ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO SOBRE UNA RED PORTADORA DE DATOS PARA CLIENTES CORPORATIVOS UTILIZANDO SNMP V.2"

EXAMEN DE GRADO (Complexivo)

Previo a la obtención del Título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

RYAN ESTIVEN BANDA TAPIA

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTOS

Mis más sinceros agradecimientos a todas las personas que creyeron en mí, sin importar el tiempo y las dificultades que existieron durante el camino.

A mis amigos y amigas, quienes nunca dejaron de alentarme en terminar éste ciclo.

Ryan Banda Tapia

DEDICATORIA

El presente proyecto lo dedico a mis dos madres (madre y tía) quienes, aunque no pudieron ver el producto de su fuerza, no han estado un solo día lejos de mí.

A mis amadas hijas Daniela, Grazzia y Paula, de las pocas cosas que puedo darles, espero que entiendan lo que significa y sirva de guía para sus vidas; fe, esfuerzo, lucha, constancia.

Espero que esto sirva de inspiración a todas las personas que aunque vean demasiadas adversidades no se rindan.

Ryan Banda Tapia

TRIBUNAL DE EVALUACIÓN

Ing. Washington Medina	**Ing. Cesar Yépez**
PROFESOR EVALUADOR	PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, me corresponde exclusivamente; y doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

.....

Ryan Banda Tapia

RESUMEN

Debido a la tendencia de expansión en el campo comercial las empresas integran constantemente sus diferentes agencias para tener un mejor manejo de sus inventarios, stock y procesos de facturación, esto conlleva una integración a nivel de datos en cada uno de los sitios. En la última década el crecimiento de la base de clientes corporativos ha sido de manera exponencial, por lo que la estructura actual de gestión resulta ineficiente y complica significativamente mantener disponibilidad de servicios debido a que no existe una visión global de los problemas físicos o lógicos suscitados, causando diagnósticos errados y por ende soluciones que demandan tiempos altos es decir afectaciones de servicios demasiado extensas.

En la actualidad el mercado de las telecomunicaciones es altamente competitivo por lo que las operadoras han definido indicadores de disponibilidad y niveles de servicio con el objetivo de captar más clientes y mantener los actuales; con la estructura disponible el cumplimiento de disponibilidad y soporte no está cumpliendo en algunos casos y en otros tiene un costo operativo muy alto para la operadora en conceptos de movilización y soporte puesto que no existe un control adecuado de los eventos en los equipos finales.

La estructura actual de monitoreo y gestión de servicios no solamente genera un impacto en la disponibilidad del servicio para el cliente sino también puede ocasionar llamados de atención, multas y el retiro de la licencia de concesión de frecuencias de operación por parte del ente regulador, por lo que resulta necesario el cambio de dicha estructura para contar con soluciones viables que permitan identificar anomalías en los servicios ofrecidos de una manera proactiva y predictiva, basándose en estadísticas de eventos ocurridos.

Implementar un Sistema de Monitoreo sobre una Red Portadora de Datos para Clientes Corporativos utilizando SNMP V.2, permitirá tomar acciones inmediatas ante las fallas que se presenten en los servicios ofrecidos por la operadora logrando disminuir los tiempos de respuesta, anticipando el escalamiento del cliente y asegurando la disponibilidad contratada (SLA´s).

Gracias a la funcionalidad del sistema de gestión y monitoreo se obtendrán reportes estadísticos de las afectaciones de los servicios indicados por los equipos terminales en cada sitio, con lo cual se espera lograr de una manera proactiva obtener soluciones para problemas frecuentes de manera más personalizada; de igual manera será muy sencillo validar el cumplimiento de los SLA´s contratados y los reportes de disponibilidad de la red evitando así, notas de créditos para los clientes y multas o suspensiones por parte del ente regulador.

Una vez integrados todos los elementos de los servicios se podrá realizar rutinas de mantenimientos no solo en lo referente al estado físico de los equipos sino también a nivel lógico. Además de contar con los respaldos de las configuraciones de los equipos terminales en los clientes.

Será de mucha ayuda para la parte comercial de la empresa, puesto que el control de ancho de banda permitirá en base a los consumos reales de cada sitio las recomendaciones de incrementos en las capacidades de los servicios.

Cabe mencionar que si bien la estructura del Proyecto corresponde a un entorno real, para efecto de éste informe se ha cambiado el direccionamiento IP privado, etiquetas, nombres de recursos y demás para garantizar la confiabilidad de la información.

ÍNDICE GENERAL

CAPÍTULO 1

1. MARCO TEÓRICO DEL PROYECTO.

Se explicará conceptos básicos y arquitectura de protocolos MPLS. Estos puntos mostrarán los criterios básicos que se aplican para las posteriores implementaciones MPLS y redes virtuales privadas (VPN´s). [1]

Es importante tener un claro entendimiento sobre el concepto del MPLS incluyendo algunas ventajas así como comparaciones al tradicional enrutamiento y describir:

- La función de tradicional sistema de red IP.
- Las características básicas del MPLS.
- Los beneficios del MPLS.
- Describir los componentes básicos de la arquitectura del MPLS.
- Describir la función de los diferentes tipos de LSR´s.

1.1 Fundamentos básicos del Direccionamiento IP

Estos temas describen las bases tradicionales del sistema de red IP, como lo muestra la Figura 1.1.

Bases del sistema tradicional de red IP

• El protocolo del sistema de red es usado para distribuir sistemas de redes.
• Trasportar decisiones está basado en:
  o paquetes de títulos
  o tablas locales de sistema de red

Figura 1.1: Bases del Sistema Tradicional de Red IP

1.2 Características Básicas del MPLS

- Es un mecanismo en cambio de paquetes.
- Fue diseñado como un protocolo de soporte múltiple de capa 3 (layer 3).
- Típicamente los niveles de MPLS corresponden a diseñar redes.
- A diferencia del modelo asociado con Cisco Express reenvío (CEF) e IMPLS, es diseñado para liberar la inteligencia asociada con el sistema de red IP.

1.2.1 Beneficios de MPLS

- MPLS soporta múltiples aplicaciones, entre ellas:
    - Unicast y enrutamiento IP multicast.
    - Virtual Privarte Network VPN.
    - TE.
    - QoS.
    - ATOM.
- Disminuye sobrecarga de reenvío.
- Puede soportar transmisión de los protocolos no IP.

1.2.2 Arquitectura MPLS: Plano de Control

El plano toma importancia para el reenvío basándose en cada dirección de destino y etiquetas, los datos planos son también conocidos como reenvíos planos, son paquetes adelantados al apropiado, interface basado en las tablas de información de LFIB o del FIB a continuación la Figura 1.2 muestra la arquitectura MPLS plano de control:

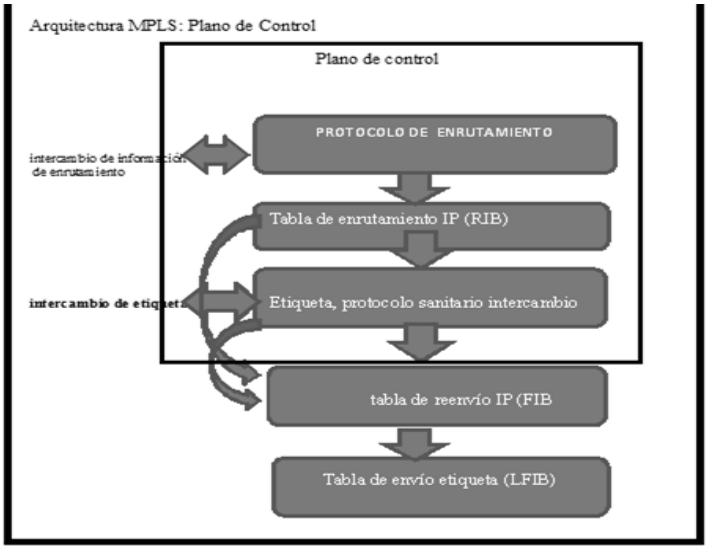

Figura 1.2: Arquitectura MPLS: Plano de Control

CAPÍTULO 2

2. FUNDAMENTOS DE LA ADMINISTRACIÓN DE RED.

La gestión de redes tiene como objetivo principal la utilización coordinada de los recursos para:

- Realizar la planificación, organización, mantenimiento, supervisión, evaluación y control de los equipos de las redes de comunicaciones.
- Monitorear para obtener información de los elementos por lo que está compuesta la red de ésta manera detectar fallas y problemas en el tráfico de datos.
- Conocer la red permite establecer el control mediante señalización o plano de control, quien se encargaría de la regularización de las comunicaciones y del tráfico en términos generales.

2.1 Objetivos de la gestión de una red

La gestión de una red de elementos integrados tiene como objetivo principal de parámetros importantes para una empresa tales como la disponibilidad y eficiencia para incrementar su rendimiento y productividad.

2.2 Aplicaciones

Las aplicaciones tienen un campo muy extenso al tratarse de las diferentes cualidades de las tecnologías que tienen hoy en día las telecomunicaciones por los servicios que estas ofrecen, la gestión de las redes tiene un grado de complejidad cuando se trata de mantener un estándar y contar un variado parque tecnológico instalado.

2.3 Clasificación de áreas funcionales de un gestor

Las áreas funcionales para la gestión de una red están definidas como:

- **Supervisión y fallos:** grupo de criterios que permiten el aislamiento y el arreglo de un problema detectado.

- **Configuración:** criterios que se utilizan para realizar la identificación el control la colección y proporcionarían la información de los objetos gestionados.
- **Contabilidad:** criterios que se utilizaran en el establecimiento de cargos por el uso de elementos determinados así como identificar el costo por su uso.
- **Prestaciones:** criterios que se toman en cuenta para realizar la evaluación en el comportamiento de actividades específicas.
- **Seguridad:** consideraciones que deben ser consideradas al momento de brindar protección a los elementos que serán gestionados.

2.4 Modelo Gestor-Agente

Los componentes de un sistema de gestión en una arquitectura Gestor-Agente se dividen de la siguiente manera:

- **Gestores:** equipos de un sistema de gestión que se interrelacionan con los operadores (personas) y emiten acciones que se necesitan para realizar los trabajos solicitados.
- **Agentes:** son los elementos de la red de gestión quienes serán administrados por el gestor.

El envío y recepción de la información en un sistema de gestión es la base entre el gestor y los elementos a gestionar.

2.5 Protocolo Simple de administración de red SNMP

El SNMP es un protocolo de capa 7 según el modelo OSI que simplifica el intercambio de la información entre los elementos de la red de gestión que ayuda a los administradores de red a tener el control del desempeño de los elementos para solucionar los problemas que se presenten así como dimensionar el crecimiento de la misma. [2] [3]**.**

2.6 Comparación entre las capas de SNMP-OSI

Entre las similitudes entre los modelos OSI y TCP tenemos que ambos se agrupan en niveles o capas. La tecnología se basa en conmutación de

paquetes. Los dos modelos poseen capa de aplicación aunque sus servicios son diferentes y poseen una capa de red o transporte en común.

El modelo OSI fue creado mucho antes de implementar los protocolos, por lo que algunos puntos necesarios fallan o no existen. TCP/IP por otra parte se diseñó después que los protocolos, por lo que se adapta a ellos perfectamente. En el modelo OSI se ocultan mejor los protocolos que en el modelo TCP/IP y se pueden cambiar fácilmente al cambiar la tecnología. La capacidad de efectuar tales cambios es uno de los principales propósitos de tener protocolos por capas en primer lugar Modelo OSI combinaban los niveles físico y de vinculación en un controlador inteligente (como una tarjeta de red). La combinación de las dos capas en una sola tenía un beneficio importante: permitía que se diseñara una subred independiente de cualesquiera protocolos de red. La Figura 2.1 muestra estos dos modelos: [4]

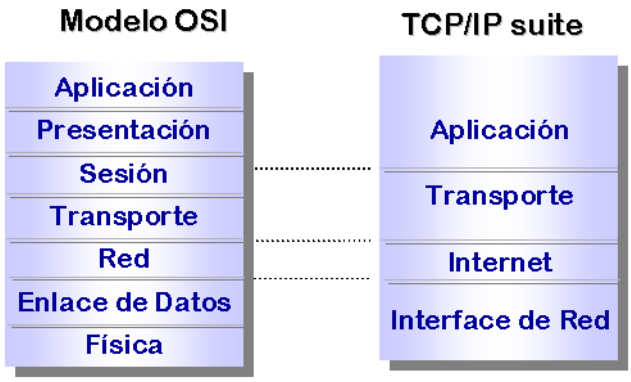

Figura 2.1: Comparación entre los modelos OSI y TCP

2.7 Base de información para administración (MIB)

Un MIB es una librería de conceptos de los recursos u elementos que se gestionaran en una red formado por clases acciones alarma, atributos, etc.

Un objeto administrado u Objeto MIB, es uno de cualquier número de características específicas de un dispositivo administrado. Los objetos administrados están compuestos de una o más instancias de objeto, que son esencialmente variables.

Un identificador de objeto (object ID) únicamente identifica un objeto administrado en la jerarquía MIB. La jerarquía MIB puede ser representada como un árbol con una raíz anónima y los niveles, que son asignados por diferentes organizaciones, esto se puede notar en la Figura 2.2.

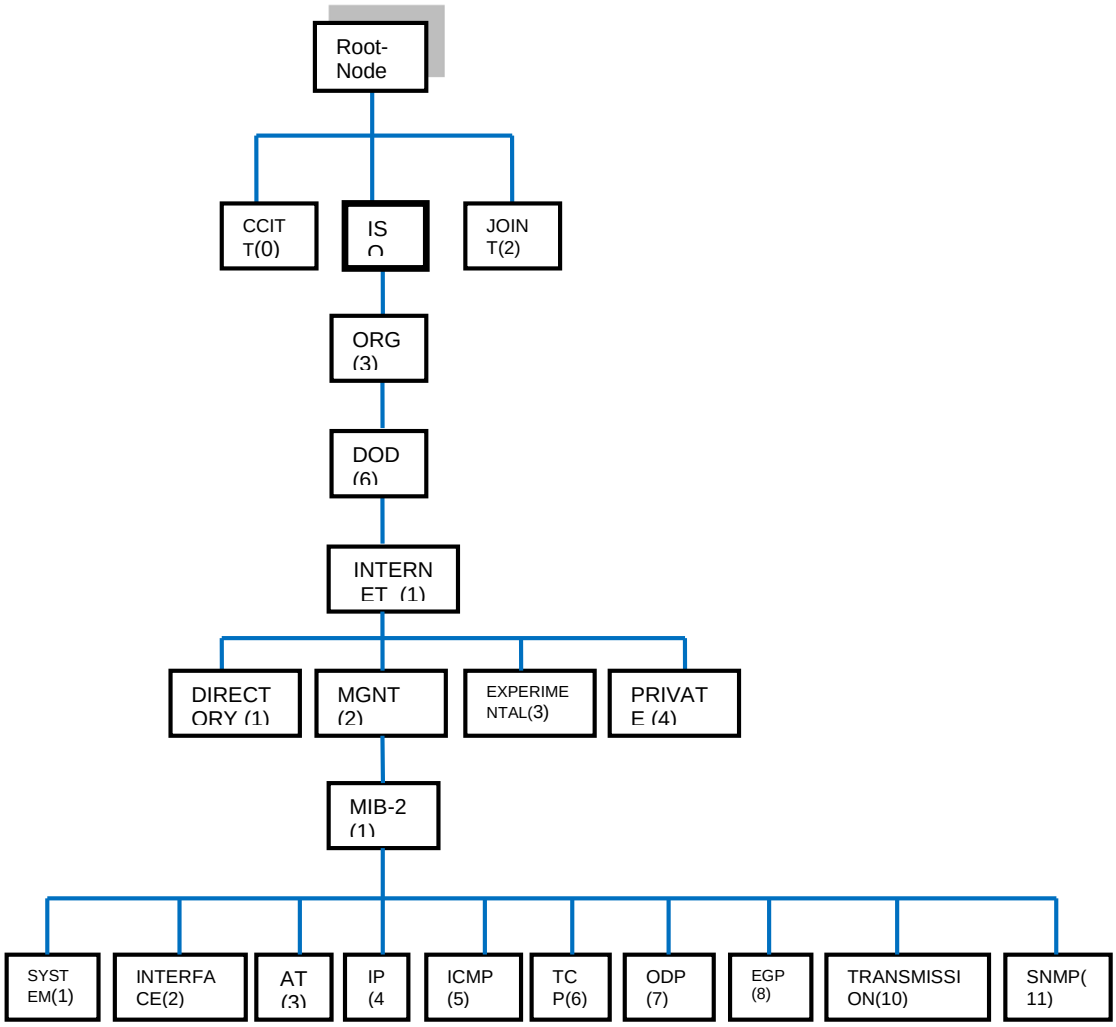

Figura 2.2: Estructura Jerárquica del árbol MIB

2.8 Alarmas de SNMP (Trap)

Los traps de SNMP no tienen nada que ver con el resto de alertas del sistema, aunque reutilizarán el sistema de acciones. Tenga en cuenta que al no existir "plantilla de alertas" aquí, las condiciones y los campos pasados como parámetro al comando funciona diferente a como funciona una alerta normal.

Los campos de datos de la alerta sobre escriben a los campos de la acción y no existen alertas de recuperación (no se puede recuperar un trap), ya que en caso de que se reciba otro trap para advertir de que algo deja de estar mal, hay que tratarlo como un trap diferente. [5], [6]

Las alertas de traps SNMP tienen varios campos que pueden ser utilizados para "buscar" datos en el trap SNMP. Los campos que se pueden usar, tanto por separado como por combinación son:

- **Description**: Comando para escribir una descripción de la alerta.
- **OID**: OID principal del Trap. Es una expresión regular. Si no se usa una expresión regular se buscará la cadena exacta, si se quiere buscar un trozo del OID, se debe usar una expresión regular, de forma que si queremos buscar, por ejemplo: 1.21.34.2.3 en un OID más largo, podemos usar la expresión regular.*1.21.34.2.3.*
- **Custom Value/OID**: Esto busca en los campos "Value" del trap, así como en los campos "Custom OID" y "Custom Value", es decir, en el resto de campos del TRAP. Aqui funciona, igualmente, la búsqueda por expresión regular. Por ejemplo si tengo un trap que envia la cadena "Testing TRAP 225" yo puedo buscar cualquier trap con la subcadena "Testing TRAP" con la expresión regular "Testing.*TRAP.*"
- **SNMP Agent**: IP del agente que envía el trap. De igual forma, podemos usar una expresión regular o una subcadena.
- **Trap type**: Filtra por tipo de trap pudiendo ser: Cold start, Warm start, Link down, Link up, Authentication failure o Other. La mayoría de los traps generados suelen ser de tipo "Other"; si no especifica nada, buscará cualquier tipo de trap.
- **Single value**: Filtra por el valor del trap. En el ejemplo igual a .666. Esto solo hace referencia al valor simple del OID principal, no de cualquier OID secundario.

- **Custom OID/Data #1-20**: Son expresiones regulares que intentan unir con las variables 1 a 20. Si hay un acierto, se dispara la alerta. El valor de la variable se guarda en la macro _snmp_fx_ correspondiente (_snmp_f1_, _snmp_f2_,...). Aunque sólo se puede especificar una expresión regular para veinte variables, las macros _snmp_fx_ macros están disponibles para todas ellas (_snmp_f11_, _snmp_f12_,...).
- **Field 1**: Campo para poner el parámetro del comando de la alarma Field 1. Este es el campo que se utilizará en el caso de elegir generar un evento, o el mail de destino en caso de elegir una acción de email (si queremos sobrescribir el mail que tenga por defecto en la acción).
- **Field 2**: Campo para poner el parámetro del comando de la alarma Field 2. En el caso de enviar un email, p.e. será el subject del mensaje. Si se deja en blanco utilizaría lo que hubiera definido en la acción.
- **Field 3**: Campo para poner el parámetro del comando de la alarma Field 3. El caso de enviar un email, sería el texto del mensaje. Si se deja en blanco utilizaría lo que hubiera definido en la acción.
- **Min. Number of Alerts**: Campo donde se define el mínimo número de traps que tienen que llegar para que salte la alarma.
- **Max. Number of Alerts**: Campo donde se define el número máximo de veces que se ejecutará la acción.
- **Time Threshold**: Campo donde se define el tiempo que debe pasar antes de resetear el contador de alarmas. Este contador es el que se usa para el campo Min. Number of alerts.
- **Priority**: Combo donde se establece la prioridad de la alarma.
- **Alert Action**: Combo donde se elige la acción que va a ejecutar la alerta. Si se elige un evento, el evento normal de generación de alerta no se generará.

- **Position**: Las alertas con menor posición se evalúan primero. Un solo trap sólo puede disparar una alerta (la que primero case con el trap).

2.9 Sistema centralizado de validación (SYSLOG)

Syslog es un estándar de facto para el envío de mensajes de registro en una red informática IP. Por *syslog* se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro.

Un mensaje de registro suele tener información sobre la seguridad del sistema, aunque puede contener cualquier información. Junto con cada mensaje se incluye la fecha y hora del envío.

2.10 Versiones de SNMP

Las versiones de SNMP más utilizadas son SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2).

SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo no ha sido mayoritariamente aceptado en la industria. [3], [5], [6]

2.10.1 SNMP v1

- Fue diseñado a mediados de los 80.
- Logra una solución temporal hasta la llegada de protocolos de gestión de red con mejores diseños y más completos.
- Se basa en el intercambio de información de red a través de mensajes (PDU's).
- No era perfecto, además no estaba pensado para poder gestionar la inmensa cantidad de redes que cada día iban apareciendo.

2.10.2 SNMP v2

- Definida en 1993 y revisado en 1995.
- Añade mecanismos de seguridad.
- Mayor detalle en la definición de las variables.

- Se añaden estructuras de la tabla de datos para facilitar el manejo de los datos.
- No fue más que un parche, es más hubo innovaciones como los mecanismos de seguridad que se quedaron en pura teoría, no se llegaron a implementar.

2.10.3 SNMP v3

Desarrollado en 1998.A esta versión se le agregan los mecanismos de seguridad que no se llegaron a implementar en la versión anterior, los cuales son:

- **Integridad del Mensaje:** asegura que el paquete no haya sido violado durante la transmisión.
- **Autenticación:** determina que el mensaje proviene de una fuente válida.
- **Encriptación:** encripta el contenido de un paquete como forma de prevención.

