cuando comienza el re-envío de paquetes. Sí un puerto continua siendo designado o raíz entra en transición a re-envío de paquetes. Los puertos que son no designados entran en estado de bloqueo.

Un puerto normalmente tarda de 30 a 50 segundos en pasar del estado de bloqueo al estado de re-envío de paquetes.

4.2.5 Descripción de Puertos Rápidos (PortFast)

STP Puertos Rápidos causa que una interfaz que se encuentra configurada en la capa 2 como puerto de acceso, pase del estado transitorio de puerto bloqueado a estado de re-envío de paquetes, sin pasar por los estados de escuchar y aprender. Se puede utilizar éste tipo de configuración a puertos que están directamente conectados a una computadora o servidor, con el fin de permitir una convergencia inmediata a red, y no esperar a que spanning tree converja.

Si una interfaz que se encuentra configurada como puerto rápido recibe una BPDU, spanning tree puede pasar el puerto al estado de bloqueo utilizando una BPDU de guardia (BPDU guard). La figura 4.15 muestra la configuración de puertos rápidos sobre un switch ethernet.

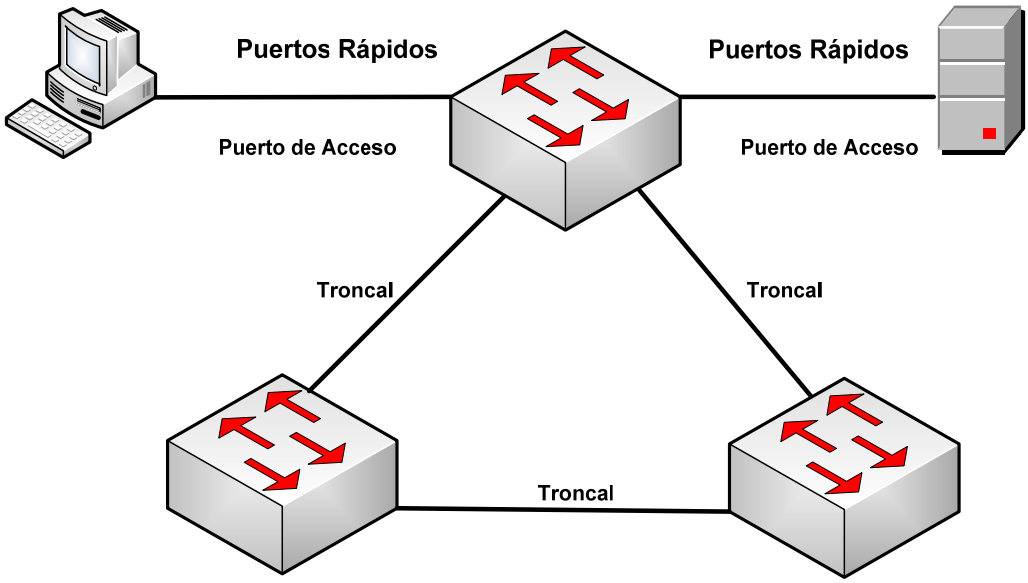

Figura 4.15 Puertos Rápidos [21]

[21] Diagrama reproducido de "*CCNP study guide, SYBEX*", Wade Edwards & Terry Jack, San Francisco, Switching & Spanning Tree Protocol, 2008.

4.2.6 Operación del protocolo de Spanning Tree

La figura 4.16, es un ejemplo que describe el estado de los puertos de los switches cuando se tiene configurado el protocolo STP.

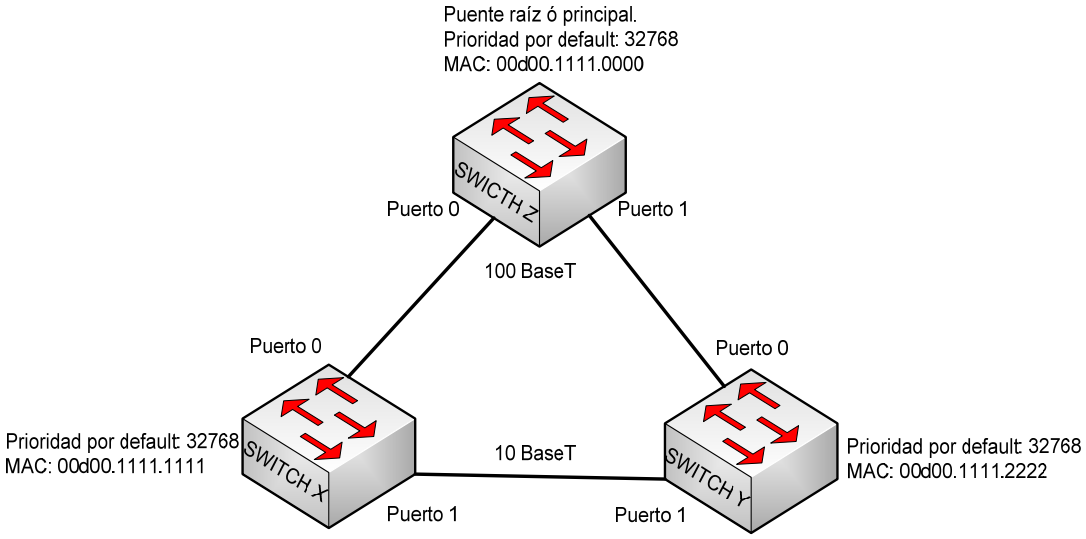

Figura 4.16 Ejemplo de operación de Spanning Tree [22]

De la figura 4.16 podemos concluir, lo siguiente:

1) El puente raíz es el switch Z, el cual tiene el menor BID.
2) El puerto raíz es el puerto 0 en los switches X y Y. El puerto 0 es la trayectoria de menor costo hacia el switch raíz o principal de ambos switches.
3) Los puertos designados en el swicth Z son los puertos 0 y 1. Todos los puertos en el switch raíz son puertos designados. El puerto 1 del swicth X es un puerto designado del segmento entre el switch X y el switch Y. El switch X y el switch Y tienen el mismo costo de la trayectoria de hacia el swicth o puente raíz, pero el puerto 1 del swicth X es designado debido a que tiene el menor BID que el switch Y.
4) El puerto 1 del switch Y es un puerto no designado del segmento y se encuentra en estado de bloqueo.
5) Todos los puertos raíces y designados se encuentran en estado de re-envío de paquetes.

[22] Diagrama reproducido de "*CCNP study guide, SYBEX*", Wade Edwards & Terry Jack, San Francisco, Switching & Spanning Tree Protocol, 2008.

4.2.7 Comandos de implementación de Protocolo STP

COMANDOS DE IMPLEMENTACION DE STP

<SwitchX> system-view

Acceso a modo de configuración

[SwicthX] stp mode [stp | rstp | mstp]

Configuración de modo de STP nivel global

[SwicthX] stp instance [*No. Instancia]* prioridad [*No. De prioridad]*

Configuración de instancia y prioridad STP

[SwicthX] stp [enable | disable]

Habilitar protocolo STP

[SwicthX] display stp [instance id | brief]

Despliegue de propiedades del protocolo stp

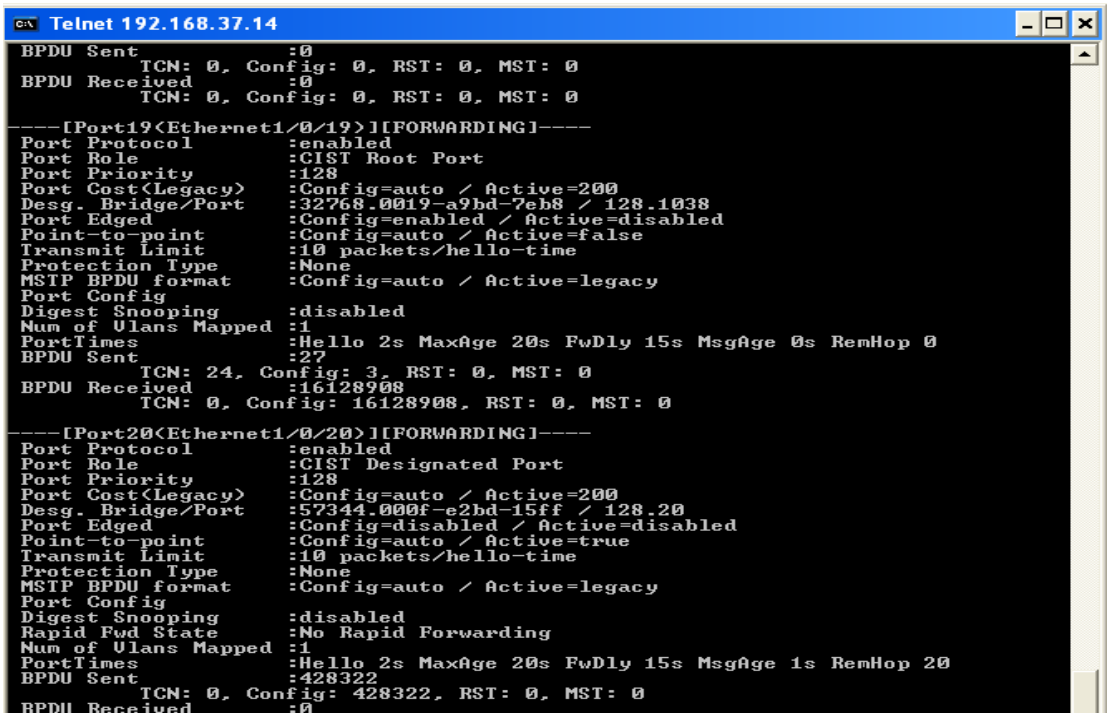

Figura 4.17 Ejemplo de despliegue de propiedades del protocolo Spanning Tree

4.2.8 Tabla de trayectoria de costos STP de acuerdo a especificaciones de IEEE

Velocidad del link	Costo (Especificación IEEE)	Costo (Especificación previa de IEEE)
10 Gb/s	2	1
1 Gb/s	4	1
100 Mb/s	19	10
10 Mb/s	100	100

Figura 4.18 Trayectoria de costos de protocolo STP [23]

[23] *Fuente*: CISCO, Inc. 2010.

4.3 Implementando VRRP (Virtual Router Redundancy Protocol)

4.3.1 Funcionamiento de protocolo VRRP

VRRP (Virtual Router Redundancy Protocol, por sus siglas en inglés), es un protocolo de respaldo redundante que aplica a redes LAN que soportan multicast o broadcast, como Ethernet. El protocolo organiza a varios dispositivos de una LAN, sobre un dispositivo virtual, llamado grupo de respaldo. En el grupo de respaldo, solamente un router se encuentra en estado activo, el cual es llamado router maestro. Los otros routers se encuentran en estado de monitoreo, y están listos para tomar el tráfico de datos, en caso de que se pierda la comunicación con el router de mayor prioridad o maestro. Estos dispositivos inactivos son llamados routers de respaldo.