CAPÍTULO 3

3. DISEÑO FÍSICO DE LA RED DE MONITOREO.

En el diseño físico e infraestructura de la red portadora de dato o de accesos de servicios CORE consta de routers MPLS interconectados entre sí con protocolos de enrutamiento, los que permitirán tomar decisiones lógicas y automáticas tales como: Enrutamiento de tráfico según criterios ya predefinidos de acuerdo a protocolos aplicados. Para el caso de la red de acceso que se utilizará para la implementación, se configurará el protocolo de enrutamiento OSPF (Open Shortest Path First ó camino más corto primero). [1]

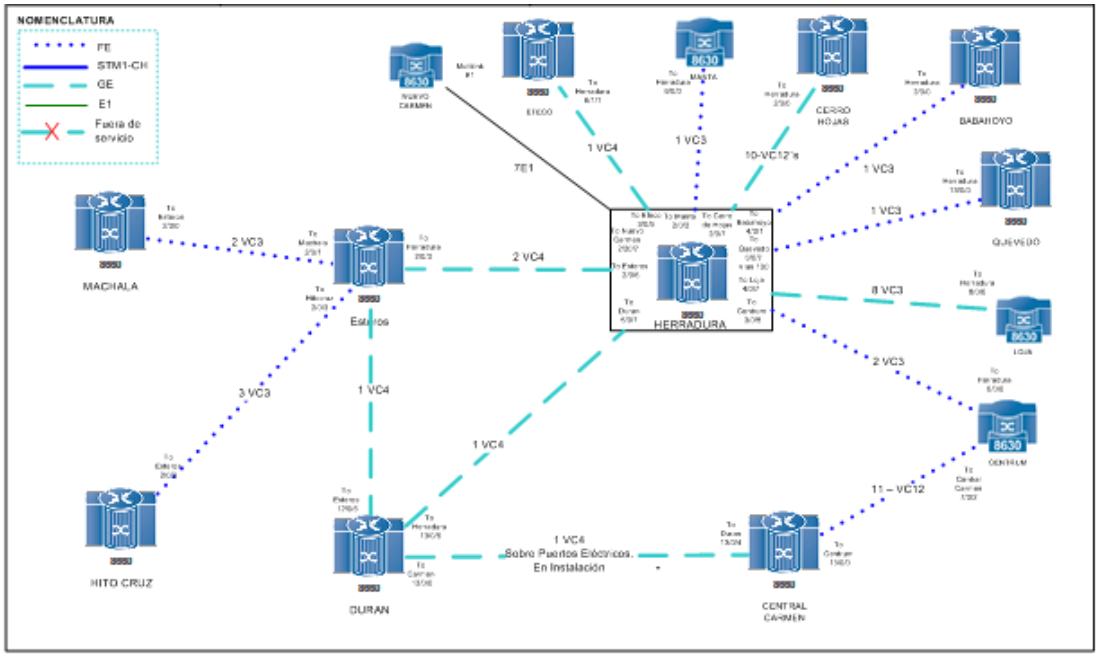

Figura 3.1: Red portadora de datos o de Accesos de Servicio.

En la Figura 3.1 se puede apreciar la red de accesos CORE que será la base sobre la cual se implementarán los servicios de capa dos para el monitoreo de los CPE´S (Equipo Local del Cliente). A continuación se realizará una reseña del protocolo OSPF para enrutamiento.

3.1 Reseña de enrutamiento del protocolo (OSPF).

Se desarrolló a partir de una necesidad en la comunidad de Internet de introducir un protocolo de Gateway interior (IGP) no propietario y de alta funcionabilidad para la familia de protocolos TCP/IP. La discusión sobre la creación de un IGP común interoperable para internet comenzó en 1988 y no se formalizó hasta 1991. En aquel momento, el grupo de trabajo OSPF solicitó que OSPF se considerara un avance para el estándar de Internet de borrador.

El protocolo OSPF se basa en tecnología de estado de enlace, la cual es una desviación del algoritmo basado en el vector Bellman-Ford que se usa en los protocolos tradicionales de enrutamiento de Internet, como por ejemplo, RIP. OSPF ha introducido conceptos nuevos, por ejemplo, la autenticación de actualizaciones de enrutamiento, máscaras de subred de longitud variable (VLSM), resumen de ruta, etc.

En los siguientes párrafos se tratará la terminología OSPF, el algoritmo, así como las ventajas y desventajas del protocolo en el diseño de las complejas redes de gran tamaño de hoy en día. [3]

3.2 OSPF versus RIP

- El rápido crecimiento y la expansión de las redes actuales han llevado al protocolo RIP al límite. Este protocolo tiene ciertas limitaciones que pueden causar problemas en las redes de gran tamaño.
- RIP tiene un límite de 15 saltos. Una red que se extiende más allá de los 15 saltos (15 routers) se considera inalcanzable.
- El protocolo RIP no puede gestionar máscaras de subred de longitud variable (VLSM). Dada la insuficiencia de direcciones IP y la flexibilidad que VLSM proporciona a la asignación eficiente de direcciones IP, esto se considera una insuficiencia importante.
- Las difusiones periódicas de la tabla de enrutamiento completa consumirían una gran cantidad de ancho de banda. Éste problema significativo en el caso de las redes de gran tamaño, especialmente en enlaces lentos y nubes WAN.

- RIP converge de manera más lenta que OSPF. En las redes de gran tamaño la convergencia se realiza en unos minutos. Los routers RIP atravesarán un periodo de retención y recolección de residuos y agotarán paulatinamente el tiempo de espera de la información que no se haya recibido recientemente. Este proceso no es adecuado para entornos de gran tamaño, ya que puede causar incoherencias en el enrutamiento.
- RIP no incluye ningún concepto de retrasos de red ni de costos de enlace. Las decisiones de enrutamiento se basan en el conteo de saltos. Siempre se prefiere el trayecto con el menor conteo de saltos de destino, incluso si el trayecto más largo cuenta con un mejor ancho de banda total de enlace y retrasos más lentos.
- Las redes RIP son redes planas. No existe ningún concepto de áreas ni límites. Con la introducción del enrutamiento sin clases y de uso inteligente de agrupación y resumen, las redes RIP parecen haber quedado atrás.
- Se han introducido algunas mejoras en una nueva versión del RIP, denominada RIP 2. Si bien es RIP2 se tratan los temas de VLSM de autenticación y de actualizaciones de enrutamiento de multidifusión, ésta versión no es una gran mejora en comparación con RIP (ahora denominado RIP 1), ya que aún presenta limitaciones en el conteo de saltos y una convergencia lenta, que son elementos esenciales en las actuales redes de gran tamaño. [3] [7]
- El OSPF, por otra parte, direcciona la mayoría de los problemas que se presentaron anteriormente:
- Con OSPF, no hay limitación para el conteo de saltos.
- El uso inteligente de VLSM es de gran utilidad a la hora de realizar la asignación de direcciones IP.
- OSPF utiliza la multidifusión IP para enviar actualizaciones de estado de enlace.

- Esto garantiza un menor procesamiento en los routers que no están a la escucha de paquetes OSPF. Además, las actualizaciones sólo se envían en caso de cambios de enrutamiento y no de manera periódica. Esto garantiza un mejor uso del ancho de banda.
- OSPF tiene mejor convergencia que RIP. Esto se debe a que los cambios en el enrutamiento se propagan de forma instantánea y no periódica.
- OSPF permite un mejor balance de carga.
- OSPF permite una definición lógica de redes en las que los routers se pueden dividir en áreas, de este modo se limita la explosión de actualizaciones de estado de enlace en toda la red, además de proporcionar un mecanismo para agregar rutas y reducir la propagación innecesaria de información de subred.
- OSPF permite la autenticación de enrutamiento a través de distintos métodos de autenticación de contraseñas.
- OSPF permite la transferencia y el etiquetado de rutas externas inyectadas en un sistema autónomo, así se realiza un seguimiento de las rutas externas inyectadas por protocolo exteriores como BGP.
- Esto, por supuesto, llevaría a una mayor complejidad en la configuración y en la solución de problemas de redes OSPF. Los administradores acostumbrados a la simplicidad de RIP se enfrentarán a algunos desafíos con la cantidad de información nueva que deben reconocer a fin de mantenerse actualizados con las redes OSPF. Además, esto generará una mayor sobrecarga en la asignación de memoria y utilización del CPU, es posible que sea necesario actualizar algunos de los routers que ejecutan RIP para administrar la sobrecarga que produce OSP.

3.3 Significado de Estados de Enlace

OSPF es un protocolo de estado de enlace. Un enlace se puede considerar como una interfaz en el router. El estado del enlace ofrece una descripción de esa interfaz y de su relación con los routers vecinos. Una descripción de la

interfaz incluiría, por ejemplo, la dirección IP de la interfaz, la máscara, el tipo de red a la que se conecta, los routers conectados a dicha red, etc. La agrupación de todos estos estados de enlace formaría una base de datos de estados de enlace.

3.4 Algoritmo del trayecto más corto

El trayecto más corto se calcula con el algoritmo Dijkstra. El algoritmo coloca cada router en la raíz de un árbol y calcula el trayecto más corto a cada destino en función del costo acumulado requerido para alcanzar dicho destino. Cada routers dispondrá de su propia vista de la topología, a pesar de que todos los routers crearán un árbol de trayecto más corto con la misma base de datos de estados de enlace. En las secciones siguientes se hace referencia a lo que comprende la creación de un árbol de trayecto más corto.

3.5 Costo de OSPF

El costo (también llamado métrica) de una interfaz en OSPF es una indicación de la sobrecarga requerida para enviar paquetes a través de una interfaz específica, es inversamente proporcional al ancho de banda de dicha interfaz. Un mayor ancho de banda indica un menor costo. El cruce de una línea serial de 56k, implica una mayor sobrecarga (costo mayor) y más retrasos de tiempo que el cruce de una línea Ethernet de 10M. La fórmula que se usa para calcular costo es:

Costo= 10000 0000/banda de ancha en bps (3.1)

Por ejemplo:

Cruzar una línea Ethernet de 10M costará:10 EXP8/10 EXP 7=10 (3.1.1)

y cruzar una línea T1 costará:10EXP 8/1544000=64 (3.1.2)

De forma determinada, el costo de una interfaz se calcula en función del ancho de banda; es posible forzar el costo de una interfaz con el comando de modo de sub configuración de interfaz: ip ospf cost <value>. [8]

3.6 Árbol del trayecto más corto

Para crear el árbol del trayecto más corto par RTA, se debe convertir a RTA en la raíz del árbol y se debe calcular el menor costo para cada destino. Se muestra en la Figura 3.2 el diagrama de la red con los costos de interfaz indicados:

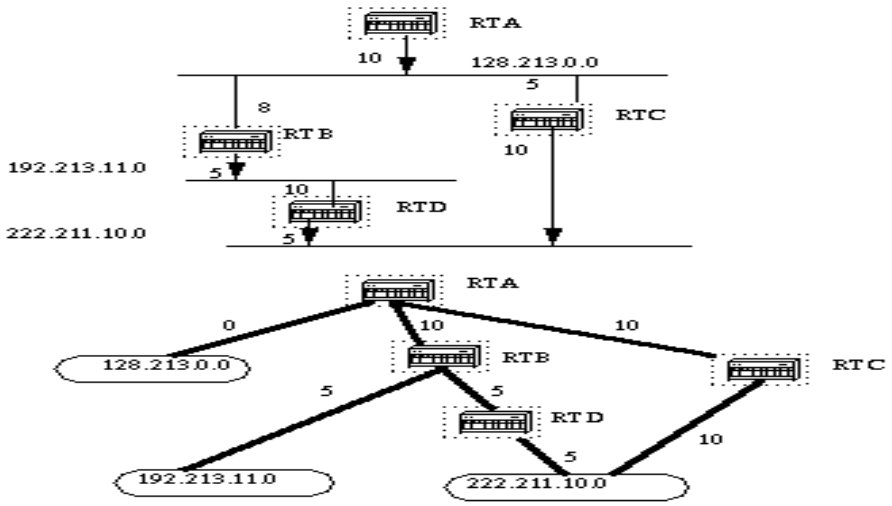

Figura 3.2: Diagrama de árbol de trayecto más corto y costos de interfaz

Arriba se muestra la vista de la red tal como se ve desde RTA. Observe la dirección de las flechas al calcular el costo. Por ejemplo: el costo de la interfaz de RTB para la red 128.213.0.0 no es pertinente cuando se calcula el costo para 192.213.11.0. RTA puede llegar a 192.213.11.0 a través de RTB con un costo de 15 (10+5). RTA también puede llegar a 222.211.10.0 a través de RTC con un costo de 20 (10+10) o a través de RTB con un costo de 20 (10+5+5). En el caso de que existan trayectos de igual costo para el mismo destino, la implementación de Cisco de OSPF realizará un seguimiento de los siguientes seis saltos (next hop) al mismo destino. [7] [9]

Después de que el router cree el árbol de trayecto más corto, comenzará a generar la tabla de enrutamiento según corresponda. Las redes conectadas directamente se alcanzarán por medio de una métrica (costo) 0 y otras redes se alcanzarán según el costo calculado en el árbol.

3.7 Routers de área y de borde

Como se mencionó anteriormente, OSPF utiliza la inundación para intercambiar las actualizaciones de estado de enlace entre los routers. Cualquier cambio en la información de enrutamiento se distribuye en forma de inundación a todos los routers en la red. Las áreas se introducen para establecer un límite en la explosión de actualizaciones de estado de enlace. La inundación y el cálculo del algoritmo Dijkstra en un router están limitados a los cambios dentro de un área. Todos los routers dentro de un área disponen de exactamente la base de datos de estados de enlace. Los routers que corresponden a varias áreas y que conectan dichas áreas al área de estructuras básica se denominan routers de borde de área (ABR). Por lo tanto, ABR deben conservar información que describa las áreas de estructura básica y de las otras áreas conectadas.

Un área es específica de la interfaz. Un router que tiene todas sus interfaces dentro de la misma área se denomina router interno (ABR), como lo muestra la Figura 3.3. Los routers que actúan como gateways (redistribución) entre los protocolos OSPF y otros protocolos de enrutamiento (IGRP, EIGRP, IS-IS, RIP, BGP, estático) u otras instancias del proceso de enrutamiento OSPF se denominan routers del límite del sistema autónomo (ASBR). Cualquier router puede ser un ABR o un ASBR.

3.8 Paquetes de Estado de enlace

La Figura 3.3 muestra los diferentes tipos de paquetes de estado de enlace que generalmente se ven en una base de datos OSPF:

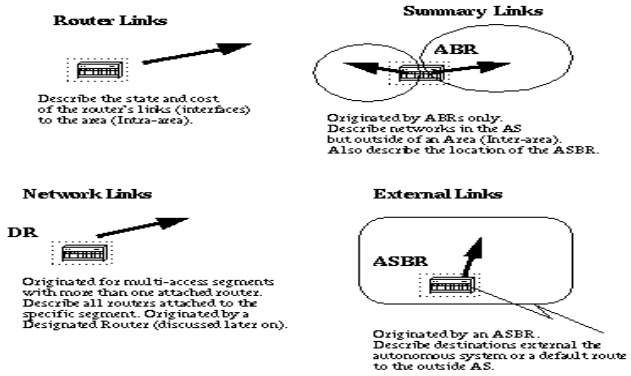

Figura 3.3: Paquetes de Estado de Enlace

Como se mencionó anteriormente, los enlaces del router son una indicación del estado de las interfaces en un router que pertenece a un área determinada. Cada router generará un enlace de router para todas sus interfaces.

Los enlaces de resumen se generan mediante routers ABR; es así como la información de alcance de la red se disemina en las diferentes áreas. Por lo general, toda la información se inyecta en la estructura básica (área 0) y ésta la pasará a otras áreas. Los ABR se ocupan también de propagar el alcance de ASBR. Así es como los routers saben la forma de llegar a rutas externas en otros AS.

Los enlaces de redes se generan mediante un router designado (DR) en un segmento (los DR serán tratados más adelante). Esta información es una indicación de todos los routers conectados a un segmento de acceso múltiple en particular como, por ejemplo, Ethernet, Token Ring y FDDI (también NBMA).

Los enlaces externos indican redes fuera de AS. Estas redes se inyectan en OSPF mediante la redistribución. El ASBR está a cargo de inyectar estas rutas en un sistema autónomo.

3.9 Habilitación de OSPF en el router

La habilitación de OSPF en el router comprende los dos pasos siguientes en el modo de configuración, lo que se visualiza en la Figura 3.4:

- Habilitación de un proceso OSPF con el comando router ospf <process-id > [3] [2].
- Asignación de áreas a las interfaces mediante el comando network <network or IP address><mask><area-id>.

El ID del proceso OSPF es un valor numérico local en el router. No es necesario que coincida con los ID del proceso en otros routers. Es posible ejecutar varios procesos OSPF en el mismo router, pero no se recomienda dado que crea múltiples instancias de bases de datos que agregan una sobrecarga adicional al router.

El comando network es un modo de asignar una interfaz a una área específica. La máscara se utiliza como un acceso directo y ayuda a colocar una lista de

interfaces en la misma área con una línea de configuración de una línea. La máscara contiene bits comodines donde el 0 es una concordancia y el 1 es un bit de "no preocuparse"; por ejemplo, 0.0.255.255 indica una concordancia en los dos primeros bytes del número de la red.

El ID de área es el número de área en el que se desea que se encuentre la interfaz. Puede ser un número entero entre 0 y 4294967295 o bien puede tomar una forma similar a una dirección IP A.B.C.D.

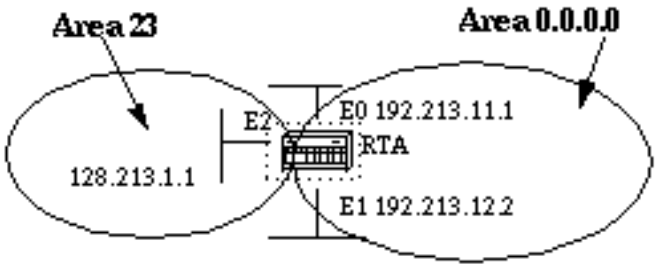

Figura 3.4: Habilitación de OSPF en el router

RTA#

interface Ethernet0

ip address 192.213.11.1 255.255.255.0

interface Ethernet1

ip address 192.213.12.2 255.255.255.0

interface Ethernet2

ip address 128.213.1.1 255.255.255.0

router ospf 100

network 192.213.0.0 0.0.255.255 area 0.0.0.0

network 128.213.1.1 0.0.0.0 area 23

La primera sentencia de red pone a E0 y E1 en la misma área 0.0.0.0, y la segunda sentencia de red pone a E2 en el área 23. Observe la máscara 0.0.0.0,

que indica una concordancia total en la dirección IP. Esta es una forma sencilla de colocar una interfaz en un área determinada si tiene problemas para obtener una máscara.

3.10 Autenticación OSPF

Es posible autenticar los paquetes OSPF para que los routers puedan participar en los dominios de enrutamiento en función de contraseñas predefinidas. De forma predeterminada, un router utiliza una autenticación nula, lo que significa que los intercambios de enrutamiento en una red no se autentican.

Existen otros dos métodos de autenticación: Autenticación simple mediante contraseña y autenticación del resumen de mensaje (MD-5).

- **Autenticación simple mediante contraseña.** La autenticación simple mediante contraseña permite configurar una contraseña (clave) por área. Los routers de la misma área que deseen participar en el dominio de enrutamiento deberán configurarse con la misma clave. El inconveniente de este método es que es vulnerable a ataques pasivos. Cualquier persona que tenga un analizador de enlace podría obtener la contraseña desde el cable fácilmente. Para habilitar la autenticación de contraseñas, utilice los comandos siguientes:

  ip ospf authentication-key key (se realiza en la interfaz específica)

  area area-id authentication (se realiza en "router ospf <process-id>")

  Aquí tiene un ejemplo:

  interface Ethernet0

  ip address 10.10.10.10 255.255.255.0

  ip ospf authentication-key mypassword

  router ospf 10

  network 10.10.0.0 0.0.255.255 area 0

  area 0 authentication

- **Autenticación del resumen de mensaje.** Es una autenticación criptográfica. En cada router se configura una clave (contraseña) y un ID de clave. El router utiliza un algoritmo basado en el paquete OSPF, en la clave y en el ID de clave para generar un "resumen de mensaje" que se agrega al paquete. A diferencia de la autenticación simple, la clave no se intercambia a través del cable. También se incluye un número de secuencia no decreciente en cada paquete OSPF para protegerlo contra los ataques de repetición.

  Este método también permite transiciones ininterrumpidas entre las claves. Esto resulta útil para los administradores que desean cambiar la contraseña OSPF sin deteriorar la comunicación. Si se configura una interfaz con una clave nueva, el router enviará varias copias del mismo paquete, cada una autenticada mediante claves diferentes. El router dejará de enviar paquetes duplicados cuando detecte que todos sus vecinos han adoptado una clave nueva.

  A continuación, se detallan los comandos que se usan para la autenticación del resumen de mensaje:

  ip ospf message-digest-key keyid md5 key (se utiliza en la interfaz)

  area area-id authentication message-digest (se utiliza en "router ospf <process-id>")

  Aquí tiene un ejemplo:

  interface Ethernet0

  ip address 10.10.10.10 255.255.255.0

  ip ospf message-digest-key 10 md5 mypassword

  router ospf 10

  network 10.10.0.0 0.0.255.255 area 0

  area 0 authentication message-digest.

3.11 La estructura básica y área 0

OSPF tiene limitaciones especiales cuando se trata de áreas múltiples. Si se ha configurado más de un área, una de estas áreas deberá ser el área 0. Esto recibe el nombre de estructura básica. Al diseñar las redes, se recomienda comenzar con el área 0 y luego expandirse hacia las otras áreas.

La estructura básica debe estar en el centro de todas las demás áreas, es decir, todas las áreas deben estar conectadas físicamente a la estructura básica. El razonamiento que subyace es que OSPF espera que todas las áreas inyecten información de enrutamiento en la estructura básica y que, en respuesta, ésta disemine la información a las otras áreas. La Figura 3.5 muestra el diagrama de flujo de información en una red OSPF:

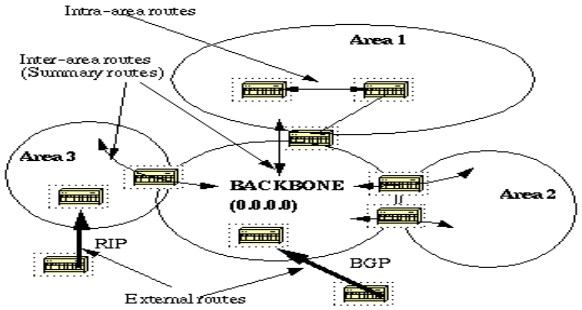

Figura 3.5: Estructura Básica y área 0. Flujo de información de red OSPF

En el diagrama anterior, todas las áreas están conectadas directamente a la estructura básica. En el caso de que se introduzca un área nueva que no pueda tener acceso físico directo a la estructura básica, se deberá configurar un enlace virtual. Los enlaces virtuales serán analizados en la próxima sección. Observe los diferentes tipos de información de enrutamiento. Las rutas que se generan desde el interior de un área (el destino pertenece al área) se llaman rutas intra-área. Por lo general, estas rutas se representan mediante la letra O en la tabla de IP Routing. Las rutas que se originan desde otras áreas se llaman inter-área o rutas de resumen. En la tabla de enrutamiento de IP, la anotación de estas rutas es O IA. Las rutas que se originan desde otros protocolos de enrutamiento (o desde procesos OSPF diferentes) y que se inyectan en OSPF

mediante la redistribución se llaman rutas externas. En la tabla de enrutamiento del IP, estas rutas se representan mediante O E2 u O E1. El orden de prioridad en los casos en los que múltiples rutas tienen el mismo destino es el siguiente: intra-área, inter-área, externa E1, externa E2. Los tipos externa E1 y externa E2 se explicarán más adelante. [7], [8].

3.12 Enlaces virtuales

Los enlaces virtuales se utilizan para dos propósitos:

- Enlace de un área que no tiene una conexión física a la estructura básica.
- Parchar la estructura básica en caso de que se produzca una discontinuidad del área 0.

3.12.1 Áreas no conectadas físicamente al área 0

Como se mencionó anteriormente, el área 0 debe estar en el centro de todas las demás áreas. En algunos casos extraños, en que es imposible tener un área físicamente conectada a la estructura básica, se utiliza un enlace virtual. El enlace virtual suministrará al área desconectada un trayecto lógico a la estructura básica. El enlace virtual debe establecerse entre dos ABR que tengan un área común, con un ABR conectado a la estructura básica. Esto se muestra en el siguiente ejemplo:

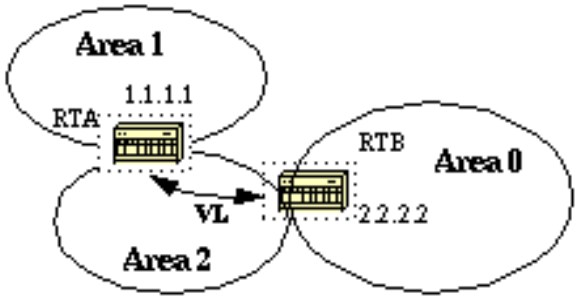

Figura 3.6: Áreas no conectadas físicamente al área 0

En el diagrama del ejemplo, Figura 3.6, el área 1 no tiene una conexión física directa al área 0. Se debe configurar un enlace virtual entre RTA y

RTB. El área 2 se utilizará como un área de tránsito y RTB es el punto de entrada en el área 0. De esta forma, RTA y el área 1 tendrán una conexión lógica a la estructura básica. Para configurar un enlace virtual, utilice el subcomando de OSPF area <area-id> virtual-link <RID> del router tanto en RTA como en RTB, donde el ID de área es el área de tránsito. En el diagrama, es el área 2. El RID es el ID del router. Generalmente, el ID del router OSPF es la dirección IP más alta del cuadro o, de existir, la dirección del bucle de retorno más alta. El ID del router solamente se calcula en el momento de arranque o cada vez que se reinicia el proceso OSPF. Para buscar el ID del router, utilice el comando show ip ospf interface. Suponiendo que 1.1.1.1 y 2.2.2.2 son los RID respectivos de RTA y RTB, la configuración OSPF de ambos routers sería:

RTA#

router ospf 10

area 2 virtual-link 2.2.2.2

RTB#

router ospf 10

area 2 virtual-link 1.1.1.1

3.13 Partición de la estructura básica

OSPF permite el enlace de partes discontinuas de la estructura básica mediante un enlace virtual. En algunos casos, es necesario entrelazar distintas áreas 0. Esto ocurre si, por ejemplo, una compañía intenta combinar dos redes OSPF distintas en una red con un área 0 común. En otras instancias, se agregan enlaces virtuales para redundancia en caso de que un error en el router divida la estructura básica en dos. Cualquiera que sea la razón, se puede configurar un enlace virtual entre los ABR independientes que entren en contacto con el área 0 desde cada lado y que tengan un área común. Esto se ilustra en la Figura 3.7, en el siguiente ejemplo:

Figura 3.7: Partición de la Estructura Básica

En el diagrama anterior, dos áreas 0 están interconectadas mediante un enlace virtual. En el caso de que no exista un área común, se podría crear un área adicional, por ejemplo el área 3, para que funcione como área de tránsito.

Si un área diferente de la estructura básica se divide, la estructura básica se ocupará de la división sin utilizar ningún enlace virtual. Una de las partes del área con partición se dará a conocer a la otra parte a través de rutas inter-área en lugar de rutas intra-área.

3.14 Vecinos

Los routers que comparten un segmento común se convierten en vecinos en ese segmento. Los vecinos son elegidos a través del protocolo de saludo. En forma periódica, se envían paquetes de saludo fuera de cada interfaz mediante multidifusión IP. Los routers se convierten en vecinos apenas se detectan dentro del paquete de saludo del vecino. De este modo, se garantiza una comunicación bidireccional. La negociación entre vecinos se aplica solamente a la dirección primaria. Las direcciones secundarias se pueden configurar en una interfaz con la restricción de que deben pertenecer a la misma área que la dirección primaria.

Dos routers no se convertirán en vecinos a menos que coincidan en lo siguiente:

ID de área. Dos segmentos que tienen un segmento común; las interfaces deben pertenecer a la misma área en ese segmento. Evidentemente, las interfaces deben pertenecer a la misma subred y tener una máscara similar.

3.14.1 Autenticación

OSPF permite la configuración de una contraseña para un área específica. Los routers que desean convertirse en vecinos deben intercambiar la misma contraseña en un segmento determinado.

Intervalo muerto e intervalo de saludo: OSPF intercambia paquetes de saludo en cada segmento. Esta es una forma de señal de mantenimiento que los routers utilizan para reconocer su existencia en un segmento y para elegir un router designado (DR) en segmentos de acceso múltiple. El intervalo de saludo especifica el tiempo en segundos entre los paquetes de saludo que un router envía sobre una interfaz OSPF. El intervalo muerto es el número de segundos durante los cuales los paquetes de saludo de un router no han sido vistos antes de que sus vecinos declaren desactivado al router OSPF.

El OSPF requiere que estos intervalos sean exactamente los mismos entre dos vecinos. Si cualquiera de estos intervalos es diferente, estos routers no se convertirán en vecinos en un segmento determinado. Los comandos de interfaz del router que se usan para configurar estos temporizadores son:

- ip ospf hello-interval seconds y
- ip ospf dead-interval seconds.

3.14.2 Indicador de zona fragmentada

Para convertirse en vecinos, dos routers deben coincidir en el indicador de zona fragmentada de los paquetes de saludo. Las zonas fragmentadas se tratarán en una sección posterior. De momento, recuerde que la definición de las zonas fragmentadas afectará al proceso de elección de vecino.

3.15 Adyacencias

Adyacencia es el paso siguiente luego del proceso de establecimiento de vecinos. Los routers adyacentes son routers que van más allá de un simple

intercambio de saludo y actúan en el proceso de intercambio de base de datos. Para reducir la cantidad de intercambio de información en un segmento determinado, OSPF selecciona un router como router designado (DR) y un router como router designado de respaldo (BDR) en cada segmento de acceso múltiple.

En caso de que falle el DR, se elige el BDR como mecanismo de respaldo. La idea detrás de esto es que los routers tienen un punto central de contacto para el intercambio de la información. En lugar de que cada router intercambie actualizaciones con cada router en el segmento, todos los routers intercambian información con el DR y el BDR. El DR y el BDR confían la información al resto.

En términos matemáticos, esto cancela el intercambio de información de O(n*n) a O(n), donde n es el número de routers en un segmento de acceso múltiple. El siguiente modelo de router de la Figura 3.8 muestra el DR y el BDR.

En el diagrama anterior Figura 3.8, todos los routers comparten un segmento de acceso múltiple común. Debido al intercambio de paquetes de saludo, se selecciona un router como DR y otro como BDR. Cada router en el segmento (que ya se haya convertido en vecino) intentará establecer una adyacencia con el DR y el BDR.

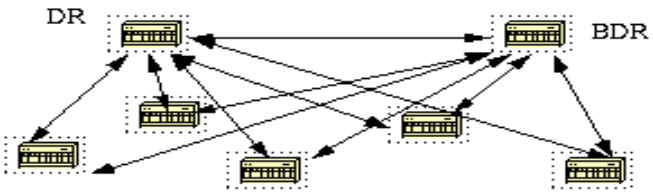

Figura 3.8: Adyacencia.- Selección de un Router como DR y otro como BDR.

3.15.1 Elección de DR

La elección de DR y BDR se lleva a cabo a través del protocolo de saludo. Los paquetes de saludo se intercambian a través de los paquetes de multidifusión IP en cada segmento. El router con la prioridad

OSPF más alta en un segmento se convierte en el DR para dicho segmento. El mismo proceso se repite para BDR. En caso de empate, triunfará el router con el RID más alto. El valor predeterminado para la prioridad de interfaz OSPF es uno. Recuerde que los conceptos DR y BDR son para cada segmento de acceso múltiple. La configuración de prioridad OSPF en una interfaz se realiza mediante el comando de interfaz ip ospf priority <value>.

Un valor de prioridad 0 indica una interfaz que no debe elegirse como DR o BDR. El estado de la interfaz con prioridad cero será DROTHER. La Figura 3.9 ilustra el diagrama de la elección DR:

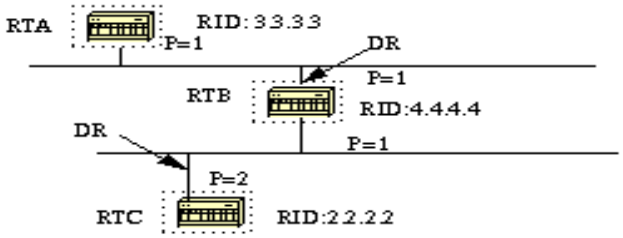

Figura 3.9: Adyacencia: Elección DR.

En el diagrama anterior, RTA y RTB tienen la misma prioridad de interfaz pero RTB tiene un RID mayor. RTB sería DR en ese segmento. RTC tiene una prioridad mayor que RTB. RTC es el DR en ese segmento.

3.15.2 Creación de adyacencias

El proceso de generación de adyacencias se aplica después de que se hayan completado varias etapas. Los routers adyacentes tendrán la misma base de datos de estados de enlace. A continuación se proporciona un breve resumen de los estados por los que pasa una interfaz antes de tornarse adyacente a otro router:

- **Down (Inactivo):** No se ha recibido información de ningún componente del segmento.
- **Intento:** En las nubes de acceso múltiple sin difusión como, por ejemplo, Frame Relay y X.25, este estado indica que no se ha

recibido ninguna información reciente del vecino. Se debería realizar un esfuerzo para comunicarse con el vecino enviando paquetes de saludo en el intervalo de sondeo de velocidad reducida.

- **Init:** La interfaz ha detectado un paquete de saludo proveniente de un vecino, pero aún no se ha establecido la comunicación bidireccional.
- **Bidireccional:** Hay comunicación bidireccional con un vecino. El router se ha visto a sí mismo en los paquetes de saludo provenientes de un vecino. Al finalizar esta etapa, se habrá llevado a cabo la elección de DR y BDR. Al final de la etapa bidireccional, los routers decidirán si deben proceder o no a la generación de una adyacencia. La decisión depende de si uno de los routers es un DR o un BDR o si el enlace es un enlace virtual o punto a punto.
- **Exstart:** Los routers intentan establecer el número de secuencia inicial que se usará en los paquetes de intercambio de información. El número de secuencia garantiza que los routers siempre recibirán la información más reciente. Un router se convertirá en primario y el otro en secundario. El router primario consultará la información al secundario.
- **Intercambio:** Los routers describirán sus bases de datos de estados de enlace completas al enviar paquetes de descripción de bases de datos. En este estado, los paquetes se pueden distribuir en forma de inundaciones a otras interfaces del router.
- **Loading (Cargando):** En este momento, los routers están finalizando el intercambio de la información. Los routers han creado una lista de peticiones de estado de enlace y una lista de retransmisión de estado de enlace. Toda la información que parezca incompleta u obsoleta se colocará en la lista de peticiones. Cualquier actualización enviada se colocará en la lista de retransmisión hasta que sea reconocida.
- **Full (Total):** En este estado, la adyacencia se ha completado. Los routers vecinos son completamente adyacentes. Los routers

adyacentes tendrán una base de datos de estado de enlace similar. Esto se muestra en la Figura 3.10.

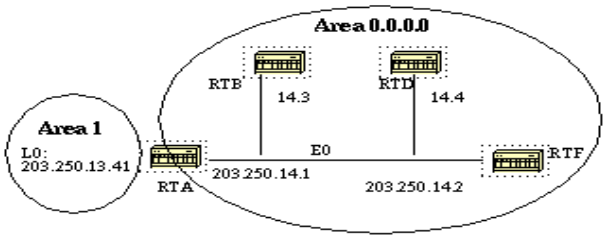

Figura 3.10: Creación de Adyacencia

RTA, RTB, RTD y RTF tienen un segmento común (E0) en el área 0.0.0.0. A continuación se muestran las configuraciones de RTA y RTF. RTB y RTD deben tener una configuración similar a RTF y no se incluirán.

RTA#
hostname RTA
interface Loopback0
ip address 203.250.13.41 255.255.255.0
interface Ethernet0
ip address 203.250.14.1 255.255.255.0
router ospf 1
network 203.250.13.41 0.0.0.0 area 1
network 203.250.0.0 0.0.255.255 area 0.0.0.0
RTF#
hostname RTF
interface Ethernet0
ip address 203.250.14.2 255.255.255.0
router ospf 10
network 203.250.0.0 0.0.255.255 area 0.0.0.0

Lo expuesto es un ejemplo simple que demuestra la utilidad de un par de comandos en la depuración de redes OSPF.

show ip ospf interface <interface>

Este comando se utiliza para verificar rápidamente que las interfaces pertenezcan a las áreas en las que supuestamente deben estar. La secuencia en la que se enumeran los comandos de red OSPF es muy importante. En la configuración de RTA, si la sentencia "network 203.250.0.0 0.0.255.255, area 0.0.0.0" se colocó antes de la sentencia "network 203.250.13.41 0.0.0.0, area 1", todas las interfaces estarían en el área 0, lo que es incorrecto dado que el bucle de retorno se encuentra en el área 1. Consideremos los resultados del comando en RTA, RTF, RTB y RTD:

RTA#show ip ospf interface e0

Ethernet0 is up, line protocol is up

Internet Address 203.250.14.1 255.255.255.0, Área 0.0.0.0

ID del proceso 10, ID del router 203.250.13.41, tipo de red BROADCAST, Cost:

10

Transmit Delay is 1 sec, Estado BDR, prioridad 1

Router designado (ID) 203.250.15.1, Interface address 203.250.14.2

Router designado de respaldo (ID) 203.250.13.41, Interface address

203.250.14.1

Timer intervals configured, Saludo 10, muerto 40, Wait 40, Retransmit 5

Hello due in 0:00:02

El conteo de vecinos es 3, el conteo de vecinos adyacentes es 3

Adjacent with neighbor 203.250.15.1 (Designated Router)

Loopback0 is up, line protocol is up

Internet Address 203.250.13.41 255.255.255.255, Area 1

Process ID 10, Router ID 203.250.13.41, Network Type LOOPBACK, Cost: 1

Loopback interface is treated as a stub Host

RTF#show ip ospf interface e0

Ethernet0 is up, line protocol is up

Internet Address 203.250.14.2 255.255.255.0, Área 0.0.0.0

ID del proceso 10, ID del router 203.250.15.1, tipo de red BROADCAST, Cost: 10

Transmit Delay is 1 sec, Estado DR, prioridad 1

Router designado (ID) 203.250.15.1, Interface address 203.250.14.2

Router designado de respaldo (ID) 203.250.13.41, Interface address

203.250.14.1

Timer intervals configured, Saludo 10, muerto 40, Wait 40, Retransmit 5

Hello due in 0:00:08

El conteo de vecinos es 3, el conteo de vecinos adyacentes es 3

Adjacent with neighbor 203.250.13.41 (Backup Designated Router)

RTD#show ip ospf interface e0

Ethernet0 is up, line protocol is up

Internet Address 203.250.14.4 255.255.255.0, Área 0.0.0.0

ID del proceso 10, ID del router 192.208.10.174, tipo de red BROADCAST, Cost:10

Transmit Delay is 1 sec, Estado DROTHER, Priority 1

Router designado (ID) 203.250.15.1, Interface address 203.250.14.2

Router designado de respaldo (ID) 203.250.13.41, Interface address

203.250.14.1Timer intervals configured, Saludo 10, muerto 40, Wait 40, Retransmit 5

Hello due in 0:00:03

El conteo de vecinos es 3, el conteo de vecinos adyacentes es 2

Adjacent with neighbor 203.250.15.1 (Designated Router)

Adjacent with neighbor 203.250.13.41 (Backup Designated Router)

RTB#show ip ospf interface e0

Ethernet0 is up, line protocol is up

Internet Address 203.250.14.3 255.255.255.0, Área 0.0.0.0

ID del proceso 10, ID del router 203.250.12.1, tipo de red BROADCAST, Cost: 10

Transmit Delay is 1 sec, Estado DROTHER, Priority 1

Router designado (ID) 203.250.15.1, Interface address 203.250.14.2

Router designado de respaldo (ID) 203.250.13.41, Interface address 203.250.14.1

Timer intervals configured, Saludo 10, muerto 40, Wait 40, Retransmit 5

Hello due in 0:00:03

El conteo de vecinos es 3, el conteo de vecinos adyacentes es 2

Adjacent with neighbor 203.250.15.1 (Designated Router)

Adjacent with neighbor 203.250.13.41 (Backup Designated Router).

El resultado anterior muestra información muy importante. Consideremos el resultado de RTA. Ethernet0 está en el área 0.0.0.0. El ID del proceso es 10 (router ospf 10) y el ID del router es 203.250.13.41. Recuerde que el RID es la dirección IP más alta del cuadro o la interfaz del bucle de retorno, calculada durante el arranque o al reiniciarse el proceso OSPF. El estado de la interfaz es BDR. Dado que todos los routers tienen la misma prioridad OSPF en Ethernet 0 (el valor predeterminado es 1), la interfaz de RTF se seleccionó como DR debido al RID más elevado. De la misma forma, RTA se seleccionó como BDR.

El RTD y el RTB no son ni un DR ni un BDR y su estado es DROTHER. [7]. [8]

Tome en cuenta también el conteo de vecinos y el conteo adyacente. RTD tiene tres vecinos y es adyacente a dos de ellos, el DR y el BDR. RTF tiene tres vecinos y es adyacente a todos ellos porque es el DR.

La información acerca del tipo de red es importante y determinará el estado de la interfaz. En redes de transmisión como Ethernet, la elección de DR y DBR debería ser irrelevante para el usuario final. No debería importar cuál es DR o cuál es BDR.

En otros casos, por ejemplo, medios NBMA como Frame Relay y X.25, esto es muy importante para que OSPF funcione correctamente. Afortunadamente, con la introducción de subinterfaces punto a punto y punto a multipunto, la elección de DR ya no es un problema. OSPF en redes NBMA se tratará en la siguiente sección.

Otro comando que debemos tener en cuenta es:

show ip ospf neighbor

Consideremos el resultado de RTD:

RTD#show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface

203.250.12.1 1 2WAY/DROTHER 0:00:37 203.250.14.3 Ethernet0

203.250.15.1 1 FULL/DR 0:00:36 203.250.14.2 Ethernet0

203.250.13.41 1 FULL/BDR 0:00:34 203.250.14.1 Ethernet0

El comando show ip ospf neighbor muestra el estado de todos los vecinos en un segmento determinado. No se alarme si el "ID de vecino" no pertenece al segmento que está mirando. En nuestro caso, 203.250.12.1 y 203.250.15.1 no están en Ethernet0. Esto es correcto ya que el "ID del vecino" es de hecho el RID que podría ser cualquier dirección IP en el cuadro. RTD y RTB son sólo vecinos, motivo por el

cual el estado es BIDIRECCIONAL/DROTHER. RTD es adyacente a RTA y RTF y el estado es FULL/DR y FULL/BDR.

Una vez teniendo una referencia sobre las características del protocolo de enrutamiento OSPF deberemos de igual manera tener referencias hacia los conceptos sobre VPN'S, VLAN'S y PSEWDOWIRE. [9]

3.16 VPN

Una red privada virtual (VPN) es una red privada construida dentro de una infraestructura de red pública, tal como la red mundial de Internet. Las empresas pueden usar redes privadas virtuales para conectar en forma segura oficinas y usuarios remotos a través de accesos a Internet económicos proporcionados por terceros, en vez de costosos enlaces WAN dedicados o enlaces de marcación remota de larga distancia.

Las organizaciones pueden usar redes privadas virtuales para reducir los costos de ancho de banda de redes WAN, y a la vez aumentar las velocidades de conexión a través de conectividad a Internet de alto ancho de banda, tal como DSL, Ethernet o cable.

Las redes privadas virtuales proporcionan el mayor nivel posible de seguridad mediante seguridad IP (IP Sec) cifrada o túneles VPN de Secure Sockets Layer (SSL) y tecnologías de autenticación. Estas tecnologías protegen los datos que pasan por la red privada virtual contra accesos no autorizados. Las empresas pueden aprovechar la infraestructura estilo Internet de la red privada virtual, cuya sencillez de abastecimiento permite agregar rápidamente nuevos sitios o usuarios. También pueden aumentar drásticamente el alcance de la red privada virtual sin expandir significativamente la infraestructura. [**7**] [**8**].

Las redes privadas virtuales extienden la seguridad a los Usuarios Remotos.

Las redes VPN SSL y VPN IPSec se han convertido en las principales soluciones de redes privadas virtuales para conectar oficinas remotas, usuarios remotos y partners comerciales, porque:

- Proporcionan comunicaciones seguras con derechos de acceso adaptados a usuarios individuales, tales como empleados, contratistas y partners.

- Aumentan la productividad al ampliar el alcance de las redes y aplicaciones empresariales.
- Reducen los costos de comunicación y aumentan la flexibilidad.

Los dos tipos de redes virtuales privadas cifradas:

- **VPN IP SEC de sitio a sitio:** Esta alternativa a Frame Relay o redes WAN de línea arrendada permite a las empresas extender los recursos de la red a las sucursales, oficinas en el hogar y sitios de los partners comerciales.
- **VPN de acceso remoto:** Esto extiende prácticamente todas las aplicaciones de datos, voz o video a los escritorios remotos, emulando los escritorios de la oficina central. Las redes VPN de acceso remoto pueden desplegarse usando redes VPN SSL, IPSEC o ambas, dependiendo de los requisitos de implementación.