En el grupo de respaldo de VRRP, cada dispositivo miembro tiene un valor de prioridad en el rango de 1 a 255. El VRRP determina el estado de cada dispositivo miembro de acuerdo a su prioridad. El dispositivo con mayor prioridad es el dispositivo maestro. La figura 4.19 muestra un grupo de respaldo compuesto de 3 routers.

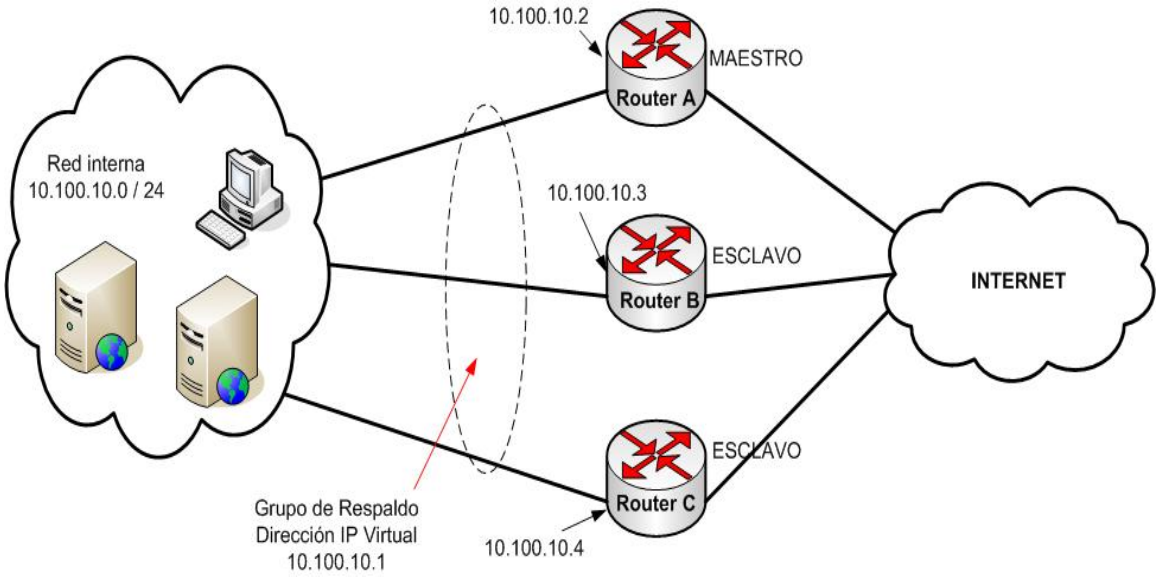

Figura 4.19 Implementación de VRRP [24]

[24] Diagrama reproducido de Huawei Technologies Co, Ltd., "*Quidway Session Engine 2300 Session Boarder Controller V200R005*", Shenzhen CHINA, VRRP principles.

Los routers A, B y C componen el grupo de respaldo (actúan como grupo de routers virtuales), en el cual la dirección IP virtual es 10.100.10.1. El router A es el maestro con la dirección IP 10.100.10.2. Los routers B y C son respaldos con las direcciones 10.100.10.3 y 10.100.10.4, respectivamente. Con el protocolo VRRP solo el router maestro puede re-enviar paquetes que toman la dirección IP virtual como siguiente espera.

Todas las computadoras o servidores de una red interna solo conocen la dirección IP virtual 10.100.10.1, en vez de la dirección IP del router Maestro o Esclavo. Así, cada computadora tiene configurada como ruta de salida la dirección IP virtual. De ésta forma, todas las computadoras o servidores de la red interna pueden comunicarse con redes externas a través del grupo de respaldo.

El modulo de VRRP en el router maestro monitorea el estado de la configuración de la interfaz física del VRRP, y envía paquetes de notificación a los routers de respaldo en forma de multicast.

Cuando el router maestro no recibe notificación de paquetes VRRP en un intervalo de tiempo en específico (falla en la interfaz física o enlace), el router de respaldo con la mayor prioridad cambiará a estado de router maestro. De ésta forma, los servicios que estaban corriendo en el router maestro, continuarán generándose en el nuevo router maestro. Como resultado de ello, el VRRP habilita la comunicación de servicios de forma in-interrumpida y asegura de forma fiable los mismos.

Cabe señalar que el VRRP se habilita entre dos o más IPs físicas y una IP virtual, la cual actúa como gateway para los demás dispositivos que se encuentran conectados a la LAN.

4.3.2 Comandos de implementación de VRRP

COMANDOS DE IMPLEMENTACIÓN DE PROTOCOLO VRRP

<SwitchX> system-view

Acceso a modo de configuración

[SwicthX] interface vlan-interface [*No. de VLAN*]

Acceso a VLAN con características de capa 3

[SwicthX] ip address [*dirección Ip*][*Máscara de red*]

Configuración de ip física sobre VLAN

[SwicthX] vrrp vrid [*id de proceso*] virtual-ip [*dirección IP virtual*]

Identificador de proceso VRRP y configuración de IP virtual sobre la intefaz física.

[SwicthX] vrrp vrid [*id de proceso*] prioridad [0 (menor) – 255 (mayor)]

Configuración de prioridad de protocolo VRRP

4.4 Implementando OSPF (Open Shortest Path First)

Open Shortest Path First (OSPF), es un protocolo utilizado dentro de redes de sistemas autónomos pertenecientes a los protocolos de ruteo por distancia de vectores. OSPF es designado por IETF (Internet Engineering Task Force, como uno de los principales IGPs (Interior Gateway Protocols)). Debido a que OSPF es un protocolo estándar ampliamente conocido, el conocimiento de su mantenimiento y configuración es esencial.

OSPF es un protocolo de estado-enlace entre dos routers. Se puede pensar como enlace en una interfaz sobre un router. El estado-enlace es una descripción de la interfaz y su relación con los routers vecinos. Una descripción de un enlace incluiría, por ejemplo, la dirección IP de la interfaz, la máscara de red, el tipo de red a la cual se encuentra conectada, los routers que están conectados a la red, etc. La colección de todos estos estados-enlaces forma una base de datos de los estados-enlace.

Un router envía paquetes de los estados del enlace (LSA), para advertir periódicamente (cada 30 minutos) e inmediatamente cuando el estado del router cambia. La información relacionada con: las interfases, métricas usadas, y otras variables son incluidas en los paquetes de LSAs. Debido a que los routers con OSPF almacenan información acumulada del estado de los enlaces, utilizan el algoritmo de SPF (Shortest Path First), para calcular la trayectoria más corta hacia cada nodo.

Una base de datos topológica (estado-enlace) es, una imagen total de las redes en relación a los routers. La base de datos topológica contiene la colección de LSAs recibidos de todos los routers en la misma área. Debido a que los routers, dentro de una misma área comparten la misma información, contienen bases de datos topológicas idénticas.

4.4.1 Jerarquía de OSPF

OSPF utiliza dos capas de redes jerárquicas. Existen dos elementos primarios en las dos capas de redes jerárquicas:

- **Área:** Un área es un grupo de redes contiguas. Las áreas son subdivisiones lógicas de sistemas autónomos.
- **Sistema Autónomo:** Un sistema autónomo consiste en una colección de redes con administración común las cuales comparten estrategias comunes de ruteo. Un sistema autónomo, algunas veces llamado dominio, pude ser lógicamente subdividido en múltiples áreas.

Dentro de un sistema autónomo, un backbone contiguo debe de ser definido. Todas las áreas restantes, no backbone, se encuentran conectadas fuera del área backbone.

El área de backbone es el área de transición porque todas las demás áreas se comunican a través de ella. Por OSPF, las áreas de no backbone pueden ser, adicionalmente, como áreas de stub (áreas con un solo enlace al área de backbone), con el fin de ayudar a reducir la base de datos de los enlace-estados y el tamaño de las tablas de ruteo.

Los routers que operan dentro de las dos capas de redes jerárquicas tienen diferentes entidades de ruteo y diferentes funciones en OSPF.

Las siguientes premisas se encuentran basadas en la figura 4.20:

- Router B es el router del backbone. El router del backbone provee conectividad entre las diferentes áreas.
- Los routers C, D y E son los routers frontera de cada área (ABR, Router Frontera de Área). Los ABRs mantienen la comunicación con los routers de su área y el router backbone, mantienen separadas las bases de datos de los estados-enlace, para cada una de las áreas a las que están conectadas, y rutean el tráfico destinado a otros áreas o tráfico de llegada al área perteneciente.
- Los routers F, G y H son routers no backbone. Los routers nonbackbone, son los routers que están conscientes de la topología dentro de sus respectivas áreas y mantienen las

bases de datos de los estados-enlaces de las áreas.

- Dependiendo de la configuración de las áreas no backbone de OSPF (áreas stub), los routers que se encuentran en otro dominio se comunican con los routers frontera a través de rutas por default, con el fin de intercambiar paquetes de tráfico.
- El router A es el router frontera del sistema autónomo (ASBR, Autonomous System Boundary Router), el cual se conecta con un dominio externo, o sistema autónomo.
- Router I, es un router que pertenece a otro dominio de ruteo, o sistema autónomo.

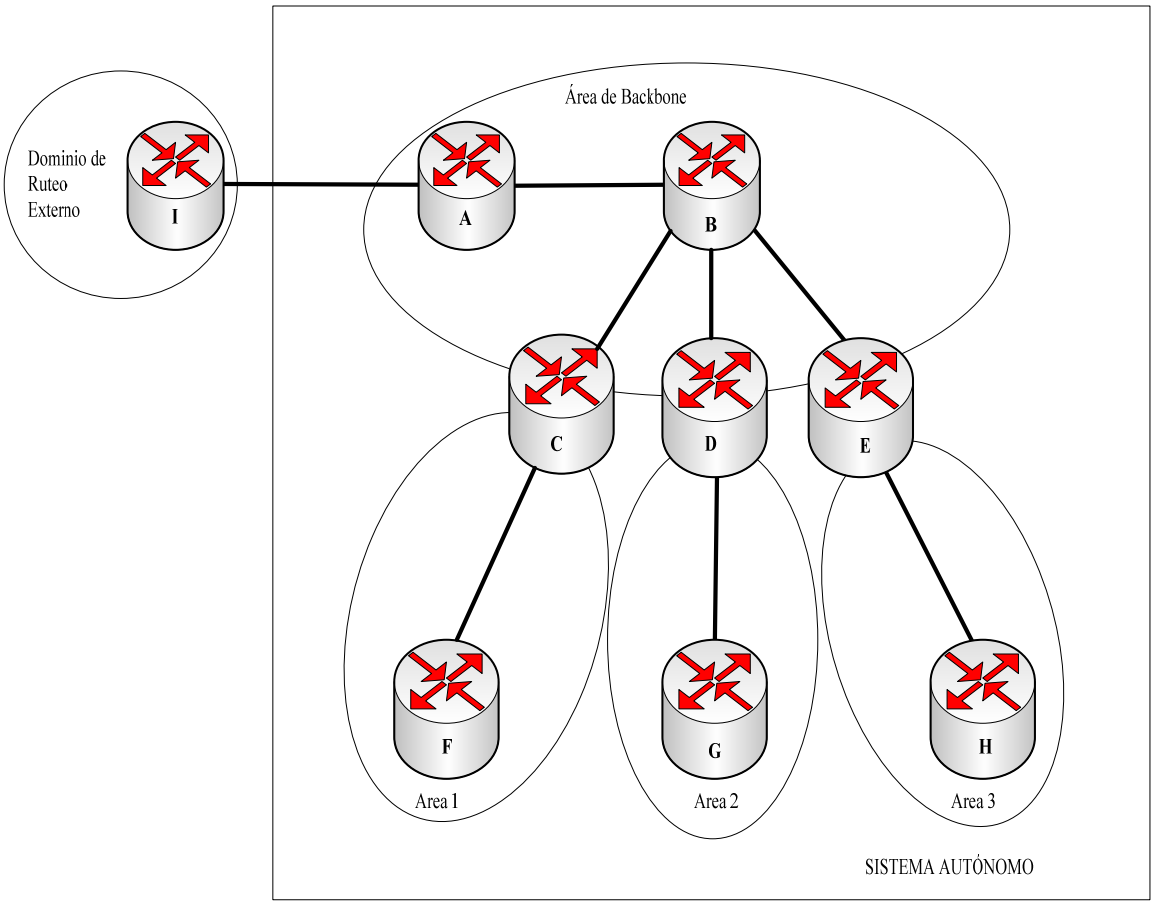

Figura 4.20 Jerarquía de OSPF [25]

[25] Diagrama reproducido de CISCO Systems Inc. "*Interconnecting Cisco Networking Devices Part 2*", San Jose USA, OSPF Operation, 2007.

4.4.2 Estableciendo adyacencias con los vecinos de OSPF

Los routers deben de reconocer cualquier otro router vecino de la red, antes de poder intercambiar información, debido a que el ruteo de OSPF depende del status del link entre ambos routers. Éste proceso es realizado, utilizando el protocolo de Hello. El protocolo de Hello establece y mantiene negociaciones con los router vecinos, asegurando comunicación bi-direccional entre ellos. La comunicación bi-direccional ocurre cuando los routers se reconocen entre ellos mismos al recibir los paquetes de hello de sus vecinos.

Cada interfaz que se encuentra participando en OSPF utiliza una dirección IP de Multicast 224.0.0.5, para que periódicamente mande paquetes de Hello. Un paquete de Hello contiene la siguiente información:

- **Router ID:** El ID de router es un número de 32 bits que identifica de manera única al router. La dirección IP más alta sobre una interfaz activa es elegida por default, a menos que una interfaz loopback o el router ID sea configurado; por ejemplo, la dirección IP 172.16.12.1 sería elegida en vez de 172.16.1.1. Está identificación es importante al establecer y manejar problemas con los routers vecinos, además de coordinar el intercambio de rutas.
- **Intervalos de paquetes de hello:** El intervalo de hello especifica la frecuencia en segundos, en la cual un router envía los paquetes de hello. Los intervalos de hello en redes de multiacceso es de 10 segundos. El intervalo de fuera de servicio del paquete (dead interval), es el tiempo en segundos en el que un router espera para escuchar al router vecino antes de declarar que el router vecino está fuera de servicio. Por default el intervalo de fuera de servicio es cuatro veces el intervalo de hello. Estos intervalos deben de ser los mismos sobre los routers vecinos; de otra forma, la adyacencia entre ellos no será establecida.
- **Routers vecinos:** El campo de routers vecinos lista los routers adyacentes al mismo, estableciendo comunicación bidireccional. La comunicación bidireccional se indica cuando el router se reconoce así mismo en la lista del campo de routers vecinos de los paquetes hello que recibe de los diferentes routers vecinos.

- **Área ID:** Para que dos routers se puedan comunicar deben de compartir un segmento

común y sus interfases deberán de pertenecer al mismo segmento del área OSPF. Los vecinos deberán de compartir la misma máscara y subred. Los routers tendrán la misma información del estado-enlace.

- **Prioridad del Router**: La prioridad del router es un número de 8 bits el cual indica la prioridad del mismo. OSPF utiliza la prioridad para seleccionar el router designado (DR) y el router backup (BDR).}
- **dirección IP del DR (Router designado) y BDR (Respaldo de Router designado)**: Estas son las direcciones IP de los DR y BDR de una red específica.
- **Contraseña de autenticación**: Si el router tiene habilitada la función de autenticación, ambos routers deberán de intercambiar la misma contraseña. La autenticación no es requerida, pero si es habilitada, ambos routers deberán de tener la misma contraseña.
- **Bandera de áreas stub**: Un área stub es un área especial. Ambos routers deberán de estar de acuerdo en la bandera del área de stub dentro de los paquetes de hello. Designar un área de stub es una técnica que reduce actualizaciones en la tabla de ruteo, re-emplazándolas por una ruta por default.

4.4.3 Comandos de implementación de Protocolo OSPF

COMANDOS DE IMPLEMENTACIÓN DE PROCESO OSPF

<SwitchX> system-view

Acceso a modo de configuración

[SwicthX] ospf [*id de proceso*]

Configuración de identificador de proceso OSPF

[SwicthX] preference [*id. de router]*

Configuración de id de router

[SwicthX] area [*id de área*]

Identificación de área asociada al proceso de OSPF

[SwicthX] network [*address*] [*wild card mask*]

Configuración de las redes IP que forman parte del proceso de OSPF

[SwicthX] display ospf peer

Despliegue de propiedades de protocolo OSPF

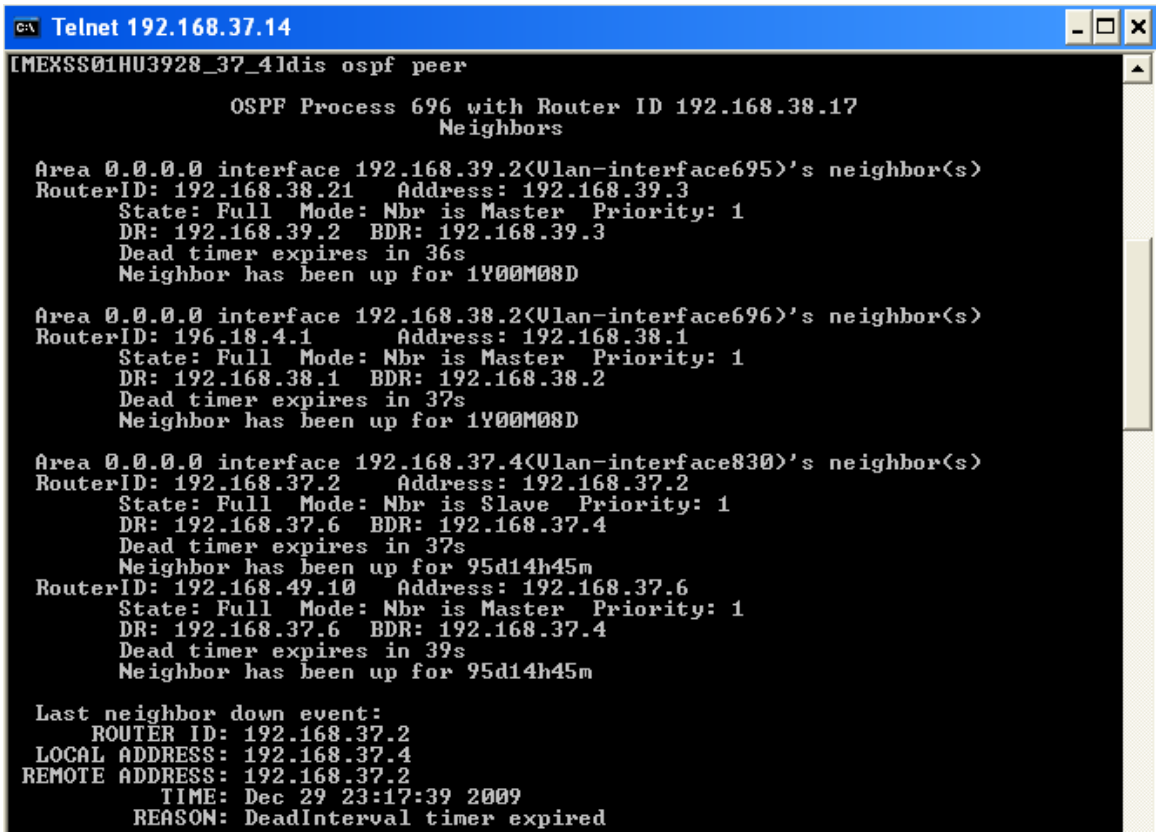

Figura 4.21 Ejemplo de despliegue de propiedades del protocolo OSPF

CAPÍTULO 5. Confiabilidad, Ruteo y Acceso IP

Las redes IP deben tener alto nivel de confiabilidad y disponibilidad para soportar todos los servicios. La confiabilidad de la red depende de múltiples factores, generalmente incluye la confiabilidad del equipo, redundancia en el diseño, disponibilidad de links y mecanismos de protección del diseño del direccionamiento. La robustez de la red puede ser optimizada por las características de software y hardware, y por el diseño de protocolos de ruteo dinámicos.

5.1 Diseño y configuración de red de tráfico de voz

5.1.1 Diseño de red de tráfico de voz

Para lograr la comunicación de voz entre las diferentes ciudades es necesario contar con dispositivos de red capaces de transportar el tráfico entre ellas. Los MGWs, realizan la conversión de los paquetes de datos de TDM a IP, y trasladan la información hacia las diferentes ciudades a través de routers.

Como se ilustra en la figura 5.1, con el fin de mantener una topología con alta disponibilidad de links, se cuenta con un enlace activo y un enlace de respaldo en la parte de transmisión, de los MGW y de los routers. Así, en el momento en que un equipo o enlace llegaran a tener problemas, los equipos realizarían la conmutación entre sus tarjetas y no habría pérdidas de datos de voz, con lo cual estaríamos asegurando la garantía de servicio en los usuarios.

En la figura 5.1, se muestra a detalle el diseño de la red de tráfico de voz.