3.17 Visión General de VLAN

Una VLAN es un grupo de estaciones finales en una red conmutada que está lógicamente segmentada por funciones o aplicaciones, sin tener en cuenta la ubicación física de los usuarios. Las VLAN's tienen los mismos atributos que las LAN físicas, pero puedes agrupar las estaciones finales, incluso si no se encuentran físicamente en el mismo segmento de LAN.

Cualquier puerto del switch puede pertenecer a una VLAN, y los paquetes de unicast, broadcast, multidifusión se reenvían y fluyen sólo a las estaciones del fin de esa VLAN. Cada VLAN se considera como una red lógica, y los paquetes con destino a las estaciones que no pertenecen a la VLAN debe ser enviada a través de un router.

La Figura 3.11 muestra las VLAN como redes lógicas. Las estaciones en el departamento de ingeniería son asignadas a una VLAN, las estaciones en el departamento de marketing se asignan a otra VLAN, y las estaciones en la contabilidad se asignan a otra VLAN.

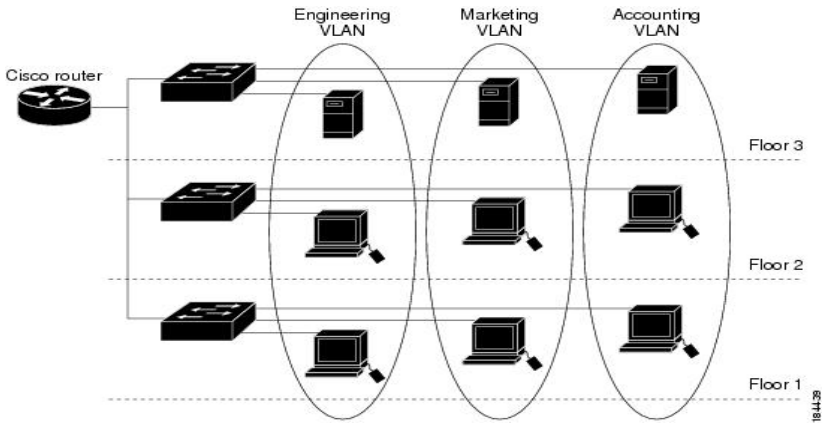

Figura 3.11: Visión general de la VLAN como redes lógicas

3.18 Detalles de la VLAN

Una VLAN es una subred IP separada de manera lógica. Las VLAN permiten que redes de IP y subredes múltiples existan en la misma red conmutada. La figura muestra una red con tres computadoras. Para que las computadoras se comuniquen en la misma VLAN, cada una debe tener una dirección IP y una máscara de subred consistente con esa VLAN. En el switch deben darse de alta las VLANs y cada puerto asignarse a la VLAN correspondiente. Un puerto de switch con una VLAN singular configurada en el mismo se denomina puerto de acceso. Recuerde que si dos computadoras están conectadas físicamente en el mismo switch no significa que se puedan comunicar. Los dispositivos en dos redes y subredes separadas se deben comunicar a través de un router (Capa 3), se utilicen o no las VLAN. No necesita las VLAN para tener redes y subredes múltiples en una red conmutada, pero existen ventajas reales para utilizar las VLAN.

3.19 Ventajas de las VLAN

La productividad del usuario y la adaptabilidad de la red son impulsores clave para el crecimiento y el éxito del negocio. La implementación de la tecnología de VLAN permite que una red admita de manera más flexible las metas comerciales [9]. Los principales beneficios de utilizar las VLAN son los siguientes:

Seguridad: los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial. Las computadoras del cuerpo docente se encuentran en la VLAN 10 y están completamente separadas del tráfico de datos del Invitado y de los estudiantes.

Reducción de costo: el ahorro en el costo resulta de la poca necesidad de actualizaciones de red caras y más usos eficientes de enlaces y ancho de banda existente.

Mejor rendimiento: la división de las redes planas de Capa 2 en múltiples grupos lógicos de trabajo (dominios de broadcast) reduce el tráfico innecesario en la red y potencia el rendimiento.

Mitigación de la tormenta de broadcast: la división de una red en las VLAN reduce la cantidad de dispositivos que pueden participar en una tormenta de broadcast. Como se analizó en el capítulo "Configure un switch", la segmentación de LAN impide que una tormenta de broadcast se propague a toda la red. En la figura puede observar que, a pesar de que hay seis computadoras en esta red, hay sólo tres dominios de broadcast: Cuerpo docente, Estudiante e Invitado.

Mayor eficiencia del personal de TI: las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN. Cuando proporciona un switch nuevo, todas las políticas y procedimientos que ya se configuraron para la VLAN particular se implementan cuando se asignan los puertos.

También es fácil para el personal de TI identificar la función de una VLAN proporcionándole un nombre. En la figura, para una identificación más fácil se nombró "Estudiante" a la VLAN 20, la VLAN 10 se podría nombrar "Cuerpo docente" y la VLAN 30 "Invitado".

Administración de aplicación o de proyectos más simples: Las VLAN agregan dispositivos de red y usuarios para admitir los requerimientos geográficos o comerciales. Tener funciones separadas hace que gestionar un

proyecto o trabajar con una aplicación especializada sea más fácil, por ejemplo una plataforma de desarrollo de e-learning para el cuerpo docente. También es fácil determinar el alcance de los efectos de la actualización de los servicios de red. En la Figura 3.12 se muestran las ventajas:

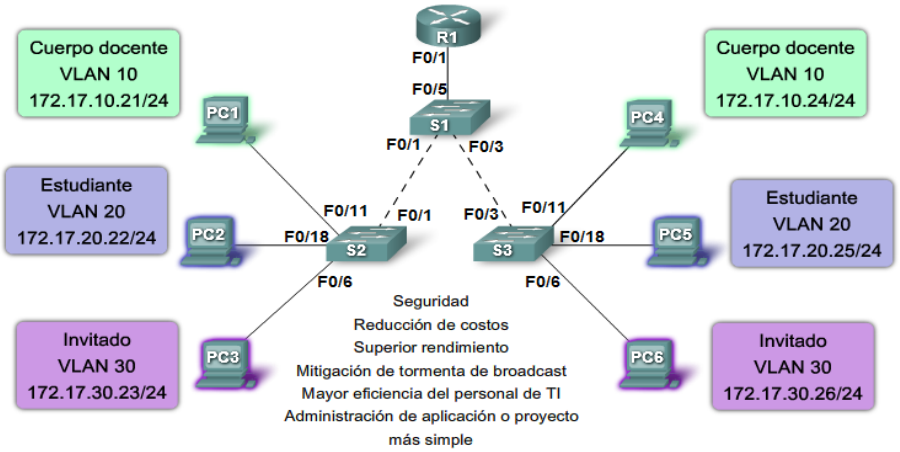

Figura 3.12: Ventajas de VLAN

3.20 Rangos del ID de la VLAN

El acceso a las VLAN está dividido en un rango normal o un rango extendido:

3.20.1 VLAN de rango normal

Se utiliza en redes de pequeños y medianos negocios y empresas. Se identifica mediante un ID de VLAN entre 1 y 1005.

Los ID de 1002 a 1005 se reservan para las VLAN Token Ring y FDDI.

Los ID 1 y 1002 a 1005 se crean automáticamente y no se pueden eliminar.

Las configuraciones se almacenan dentro de un archivo de datos de la VLAN, denominado vlan.dat. El archivo vlan.dat se encuentra en la memoria flash del switch.

El protocolo de enlace troncal de la VLAN (VTP), que ayuda a gestionar las configuraciones de la VLAN entre los switches, sólo puede asimilar

las VLAN de rango normal y las almacena en el archivo de base de datos de la VLAN.

3.20.2 VLAN de rango extendido

Posibilita a los proveedores de servicios que amplíen sus infraestructuras a una cantidad de clientes mayor. Algunas empresas globales podrían ser lo suficientemente grandes como para necesitar los ID de las VLAN de rango extendido.

Se identifican mediante un ID de VLAN entre 1006 y 4094. Admiten menos características de VLAN que las VLAN de rango normal. Se guardan en el archivo de configuración en ejecución. VTP no aprende las VLAN de rango extendido.

3.21 255 VLAN configurables

Un switch de Cisco Catalyst 2960 puede admitir hasta 255 VLAN de rango normal y extendido, a pesar de que el número configurado afecta el rendimiento del hardware del switch.

Debido a que la red de una empresa puede necesitar un switch con muchos puertos, Cisco ha desarrollado switches a nivel de empresa que se pueden unir o apilar juntos para crear una sola unidad de conmutación que consiste en nueve switches separados.

Cada switch por separado puede tener 48 puertos, lo que suma 432 puertos en una sola unidad de conmutación. En este caso, el límite de 255 VLAN por un solo switch podría ser una restricción para algunos clientes de empresas.

3.22 Características del VLAN

La Figura 3.13 hace referencia a las características de VLAN:

Figura 3.13: Características de VLAN

3.23 Tipos de VLAN

A continuación la Figura 3.14 detalla dinámicamente los tipos de VLAN:

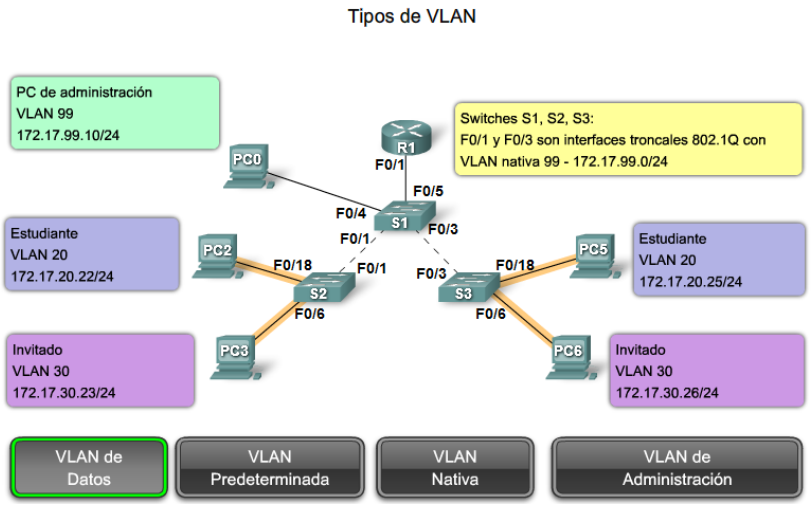

Figura 3.14: Tipos de VLAN

3.24 VLAN de voz

Es fácil apreciar por qué se necesita una VLAN separada para admitir la Voz sobre IP (VoIP). Imagine que está recibiendo una llamada de urgencia y de

repente la calidad de la transmisión se distorsiona tanto que no puede comprender lo que está diciendo la persona que llama. El tráfico de VoIP requiere:

- Ancho de banda garantizado para asegurar la calidad de la voz.
- Prioridad de la transmisión sobre los tipos de tráfico de la red.
- Capacidad para ser enrutado en áreas congestionadas de la red.
- Demora de menos de 150 milisegundos (ms) a través de la red.

Para cumplir estos requerimientos, se debe diseñar la red completa para que admita VoIP.

Los detalles sobre cómo configurar una red para que admita VoIP están más allá del alcance del curso, pero es útil resumir cómo una VLAN de voz, funciona entre un switch, un teléfono IP de Cisco y una computadora.

En la Figura 3.15, la VLAN 150 se diseña para enviar tráfico de voz. La computadora del estudiante PC5 está conectada al teléfono IP de Cisco y el teléfono está conectado al switch S3. La PC5 está en la VLAN 20 que se utiliza para los datos de los estudiantes. El puerto F0/18 en S3 se configura para que esté en modo de voz a fin de que diga al teléfono que etiquete las tramas de voz con VLAN 150. Las tramas de datos que vienen a través del teléfono IP de Cisco desde la PC5 no se marcan.

Los datos que se destinan a la PC5 que llegan del puerto F0/18 se etiquetan con la VLAN 20 en el camino al teléfono, que elimina la etiqueta de la VLAN antes de que los datos se envíen a la PC5. Etiquetar se refiere a la adición de bytes a un campo en la trama de datos que utiliza el switch para identificar a qué VLAN se debe enviar la trama de datos.

3.25 Un teléfono de Cisco es un switch

El teléfono IP de Cisco contiene un switch integrado de tres puertos 10/100, como se muestra en la figura. Los puertos proporcionan conexiones dedicadas para estos dispositivos:

- El puerto 1 se conecta al switch o a otro dispositivo de voz sobre IP (VoIP).

- El puerto 2 es una interfaz interna 10/100 que envía el tráfico del teléfono IP.
- El puerto 3 (puerto de acceso) se conecta a una PC u otro dispositivo.

La función de la VLAN de voz permite que los puertos de switch envíen el tráfico de voz IP desde un teléfono IP.

Cuando se conecta el switch a un teléfono IP, el switch envía mensajes que indican al teléfono IP conectado que envíe el tráfico de voz etiquetado con el ID 150 de VLAN de voz.

El tráfico de la PC conectada al teléfono IP pasa por el teléfono IP sin etiquetar. Cuando se configuró el puerto del switch con una VLAN de voz, el enlace entre el switch y el teléfono IP funciona como un enlace troncal para enviar tanto el tráfico de voz etiquetado como el tráfico de datos no etiquetado.

La comunicación entre el switch y el teléfono IP la facilita el protocolo CDP. Este protocolo se analizará en detalle en CCNA Exploration: Curso sobre Conceptos y protocolos de enrutamiento.

3.26 Ejemplo de configuración

La Figura 3.15 también muestra el resultado del ejemplo. Un análisis de los comandos IOS de Cisco está más allá del alcance de este curso pero puede observar que las áreas destacadas en el resultado del ejemplo muestran la interfaz F0/18 configurada con una VLAN configurada para datos (VLAN 20) y una VLAN configurada para voz (VLAN 150).

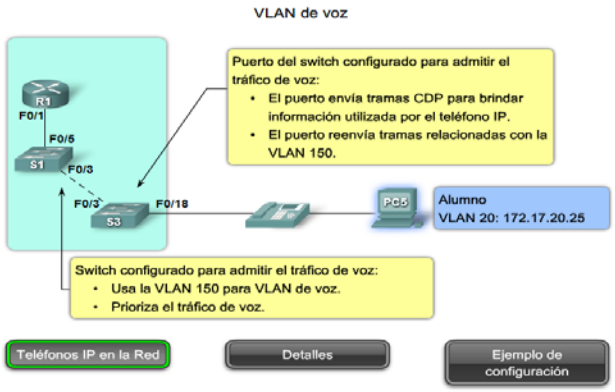

Figura 3.15: VLAN de voz

3.27 Tipos de tráfico de red

En CCNA Exploration: En Aspectos básicos de redes, aprendió sobre los diferentes tipos de tráfico que puede manejar una LAN. Debido a que una VLAN tiene todas las características de una LAN, una VLAN debe incorporar el mismo tráfico de red que una LAN.

3.28 Administración de red y tráfico de control

Muchos tipos diferentes de tráfico de administración de red y de control pueden estar presentes en la red, como las actualizaciones de Cisco Discovery Protocol (CDP), Simple Network Management Protocol (SNMP) y tráfico de Remote Monitoring (RMON).

- **Telefonía IP**

  Los tipos de tráfico de telefonía IP son el tráfico de señalización y el tráfico de voz. El tráfico de señalización es responsable de la configuración de la llamada, el progreso y la desconexión y atraviesa la red de extremo a extremo. El otro tipo de tráfico de telefonía consiste en paquetes de datos de la conversación de voz existente. Como acaba de ver, en una red configurada con VLAN, se recomienda con énfasis asignar una VLAN diferente a la VLAN 1 como VLAN de administración. El tráfico de datos debe asociarse con una VLAN de datos (diferente a la VLAN 1) y el tráfico de voz se asocia con una VLAN de voz.

- **IP Multicast**

  El tráfico IP multicast se envía desde una dirección de origen particular a un grupo multicast que se identifica mediante un único IP y un par de direcciones MAC de grupo de destino. Broadcasts Cisco IP/TV son ejemplos de aplicaciones que genera este tipo de tráfico. El tráfico multicast puede producir una gran cantidad de datos que se transmiten a través de la red. Cuando la red debe admitir tráfico multicast, las VLAN deben configurarse para asegurarse de que el tráfico multicast se dirija sólo a aquellos dispositivos de usuario que utilizan el servicio proporcionado, como aplicaciones de audio o video remoto. Los routers se deben

configurar para asegurar que el tráfico multicast se envíe a las áreas de red cuando se le solicita.

- **Datos normales**

  El tráfico de datos normales se relaciona con el almacenamiento y creación de archivos, servicios de impresión, acceso a la base de datos del correo electrónico y otras aplicaciones de red compartidas que son comunes para usos comerciales. Las VLAN son una solución natural para este tipo de tráfico, ya que pueden segmentar a los usuarios por sus funciones o área geográfica para administrar de manera más fácil las necesidades específicas.

- **Clase Scavenger**

  Se pretende que la clase Scavenger proporcione servicios less-than-best-effort a ciertas aplicaciones. Las aplicaciones que se asignan a esta clase contribuyen poco o nada a los objetivos organizativos de la empresa y están generalmente orientadas, por su naturaleza, al entretenimiento. Esto incluye aplicaciones compartidas de medios entre pares (KaZaa, Morpheus, Groekster, Napster, iMesh, y demás), aplicaciones de juegos (Doom, Quake, Unreal Tournament, y demás) y cualquier aplicación de video de entretenimiento.

3.29 Modos de Membresía del puerto de switch

3.29.1 Puertos de switch

Los puertos de switch son interfaces de Capa 2 únicamente asociados con un puerto físico. Los puertos de switch se utilizan para manejar la interfaz física y los protocolos asociados de Capa 2. No manejan enrutamiento o puenteo. Los puertos de switch pertenecen a una o más VLAN. La Figura 3.16 muestra las membresías.

3.29.2 Modos de puertos de switch de VLAN

Cuando configura una VLAN, debe asignarle un número de ID y le puede dar un nombre si lo desea. El propósito de las implementaciones de la

VLAN es asociar con criterio los puertos con las VLAN particulares. Se configura el puerto para enviar una trama a una VLAN específica. Como se mencionó anteriormente, el usuario puede configurar una VLAN en el modo de voz para admitir tráfico de datos y de voz que llega desde un teléfono IP de Cisco. El usuario puede configurar un puerto para que pertenezca a una VLAN mediante la asignación de un modo de Membresía que especifique el tipo de tráfico que envía el puerto y las VLAN a las que puede pertenecer. Se puede configurar un puerto para que admita estos tipos de VLAN:

- **VLAN estática.**

  Los puertos en un switch se asignan manualmente a una VLAN. Las VLAN estáticas se configuran por medio de la utilización del CLI de Cisco. Esto también se puede llevar a cabo con las aplicaciones de administración de GUI, como el Asistente de red Cisco. Sin embargo, una característica conveniente del CLI es que si asigna una interfaz a una VLAN que no existe, se crea la nueva VLAN para el usuario. Para ver un ejemplo de configuración de VLAN estática, haga clic en el botón Ejemplo de Modo Estático en la figura. Cuando haya finalizado, haga clic en el botón Modos de Puertos en la figura. Esta configuración no se examinará en detalle.

- **VLAN dinámica**

  Este modo no se utiliza ampliamente en las redes de producción y no se investiga en este curso. Sin embargo, es útil saber qué es una VLAN dinámica. La membrecía de una VLAN de puerto dinámico se configura utilizando un servidor especial denominado Servidor de política de membrecía de VLAN (VMPS). Con el VMPS, asigna puertos de switch a las VLAN basadas en forma dinámica en la dirección MAC de origen del dispositivo conectado al puerto. El beneficio llega cuando traslada un host desde un puerto en un switch en la red hacia un puerto sobre otro switch en la red. El switch asigna

en forma dinámica el puerto nuevo a la VLAN adecuada para ese host.

- **VLAN de voz**

  El puerto está configurado para que esté en modo de voz a fin de que pueda admitir un teléfono IP conectado al mismo. Antes de que configure una VLAN de voz en el puerto, primero debe configurar una VLAN para voz y una VLAN para datos. En la figura, la VLAN 150 es la VLAN de voz y la VLAN 20 es la VLAN de datos. Se supone que la red ha sido configurada para garantizar que el tráfico de voz se pueda transmitir con un estado prioritario sobre la red.

  Cuando se enchufa por primera vez un teléfono en un puerto de switch que está en modo de voz, éste envía mensajes al teléfono proporcionándole la configuración y el ID de VLAN de voz adecuado. El teléfono IP etiqueta las tramas de voz con el ID de VLAN de voz y envía todo el tráfico de voz a través de la VLAN de voz.

  El comando de configuración mls qos trust cos garantiza que el tráfico de voz se identifique como tráfico prioritario. Recuerde que toda la red debe prepararse para que priorice el tráfico de voz. No puede simplemente configurar el puerto con este comando.

  El comando switchport voice VLAN 150 identifica a la VLAN 150 como VLAN de voz. Puede observar esto verificado en la parte inferior de la captura de la pantalla: VLAN de voz: 150 (VLAN0150).

  El comando switchport access VLAN 20 configura la VLAN 20 como la VLAN de modo de acceso (datos). Puede observar esto verificado en la parte inferior de la captura de la pantalla: VLAN de modo de acceso: 20 (VLAN0020).

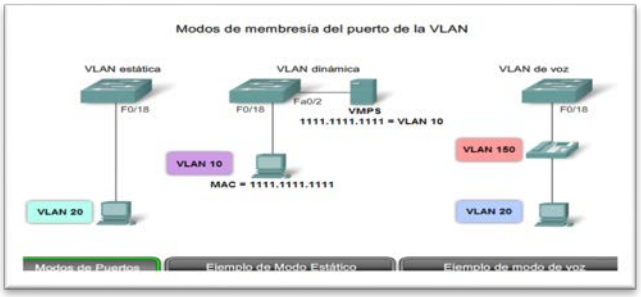

Figura 3.16: Modos de Membresía del puerto VLAN

3.30 Control de dominios de los broadcast en las VLAN

3.30.1 Red sin VLAN

En funcionamiento normal, cuando un switch recibe una trama de broadcast en uno de sus puertos, envía la trama a todos los demás puertos. En la figura, toda la red está configurada en la misma subred, 172.17.40.0/24. Como resultado, cuando la computadora del cuerpo docente, PC1, envía una trama de broadcast, el switch S2 envía esa trama de broadcast a todos sus puertos. La red completa la recibe finalmente; la red es un dominio de broadcast.