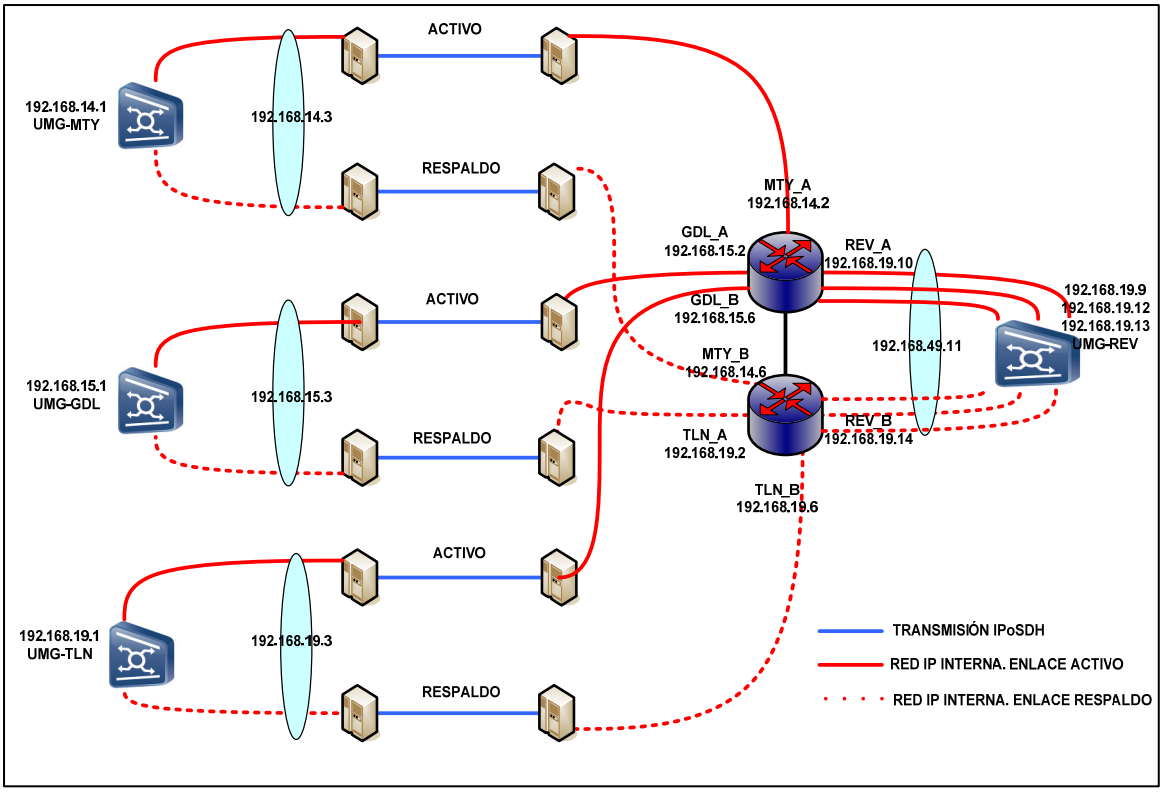

Figura 5.1 Topología de red de tráfico de voz [26]

[26] Diagrama realizado por el propio autor Raúl Gualito Olea.

La construcción de la red facilita la futura expansión, debido a que los servicios de acceso son independientes uno de otro (Voz, señalización, gestión).

5.1.2 Direccionamiento IP para tráfico de voz

Durante el diseño de la red de tráfico de voz es necesario tomar en cuenta el direccionamiento IP, el cual es esencial para lograr una buena configuración entre los dispositivos involucrados. Juega un papel importante definir el número de IPs, VLANs, número de interfases, y número de equipos a interconectar.

Para lograr la comunicación entre los diferentes MGW, se utilizan diferentes VLANs, y se configuran VRRPs entre los routers. Los MGWs apuntan a los VRRPs y a través de comunicación entre VLAN´s y diferentes protocolos de ruteo se permite la comunicación entre ellos. Se implementa el protocolo STP, para eliminar cualquier loop que se pudiera presentar en el diseño de la red.

El MGW contiene una par de tarjetas (Activa / Stand by) llamadas HRUs (High-speed Routing Unit), quienes son las encargadas de transmitir los paquetes IP hacia la red interna. Las tarjetas HRUs cuentan con 8 puertos de transmisión de datos de 100 Mbps, por tanto son capaces de soportar hasta 800 Mbps de transmisión de datos IP, en configuración de carga balanceada.

Basados en la cantidad total de ancho de banda de tráfico de voz por ciudad (Véase tabla 3.5 “Total de Ancho de Banda de voz por ciudad”) los enlaces entre Guadalajara, Monterrey, y Tlalnepantla (sitios remotos) con Revolución, no superan los 100 Mbps. Por lo cual, la cantidad de enlaces entre los sitios remotos con el sitio de Revolución solo cuenta con una sola conexión. En el caso del sitio de Revolución, debido a que recibe el tráfico de todos los sitios remotos, la cantidad de conexiones del router al MGW es de tres.

Cada interfaz de cada MGW requiere de una dirección IP y de un gateway (VRRP) para comunicación con los diversos mercados. Se recomienda mantener a cada sitio involucrado en un segmento de red diferente, y por tanto en una VLAN diferente. Es

importante contar con un segmento de red clase C y realizar el subneteo pertinente para lograr la segmentación correspondiente.

Cada sitio remoto (Monterrey, Guadalajara, Tlalnepantla) requiere de al menos 4 IPs, las cuales se encuentran distribuidas de la siguiente manera:

- 1 IP física perteneciente a la interfaz de la HRU del MGW.
- 2 IPs físicas pertenecientes a la configuración del VRRP en los routers.
- 1 IP lógica para la configuración del gateway.

En el caso del sitio de Revolución, la cantidad de IPs necesarias es de al menos 6, las cuales se encuentran distribuidas de la siguiente manera:

- 3 IPs físicas pertenecientes a las interfases de la tarjeta HRU del MGW.
- 2 IPs físicas pertenecientes a la configuración del VRRP en los routers.
- 1 IP lógica para la configuración del gateway.

Basados en la cantidad de IPs a utilizar y por cuestiones de seguridad, es necesario contar con un segmento de red clase C con máscara de red /29 (255.255.255.248) para cada sitio, lo cual permite la ocupación de 6 direcciones IPs para hosts, y mantiene el ahorro de direcciones IPs privadas a la operadora móvil.

Con base a lo anterior, se han asignado los siguientes segmentos de red, y sus respectivas VLANs **:

- Monterrey | Red: 192.168.14.0; Máscara: 255.255.255.248 | VLAN 665.
- Guadalajara | Red: 192.168.15.0; Máscara: 255.255.255.248 | VLAN 670.
- Tlalnepantla | Red: 192.168.19.0; Máscara: 255.255.255.248 | VLAN 691.
- Revolución | Red: 192.168.19.8; Máscara: 255.255.255.248 | VLAN 690.

** NOTA: Por cuestiones de seguridad las IPs mostradas han sido modificadas y no pertenecen al segmento real de la red implementada.

En la tabla 5.1 se muestra el direccionamiento IP adecuado para la red de voz.

PLAN IP TLALNEPANTLA

Comunicación entre MGWs. Tráfico de voz					
MGW IP	IPs para configuración de VRRP en router	Gateway IP	Máscara de red	VLAN	Red
Interfaz0: 192.168.19.1	192.168.19.2 192.168.19.6	192.168.19.3	255.255.255.248	VLAN 691	192.168.19.0

PLAN IP REVOLUCIÓN

Comunicación entre MGWs. Tráfico de voz					
MGW IP	IPs para configuración de VRRP en router	Gateway IP	Máscara de red	VLAN	Red
Interfaz0: 192.168.19.9 **Interfaz1:** 192.168.19.12 **Interfaz2:** 192.168.19.13	192.168.19.10 192.168.19.14	192.168.19.11	255.255.255.248	VLAN 690	192.168.19.8

PLAN IP MONTERREY

Comunicación entre MGWs. Tráfico de voz					
MGW IP	IPs para configuración de VRRP en router	Gateway IP	Máscara de red	VLAN	Red
Interfaz0: 192.168.14.1	192.168.14.2 192.168.14.6	192.168.14.3	255.255.255.248	VLAN 665	192.168.14.0

PLAN IP GUADALAJARA

Comunicación entre MGWs. Tráfico de voz					
MGW IP	IPs para configuración de VRRP en router	Gateway IP	Máscara de red	VLAN	Red
Interfaz0: 192.168.15.1	192.168.15.2 192.168.15.6	192.168.15.3	255.255.255.248	VLAN 670	192.168.15.0

Tabla 5.1 Direccionamiento IP para tráfico de voz

5.1.3 Configuración en Routers

Una vez completado el direccionamiento IP, y la topología de red de tráfico de voz, se procede con la configuración de los equipos.

En las siguientes tablas se muestra a detalle la configuración del router maestro tomando en cuenta el direccionamiento IP mostrado en la tabla 5.1.

Descripción de comandos	**Comando**
Configuración de función FTP (File Transfer Protocol) entre Router y servidores MSC y MGW	FTP enable
Función que verifica la temperatura límite del router en °C. (grados celsius)	lpu temperature-limit 4 60
Vlans configuradas en el router	Vlan batch 665 670 690 to 691 830
Configuración de función STP a nivel global, instancia de mayor prioridad	stp mode stp stp instance 0 priority 49152 stp enable
Interfaz configurada por default en routers	interface Aux0/0/1 async mode flow undo shutdown
Crear VLAN 665	interface Vlanif665
Descripción de VLAN Enlace de Tráfico a la Cd. De Monterrey	description LINK HACIA MTY-MGW TRÁFICO
Configuración de protocolo VRRP. IP física	ip address 192.168.14.2 255.255.255.248
Configuración de protocolo VRRP. IP virtual	vrrp vrid 65 virtual-ip 192.168.14.3
Configuración de prioridad sobre protocolo VRRP	vrrp vrid 65 priority 120
Encender VLAN 665	undo shutdown
Configuración de VLAN 670	interface Vlanif670

Tabla 5.2 Configuración en routers de tráfico de voz

Descripción de comandos	Comando
Descripción de VLAN Enlace de Tráfico a la Cd. De Guadalajara	description LINK HACIA GDL-MGW TRÁFICO
Configuración de protocolo VRRP. IP física	ip address 192.168.15.2 255.255.255.248
Configuración de protocolo VRRP. IP virtual	vrrp vrid 70 virtual-ip 192.168.15.3
Configuración de prioridad sobre protocolo VRRP	vrrp vrid 70 priority 120
Encender VLAN 670	undo shutdown
Configuración de VLAN 690	interface Vlanif690
Descripción de VLAN Enlace de Tráfico al Sitio Revolución (Cd. De México).	description LINK HACIA REV-MGW TRÁFICO
Configuración de protocolo VRRP. IP física	ip address 192.168.19.10 255.255.255.248
Configuración de protocolo VRRP. IP virtual	vrrp vrid 90 virtual-ip 192.168.19.11
Configuración de prioridad sobre protocolo VRRP	vrrp vrid 90 priority 120
Encender VLAN 690	undo shutdown
Configuración de VLAN 691	interface Vlanif691
Descripción de VLAN Enlace de Tráfico al Sitio Tlalnepantla (Cd. De México)	description LINK HACIA TLN-MGW TRÁFICO
Configuración de protocolo VRRP. IP física	ip address 192.168.19.2 255.255.255.248
Configuración de protocolo VRRP. IP virtual	vrrp vrid 90 virtual-ip 192.168.19.11
Configuración de prioridad sobre protocolo VRRP	vrrp vrid 90 priority 120
Encender VLAN 691	undo shutdown
Configuración de VLAN 830	interface Vlanif830
Enlace de O&M, para gestión del router.	description O&M VLAN
Encender VLAN 830	undo shutdown
Configuración de IP de O&M del router	ip address 192.168.17.6 255.255.255.0

Tabla 5.2 Configuración en routers de tráfico de voz

Descripción de comandos	Comando
Configuración de troncal entre ambos routers (maestro y esclavo)	interface Eth-Trunk0
Descripción de enlace con router esclavo	description LINK hacia ROUTER ESCLAVO
Configuración de puerto con tráfico taggeado Comunicación de vlans entre ambos routers	port trunk allow-pass vlan 665 670 690 to 691 830
Protección para evitar loops entre ambos routers	stp loop-protection
Configuración de puerto 4/0/0	interface Ethernet4/0/0
Descripción de puerto Enlace a Lan switch de O&M	description LINK HACIA Lan switch de O&M.
Ligado de puerto 4/0/0 a VLAN de O&M	portswitch vlan 830
Configuración de puerto 4/0/1	interface Ethernet4/0/1
Descripción de puerto Enlace de O&M a MGW Revolución	description LINK HACIA tarjeta de O&M de REV-MGW.
Ligado de puerto 4/0/1 a VLAN 830 de O&M	Portswitch VLAN 830
Configuración de puerto 4/0/2	Interface Ethernet4/0/2
Descripción de puerto Enlace de tráfico a MGW Revolución._1	description LINK HACIA tarjetas de tráfico REV-MGW_01
Ligado de puerto 4/0/2 a VLAN 690 de Tráfico	Portswitch vlan 690
Configuración de puerto 4/0/3	Interface Ethernet4/0/3
Descripción de puerto Enlace de tráfico a MGW Revolución_2	description LINK HACIA tarjetas de tráfico REV-MGW_02
Ligado de puerto 4/0/3 a VLAN 690 de Tráfico	Portswitch vlan 690
configuración de puerto 4/0/4	Interface Ethernet4/0/3
Enlace de tráfico a MGW Revolución_3	description LINK HACIA tarjetas de tráfico REV-MGW_03
Ligado de puerto 4/0/4 a VLAN 690 de Tráfico	Portswitch vlan 690
Configuración de puerto 4/0/5	interface Ethernet4/0/5
Descripción de puerto Enlace de tráfico a MGW Tlalnepantla	description LINK HACIA tarjetas de tráfico TLN-MGW_01
Ligado de puerto 4/0/5 a VLAN 691 de Tráfico	Portswitch vlan 691
Configuración de puerto 4/0/7	interface Ethernet4/0/7

Tabla 5.2 Configuración en routers de tráfico de voz

Descripción de comandos	Comando
Descripción de puerto Enlace de tráfico a MGW Guadalajara	description LINK HACIA tarjetas de trafico GDL-MGW_01
Ligado de puerto 4/0/7 a VLAN 670 de Tráfico	portswitch vlan 670
Configuración de puerto 4/0/9	interface Ethernet4/0/9
Enlace de tráfico a MGW Monterrey	description LINK HACIA tarjetas de tráfico MTY-MGW_01
Ligado de puerto 4/0/9 a VLAN 665 de Tráfico	portswitch vlan 665
Configuración de puerto 4/0/14	interface Ethernet4/0/14
Enlace de troncal con Router B. Redundancia de tráfico entre ambos routers	description LINK HACIA ROUTER ESCLAVO PARA REDUNDANCIA DE TRÁFICO
Ligado de puerto físico 4/0/14 a la troncal entre ambos routers (arriba definida como eth-trunk 0)	Eth-trunk 0
Habilitar sesión de consola a través de puerto serial	User-interface aux 0
Habilitar 2 sesiones de TELNET, hacia el dispositivo	User-interface vty 0 1
Usuarios con privilegios de administrador	user privilege level 3
Configuración de password no encriptado	set authentication password simple router A
Solicitar password al momento de ingresar al router	Authentication-mode password

Tabla 5.2 Configuración en routers de tráfico de voz

5.2 Diseño y configuración de red de tráfico de gestión

5.2.1 Diseño de red de tráfico de gestión

La red de gestión mantiene todos los elementos de red de forma centralizada. Es decir, todos los MGWs, MSC, routers, switches de señalización se conectan a los switches de gestión ubicados en Tlalnepantla. Véase figura 5.2.

NEXTEL de México proporciona los enlaces de comunicación de Guadalajara, Monterrey y Revolución hacia Tlalnepantla a través de tarjetas de comunicación ESU (Tellabs). La red de gestión considera, de igual forma que la red de tráfico de voz, alta disponibilidad entre enlaces lógicos y físicos, con lo cual se asegura que siempre se mantenga el monitoreo de los equipos. La figura 5.2 muestra la topología de red de operación y mantenimiento.

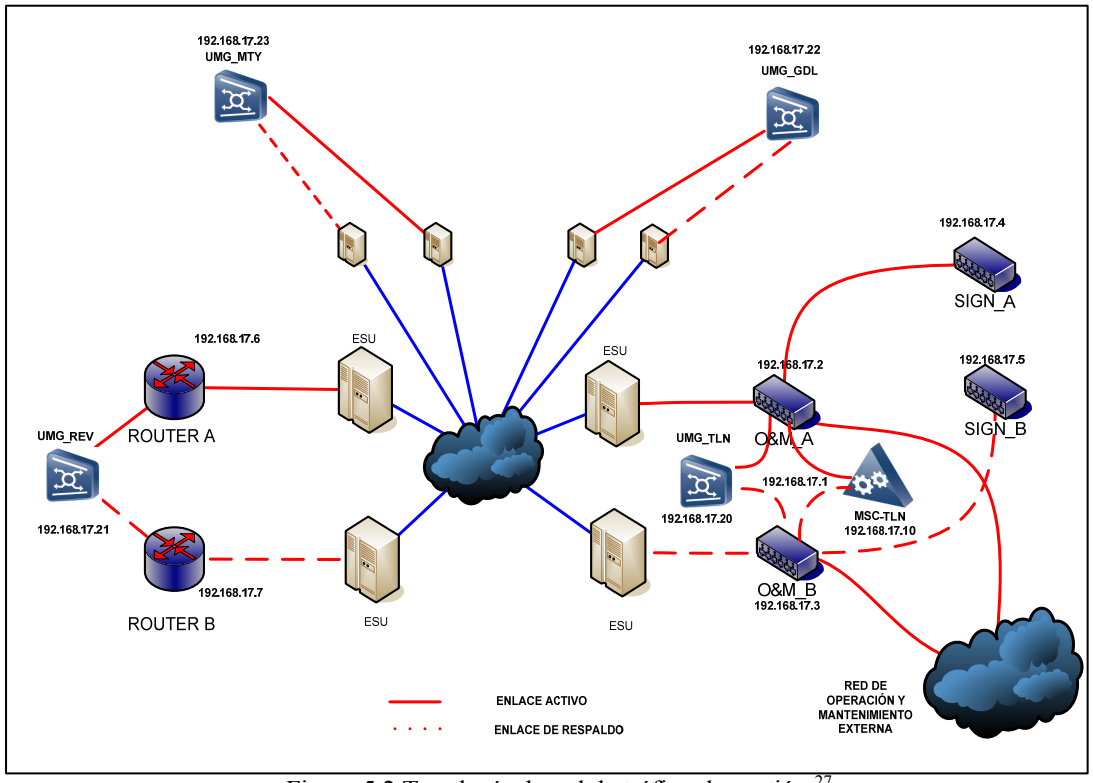

Figura 5.2 Topología de red de tráfico de gestión [27]

[27] Diagrama realizado por el propio autor Raúl Gualito Olea.

5.2.2 Direccionamiento IP para tráfico de gestión

La red de tráfico de gestión requiere de una correcta planeación de IPs en donde se encuentren todos los elementos de red en cuestión.

El MGW, al igual que el MSC contienen una par de tarjetas (Activa / Stand by) llamadas OMUs (Operation-Maintenance Unit), quienes son las encargadas de administrar y permitir el mantenimiento de todas sus tarjetas internas.

En el caso de los routers de tráfico y switches de señalización se dispone de una VLAN exclusivamente dedicada a operación y mantenimiento.

A continuación se listan todos los elementos que forman parte de la red:

- Lan Switch-A O&M.
- Lan Swicth-B O&M.
- Lan Swicth-A Señalización.
- Lan Swicth-B Señalización.
- MSC.
- IGWA_0 (Servidor de CDRs).
- IGWB_1 (Servidor de CDRs).
- IGWB_VIRTUAL.
- MGW_TLANE.
- Router-A O&M.
- Router-B O&M.
- MGW REV.
- MGW MTY.
- MGW GDL.

Basados en la cantidad de elementos a ser administrados por la red de gestión, se requiere de 19 IPs (14 IPs para cada uno de los equipos involucrados, 4 IPs flotantes y 1 IP lógica para configuración de VRRP). Por lo anterior, es necesario contar con un segmento de red clase C, con máscara de red /27 (255.255.255.224), lo cual permite la ocupación de 30 direcciones IPs para hosts, y mantiene el ahorro de direcciones IPs privadas a la operadora móvil.

En base a lo anterior, se ha asignado el siguiente segmento de red, con su respectiva VLAN:

ASIGNACIÓN IP
OPERACIÓN Y MANTENIMIENTO

Sitios:	Red:	Máscara de red:	VLAN:
Guadalajara Monterrey Tlalnepantla Revolución	192.168.17.0	255.255.255.224	830

** NOTA: Por cuestiones de seguridad las IPs mostradas han sido modificadas y no pertenecen al segmento real de la red implementada.

La tabla 5.3, muestra el direccionamiento IP adecuado para la red de gestión.

SITIO		Rango			
TLANEPANTLA	**Equipos**	**192.168.17.0 -192.168.17.31**	**Máscara de red**	**Gateway**	**VLAN**
TLANEPANTLA	Lan Switch-A O&M	192.168.17.2	255.255.255.224	192.168.17.1	VLAN 830
TLANEPANTLA	Lan Swicth-B O&M	192.168.17.3	255.255.255.224	192.168.17.1	VLAN 830
TLANEPANTLA	Lan Swicth-A Señalización	192.168.17.4	255.255.255.224	192.168.17.1	VLAN 830
TLANEPANTLA	Lan Swicth-B Señalización	192.168.17.5	255.255.255.224	192.168.17.1	VLAN 830
TLANEPANTLA	MSC	192.168.17.6	255.255.255.224	192.168.17.1	VLAN 830
TLANEPANTLA	IGWA_0	192.168.17.11	255.255.255.224	192.168.17.1	VLAN 830
TLANEPANTLA	IGWB_1	192.168.17.12	255.255.255.224	192.168.17.1	VLAN 830
TLANEPANTLA	IGWB_VIRTUAL	192.168.17.13	255.255.255.224	192.168.17.1	VLAN 830
TLANEPANTLA	IP_flotantes	192.168.17.14 - 17	255.255.255.224	192.168.17.1	VLAN 830
TLANEPANTLA	MGW_TLANE	192.168.17.20	255.255.255.224	192.168.17.1	VLAN 830
SITIO		Rango			
REVOLUCIÓN	**Equipos**	**192.168.17.0 -192.168.17.31**	**Máscara de red**	**Gateway**	**VLAN**
REVOLUCIÓN	Router-A O&M	192.168.17.6	255.255.255.224	192.168.17.1	VLAN 830
REVOLUCIÓN	Router-B O&M	192.168.17.7	255.255.255.224	192.168.17.1	VLAN 830
REVOLUCIÓN	MGW REV	192.168.17.21	255.255.255.224	192.168.17.1	VLAN 830
SITIO		Rango			
MONTERREY	**Equipos**	**192.168.17.0 -192.168.17.31**	**Máscara de red**	**Gateway**	**VLAN**
MONTERREY	MGW MONT	192.168.17.23	255.255.255.224	192.168.17.1	VLAN 830
SITIO		Rango			
GUADALAJARA	**Equipos**	**192.168.17.0 -192.168.17.31**	**Máscara de red**	**Gateway**	**VLAN**
GUADALAJARA	MGW GUAD	192.168.17.22	255.255.255.224	192.168.17.1	VLAN 830

Tabla 5.3 Direccionamiento IP para tráfico de operación y mantenimiento

5.2.3 Configuración en Lan switches de Operación y Mantenimiento

Una vez completado el direccionamiento IP, y la topología de red de tráfico de gestión, se procede con la configuración de los equipos.