3.30.2 Red con VLAN

En la Figura 3.15, se dividió la red en dos VLAN: Cuerpo docente como VLAN 10 y Estudiante como VLAN 20. Cuando se envía la trama de broadcast desde la computadora del cuerpo docente, PC1, al switch S2, el switch envía esa trama de broadcast sólo a esos puertos de switch configurados para admitir VLAN 10.

En la Figura 3.15, los puertos que componen la conexión entre los switches S2 y S1 (puertos F0/1) y entre S1 y S3 (puertos F0/3) han sido configurados para admitir todas las VLAN en la red. Esta conexión se denomina enlace troncal. Más adelante en este capítulo aprenderá más acerca de los enlaces troncales.

Cuando S1 recibe la trama de broadcast en el puerto F0/1, S1 envía la trama de broadcast por el único puerto configurado para admitir la VLAN

10, puerto F0/3. Cuando S3 recibe la trama de broadcast en el puerto F0/3, envía la trama de broadcast por el único puerto configurado para admitir la VLAN 10, puerto F0/11. La trama de broadcast llega a la única otra computadora en la red configurada en la VLAN 10, la computadora PC4 del cuerpo docente.

Cuando las VLAN se implementan en un switch, la transmisión del tráfico de unicast, multicast y broadcast desde un host en una VLAN en particular, se limitan a los dispositivos presentes en la VLAN.

3.31 Control de dominios broadcast : switches y routers

La fragmentación de un gran dominio de broadcast en varias partes más pequeñas reduce el tráfico de broadcast y mejora el rendimiento de la red. La fragmentación de dominios en VLAN permite además una mejor confidencialidad de información dentro de una organización. La fragmentación de dominios de broadcast puede realizarse con las VLAN (en los switches) o con routers. Cada vez que dispositivos en diferentes redes de Capa 3 necesiten comunicarse, es necesario un router sin tener en cuenta si las VLAN están en uso.

3.31.1 Comunicación dentro de la VLAN

En la Figura 3.16, la PC1 desea comunicarse con otro dispositivo, la PC4. La PC1 y la PC4 se encuentran en la VLAN 10. La comunicación con un dispositivo en la misma VLAN se denomina comunicación inter VLAN. A continuación se describe cómo se realiza este proceso:

Paso 1. La PC1 en la VLAN 10 envía su trama de petición ARP (broadcast) al switch S2. Los switches S2 y S1 envían la trama de petición ARP a todos los puertos en la VLAN 10. El switch S3 envía la petición ARP al puerto F0/11 para la PC4 en la VLAN 10.

Paso 2. Los switches en la red envían la trama de respuesta ARP (unicast) a todos los puertos configurados para la VLAN 10. La PC1 recibe la respuesta que contiene la dirección MAC de la PC4.

Paso 3. Ahora la PC1 tiene la dirección MAC de destino de la PC4 y la utiliza para crear una trama unicast con la dirección MAC de la PC4 como destino. Los switches S2, S1 y S3 envían la trama a la PC4.

Paso 4. Haga clic en el botón Comunicación entre VLAN y en el ícono reproducir para que comience la animación.

3.31.2 Comunicación entre VLAN

La PC1 en la VLAN 10 desea comunicarse con la PC5 en la VLAN 20. La comunicación con un dispositivo en otra VLAN se denomina comunicación entre VLAN.

Nota: Existen dos conexiones desde el switch S1 hasta el router: una para enviar transmisiones en la VLAN 10 y la otra para enviar transmisiones en la VLAN 20 hacia la interfaz del router.

A continuación se describe cómo se realiza este proceso:

Paso 1. La PC1 en la VLAN 10 desea comunicarse con la PC5 en la VLAN 20. La PC1 envía una trama de petición ARP para la dirección MAC del gateway predeterminado R1.

Paso 2. El router R1 responde con una trama de respuesta ARP desde su interfaz configurada en la VLAN 10.

Todos los switches envían la trama de respuesta ARP y la PC1 la recibe. La respuesta ARP contiene la dirección MAC del gateway predeterminado.

Paso 3. La PC1 crea, entonces, una trama de Ethernet con la dirección MAC del Gateway predeterminado. La trama se envía desde el switch S2 al S1.

Paso 4. El router R1 envía una trama de petición ARP en la VLAN 20 para determinar la dirección MAC de la PC5. Los switches S1, S2 y S3, emiten la trama de petición ARP a los puertos configurados para la VLAN 20. La PC5 en la VLAN 20 recibe la trama de petición ARP del router R1.

Paso 5. La PC5 en la VLAN 20 envía una trama de respuesta ARP al switch S3. Los switches S3 y S1 envían la trama de respuesta ARP al router R1 con la dirección MAC de destino de la interfaz F0/2 en el router R1.

Paso 6. El router R1 envía la trama recibida de la PC1 a S1 y S3 a la PC5 (en la VLAN 20).

3.32 Control de dominios: VLAN y reenvío de capa 3

En la Figura 3.17 se muestra el switch Catalyst 3750G-24PS, uno de los tantos switches de Cisco que admite el enrutamiento de Capa 3. El ícono que representa el switch de Capa 3 se visualiza. La explicación sobre la conmutación de la Capa 3 excede el alcance de este curso, pero es útil una breve descripción de la tecnología de interfaz virtual del switch (SVI, por su sigla en inglés) que permite al switch de Capa 3 enrutar transmisiones entre las VLAN.

Figura 3.17: Control de Dominios con VLAN y reenvío de Capa 3

SVI es una interfaz lógica configurada para una VLAN específica. Es necesario configurar una SVI para una VLAN si desea enrutar entre las VLAN o para proporcionar conectividad de host IP al switch. De manera predeterminada, una SVI se crea por la VLAN predeterminada (VLAN 1) para permitir la administración de switch remota.

Haga clic en el botón Ejemplo de Reenvío de Capa 3 en la figura para ver la animación que presenta una representación simplificada de cómo un switch de Capa 3 controla dominios de broadcast.

3.33 Reenvío de capa 3

Un switch de Capa 3 tiene la capacidad de enrutar transmisiones entre las VLAN, la Figura 3.18 lo muestra.

El procedimiento es el mismo que se describió para la comunicación entre VLAN utilizando un router distinto, excepto que las SVI actúan como las interfaces del router para enrutar los datos entre las VLAN. La animación describe este proceso.

En la animación, la PC1 desea comunicarse con la PC5. Los siguientes pasos detallan la comunicación a través del switch S1 de Capa 3:

Paso 1. La PC1 envía un broadcast de petición ARP en la VLAN10. S2 envía la petición ARP a todos los puertos configurados para la VLAN 10.

Paso 2. El switch S1 envía la petición ARP a todos los puertos configurados para la VLAN 10, incluida la SVI para la VLAN 10. El switch S3 envía la petición ARP a todos los puertos configurados para la VLAN 10.

Paso 3. La SVI para la VLAN 10 en el switch S1 conoce la ubicación de la VLAN 20. La SVI para la VLAN 10 en el switch S1 envía una respuesta ARP de vuelta a la PC1 con esta información.

Paso 4. La PC 1 envía datos, destinados a la PC5, como trama de unicast a través del switch S2 a la SVI para la VLAN 10 en el switch S1.

Paso 5. La SVI para la VLAN 20 envía un broadcast de petición ARP a todos los puertos de switch configurados para la VLAN 20. El switch S3 envía ese broadcast de petición ARP a todos los puertos de switch configurados para la VLAN 20.

Paso 6. La PC5 en la VLAN 20 envía una respuesta ARP. El switch S3 envía esa respuesta ARP a S1. El switch S1 envía la respuesta ARP a la SVI para la VLAN 20.

Paso 7. La SVI para la VLAN 20 envía los datos enviados desde la PC1 en una trama de unicast a la PC5, mediante la utilización de la dirección de destino que obtuvo de la respuesta ARP en el paso 6.

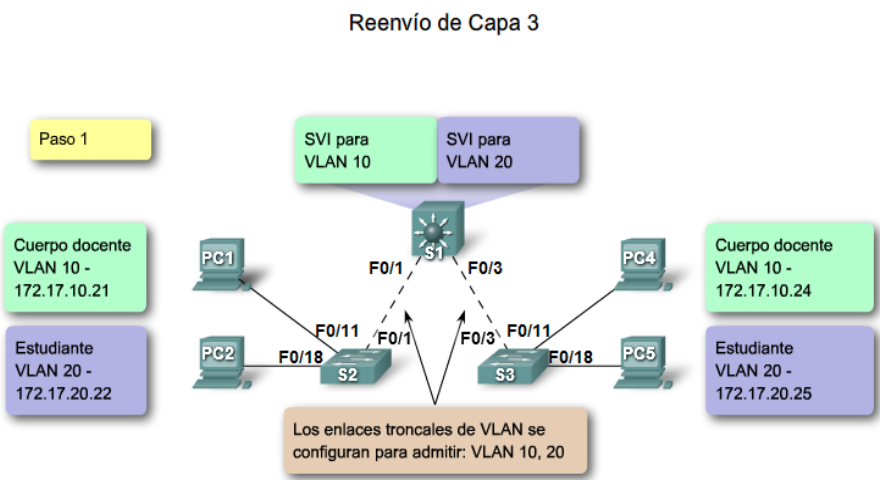

Figura 3.18: Reenvío de capa 3

3.34 Enlaces Troncales de las VLAN

Es difícil describir las VLAN sin mencionar los enlaces troncales de la VLAN. En párrafos anteriores se aprendió a controlar broadcasts de la red con segmentación de la VLAN y observó la manera en que los enlaces troncales de la VLAN transmitieron tráfico a diferentes partes de la red configurada en una VLAN.

En la Figura 3.19, los enlaces entre los switches S1 y S2 y entre S1 y S3 están configurados para transmitir el tráfico que proviene de las VLAN 10, 20, 30 y 99. Es posible que esta red no funcione sin los enlaces troncales de la VLAN, la mayoría de las redes que encuentra están configuradas con enlaces troncales de la VLAN.

Esta sección une los conocimientos previos sobre el enlace troncal de la VLAN y proporcionar los detalles necesarios para poder configurar el enlace troncal de la VLAN en una red.

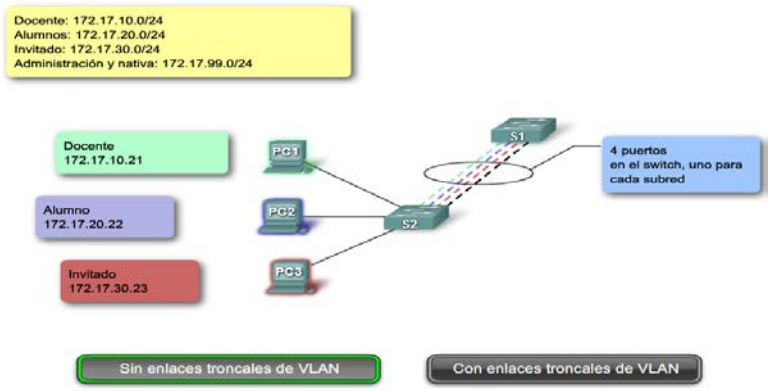

Figura 3.19: comparativo entre troncales VLAN con y sin enlace

3.34.1 Definición de enlace troncal de la VLAN

Un enlace troncal es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN. Como se visualiza en la Figura 3.20, un enlace troncal de VLAN le permite extender las VLAN a través de toda una red. Cisco admite IEEE 802.1Q para la coordinación de enlaces troncales en interfaces Fast Ethernet y Gigabit Ethernet. Más adelante en esta sección, aprenderá acerca de 802.1Q.

Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre switches y routers.

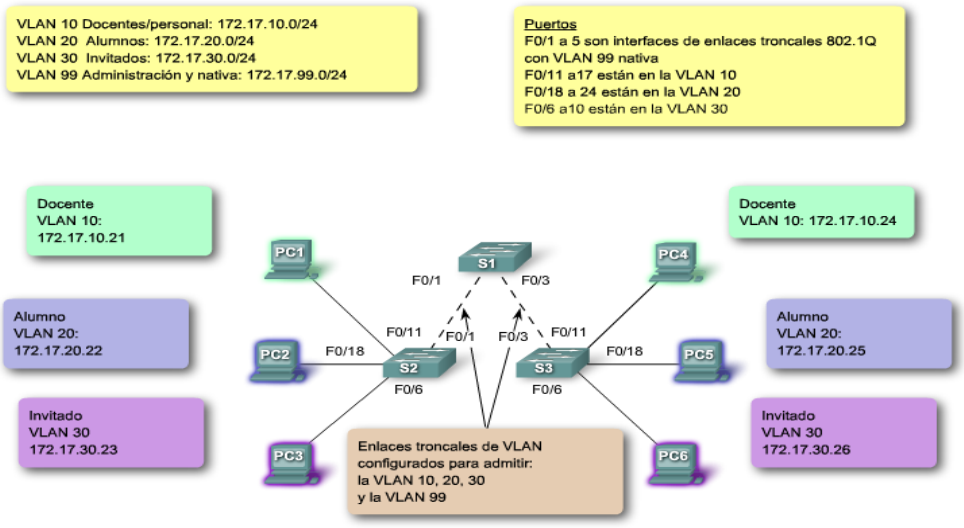

Figura 3.20: Definición de enlace troncal de VLAN

3.34.2 Etiquetado de trama 802.1Q

Los switches son dispositivos de capa 2. Sólo utilizan la información del encabezado de trama de Ethernet para enviar paquetes. El encabezado de trama no contiene la información que indique a qué VLAN pertenece la trama. Posteriormente, cuando las tramas de Ethernet se ubican en un enlace troncal, necesitan información adicional sobre las VLAN a las que pertenecen. Esto se logra por medio de la utilización del encabezado de encapsulación 802.1Q. Este encabezado agrega una etiqueta a la trama de Ethernet original y especifica la VLAN a la que pertenece la trama.

El etiquetado de la trama se mencionó en diferentes oportunidades. La primera vez se hizo en referencia a la configuración del modo de voz en un puerto de switch. En esa sección aprendió que una vez que se configura, un teléfono de Cisco (que incluye un switch pequeño) etiqueta las tramas de voz con un ID de VLAN. Los ID de VLAN pueden estar en un rango normal, 1-1005 y en un rango ampliado, 1006-4094. ¿De qué manera se insertan los ID de la VLAN en la trama?

3.34.3 Descripción del etiquetado de trama de VLAN

Antes de explorar los detalles de una trama 802.1Q, es útil comprender lo que hace un switch al enviar una trama a un enlace troncal. Cuando el switch recibe una trama en un puerto configurado en modo de acceso con una VLAN estática, el switch quita la trama e inserta una etiqueta de VLAN, vuelve a calcular la FCS y envía la trama etiquetada a un puerto de enlace troncal.

3.34.4 Detalles del campo de etiqueta de VLAN

El campo de etiqueta de la VLAN consiste de un campo EtherType, un campo de información de control de etiqueta y del campo de FCS. Según la muestra la Figura 3.21.

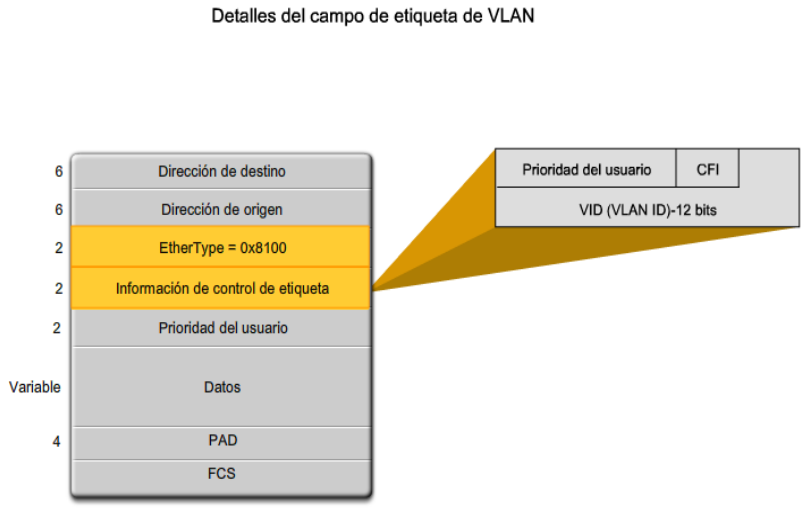

Figura 3.21: Detalle del campo de etiqueta VLAN

3.34.5 Campo EtherType

Establecido al valor hexadecimal de 0x8100. Este valor se denomina valor de ID de protocolo de etiqueta (TPID, por su sigla en inglés). Con el campo EtherType configurado al valor TPID, el switch que recibe la trama sabe buscar la información en el campo de información de control de etiqueta.

3.34.6 Campo Información de control de etiqueta

El campo de información de control de etiqueta contiene:

- Tres (3) bits de prioridad del usuario: utilizado por el estándar 802.1p, que especifica cómo proporcionar transmisión acelerada de las tramas de la Capa 2.
- Una descripción de IEEE 802.1p está más allá del alcance de este curso; sin embargo el usuario aprendió algo sobre esto anteriormente en el análisis sobre las VLAN de voz.
- Un (1) bit de Identificador de formato ideal (CFI, por su sigla en inglés): permite que las tramas Token Ring se transporten con facilidad a través de los enlaces Ethernet.

- Doce (12) bits del ID de la VLAN (VID): números de identificación de la VLAN; admite hasta 4096 ID de VLAN.

3.34.7 Campo FCS

Luego de que el switch inserta los campos de información de control de etiqueta y EtherType, vuelve a calcular los valores FCS y los inserta en la trama.

3.35 VLAN nativas y enlace troncal 802.1Q

VLAN nativa admite el switch en el manejo de tramas etiquetadas y sin etiquetar que llegan en un puerto de enlace troncal 802.1Q. Esto se muestra en la Figura 3.22.

VLAN Nativas y Enlace troncal 802.1Q

```
S1#show interfaces F0/1 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 50
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
…
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
….
Trunking VLANs Enabled: ALL
```

Figura 3.22: VLAN nativas y enlace Troncal 802.1Q

3.35.1 Tramas etiquetadas en la VLAN nativa

Algunos dispositivos que admiten enlaces troncales etiquetan la VLAN nativa como comportamiento predeterminado. El tráfico de control enviado en la VLAN nativa debe estar sin etiquetar. Si un puerto de enlace troncal 802.1Q recibe una trama etiquetada en la VLAN nativa, éste descarta la trama.

Como consecuencia, al configurar un puerto de switch en un switch Cisco, es necesario identificar estos dispositivos y configurarlos de manera que no envíen tramas etiquetadas en la VLAN nativa. Los dispositivos de otros proveedores que admiten tramas etiquetadas en la VLAN nativa incluyen: teléfonos IP, servidores, routers y switches que no pertenecen a Cisco.

3.35.2 Tramas sin etiquetar en la VLAN nativa

Cuando un puerto de enlace troncal de switch Cisco recibe tramas sin etiquetar, éste envía esas tramas a la VLAN nativa. Como debe recordar, la VLAN nativa predeterminada es la VLAN 1. Al configurar un puerto de enlace troncal 802.1Q, se asigna el valor del ID de la VLAN nativa al ID de la VLAN de puerto predeterminado (PVID).

Todo el tráfico sin etiquetar que ingresa o sale del puerto 802.1Q se envía en base al valor del PVID. Por ejemplo: si la VLAN 99 se configura como la VLAN nativa, el PVID es 99 y todo el tráfico sin etiquetar se envía a la VLAN 99. Si la VLAN nativa no ha sido configurada nuevamente, el valor de PVID se configura para la VLAN 1.

En este ejemplo, la VLAN 99 se configura como VLAN nativa en el puerto F0/1 en el switch S1. Este ejemplo muestra cómo volver a configurar la VLAN nativa desde su configuración predeterminada de la VLAN 1.

Comenzando en el modo EXEC privilegiado, la figura describe la manera de configurar la VLAN nativa en el puerto F0/1 en el switch S1 como un enlace troncal IEEE 802.1Q con la VLAN 99 nativa.

Al utilizar el comando show interfaces interface-id switchport puede verificar rápidamente si ha vuelto a configurar la VLAN nativa desde la VLAN 1 a la VLAN 99 de manera correcta. El resultado resaltado en la captura de pantalla indica que la configuración fue un éxito. La Figura 3.23 muestra las tramas y etiquetas VLAN nativas:

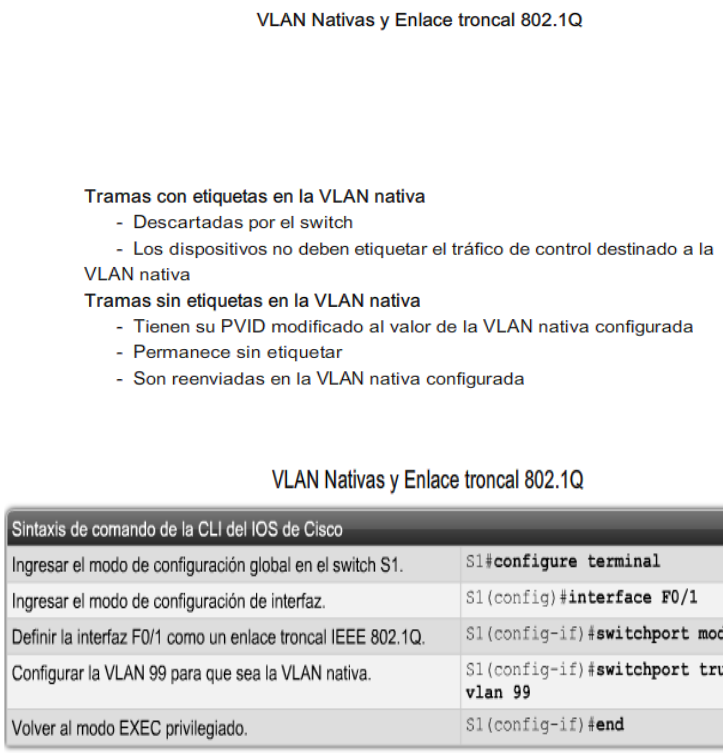

Figura 3.23: Tramas VLAN Nativas y Enlace Troncal 802.1Q

El usuario ha aprendido la manera en que el enlace troncal 802.1Q funciona en los puertos de switch de Cisco. Ahora es momento de examinar las opciones de configuración del modo de puerto de enlace troncal 802.1Q. Primero, es necesario analizar un protocolo de enlace troncal anterior de Cisco denominado enlace entre switch (ISL, Inter-Switch Link), debido a que verá esta opción en las guías de configuración de software del switch.

3.36 IEEE, no ISL

Aunque se puede configurar un switch de Cisco para admitir dos tipos de puertos de enlace troncal, IEEE 802.1Q e ISL; en la actualidad, sólo se usa el 802.1Q. Sin embargo, las redes antiguas siguen usando ISL, y es útil aprender sobre cada tipo de puerto de enlace troncal.