En las siguientes tablas se muestra a detalle la configuración del lan switch de gestión maestro, el cual toma en cuenta el direccionamiento IP mostrado en la tabla 5.3.

Descripción de comandos	**Comando**
Nombre del sistema	sysname LAN SWITCH_A
Habilitar paquetes ICMP, para poder alcanzar las IPs asignadas a los VRRPs.	vrrp ping-enable
Autenticación simple a usuario switch A, a través de ssh, con privilegios de administrador	local-user switchA
	Password simple switchA
	service-type ssh
	level 3
Habilitar protocolo STP, instancia de mayor prioridad, a nivel global	stp mode stp
	stp instance 0 priority 57344
Habilitar 7 sesiones de consola a través de puerto serial	user-interface aux 0 7
Habilitar 4 sesiones de TELNET, hacia el dispositivo	user-interface vty 0 4
Usuarios con privilegios de administrador	user privilege level 3
Configuración de password de acceso al dispositivo	set authentication password simple switchA
Configuración de Vlan 830 (operación y Mantenimiento)	interface Vlan-interface830
Descripción de VLAN	description O&M VLAN
Configuración de protocolo VRRP. IP física	ip address 192.168.17.2 255.255.255.0

Tabla 5.4 Configuración en lan switches de operación y mantenimiento

Descripción de comandos	Comando
Configuración de protocolo VRRP. IP virtual	vrrp vrid 5 virtual-ip 192.168.17.1 255.255.255.0
configuración de prioridad sobre protocolo VRRP	vrrp vrid 5 priority 120
Acceso a Interfaz Ethernet 1/0/1	interface Ethernet1/0/1
Puerto apagado	Shutdown
Acceso a Interfaz Ethernet 1/0/2	interface Ethernet1/0/2
Descripción de enlace hacia medio de transmisión. A través del enlace se alcanzarán los equipos que se encuentran en los sitios remotos.	description LINK HACIA tarjetas de transmisión de O&M
Puerto configurado con acceso a la vlan 830	portswitch access vlan 830
Configuración de puerto a full duplex, y velocidad de 100 Mbps	duplex full. Speed 100
Acceso a Interfaz Ethernet 1/0/4	interface Ethernet1/0/4
Puerto apagado	Shutdown
Acceso a Interfaz Ethernet 1/0/5	interface Ethernet1/0/5
Puerto apagado	Shutdown
Puerto configurado con acceso a la vlan 830	portswitch access vlan 830
Acceso a Interfaz Ethernet 1/0/6	interface Ethernet1/0/6
Puerto apagado	Shutdown
Puerto configurado con acceso a la vlan 830	portswitch access vlan 830
Acceso a Interfaz Ethernet 1/0/7	interface Ethernet1/0/7
Puerto apagado	Shutdown
Puerto configurado con acceso a la vlan 830	portswitch access vlan 830
Acceso a Interfaz Ethernet 1/0/8	interface Ethernet1/0/8
Puerto apagado	Shutdown

Tabla 5.4 Configuración en lan switches de operación y mantenimiento

Descripción de comandos	Comando
Puerto configurado con acceso a la vlan 830	portswitch access vlan 830
Acceso a Interfaz Ethernet 1/0/9	interface Ethernet1/0/9
Descripción de enlace hacia router cisco	description LINK hacia router cisco_red externa de operación y mantenimiento
Configuración de puerto a tipo troncal.	port link-type trunk
Configuración de troncal para permitir el acceso a la vlan 830. Salida a red externa de O&M	port trunk permit vlan 830
Configuración de puerto a full duplex, y velocidad de 100 Mbps	duplex full. Speed 100
Acceso a Interfaz Ethernet 1/0/10.	interface Ethernet1/0/10
Descripción de enlace hacia tarjeta de gestión del MGW de TLN	description LINK hacia MGW de TLN_O&M
Puerto configurado con acceso a la vlan 830	portswitch access vlan 830
Acceso a Interfaz Ethernet 1/0/11.	interface Ethernet1/0/11
Descripción de enlace hacia servidor IGWb	description LINK hacia IGWb
Puerto configurado con acceso a la vlan 830	portswitch access vlan 830
Acceso a Interfaz Ethernet 1/0/12.	interface Ethernet1/0/12
Descripción de enlace hacia servidor MSC.	description LINK hacia MSC
Puerto configurado con acceso a la vlan 830	portswitch access vlan 830
Puerto de acceso a la VLAN 830. Puerto de mantenimiento	interface Ethernet1/0/13
	portswitch access vlan 830
Puerto de acceso a la VLAN 830. Puerto de mantenimiento.	interface Ethernet1/0/14
	portswitch access vlan 830
Puerto de acceso a la VLAN 830. Puerto de mantenimiento.	interface Ethernet1/0/15
	portswitch access vlan 830

Tabla 5.4 Configuración en lan switches de operación y mantenimiento

Descripción de comandos	Comando
Puerto de acceso a la VLAN 830 Puerto de mantenimiento. Puerto apagado	interface Ethernet1/0/16
	portswitch access vlan 830
Puerto de acceso a la VLAN 830 Puerto de mantenimiento. Puerto apagado	interface Ethernet1/0/17
	Shutdown
	portswitch access vlan 830
Puerto de acceso a la VLAN 830 Puerto de mantenimiento.	interface Ethernet1/0/18
	portswitch access vlan 830
Puerto de acceso a la VLAN 830 Puerto de mantenimiento. Puerto apagado	interface Ethernet1/0/19
	Shutdown
	portswitch access vlan 830
Puerto de acceso a la VLAN 830.Puerto de mantenimiento. Puerto apagado	interface Ethernet1/0/20
	Shutdown
	portswitch access vlan 830
Puerto de acceso a la VLAN 830 Puerto de mantenimiento. Puerto apagado	interface Ethernet1/0/21
	Shutdown
	portswitch access vlan 830
Puerto de acceso a la VLAN 830.Puerto de mantenimiento.	interface Ethernet1/0/22
	portswitch access vlan 830
Acceso a Interfaz Ethernet 1/0/23.	interface Ethernet1/0/23
Descripción de enlace hacia LS de señalización	description LINK hacia Lan switch_A_señalización pto. 1/0/23.
Puerto configurado con acceso a la vlan 830	portswitch access vlan 830
Puertos GE no configurados	interface GigabitEthernet1/1/1
	interface GigabitEthernet1/1/2
	interface GigabitEthernet1/1/3
	interface GigabitEthernet1/1/4
Configuración de ruta estática hacia la red externa de O&M	ip route-static 0.0.0.0 0.0.0.0 192.168.17.253 preference 60

Tabla 5.4 Configuración en lan switches de operación y mantenimiento

5.3 Diseño y configuración de red de tráfico de señalización

5.3.1 Diseño de red de tráfico de señalización

La red de señalización mantiene todos los elementos de red de forma centralizada. Es decir, todos los MGWs y el nuevo MSC, se conectan a los switches de señalización ubicados en Tlalnepantla. Véase figura 5.3.

Como se muestra en la figura 5.3, y al igual que la topología de tráfico de voz y gestión, con el fin de mantener una topología con alta disponibilidad de links, se cuenta con un enlace activo y un enlace de respaldo en la parte de transmisión, de los MGW y de los routers. Así, en el momento en que un equipo o enlace llegaran a tener problemas, los equipos realizarían la conmutación entre sus tarjetas y no habría pérdidas de datos de voz, con lo cual estaríamos asegurando la garantía de servicio en los usuarios.

Para realizar la comunicación entre el nuevo MSC y los diversos MSCs de NEXTEL de México, se encuentra configurado el protocolo OSPF entre los switches de señalización y el switch de NEXTEL de México; a través de ellos se logra la conexión al STP de la operadora móvil, quien realiza las traslaciones necesarias para lograr la comunicación entre los MSCs, y con ello mantener el control de las llamadas.

La figura 5.3 muestra a detalle la topología de red de señalización.

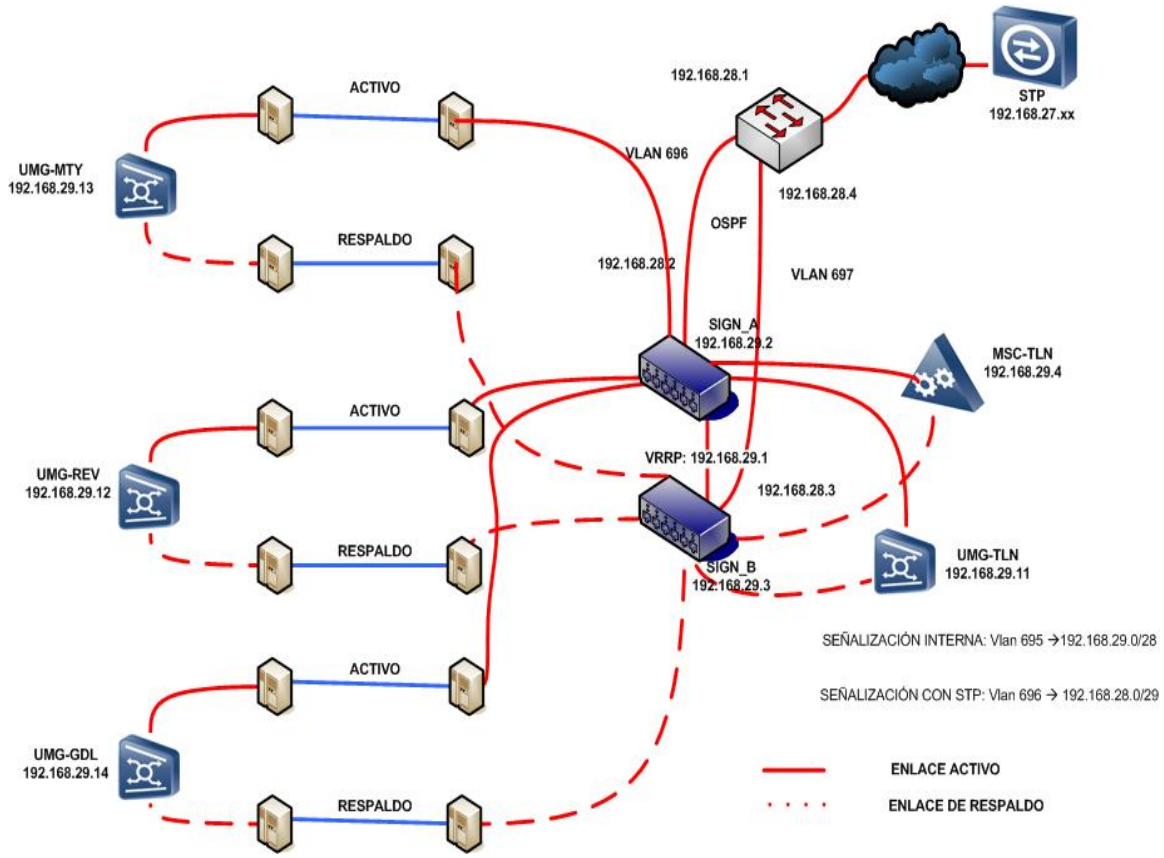

Figura 5.3 Topología de red de tráfico de señalización [28]

[28] Diagrama realizado por el propio autor Raúl Gualito Olea.

5.3.2 Direccionamiento IP para tráfico de señalización

La red de tráfico de señalización es la encargada de realizar el control de las llamadas, por lo cual mantener una comunicación estable entre MGWs, MSCs, STPs es indispensable.

En el caso de la red de señalización, para lograr la comunicación entre los diferentes MGWs, se utiliza una VLAN independiente, y se configuran VRRPs entre los switches de señalización. Los MGWs apuntan a los VRRPs y se permite la comunicación entre ellos. Se implementa el protocolo STP, para eliminar cualquier loop que se pudiera presentar en el diseño de la red.

Los MGWs y el MSC contienen una par de tarjetas (Activa / Stand by) llamadas PPUs (Protocol Processing Unit), quienes son las encargadas de procesar los paquetes de señalización. Las tarjetas PPUs cuentan con 2 puertos de transmisión de datos de 100 Mbps, por tanto son capaces de soportar hasta 200 Mbps de transmisión de datos IP.

Cada interfaz de cada MGW y del MSC requiere de una dirección IP y de un gateway (VRRP) para comunicación con los diversos mercados. Se recomienda mantener a todos los sitios involucrados en un mismo segmento de red. Es importante contar con un segmento de red clase C y realizar el subneteo pertinente para lograr la segmentación correspondiente.

Cada sitio remoto (Revolución, Monterrey, Guadalajara) requiere de al menos 1 IP física perteneciente a la interfaz de la tarjeta PPU del MGW. Todos los MGWs apuntan a un solo VRRP, el cual se encuentra configurado en los switches de señalización.

En el caso del sitio de Tlalnepantla, la cantidad de IPs necesarias es de 5, las cuales se encuentran distribuidas de la siguiente manera:

- 1 IP física perteneciente a la interfaz de la tarjeta PPU del MGW.
- 1 IP física perteneciente a la interfaz de la tarjeta PPU del MSC.
- 2 IPs físicas pertenecientes a la configuración del VRRP en los switches de señalización.
- 1 IP lógica para la configuración del gateway.

Basados en la cantidad de IPs a utilizar (8 IPs de señalización) y considerando la seguridad de la red, es necesario contar con un segmento de red clase C con máscara de red /28 (255.255.255.240), lo cual permite la ocupación de 14 direcciones IPs para hosts, y mantiene el ahorro de direcciones IPs privadas a la operadora móvil. Del mismo modo es indispensable conocer el segmento de red con el cual se tiene la trayectoria hacia los STPs, para considerar la configuración de OSPF.

En base a lo anterior, se ha asignado el siguiente segmento de red, y su respectiva VLANs.

ASIGNACIÓN IP
SEÑALIZACIÓN

Sitios:	Red:	Máscara de red:	VLAN:
Guadalajara Monterrey Tlalnepantla Revolución	192.168.29.0	255.255.255.240	695

ASIGNACIÓN IP
OSPF (Comunicación con STPs)

IPs proceso OSPF	Redes a anunciar	VLAN.
Lanswitch_A: 192.168.28.2 / 29 Lanswitch_B: 192.168.28.3 / 29	192.168.28.0 192.168.29.0	Lanswitch_A: VLAN 696 Lanswitch_B: VLAN 697

** NOTA: Por cuestiones de seguridad las IPs mostradas han sido modificadas y no pertenecen al segmento real de la red implementada.

La tabla 5.5, muestra el direccionamiento IP adecuado para la red de señalización.

PLAN IP TLALNEPANTLA

Comunicación entre MSC y MGWs. Tráfico de Señalización			
MGW, MSC IP	**Gateway & VRRP IPs**	**Máscara de red**	**VLAN**
MSC: 192.168.29.4 MGW: 192.168.29.11	Lanswitch_A: 192.168.29.2 Lanswitch_B: 192.168.29.3 Gateway: 192.168.29.1	255.255.255.240	VLAN 695
IPs para Proceso OSPF	**Redes a anunciar**	**Máscara de red**	**VLAN**
192.168.28.2 (Lanswitch_A)	192.168.28.0	255.255.255.248	VLAN 696
192.168.28.1 (RouterA_salida_STP)	192.168.29.0	255.255.255.248	VLAN 696
192.168.28.3 (Lanswitch_B)	192.168.28.0	255.255.255.248	VLAN 697
192.168.28.4 (RouterB_salida_STP)	192.168.29.0	255.255.255.248	VLAN 697

PLAN IP REVOLUCIÓN

Comunicación entre MSC y MGWs. Tráfico de Señalización			
MGW IP	**Gateway IP**	**Máscara de red**	**VLAN**
192.168.29.12	192.168.29.1	255.255.255.240	VLAN 695

PLAN IP MONTERREY

Comunicación entre MSC y MGWs. Tráfico de Señalización			
MGW IP	**Gateway IP**	**Máscara de red**	**VLAN**
192.168.29.13	192.168.29.1	255.255.255.240	VLAN 695

PLAN IP GUADALAJARA

Comunicación entre MSC y MGWs. Tráfico de Señalización			
MGW IP	**Gateway IP**	**Máscara de red**	**VLAN**
192.168.29.14	192.168.29.1	255.255.255.240	VLAN 695

Tabla 5.5 Direccionamiento IP para tráfico de señalización

5.3.3 Configuración en Lan switches de señalización

Una vez completado el direccionamiento IP, y la topología de red de tráfico de señalización, se procede con la configuración de los equipos.

En las siguientes tablas se muestra a detalle la configuración del lan switch de señalización maestro, el cual toma en cuenta el direccionamiento IP mostrado en la tabla 5.5.

Descripción de comandos	**Comando**
Nombre del sistema	sysname LAN SWITCH_A
Habilitar paquetes ICMP, para poder alcanzar las IPs asignadas a los VRRPs	vrrp ping-enable
Autenticación simple a usuario control_A, a través de ssh Usuario con privilegios de administrador	local-user switchA
	password simple control
	service-type ssh
	level 3
Habilitar protocolo STP, de manera global en el switch (instancia de mayor prioridad)	stp mode stp
	stp instance 0 priority 57344
Habilitar 7 sesiones de consola a través de puerto serial	user-interface aux 0 7
Habilitar 4 sesiones de TELNET, hacia el dispositivo	user-interface vty 0 4
Usuarios con privilegios de administrador	user privilege level 3
Configuración de password de acceso al dispositivo	set authentication password simple control_A
Configuración de Vlan 10	Interface Vlan-interface10
Descripción de VLAN. interconexión de elementos para señalización interna del MSC	Description interconexión_señalización_interna
Configuración de IP para señalización interna	ip address 130.1.2.3 255.255.255.0
Configuración de Vlan 695	Interface Vlan-interface695

Tabla 5.6 Configuración en lan switches de señalización

Descripción de comandos	**Comando**
Descripción de VLAN. VLAN para comunicación de señalización H.248 entre MGWs y MSC	description vlan para comunicación entre MSC y MGWs.
Configuración de protocolo VRRP. IP física	ip address 192.168.29.2 255.255.255.0
Configuración de protocolo VRRP. IP virtual	vrrp vrid 6 virtual-ip 192.168.29.1
Configuración de prioridad sobre protocolo VRRP	vrrp vrid 6 priority 120
Configuración de Vlan 696	Interface Vlan-interface696
Descripción de VLAN Configuración de OSPF con router_A para comunicación con STP	description OSPF_para_conexión_con STPs
Configuración de IP para configurar OSPF con router_A	ip address 192.168.28.2 255.255.255.248
Configuración de Vlan 830	Interface Vlan-interface830
Descripción de Puerto Configuración de O&M LS_control_A	description O&M VLAN
Configuración de IP de O&M de LS	ip address 192.168.17.4 255.255.255.0
Acceso a interfaz Ethernet 1/0/1	Interface Ethernet1/0/1
Descripción de Puerto Conexión hacia servidor MSC	description LINK hacia servidor MSC.
Descripción de Puerto Puerto configurado con acceso a la VLAN 10	portswitch access vlan 10
Acceso a interfaz Ethernet 1/0/2	Interface Ethernet1/0/2
Descripción de Puerto Conexión a tarjetas de señalización interna	description LINK hacia tarjeta de señalización interna
Puerto configurado con acceso a la VLAN 10	portswitch access vlan 10
Acceso a interfaz Ethernet 1/0/3	Interface Ethernet1/0/3
Puerto de acceso a la VLAN 10	port access vlan 10
Acceso a interfaz Ethernet 1/0/4	Interface Ethernet1/0/4
Puerto de acceso a la VLAN 695	portswitch access vlan 695
Acceso a interfaz Ethernet 1/0/5	Interface Ethernet1/0/5
Descripción de Puerto Conexión interna a servidor iGWb1 Esclavo (Almacenamiento de CDRs)	description LINK hacia igwb1 esclavo
Puerto configurado con acceso a la VLAN 10	portswitch access vlan 10

Tabla 5.6 Configuración en lan switches de señalización

Descripción de comandos	Comando
Acceso a interfaz Ethernet 1/0/6	Interface Ethernet1/0/6
Conexión interna a servidor iGWb0 Maestro (Almacenamiento de CDRs)	description LINK hacia igwb0 maestro
Puerto configurado con acceso a la VLAN 10	portswitch access vlan 10
Acceso a interfaz Ethernet 1/0/7	Interface Ethernet1/0/7
Puerto apagado	Shutdown
Acceso a interfaz Ethernet 1/0/8	Interface Ethernet1/0/8
Puerto configurado con acceso a la VLAN 10	portswitch access vlan 10
Descripción de puerto Conexión para señalización interna	description LINK hacia tarjeta MSC para señalización interna
Acceso a interfaz Ethernet 1/0/9	Interface Ethernet1/0/9
Puerto de acceso a la VLAN 695	portswitch access vlan 10
Acceso a interfaz Ethernet 1/0/10	Interface Ethernet1/0/10
Puerto de acceso a la VLAN 695	portswitch access vlan 10
Acceso a interfaz Ethernet 1/0/11	Interface Ethernet1/0/11
Puerto de acceso a la VLAN 695	portswitch access vlan 10
Acceso a interfaz Ethernet 1/0/12	Interface Ethernet1/0/12
Puerto de acceso a la VLAN 10	portswitch access vlan 10
Acceso a interfaz Ethernet 1/0/13	Interface Ethernet1/0/13
Puerto de acceso a la VLAN 695	portswitch access vlan 695
Descripción de puerto Enlace de señalización a MGW de Revolución	description LINK de señalización a MGW REVOLUCION
Acceso a interfaz Ethernet 1/0/14	Interface Ethernet1/0/14
Puerto configurado con acceso a la VLAN 695	portswitch access vlan 695
Descripción de puerto Enlace de señalización a UMG de Guadalajara	description LINK de señalización a MGW GUADALAJARA
Acceso a interfaz Ethernet 1/0/15	Interface Ethernet1/0/15
Puerto configurado con acceso a la VLAN 695	portswitch access vlan 695
Descripción de puerto Enlace de señalización a UMG de Monterrey	description LINK de señalización a MGW MONTERREY.