Un puerto de enlace troncal IEEE 802.1Q admite tráfico simultáneo etiquetado y sin etiquetar. A un puerto de enlace troncal 802.1Q se le asigna un PVID

predeterminado y todo el tráfico sin etiquetar se transporta en el PVID predeterminado del puerto. Se supone que todo el tráfico etiquetado y sin etiquetar con un ID nulo de la VLAN pertenece al PVID predeterminado del puerto. El paquete con un ID de VLAN igual al PVID predeterminado del puerto de salida se envía sin etiquetar. El resto del tráfico se envía con una etiqueta de VLAN.

En un puerto de enlace troncal ISL se espera que todos los paquetes recibidos sean encapsulados con un encabezado ISL y que todos los paquetes transmitidos se envíen con un encabezado ISL. Las tramas nativas (sin etiquetar) recibidas de un puerto de enlace troncal ISL se descartan. ISL ya no es un modo de puerto de enlace troncal recomendado y no se admite en varios de los switches de Cisco.

3.37 DTP

El protocolo de enlace troncal dinámico (DTP) es un protocolo propiedad de Cisco. Los switches de otros proveedores no admiten el DTP. El DTP es habilitado automáticamente en un puerto de switch cuando algunos modos de enlace troncal se configuran en el puerto de switch.

El DTP administra la negociación de enlace troncal sólo si el puerto en el otro switch se configura en modo de enlace troncal que admita DTP. El DTP admite los enlaces troncales ISL y 802.1Q. Este curso se concentra en la implementación de 802.1Q del DTP. Un análisis detallado sobre el DTP está más allá de este curso, sin embargo aprenderá sobre esto en las prácticas de laboratorio y actividades asociadas con este capítulo. Los switches no necesitan que el DTP realice enlaces troncales, y algunos switches y routers de Cisco no admiten al DTP.

3.38 Modos de enlaces troncales

Un puerto de switch en un switch de Cisco admite varios modos de enlaces troncales. El modo de enlace troncal define la manera en la que el puerto negocia mediante la utilización del DTP para configurar un enlace troncal con

su puerto par. A continuación, se describe brevemente los modos de enlaces troncales disponibles y la manera en que el DTP se implementa en cada uno.

3.38.1 Activación de manera predeterminada

El puerto del switch envía periódicamente tramas de DTP, denominadas notificaciones, al puerto remoto. El comando utilizado es "switchport mode trunk". El puerto de switch local notifica al puerto remoto que está cambiando dinámicamente a un estado de enlace troncal. Luego, el puerto local, sin importar la información de DTP que el puerto remoto envía como respuesta a la notificación, cambia al estado de enlace troncal. El puerto local se considera que está en un estado de enlace troncal (siempre activado) incondicional.

3.38.2 Dinámico automático

El puerto del switch envía periódicamente tramas de DTP al puerto remoto. El comando utilizado es switchport mode dynamic auto. El puerto de switch local notifica al puerto de switch remoto que puede establecer enlaces troncales pero no solicita pasar al estado de enlace troncal. Luego de una negociación de DTP, el puerto local termina en estado de enlace troncal sólo si el modo de enlace troncal del puerto remoto ha sido configurado para estar activo o si es conveniente. Si ambos puertos en los switches se configuran en automático, no negocian para estar en un estado de enlace troncal. Negocian para estar en estado de modo de acceso (sin enlace troncal).

3.39 Las tramas de DTP convenientes y dinámicas

Las tramas de DTP se envían periódicamente al puerto remoto. El comando utilizado es "switchport mode dynamic desirable". El puerto de switch local notifica al puerto de switch remoto que puede establecer enlaces troncales y solicita al puerto de switch remoto pasar al estado de enlace troncal. Si el puerto local detecta que el remoto ha sido configurado en modo activado, conveniente o automático, el puerto local termina en estado de enlace troncal. Si el puerto

de switch remoto está en modo sin negociación, el puerto de switch local permanece como puerto sin enlace troncal.

3.40 Desactivación del DTP

Puede desactivar el DTP para el enlace troncal para que el puerto local no envíe tramas de DTP al puerto remoto. Utilice el comando "switchport nonegotiate". Entonces el puerto local se considera que está en un estado de enlace troncal incondicional. Utilice esta característica cuando necesite configurar un enlace troncal con un switch de otro proveedor.

3.41 Ejemplo de modo de enlace troncal

En la Figura 3.24, los puertos F0/1 en los switches S1 y S2 se configuran con modo de enlace troncal activado. Los puertos F0/3 en los switches S1 y S3 se configuran para que estén en modo de enlace troncal automático. Cuando se completen las configuraciones de switch y los switches están configurados por completo, ¿Qué enlace se configurará como enlace troncal?

El enlace entre los switches S1 y S2 se convierte en enlace troncal porque los puertos F0/1 en los switches S1 y S2 se configuran para ignorar todas las notificaciones del DTP y aparecen y permanecen en modo de puerto de enlace troncal. Los puertos F0/3 en los switches S1 y S3 se establecen en automático, entonces negocian para estar en estado predeterminado, el estado de modo de acceso (sin enlace troncal). Esto da por resultado un enlace troncal inactivo. Cuando configura un puerto de enlace troncal para que esté en modo de puerto de enlace troncal, no existe ambigüedad sobre en qué estado se encuentra el enlace troncal: está siempre activo. Además, es fácil recordar en qué estado están los puertos de enlaces troncales: si se supone que el puerto es un enlace troncal, el modo de enlace troncal es activo.

Es importante considerar que el modo switchport predeterminado para una interfaz en un switch Catalyst 2950 es conveniente y dinámico, pero el modo switchport predeterminado para una interfaz en un switch Catalyst 2960 es automático y dinámico. Si S1 y S3 fueran switches Catalyst 2950 con interfaz

F0/3 en modo switchport predeterminado, el enlace entre S1 y S3 se convertiría en un enlace troncal activo.

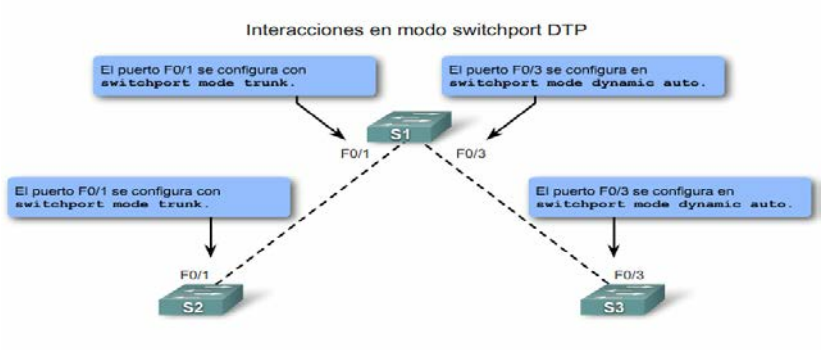

Figura 3.24: Enlace troncal interacción en modo SWITCHPORT DTP

3.42 Configuración de las VLAN y enlaces troncales

La configuración de VLAN requiere el uso de comandos clave IOS de Cisco necesarios para crear, eliminar y verificar las VLAN y los enlaces troncales de las VLAN. Por lo general, estos comandos poseen muchos parámetros opcionales que extienden las capacidades de la tecnología de las VLAN y enlaces troncales de las VLAN. Estos comandos opcionales no se presentan; sin embargo, se hace referencia en caso de que sea necesario usar estas opciones.

Esta sección muestra la sintaxis de configuración y verificación para un lado de la VLAN o del enlace troncal. De ser necesario mantener la configuración activa recién configurada, se debe guardarla en la configuración de inicio.

3.43 Agregue una VLAN

Para agregar una VLAN se debe a crear una VLAN estática en un switch “Cisco Catalyst” mediante el modo de configuración global de la VLAN se muestra en la Figura 3.25. Existen dos modos diferentes para configurar las VLAN en un switch Cisco Catalyst:

- Modo de configuración de base de datos.
- Modo de configuración global.

A pesar de que la documentación de Cisco menciona el modo de configuración de base de datos de la VLAN, se elimina a favor del modo de configuración global de la VLAN.

El manual sugiere configurar las VLAN con los ID en el rango normal. Existen dos rangos de ID de la VLAN:

- Rango normal incluye los ID 1 a 1001
- Rango ampliado consiste de los ID 1006 a 4094. VLAN 1 y 1002 a 1005 son números de ID reservados.

Cuando configura las VLAN de rango normal, los detalles de configuración se almacenan automáticamente en la memoria flash del switch en un archivo llamado vlan.dat. Debido a que el usuario configura frecuentemente otros aspectos de un switch Cisco al mismo tiempo, es una buena práctica guardar los cambios de la configuración activa en la configuración de inicio.

Sintaxis de comando de la CLI del IOS de Cisco	
Cambiar de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Crear una VLAN. El id de la VLAN es el número de VLAN que se creará. Switches para el modo de configuración de VLAN para el vlan id de la VLAN.	`S1(config)#vlan vlan id`
(Opcional) Especificar un único nombre de VLAN para identificar la misma. Si no se ingresa ningún nombre, el número de la VLAN, relleno con ceros, se anexa a la palabra 'VLAN', por ejemplo, VLAN0020.	`S1(config-vlan)#name Nombre de VLAN`
Volver a modo EXEC privilegiado. Debe finalizar su sesión de configuración para que la configuración se guarde en el archivo vlan.dat y para que la configuración entre en vigencia.	`S1(config-vlan)#end`

Figura 3.25: Modo de agregar una VLAN

3.44 Administración de las VLAN

3.44.1 Asignación de un puerto de switch

Después de crear una VLAN, hay que asignar un puerto o más. Cuando asigna un puerto de switch a una VLAN en forma manual, se lo conoce como puerto de acceso estático. Un puerto de acceso estático puede pertenecer a sólo una VLAN por vez.

Al hacer clic en el botón Sintaxis del comando en la Figura 3.26 para revisar los comandos IOS de Cisco se asigna un puerto de acceso

estático a la VLAN. Si se hace clic en el botón Ejemplo en la figura para ver cómo la VLAN del estudiante, VLAN 20, se asigna estáticamente al puerto F0/18 en el switch S1. El puerto F0/18 se ha asignado a la VLAN 20, de manera que la computadora del estudiante, PC2, está en la VLAN 20. Cuando la VLAN 20 se configura en otros switches, el administrador de red sabe configurar las otras computadoras de estudiantes para encontrarse en la misma subred que PC2: 172.17.20.0 /24.Haga clic en el botón Verificación en la figura para confirmar que el comando show VLAN brief muestra los contenidos del archivo vlan.dat. En la captura de pantalla se resalta la VLAN del estudiante, VLAN 20.

Sintaxis del comando de la CLI del IOS de Cisco	
Ingrese el modo de configuración global.	S1#**configure terminal**
Ingresar la interfaz para asignar la VLAN.	S1(config)#**interface** *interface id*
Definir el modo de asociación de VLAN para el puerto.	S1(config-if)#**switchport mode access**
Asignar el puerto a una VLAN.	S1(config-if)#**switchport access vlan** *vlan id*
Volver al modo EXEC privilegiado.	S1(config-if)#**end**

Figura 3.26: Asignación de un Puerto Switch

3.44.2 Verificación de vinculaciones de puerto y de VLAN

Después de configurar la VLAN, puede validar las configuraciones de la VLAN mediante la utilización de los comandos show del IOS de Cisco, en la Figura 3.27 se muestra la verificación de las vinculaciones.

Verificación de las vinculaciones de puerto y de las VLAN

Mostrar el comando VLAN

Sintaxis del comando de CLI IOS de Cisco	
show vlan [brief | id *vlan-id* **| name** *Nombre de VLAN* **| summary].**	
Mostrar una línea para cada VLAN con el nombre, estado y los puertos de la VLAN.	**brief**
Mostrar información sobre una sola VLAN identificada por el número de ID de la VLAN. Para la vlan-id, el intervalo es de 1 a 4094.	**id** *vlan-id*
Mostrar información sobre una sola VLAN identificada por el nombre de VLAN. El nombre de la VLAN es una cadena ASCII de 1 a 32 caracteres.	**name** *Nombre de VLAN*
Mostrar el resumen de información de la VLAN.	**resumen**

Mostrar el comando de interfaces

Sintaxis del comando de CLI IOS de Cisco	
show interfaces *[interface-id* **| vlan** *vlan-id]* **| switchport**	
Las interfaces válidas incluyen puertos físicos (incluidos tipo, módulo y número de puerto) y canales de puerto. El intervalo de canales de puerto es de 1 a 6.	*interface-id*
Identificación de VLAN. El intervalo es de 1 a 4094.	**vlan** *vlan-id*
Mostrar el estado de administración y operación de un puerto de conmutación, incluidas las configuraciones de bloqueo y protección del puerto.	**switchport**

Figura 3.27: Verificación de las vinculaciones de puerto VLAN

3.44.3 Reasignar un puerto a la VLAN 1

Para reasignar un puerto a la VLAN 1, el usuario puede usar el comando no SWITCHPORT ACCESS VLAN en modo de configuración de interfaz. Examine la salida del comando SHOW VLAN BRIEF que aparece inmediatamente a continuación. Note cómo VLAN 20 sigue activa. Sólo se la ha eliminado de la interfaz F0/18. En el comando show interfaces f0/18 switchport, se puede ver que la VLAN de acceso para interfaz F0/18 se ha reestablecido a la VLAN 1.

3.44.4 Reasignar la VLAN a otro puerto

Un puerto de acceso estático sólo puede tener una VLAN. Con el software IOS de Cisco, no necesita quitar primero un puerto de una VLAN para cambiar su membresía de la VLAN. Cuando reasigna un puerto de acceso estático a una VLAN existente, la VLAN se elimina automáticamente del puerto anterior. En el ejemplo, el puerto F0/11 se reasigna a la VLAN 20. La Figura 3.28 muestra la sintaxis de configuración.

Sintaxis de comando de la CLI del IOS de Cisco	
Ingrese el modo de configuración global.	`S1#configure terminal`
Ingresar el modo de configuración de interfaz para que se configure la interfaz.	`S1(config)#interface` *interface id*
Eliminar la asignación de VLAN en esa interfaz de puerto de switch y cambiarla a la pertenencia de la VLAN predeterminada de VLAN 1.	`S1(config-if)#no switchport access vlan`
Volver al modo EXEC privilegiado.	`S1(config-if)#end`

Figura 3.28: Administración o reasignación de pertenencia al puerto.

3.44.5 Eliminación de las VLAN

Al tomar como ejemplo de uso del comando de configuración global no VLAN VLAN-ID para eliminar la VLAN 20 del sistema, el comando SHOW VLAN BRIEF verifica que la VLAN 20 ya no está en el archivo vlan.dat. Alternativamente, el archivo completo vlan.dat puede eliminarse con el comando DELETE FLASH: VLAN.DAT del modo EXEC privilegiado. Después de que el switch se haya vuelto a cargar, las VLAN

configuradas previamente ya no estarán presentes. Esto ubica al switch, en forma efectiva, en "de fábrica de manera predeterminada" con respecto a las configuraciones de la VLAN.

Antes de eliminar una VLAN, asegúrese de reasignar primero todos los puertos miembros a una VLAN diferente. Todo puerto que no se ha movido a una VLAN activa no puede comunicarse con otras estaciones luego de eliminar la VLAN.

3.44.6 Configuración de enlaces troncales troncal 802.1Q

Sintaxis de comando de la CLI del IOS de Cisco	
Ingresar el modo de configuración global.	S1#**configure terminal**
Ingresar el modo de configuración de interfaz para la interfaz definida.	S1(config)#**interface** *interface id*
Hacer que el enlace que conecta los switches sea un enlace troncal.	S1(config-if)#**switchport mode trunk**
Especificar otra VLAN como la VLAN nativa para los enlaces troncales IEEE 802.1Q sin etiquetar.	S1(config-if)#**switchport trunk native vlan** *vlan id*
Volver al modo EXEC privilegiado.	S1(config-if)#**end**

Figura 3.29: Configuración de enlace troncal 802.1Q

Para configurar un enlace troncal en un puerto de switch, utilice el comando switchport mode trunk. Cuando ingresa al modo enlace troncal, la interfaz cambia al modo permanente de enlace troncal y el puerto ingresa a una negociación de DTP para convertir el vínculo a un vínculo de enlace troncal, por más que la interfaz que la conecta no acepte cambiar. En este curso configurará un enlace troncal utilizando únicamente el comando switchport mode trunk. En la figura se muestra la sintaxis de comando IOS de Cisco para especificar una VLAN nativa diferente a la VLAN 1. En el ejemplo, el usuario configura la VLAN 99 como la VLAN nativa. Se muestra la sintaxis de comando utilizada para admitir una lista de las VLAN en el enlace troncal. En este puerto de enlace troncal, admita las VLAN 10, 20 y 30.

Al conocer esta topología las VLAN 10, 20 y 30 admitirán las computadoras del Cuerpo Docente, del Estudiante y del Invitado: PC1, PC2 y PC3. El puerto F0/1 en el switch S1 se configura como un puerto

de enlace troncal para admitir las VLAN 10, 20 y 30. La VLAN 99 se configura como la VLAN nativa.

El ejemplo configura al puerto F0/1 en el switch S1 como puerto de enlace troncal. Éste vuelve a configurar la VLAN nativa como VLAN 99 y agrega las VLAN 10, 20 y 30 como las VLAN admitidas en el puerto F0/1.

3.44.7 Verificación de la configuración del enlace troncal

La Figura 3.29 muestra la configuración del puerto de switch F0/1 en el switch S1. El comando utilizado es el comando show interfaces interface-ID switchport. La primera área resaltada muestra que el puerto F0/1 tiene el modo administrativo establecido en Enlace Troncal.

El puerto se encuentra en modo de enlace troncal. La siguiente área resaltada verifica que la VLAN nativa sea la VLAN 99, la VLAN de administración. En la parte inferior del resultado, la última área resaltada muestra que las VLAN del enlace troncal habilitadas son las VLAN 10, 20 y 30.

3.44.8 Administración de una configuración de enlace troncal

En la Figura 3.30, se muestran los comandos para restablecer las VLAN admitidas y la VLAN nativa del enlace troncal al estado predeterminado. También se muestra el comando para restablecer el puerto de switch a un puerto de acceso y, en efecto, eliminar el puerto de enlace troncal.

Los comandos utilizados para restablecer todas las características de enlace troncal de una interfaz de enlace troncal a las configuraciones predeterminadas, están resaltados en el resultado de muestra.

El comando show interfaces f0/1 switchport revela que el enlace troncal se ha reconfigurado a un estado predeterminado. El resultado de la figura muestra los comandos utilizados para eliminar la característica de enlace troncal del puerto de switch F0/1 en el switch S1. El comando show interfaces f0/1 switchport revela que la interfaz F0/1 está ahora en modo de acceso estático.

Sintaxis de comando de la CLI del IOS de Cisco	
Utilice este comando en el modo de configuración de interfaz para restablecer todas las VLAN configuradas en la interfaz del enlace troncal.	S1(config-if)#**no switchport trunk allowed vlan**
Utilice este comando en el modo de configuración de interfaz para restablecer la VLAN nativa nuevamente a VLAN1.	S1(config-if)#**no switchport trunk native vlan**
Utilice este comando en el modo de configuración de interfaz para restablecer la interfaz de puerto de enlace troncal nuevamente a un puerto de modo de acceso estático.	S1(config-if)#**switchport mode access**

Figura 3.30: Administración de configuración de enlace

Las VPNs (redes privadas virtuales) han evolucionado de forma considerable desde su introducción a principios de los años ochenta, cuando fueron construidas usando líneas alquiladas dedicadas. “Frame relay”, introducido en los años 90, es actualmente la oferta VPN predominante a escala mundial.

Después de la introducción de MPLS (comunicación por etiquetas multiprotocolo) a finales de los noventa, se definieron nuevos tipos de VPN. La aceptación por los proveedores de servicio del MPLS como la tecnología de convergencia de red a elegir llevó a poner una gran atención en las VPNs basadas en MPLS, que ofrecen fácil suministro de servicios dentro de las redes de los proveedores de servicios, además de la entrega de servicios a los usuarios.

Los diferentes tipos de VPN basadas en MPLS pueden clasificarse de distintas formas. Una de las más sencillas es basar la clasificación en el servicio que se está ofreciendo al cliente. Usualmente es un servicio multipunto o punto-a-punto de capa 2 [1, 2] o capa 3. Esto da lugar a los siguientes tipos de VPN:

- **VPNs multipunto de capa 3 o VPNs IP (protocolo Internet);** se denominan normalmente como VPRN (Redes enrutadas privadas virtuales).
- **VPNs punto a punto de capa 2,** que consisten básicamente en una colección de VLLs (líneas alquiladas virtuales) distintas o PWs (pseudowires).

- **VPNs multipunto de capa 2, o VPLSs (servicios LAN privados virtuales).**

Las VPNs IP basadas en MPLS, introducidas hace algunos años, disfrutan actualmente de un crecimiento saludable. Los dos puntos fuertes de este servicio VPN son su naturaleza multipunto y su soporte de IP. Las VLLs, introducidas más recientemente, ofrecen una clara migración de las tradicionales VPNs de FR/ATM (frame relay/modo de transferencia asíncrona) a la red MPLS convergente sin sustituir equipo en las instalaciones del cliente y sin afectar a la experiencia de servicio del cliente.

Aunque los servicios VPLS sólo han sido introducidos de forma reciente, un gran número de operadores ya los están ofreciendo comercialmente. Como las VPNs IP basadas en MPLS, el VPLS es un servicio multipunto, pero a diferencia de las VPNs IP éste puede transportar tráfico no-IP; también se beneficia de las bien conocidas ventajas de Ethernet. VPLS también se utiliza dentro de una red de proveedores de servicios para agregar servicios a suministrar a clientes de empresas y residenciales.

3.45 VPLS sobre MPLS: Descripción de la solución

VPLS, también conocido como TLS (servicio de LAN transparente) o servicio E-LAN, es una VPN multipunto de capa 2 que permite conectar múltiples sitios en un único dominio puenteado sobre una red MPLS/IP gestionada por el proveedor.