Tabla 5.6 Configuración en lan switches de señalización

Descripción de comandos	Comando
Acceso a interfaz Ethernet 1/0/16	Interface Ethernet1/0/16
Puerto de acceso a la VLAN 695	portswitch access vlan 695
Descripción de puerto. Enlace de señalización a UMG de Tlalnepantla	description LINK de señalización a MGW TLALNEPANTLA
Acceso a interfaz Ethernet 1/0/17	Interface Ethernet1/0/17
Puerto configurado con acceso a la VLAN 695	portswitch access vlan 695
Acceso a interfaz Ethernet 1/0/18	Interface Ethernet1/0/18
Puerto configurado con acceso a la VLAN 695	portswitch access vlan 695
Acceso a interfaz Ethernet 1/0/19	Interface Ethernet1/0/19
Puerto configurado con acceso a la VLAN 696	portswitch access vlan 696
Descripción de puerto Enlace a Router_A proceso de OSPF	description LINK hacia router_A para proceso de OSPF
Acceso a interfaz Ethernet 1/0/20	Interface Ethernet1/0/20
Puerto no configurado	Shutdown
Acceso a interfaz Ethernet 1/0/21	Interface Ethernet1/0/21
Puerto configurado con acceso a la VLAN 695	portswitch access vlan 695
Descripción de puerto conexión para señalización entre MGWs y MSC	description LINK hacia tarjeta de señalización para comunicación entre MGW y MSC.
Acceso a interfaz Ethernet 1/0/22	Interface Ethernet1/0/22
Puerto apagado	Shutdown
Acceso a interfaz Ethernet 1/0/23	Interface Ethernet1/0/23
Puerto configurado con acceso a la VLAN 830	portswitch access vlan 830
Descripción de puerto Puerto de acceso a LS de señalización esclavo	description acceso de O&M a Lan switch de control esclavo.
Acceso a interfaz Ethernet 1/0/24	Interface Ethernet1/0/24
Descripción de puerto configuración de troncal entre LS maestro y esclavo	description LINK troncal entre LS maestro y esclavo
Configuración de puerto a tipo troncal	port link-type trunk

Tabla 5.6 Configuración en lan switches de señalización

Descripción de comandos	Comando
Configuración de VLANs permitidas entre Lan switches	port trunk permit vlan 10 695
Puertos GE no configurados	Interface GigabitEthernet1/1/1
	Interface GigabitEthernet1/1/2
	Interface GigabitEthernet1/1/3
	Interface GigabitEthernet1/1/4
Configuración de identificador de proceso OSPF	ospf 696
Configuración de preferencia de Lan switch	preference 20
Área asociada con el proceso de OSPF	area 0.0.0.0
Redes propias del proceso de OSPF. Redes a ser anunciadas	network 192.168.28.0 0.0.0.7
Redes propias del proceso de OSPF Redes a ser anunciadas	network 192.168.29.0 0.0.0.255

Tabla 5.6 Configuración en lan switches de señalización

La explicación a detalle de cada uno de los comandos configurados en el lan switch de señalización, se encuentra explicada en el capítulo 4 de la presente investigación.

Conclusiones

El diseño de Redes de Telecomunicaciones es una actividad que ha ido creciendo considerablemente, en la medida que las nuevas tecnologías han acelerado la convergencia de voz, datos, imágenes y agregado nuevos servicios que incluyen una creciente movilidad. Al no existir tecnologías claramente dominantes, el transporte de información sobre redes heterogéneas caracteriza al entorno de las telecomunicaciones en la actualidad y explica gran parte de su complejidad.

En el comienzo de la planificación de la red, una de las cuestiones más complicadas y críticas fue identificar las exigencias y limitaciones del proyecto, ya que se tuvo que tomar en cuenta los diversos problemas que pudieron surgir durante el desarrollo y la ejecución del mismo. Fue necesario tomar en cuenta la inspección del sitio, las características físicas de los equipos, medios de transmisión de datos, enlaces de alta disponibilidad con otros equipos, direccionamiento IP, modelos de tráfico, mecanismos de protección de tráfico de voz, tipos de conexión a utilizar, además de tener una identificación correcta de la topología de red a utilizar.

Durante el proceso de desarrollo de la investigación, fue necesario definir con claridad los objetivos y el alcance del mismo, además de desglosar todos los criterios de desempeño esperado, los cuales fueron cubiertos satisfactoriamente.

Fue importante revisar los aspectos de cobertura, modelos de tráfico y desempeño, así como el transporte necesario para la comunicación entre los sitios remotos (Guadalajara y Monterrey) y los sitios locales (Revolución y Tlalnepantla), además de identificar todos los requisitos de interconexión y funcionamiento de equipos de datos y equipos de comunicación de tercera generación.

La red de comunicación móvil diseñada, construida e implementada, permite:

- La conexión de llamadas entre los diferentes mercados.

- Enlaces de señalización entre los MSCs a través de los lan switches de señalización y los STPs, verifican el perfil del usuario móvil y permiten la comunicación de enlace de llamada entre dos usuarios móviles de tercera generación

- La transmisión de voz entre usuarios móviles de la PSTN de Guadalajara, Monterrey, con Distrito Federal y Estado de México.

- Las conexiones entre los MGWs y los routers permiten que se transmita la voz entre los diferentes mercados. Los mecanismos de protección de voz configurados en los equipos de datos (routers), permiten que la solución sea de alta disponibilidad tanto a nivel físico, como a nivel lógico. El servicio no será afectado, en dado caso que una falla física, lógica o de enlace se presentará.

- Todos los equipos (routers, MSC, MGWs, lan switches) se mantienen en constante gestión, se puede acceder a los equipos a través de consolas y realizar rutinas de operación y mantenimiento.

Las redes con servicios múltiples (por ejemplo, la tecnología IMS (Subsistema Multimedia IP)) prometen una mayor homogeneidad pero todavía se encuentran en fase de desarrollo e implementación. En consecuencia, el diseño de redes enfrenta a cada momento el desafío de lograr establecer parámetros y criterios sobre los cuales diseñar una red maximizando sus prestaciones, su rentabilidad en el tiempo, su eficiencia en costos, y asegurando a la vez una adecuada evolución futura.

REFERENCIAS

- Cisco Systems, Inc. *"Interconnecting CISCO Networking Devices Part I"*, 2009 USA, Chapter 4 Constructing a Network Addressing Scheme.
- Thomas M. Thomas II**, "***OSPF Network Design Solutions, Second Edition", [en línea],* Indianapolis USA*,* Cisco Systems, Inc. URL: ttp://docstore.mik.ua/cisco/pdf/OSPF%20Network%20Design%20Solutions%20(2nd%20edition).pdf
- Huawei Technologies Co., Ltd., "*Mobile Softswitch Center documentation V100R007*", Shenzhen CHINA, Introduction & Product Orientation.
- Huawei Technologies Co., Ltd., "*Universal Media Gateway documentation V200R007, UMTS*", Shenzhen CHINA, Description & Product Orientation.
- Craig Hunt, *"TCP/IP Network Administration, Second Edition",* O'Reilly & Associates*,* 1997, Overview of TCP/IP, 317pp.
- NETGEAR*,* Inc, *"TCP/IP Networking Basics",* 2005, Chapter 2-2 Networking Basics.
- Craig Hunt, *"TCP/IP Network Administration, Second Edition",* O'Reilly & Associates*,* 1997, Overview of TCP/IP, 317pp.
- Behrouz A. Forouzan, *"transmisión de Datos y Redes de Comunicaciones, Segunda Edición",* Madrid, Mc Graw Hill, 2002, 355-378 pp.
- Heikki Karanen, Ari Ahtiainen, "*Redes UMTS. Arquitectura, movilidad y servicios*", Alfaomega Grupo Editor, 2006, Capítulo 4 Introducción a las tecnologías de acceso rápido.
- Millán Tejedor Ramón Jesús, Huidobro Moya José "*Redes de datos y convergencia Ip* ", Creaciones Copyright, 2007, Capítulo 7 Redes troncales, Capítulo 10 gestión de Red, Capítulo 5 Redes Locales.
- Cisco Systems, Inc. *"Interconnecting CISCO Networking Devices Part II"*, 2009 USA, Chapter 2 Implementing Spanning Tree Protocol.

- Huawei Technologies Co, Ltd., "*Quidway NE40 Engine, router*", Shenzhen CHINA, System Capacity.
- Cisco Systems, Inc. "*IEEE 802.1Q Frame Format*", {en línea}, dirección URL: http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094665.shtml {consulta Mayo 2010}.
- Cisco Systems, Inc. "*802.1Q native VLANs*", {en línea}, dirección URL: http://www.cisco.com/en/US/tech/tk389/tk689/nativevlan_example09186a0080094784.shtml,{consulta: Abril 2010}.
- SYBEX, "*CCNP study guide, SYBEX*", Wade Edwards & Terry Jack, San Francisco, Switching & Spanning Tree Protocol, 2008.
- Cisco Systems, Inc. "*VLAN trunking protocol*", {en línea}, dirección URL: http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml {consulta: Diciembre 2009}.
- Cisco Systems, Inc. "*Understanding Spanning Tree Protocol*", {en línea}, dirección URL:http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/sw_ntman/cwsimain/cwsi2/cwsiug2/vlan2/stpapp.htm {consulta: Enero 2010}.
- Huawei Technologies Co, Ltd., "*Quidway Session Engine 2300 Session Boarder Controller V200R005*", Shenzhen CHINA, VRRP principles.