Todos los sitios del cliente en un caso de VPLS (es decir, un VPLS para una empresa particular) parecen estar en la misma LAN (red de área local), sin tener en cuenta sus localizaciones. VPLS utiliza una interfaz Ethernet con el cliente, simplificando la frontera LAN/WAN (red de área extensa) y permitiendo un aprovisionamiento rápido y flexible del servicio. [**10**]

Una red con VPLS consta de CEs (bordes de cliente), PEs (bordes de proveedor) y de una red central MPLS:

- El dispositivo CE es un router o conmutador situado en las instalaciones del cliente; puede pertenecer y gestionarse por el cliente o por el proveedor de servicios. Se conecta al PE mediante un AC (circuito de conexión). En el caso de VPLS, se asume que Ethernet es la interfaz entre CE y PE. El dispositivo PE es donde reside toda la inteligencia de VPN, donde el VPLS comienza y termina y donde se establecen todos los túneles necesarios para conectar con todos los otros PEs. Ya que el VPLS es un servicio Ethernet de capa 2, el PE debe ser capaz de conocer, puentear y replicar el MAC (control de acceso a los medios) en base a VPLSs. La red central MPLS/IP interconecta los PEs; no participa realmente en la funcionalidad de VPN. El tráfico se conmuta simplemente basándose en etiquetas MPLS.
- La base de cualquier servicio VPN multipunto (VPN IP o VPLS) es una malla completa de túneles MPLS (LSPs – trayectos conmutados por etiquetas, también llamados túneles externos) que se establecen entre todos los PEs que participan en el servicio VPN. LDP (protocolo de distribución de etiqueta) se utiliza para establecer estos túneles. Las VPNs multipunto pueden crearse encima de esta malla completa, ocultando la complejidad de la VPN desde los routers centrales.
- Para cada instancia VPLS se crea una malla completa de túneles internos (llamados pseudowires) entre todos los PEs que participan en la instancia VPLS. Un mecanismo de auto-detección localiza todos los PEs que participan en la instancia VPLS. Este mecanismo no se ha incluido en las especificaciones previas, de esta forma el proveedor de servicio puede configurar el PE con las identidades de todos los otros PEs en un VPLS concreto, o puede seleccionar el mecanismo de auto-detección que prefiera, por ejemplo, RADIUS (servicio de autenticación remota de marcación de entrada de usuario).
- La tecnología pseudowire está normalizada por el IETF (grupo de tareas sobre ingeniería de Internet) PWE3 (Pseudo Wire Emulation Edge to Edge) Working Group. Los PWs son conocidos históricamente como “túneles Martini”, y a las extensiones al protocolo LDP para permitir la señalización de PWs se las denomina frecuentemente “señalización Martini”.

- Un PW consta de un par de LSPs unidireccionales punto-a-punto de un solo salto en direcciones opuestas, cada uno identificado por una etiqueta PW, también llamada VC (conexión virtual). Las etiquetas PW se intercambian entre un par de PEs usando el mencionado protocolo de señalización LDP. El identificador VPLS se intercambia con las etiquetas, así ambos PWs pueden enlazarse y asociarse a una instancia VPLS particular.

  Al observar que este intercambio de etiquetas PW tiene que darse entre cada pareja de PEs participantes en una instancia VPLS concreta, y que las etiquetas PW tienen solamente un significado local entre cada una de esas parejas. La creación de PWs con una pareja de LSPs permite a un PE participar en el aprendizaje del MAC: cuando PE recibe una trama Ethernet con una dirección de fuente MAC desconocida, PE sabe en qué VC se envió.

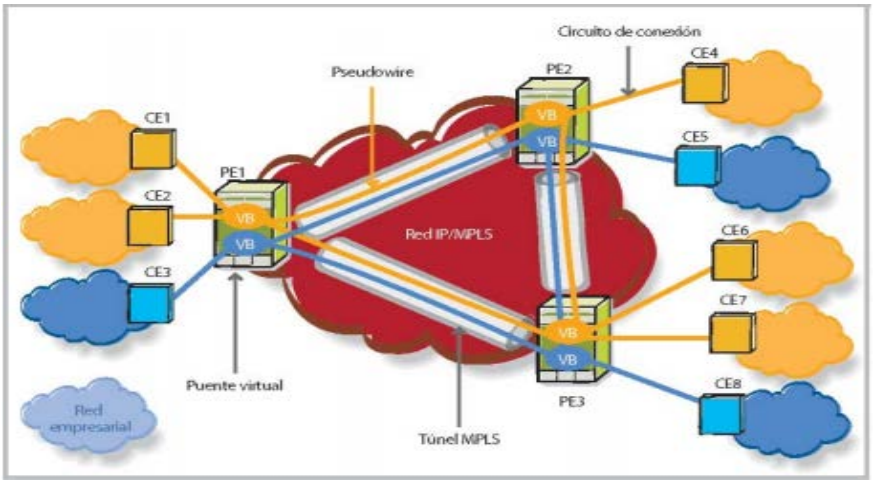

Figura 3.31: Modelo de referencias de VPLS

- Los routers PE deben soportar todas las prestaciones “clásicas” Ethernet, como aprendizaje del MAC, replicación y envío de paquetes. Conocen las direcciones MAC de la fuente MAC del tráfico que llega a sus puertos de acceso y de red.
- Desde un punto de vista funcional, esto significa que los PEs deben implementar un puente por cada instancia VPLS, al que se le suele llamar VB (puente virtual), como se muestra en la Figura 3.31. La funcionalidad VB

se lleva a cabo en el PE mediante una FIB (retransmisión de base de información) para cada supuesto de VPLS; esta FIB se popula con todas las direcciones MAC aprendidas.

Todo el tráfico se conmuta en base a las direcciones MAC y se reenvía entre todos los routers PE participantes, usando túneles LSP. Los paquetes desconocidos (es decir, las direcciones de destino MAC que no han sido aprendidas) se replican y reenvían en todos los LSPs a todos los routers PE que participan en ese servicio hasta que responde la estación de destino y la dirección MAC es aprendida por los routers PE asociados con dicho servicio. ***[10]***

- Para evitar bucles de reenvío se usa la regla llamada “Split Horizon (partir el horizonte)”. En el contexto VPLS, esta regla implica básicamente que un PE nunca debe enviar un paquete a un PW si ese paquete se ha recibido de un PW. Esto asegura que el tráfico no pueda formar un bucle sobre la red de backbone usando PWs. El hecho de que haya siempre una malla completa de PWs entre los dispositivos PE asegura que cada paquete emitido alcanzará su destino dentro del VPLS.

3.46 ¿Cómo funciona VPLS?

Se da por sentado que hay una malla completa de túneles MPLS entre los cuatro Pe’ s conectados a la red MPLS. Ha de crearse una instancia VPLS identificada por Svc-id 101 (identificador de servicio 101) entre PE1, PE2 y PE3; PE4 no participa en la instancia VPLS considerada.

Se considera que esta configuración se determinó usando un mecanismo de auto-detección no especificado. M1, M2, M3 y M4 son estaciones finales en distintas localizaciones del cliente y sus ACs a sus respectivos dispositivos PE (ver Figura 3.32) han sido configurados en los PEs para pertenecer a una instancia VPLS concreta: Svc-id 101.

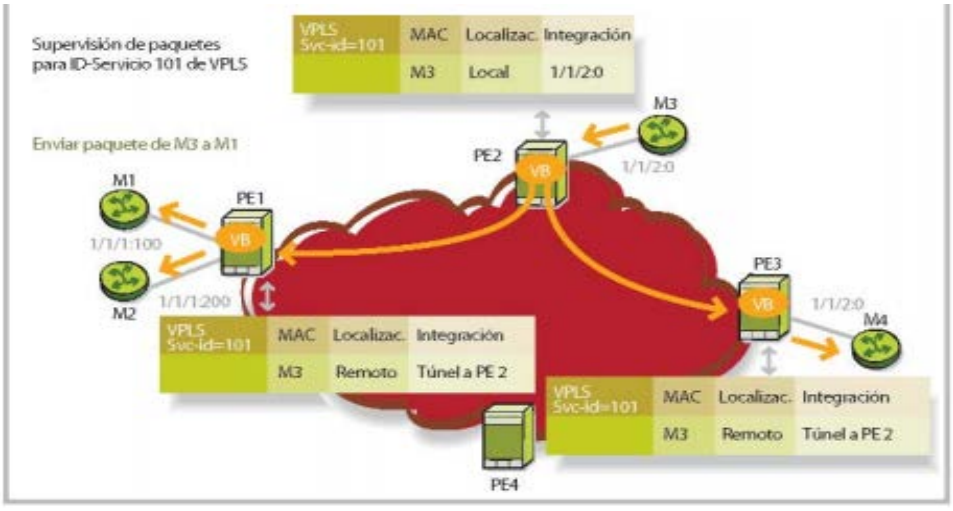

Figura 3.32: Funcionamiento de VPLS

3.46.1 Creación de los pseudowires

Se necesita crear tres PWs, cada uno con un par de LSPs unidireccionales, o conexiones virtuales. Para señalizar la etiqueta-VC entre PEs, cada PE inicia una sesión LDP que tiene como objetivo el PE par y le comunica qué etiqueta VC usar cuando envía paquetes al VPLS en cuestión. La instancia VPLS específica se identifica en el intercambio de señalización usando un identificador de servicio (p. ej., Svc-id 101).Ver Figura 3.33.

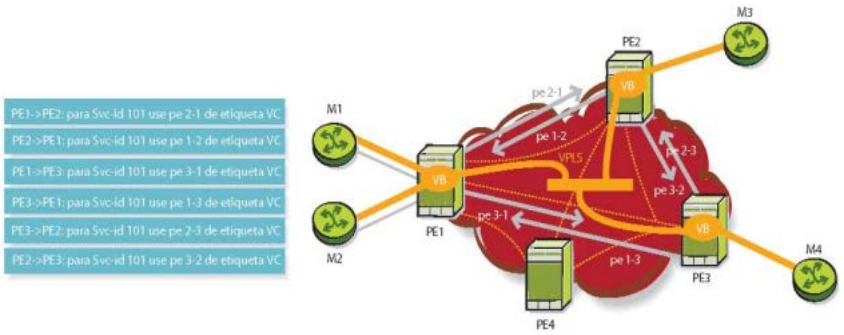

Figura 3.33: Creación y Señalización pseudowire

3.46.2 Envío de Paquetes VPLS

En el ejemplo PE1 indica a PE2: “si tienes tráfico que enviarme por Svc-id 101, usa el pe2-1 de la etiqueta VC en el encapsulado de paquetes”.

A su vez, PE2 indica a PE1: “si tienes tráfico que enviarme por Svc-id 101, usa la etiqueta pe1-2 de la etiqueta VC en el encapsulado de paquetes”. De este modo se crea el primer PW.

Aprendizaje del MAC y envío de paquetes Una vez que creada la instancia VPLS con Svc-id 101, pueden enviarse los primeros paquetes y comienza el aprendizaje del MAC.

Ejemplo: Se supone que M3 está enviando un paquete al PE2 destinado a M1 (M3 y M1 quedan identificados por una sola dirección MAC), según se muestra en la Figura 3.34

PE2 recibe el paquete y reconoce (desde la dirección MAC de la fuente) que ese M3 se puede alcanzar en el puerto local 1/1/2:0; almacena esta información en el FIB para Svc-id 101.

PE2 no conoce todavía el M1 de la dirección MAC de destino, así que inunda el paquete a PE1 con el pe2-1 de la etiqueta VC (en el túnel externo MPLS correspondiente) y a PE3 con el pe2-3 de la etiqueta VC (en el túnel externo MPLS correspondiente). [**10**]

PE1 retira el pe2-1 de la etiqueta, no conoce el M1 de destino e inunda el paquete a los puertos 1/1/1:100 y 1/1/1:200; PE1 no inunda el paquete a PE3 debido a la regla Split-Horizon. PE3 retira el pe2-3 de la etiqueta, no conoce el M1 de destino y envía el paquete al puerto 1/1/2:0; PE3 no inunda el paquete a PE1 debido a la regla del Split-Horizon. M1 recibe el paquete.

Cuando M1 recibe el paquete de M3, responde con un paquete aM3

PE1 recibe el paquete de M1, reconoce que M1 está en el puerto local 1/1/1:100 y almacena esta información en el FIB para Svc-id 101. PE1 ya sabe que M3 se puede alcanzar vía PE2 y, por ello, solamente envía el paquete a PE2 usando la etiqueta VC pe1-2. PE2 recibe el paquete para M3 y sabe que M3 es accesible por el puerto 1/1/2:0. M3 recibe el paquete.

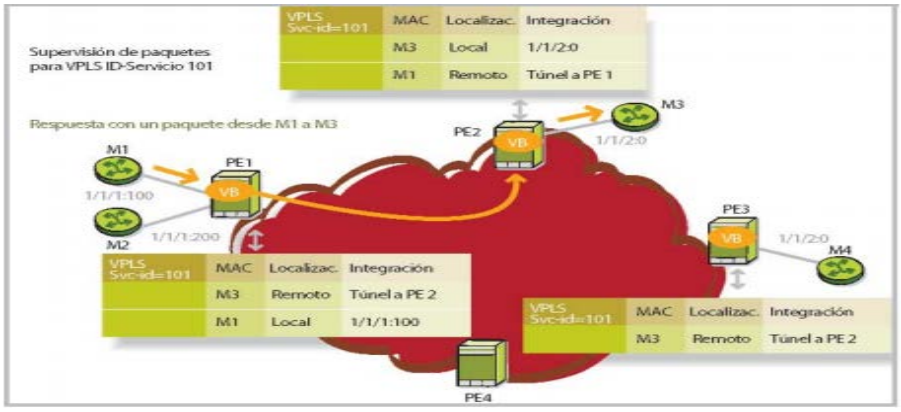

Figura 3.34: Envío de paquetes VPLS

3.46.3 VPLS jerárquico

La arquitectura H-VPLS se construye sobre la base de la solución VPLS, ampliándola para proporcionar distintas ventajas operacionales y de escala [4]. Es especialmente útil en despliegues a gran escala con un gran número de PEs y/o MTU (unidades multiusuario).

Los proveedores de servicio instalan MTUs en edificios compartidos para dar servicio a distintas empresas radicadas en ellos; cada empresa puede, potencialmente, pertenecer a diferentes VPN VPLS. Los proveedores del servicio necesitan entonces agregar tráfico MTU hacia el dispositivo PE en la central principal o PoP (punto de presencia), según se muestra en la Figura 3.35. Una MTU tradicional es un dispositivo Ethernet que soporta todas las funciones de conmutación de la capa 2, incluyendo las funciones normales de derivación de aprendizaje y replicación en todos sus puertos; está dedicada normalmente a una empresa. Para compartir los recursos WAN de forma eficaz entre los clientes existe la posibilidad de ampliar la funcionalidad VPLS a los MTUs. En este caso, los MTUs actúan como dispositivos PE, llevando a un gran número de PEs participantes en el VPLS. Una red con numerosos MTUs/PEs, nos llevaría a limitaciones en la escalabilidad en términos del número de PWs a mantener, paquetes a replicar y direcciones MAC a mantener.

Las ventajas del escalamiento del H-VPLS se obtienen introduciendo la jerarquía, eliminando así la necesidad de una malla total de LSPs y de PWs entre todos los dispositivos participantes. La jerarquía se alcanza aumentando la malla principal del VPLS base del PE al PWs de PE (llamados hub PWs) con PWs de acceso (llamados spoke PWs) para formar un modelo VPLS jerárquico de dos niveles, como se muestra en la Figura 3.35.

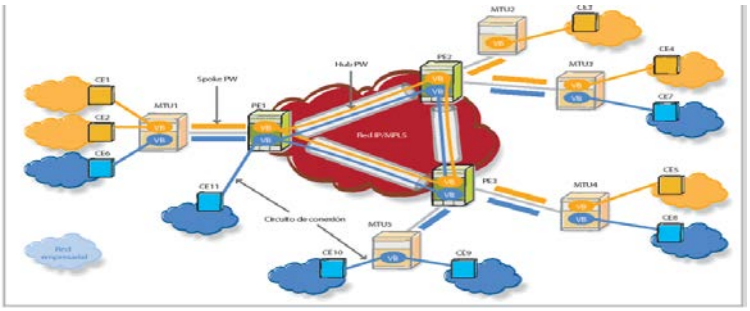

Figura 3.35: Modelo de referencia de H- VPLS

Los spoke PWs se crean entre los MTUs y los routers PE. H-VPLS ofrecen la flexibilidad de utilizar distintos tipos de conexión para la implementación del spoke PW: o una conexión etiquetada IEEE 802.1Q, o un LSP MPLS con señalización LDP.

H-VPLS ofrece también distintas ventajas operacionales centralizando en los routers PE del PoP las funciones principales (p. ej.. auto-detección del punto final VPLS, participando en un backbone enrutado, manteniendo una malla completa de túneles LSPs y múltiples mallas totales de PWs). Esto hace posible utilizar dispositivos MTU de bajo costo y mantenimiento, reduciendo así el desembolso de capital total y de los gastos de explotación ya que, normalmente, hay un número mayor de dispositivos MTU que de routers PE.

Otra ventaja operacional ofrecida por H-VPLS es el aprovisionamiento centralizado con pocos elementos a intervenir para reactivar el servicio de un cliente.

Añadir un nuevo dispositivo de MTU requiere alguna configuración del router PE local, pero no requiere señalización alguna con otros routers PE o dispositivos MTU, simplificando de manera importante el proceso de aprovisionamiento.

En H-VPLS, un CE se conecta a una MTU mediante un circuito de conexión. Un AC de un cliente específico se asocia (por configuración) con un puente virtual dedicado a ese cliente dentro de la MTU considerada. Un AC puede ser un puerto físico o lógico etiquetado de VLAN (LAN virtual). En el escenario básico, una MTU tiene un canal de ida a un PE. Este canal de ida consta de un spoke PW para cada VPLS servido por la MTU. Los extremos de este spoke PW son una MTU y un PE. Los spoke PWs se pueden implementar usando PWs MPLS de LDP señalizado, si MTU permite MPLS. Alternativamente, pueden implementarse usando P-VLAN (VLAN de proveedor) por lo que cada VLAN en el canal de ida MTU-PE de una red de agregación Ethernet identifica un spoke PW. En el canal de ida entre MTU1 y PE1 transporta dos PWs, ya que MTU1 tiene dos clientes VPLS conectados. Como MTU tiene solo un PW por VPLS, su operación es sencilla:

Las tramas Ethernet con direcciones MAC aprendidas se conmutan consecuentemente dentro del VPLS. Las tramas con direcciones MAC difundidas o desconocidas recibidas del PW se replican y envían a todos los dispositivos CE conectados dentro del VPLS.

Las tramas con direcciones MAC difundidas o desconocidas recibidas desde un dispositivo CE se envían por el PW al PE y a todos los restantes dispositivos conectados al CE dentro del VPLS. Las direcciones MAC desconocidas se aprenden y aged1 dentro del VPLS (tanto las tramas que provienen del PW como las de dispositivos CE).

El dispositivo PE necesita implementar un VB por cada VPLS servido por los MTUs conectados al PE; los spoke PWs son vistos como ACs de diferentes clientes. Como tal, un spoke PW particular se asocia con VB PE dedicado a la instancia VPLS considerada. En la red central, PE tiene

una malla de conexión completa de PWs a todos los otros PEs que sirven el VPLS (como en el escenario normal de VPLS). Estos PWs centrales se llaman hub PWs. Desde un punto de vista del nivel del plano de control y del plano de datos, la operación de los PE es la misma que en el escenario VPLS básico.

3.46.4 El servicio inter-metropolitano

H-VPLS permite que los servicios VPLS se extiendan por múltiples redes metropolitanas, como se muestra en la Figura 3.36. Se utiliza una conexión spoke para conectar cada servicio VPLS entre dos áreas metropolitanas. En su forma más simple, podría ser un LSP de túnel. Un conjunto de etiquetas PW de ingreso y egreso se intercambian entre los dispositivos PE de borde para crear un PW por cada instancia de servicio VPLS a transportar sobre este LSP. Los routers PE en cada extremo tratan este PW inter-metropolitano como una conexión spoke virtual para el servicio VPLS, de la misma manera que tratan las conexiones PE-MTU. Esta arquitectura reduce al mínimo la tara de señalización y evita una malla total de VCs y LSPs entre las dos redes metropolitanas.

Aunque los servicios de capa 2 basados en MPLS, como VLL y VPLS, son relativamente nuevos, los proveedores de servicio ya los ofrecen en todo el mundo. Su éxito inicial se puede atribuir al hecho de que utilizan MPLS en la red del proveedor de servicios combinado con FR/ATM y Ethernet como traspaso a la empresa para VLL y Ethernet para VPLS. Los servicios de capa 2 basados en MPLS ofrecen a los clientes de empresa lo que necesitan exactamente para la conectividad entre sucursales: transparencia de protocolo, ancho de banda escalable y granular a partir de 64 kbit/s y hasta 1 Gbit/s, rápida activación y suministro de servicios y una frontera de LAN/WAN simplificada. VPLS también permite a los proveedores de servicios suministrar una oferta de servicios VPN escalable que puede combinarse con el acceso a Internet en una infraestructura consolidada IP/MPLS, reduciendo así los gastos de explotación.

VPLS ha recibido ya el apoyo generalizado de la industria, tanto de fabricantes como de proveedores de servicios. Alcatel soporta VPLS y H-VPLS en una amplia gama de productos que incluyen productos ópticos y datos, complementados por una potente gestión de red y servicios.

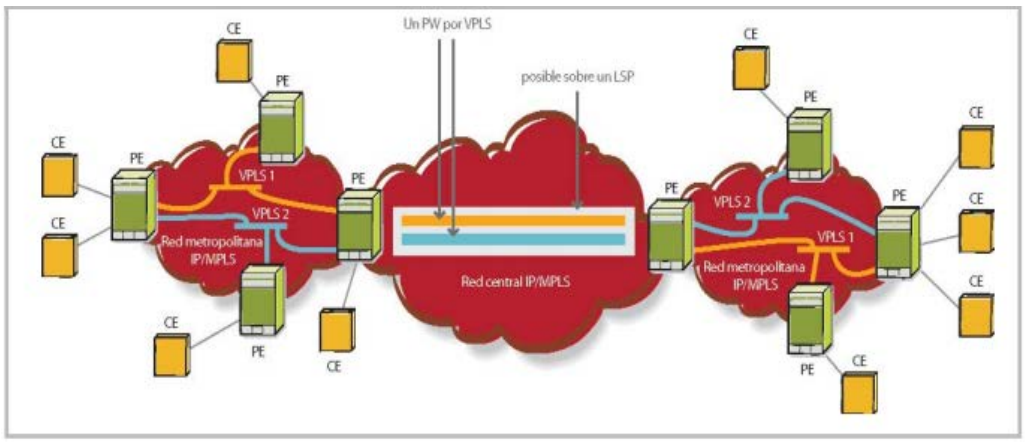

Figura 3.36: H- VPLS Usado como servicio intermetropolitano

3.46.5 Costo de Instalación

En este punto haremos una reseña sobre el costo para la instalación del sistema de gestión, que en este caso al implementarse en una red de CORE y CORPORATIVA ya existente solo se tomara en cuenta el costo de la implementación de la solución adquirida según sea la marca elegida.

El análisis de las propuestas solicitadas para la implementación de esta solución de gestión de red serán revisadas tan solo como proformas y basándose en costos en primera instancia, en la solución adquirida para este proyecto en la red de la compañía la elección fue basada en directrices adoptadas por la matriz.

3.47 Diseño lógico de la Red de monitoreo: Topología

En este punto se muestra el diseño que se implementara para la red de monitoreo, entiéndase como un diagrama consolidado de todos los elementos

que se utilizaran para lograr la conectividad de los terminales CEP´s que serán administrados y monitoreados como objeto de este trabajo.

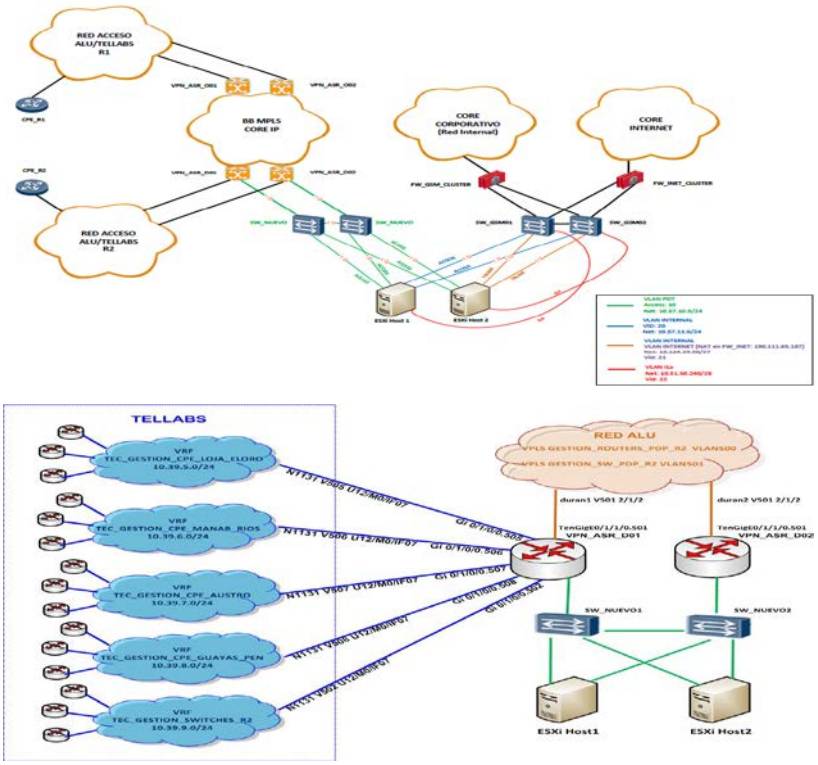

Figura 3.37: Diseño de Red.

El modelo de la red de monitoreo y gestión a implementarse utilizara la infraestructura de la red corporativa y de accesos de servicios, puesto que estos se configuran como servicios paralelos de baja capacidad hacia los equipos terminales de la red

Los equipos a monitorear CPE'S para enviar los traps hacia los servidores de gestión utilizaran servicios virtuales de capa dos que serán configurados en primera instancia sobre la plataforma de accesos de servicios, en este caso en particular usaremos como referencia la plataforma de marca TELLABS MPLS de la familia 86XX y ALU MPLS de la familia SAR-M .

Estos servicios de capa dos configurados dentro de las plataformas de datos y terminan en una conexión hacia la red de CORE. Esta conexión es redundante hacia los equipos de la red corporativa.

En la red corporativa se configuran servicios troncales que llevaran la información por medio de switches configurados en redundancia hasta los servidores de gestión.

Como se puede observar los servidores (para el caso particular de esta implementación se utilizó HP PROLIANT G8) tienen conexiones redundantes hacia la red de CORE, corporativa y CORE de Internet.

Los requerimientos de los usuarios ya sean estos clientes corporativos o clientes externos pasaran por un los FW respectivos según sea el caso de cada uno.

Para la gestión de los routers y switches de administración de PDP R2, se han creado las siguientes VRFs en Tellabs:

TEC_GESTION_CPE_LOJA_ELORO

TEC_GESTION_CPE_MANAB_RIOS

TEC_GESTION_CPE_AUSTRO

TEC_GESTION_CPE_GUAYAS_PEN

TEC_GESTION_SWITCHES_R2

En ALU están creadas las VPLSs:

TEC_GESTION_ROUTERS_PDP_R2

TEC_GESTION_SW_PDP_R2

Todas las VRFs y VPLSs previamente mencionadas se han conectado hacia los routers VPM_ASR_DURAN_D01 y VPN_ASR_DURAN_D02 administrados por BOD para que puedan tener conexión con el servidor donde se tiene instalado el sistema para gestión de equipos NMIS; siendo su esquema de conexión el siguiente:

En el caso que se desee ingresar un nuevo dispositivo al sistema de gestión NMIS, se debe de tomar en cuenta si se conecta a la red Tellabs o a la red ALU, y además si se trata de un CPE o un switch de la empresa.

3.48 Modelo de Direccionamiento

Para el caso de la instalación de este sistema de gestión se han tomado varios consideraciones, puesto que se ha debido generar un modelo de direccionamiento lo bastante flexible ya que se debe tomar en cuenta factores como el crecimiento los puntos hacia donde se hará converger los servicios que se crearan desde cada CPE.

Para el caso se ha considerado en la subdivisión de la región en zonas a monitorear que tendrán puntos de convergencia común. La red a utilizarse 10.39.0.0/16.

3.49 Configuración del servidor de gestión y terminales

Para tratar un modelo de configuración del servidor de gestión se considerarían aspectos generales o básicos que estarán presentes siempre sin importar la solución adquirida, para más tarde según se haya realizado el análisis y la elección del software a implementarse se complementaran los campos que sean necesarios según la solución así lo demande.

De igual manera la configuración en los CPE's o equipos terminales también se deberán habilitar protocolos y servicios básicos en cada uno de ellos, en este caso si con nombres propietarios elegidos según el criterio de cada administrador de red.

Para el caso se detalla la configuración de los elementos básicos elegidos en este análisis:

CPE: ROUTER CISCO 881

SISTEMA DE GESTION: NMIS

3.50 Creación de servicios en la red portadora

Es este punto mostraremos la configuración de un servicio básico de PseudoWire en una red sencilla.

Para efecto tomaremos en cuenta que un PW3 o pseudowire es un servicio de capa 2 que permite transportar cualquier tipo de paquete multiprotocolo a través de una red MPLS de extremo a extremo.

3.51 Selección del software de Monitoreo.

3.51.1 Análisis del Software CA SPECTRUM

CA SPECTRUM le permite administrar proactivamente entornos de red compleja, heterogénea y de múltiples proveedores.

Identifica automáticamente la causa de origen de los problemas de red, suprime las alarmas sintomáticas, pone de relieve el impacto en el negocio, y le permite cumplir y superar los acuerdos de niveles de servicio.

Permite el monitoreo proactivo, la correlación de eventos, el análisis de las causas de origen, la creación de tendencias, la generación de reportes sobre activos, la verificación de los tiempos de respuesta, y la integración con sistemas de administración de CA y de terceros

CA SPECTRUM brinda soporte para redes capa 2 y capa 3, incluyendo redes LAN, WAN, conectadas, inalámbricas, físicas y virtuales, así como las tecnologías y los servicios IP provistos sobre ellas.

La implementación de este sistema fue desechada por el alto costo del mismo.

3.51.2 Análisis del Software HARRYS NETBOSS

Este sistema aunque brinda excelentes prestaciones no fue considerado para su implementación debido a que no se realizó una presentación oficial por parte del proveedor.

3.51.3 Análisis del Software BEM

Este sistema de monitorio fue considerado por que esta ya implementado para otras aplicaciones, los costos y el licenciamiento son bastante flexibles puesto que se maneja de una forma modular, desafortunadamente este sistema no posee un módulo para el análisis estadístico ni de estado de los elementos de la red por lo que luego fue desechado.

El sistema seleccionado fue el NMIS (NETWORK MANAGEMENT INFORMATION SYSTEM), este sistema tiene mucha flexibilidad puesto que se trata de una aplicación de código abierto por lo que se puede personalizar dependiendo de la demanda.

EL NMIS ofrece reportes detallados del comportamiento del servicio, estadísticas de tráfico y envió de alarmas.

3.51.4 Análisis de la seguridad en la Red corporativa

A nivel de red corporativa este es un punto de extrema importancia para la empresa quien implementara esta solución para la gestión y revisión de alarmas de los elementos de servicios, puesto que se debe tener un control absoluto de los integrantes o áreas que podrán mantener este control.

Los sistemas de gestión tienen también la funcionalidad de mostrar estadísticas de tráfico e históricos de operación en un entorno de clientes ya que según sea el modelo adoptado se puede ofrecer permisos a usuarios quienes podrían realizar revisiones de sus servicios, en cuyo caso según sea lo ofrecido el acceso al cliente se deberá considerar firewall’s de seguridad tanto en la red interna como hacia la nube de internet si es que esta vía es permitida por la empresa.

CAPÍTULO 4

4. IMPLEMENTACIÓN DE SERVICIOS EN RED PORTADORA

En este capítulo se hará referencia a la construcción de servicios en la red portadora según se muestra en el procedimiento mostrado.

4.1 Configuración de terminales de red de los clientes VIP

4.1.1 CPE de la empresa conectado mediante red ALU

Se debe de configurar una IP disponible del segmento 10.39.0.0/24 y agregar lo siguiente:

ip cef

ip vrf **GESTION-NMIS**

En sub interfaz corresponde:

dot1Q **500**

ip vrf forwarding **GESTION-NMIS**

ip address 10.39.0.2 255.255.255.0

snmp-server community **pdp$nmp** RO

snmp-server host **10.57.10.51** version 2c **pdp$nmp**

ip route vrf **GESTION-NMIS** 0.0.0.0 0.0.0.0 **10.39.0.254**

snmp-server location **CENTRAL-HERRADURA**

snmp-server contact teccorpdpgye@empresa.com.ec

Se crea la vrf “GESTION-NMIS” localmente en el router para que el direccionamiento de gestión no interfiera con el direccionamiento del cliente y para que no pueda acceder desde su red interna al NMIS. [**4**] [**2**]

pdp$nmp Comunidad SNMP

10.57.10.51 Servidor NMIS

10.39.0.254 IP de interfaz VPN_ASR_D01

CENTRAL-HERRADURA lugar donde está instalado el router (cliente o nodo)

teccorpdpgye@empresa.com.ec email grupal PDP R2

El puerto correspondiente hay que agregarlo a la VPLS TEC_GESTION_ROUTERS_PDP_R2.

CPE de empresa conectado a Tellabs.

Dependiendo de la zona en la que se encuentre el CPE puede tomar IPs de los siguientes rangos. Ver Tabla 1:

RANGOS IP	LUGAR	VLAN
10.39.5.0/24	LOJA, EL ORO	VLAN 505
10.39.6.0/24	MANABI, LOS RIOS	VLAN 506
10.39.7.0/24	AUSTRO	VLAN 507
10.39.8.0/24	GUAYAS, PENINSULA	VLAN 508

Tabla 1: Rangos de IP

La configuración en el CPE sería la misma que en el caso de conectarse a la red ALU, variando la VLAN en función de la zona, la máscara será /30 en lugar de /24 y el GW será la IP que se configure en la VLAN correspondiente en Tellabs.

VRFs configuradas en Tellabs para la gestión de CPEs:

TEC_GESTION_CPE_LOJA_ELORO

TEC_GESTION_CPE_MANAB_RIOS

TEC_GESTION_CPE_AUSTRO

TEC_GESTION_CPE_GUAYAS_PEN

4.2 Configuración del Servidor de gestión de red.

Para la configuración de los dispositivos en el servidor se requiere el ingreso mediante un explorador según se indica en la Figura 4.1, este ingreso es previamente autenticado.

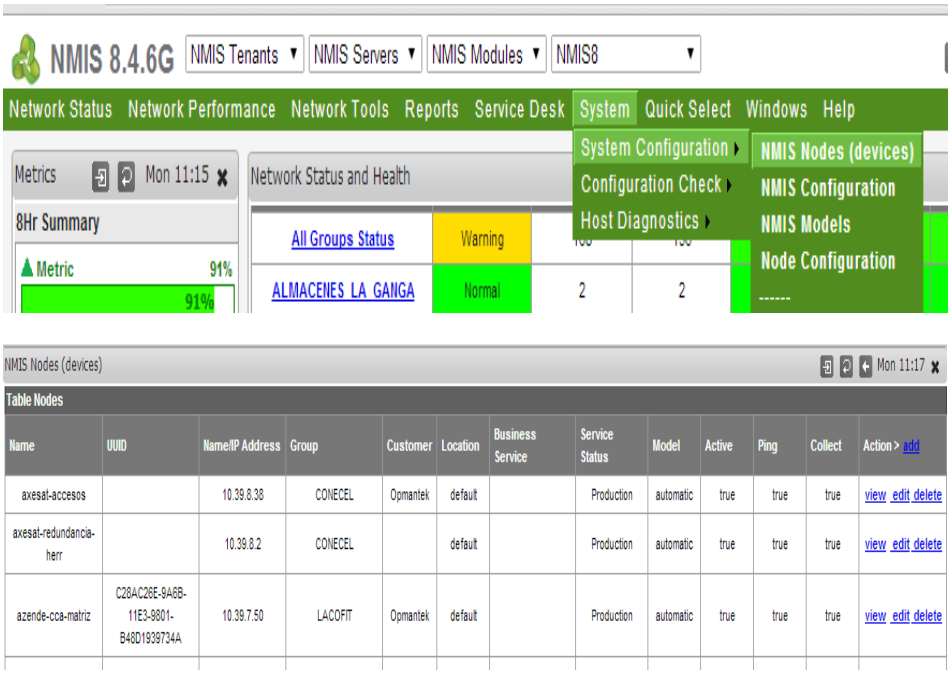

Figura 4.1: System / System Configuration /NMIS Nodes (devices) NMIS NOTES.

4.3 Información del dispositivo y Comunidad SNMP

Se agrega la información del dispositivo a monitorear y la comunidad SNMP. Información mínima que se debe de ingresar es la siguiente y se visualiza en la Figura 4.2.

- Name: nombre del dispositivo
- Name/IP Address: IP del dispositivo a poner en gestión
- SNMP Version: Version SNMP configurada en el dispositivo
- SNMP Community: Comunidad SNMP

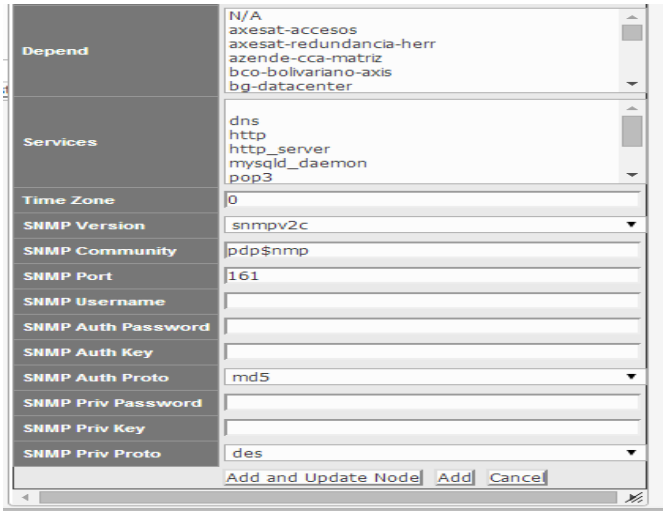

Figura 4.2: Configuración SNMP

4.4 Instalación del sistema operativo.

Para la instalación del OS se toma en cuenta las recomendaciones indicadas o requisitos básicos para soportar el programa de gestión de red que se utilizaría.

Una vez tomado en cuenta estos requerimientos se procede con la instalación en este caso se trabajaría con LINUX CENTOS. Por flexibilidad y costo.

4.5 Instalación de aplicación de gestión

La aplicación a utilizarse NMIS es una aplicación de tipo cliente-servidor, la instalación del servidor como tal consta de varios módulos que ya que es dividida en procesamiento, alarmas y colectores básicamente, este se realizó mediante la virtualización de servidores dentro de los equipos físicos antes mencionados en la topología de la red de gestión.

- **NMIS:** monitorea el estado y el desempeño de los elementos IT (intelligent technologies) por lo incide en la rectificación a las fallas que son reportadas.
- **OPENAUDIT** realiza un descubrimiento y realiza un inventario de todos IT que se soliciten dentro de un segmento predeterminado.
- **OPFLOW** realiza unos análisis basados en el flujo de la información del comportamiento de los elementos de la red, tales como graficas de consumo de ancho de banda, tráfico inusual, identificación de congestión, etc.

- **OPMAPS** realiza la geolocalización del elemento que está siendo monitoreado basado en parámetros configurados en esta (longitud y esta latitud), esta aplicación usa como motor de localización GOOGLE MAPS.
- **OPREPORTS** realiza un análisis de potenciales impactos al negocio.
- **OPHA** Este módulo permite el funcionamiento de la redundancia mediante el esquema de Maestro-Esclavo para una alta disponibilidad.
- **OPCONFG** Realiza el respaldo de la configuración de los elementos seleccionados en la red.

Esta instalación fue realizada por la compañía contratada. Con respecto a este punto no se revisara a detalle por motivos de confidencialidad.

La aplicación como Cliente no necesita ser instalada puesto que se tiene acceso mediante una página web con la dirección del servidor de comunicación y el usuario es autenticado mediante un USER y PASSWORD asignado por el administrador.

4.6 Configuración de Agentes en los elementos de Red

En este ítem se mostrara las configuraciones de los elementos que están conectados hacia los nodos de acceso.

4.6.1 Switch de la empresa conectado a Tellabs

Se debe de configurar una IP disponible del segmento 10.39.9.0/24 y agregar la siguiente configuración en el switch:

Int vlan **502**

description GESTION-empresa

ip address **10.39.9.X** 255.255.255.252

snmp-server community **pdp$nmp** RO

snmp-server host **10.57.10.51** version 2c **pdp$nmp**

ip default-gateway **10.39.9.Y**

snmp-server location **JIPIJAPA**

snmp-server contact teccorpdpgye@empresa.com.ec

pdp$nmp Comunidad SNMP

502 VLAN asignada a la VRF

10.57.10.51 Servidor NMIS

10.39.9.Y GW configurado en la interfaz Tellabs JIPIJAPA

donde está instalado el switch teccorpdpgye@empresa.com.ec email grupal PDP R2.

4.6.2 Switch de la empresa conectado mediante red ALU

Se debe de configurar una IP disponible del segmento 10.39.3.0/24 y agregar la siguiente configuración:

Int vlan **501**

description GESTION-empresa

ip address **10.39.3.x** 255.255.255.0

snmp-server community **pdp$nmp** RO

snmp-server host **10.57.10.51** version 2c **pdp$nmp**

ip default-gateway **10.39.3.254**

snmp-server location **PORTETE**

snmp-server contact teccorpdpgye@empresa.com.ec

pdp$nmp Comunidad SNMP

10.57.10.51 Servidor NMIS

10.39.3.254 IP de interfaz VPN_ASR_D01

PORTETE nodo donde está instalado el switch

teccorpdpgye@empresa.com.ec email grupal PDP R2

El puerto correspondiente hay que agregarlo a la VPLS TEC_GESTION_SW_PDP_R2.

4.7 Análisis de gráficas del Sistema de Gestión SNMPv2

A continuación se muestran gráficos del análisis del Sistema de Gestión (Ver Figura 4.3):

- Ingresar con Google Chrome o Mozilla Firefox
- Ventanas desplegadas:System / System Configuration /NMIS Nodes (devices):
- Metrics, Quick Search, Network Metrics and Health, Log of Slave Event log. Se describen las siguientes definiciones:
    - Group – razón social
    - Node – dispositivo en monitoreo
    - Node down – dispositivo al que se ha perdido monitoreo.
    - Node degraded- dispositivo en monitoreo pero con métricas que reflejan posible degradación del servicio.
    - Metric – reachability, health, status y availability
    - Reachability – si es alcanzable con ping o no
    - Health – medida de salud del enlace

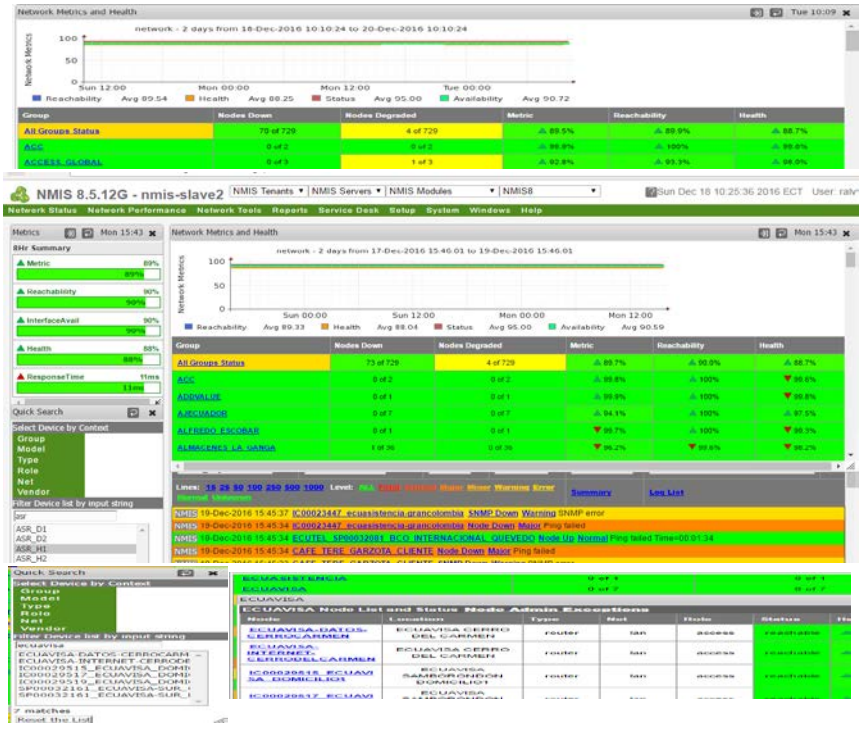

Figura 4.3: Ventanas desplegadas Metrics, Quick Search, Network Metrics and Health, Log of Slave Event log.

- Parámetros con que se calcula el “Health”:
  - Reachability
  - Availability
  - Response time
  - CPU Utilisation
  - Memory Utilisation
  - Interface Utilisation
  - Disk Utilisation
  - Swap Utilisation

Los parámetros disk y SWAP UTILISATION no lo tienen todos los dispositivos. Ej.: routers CISCO. (Ver Figura 4.4)

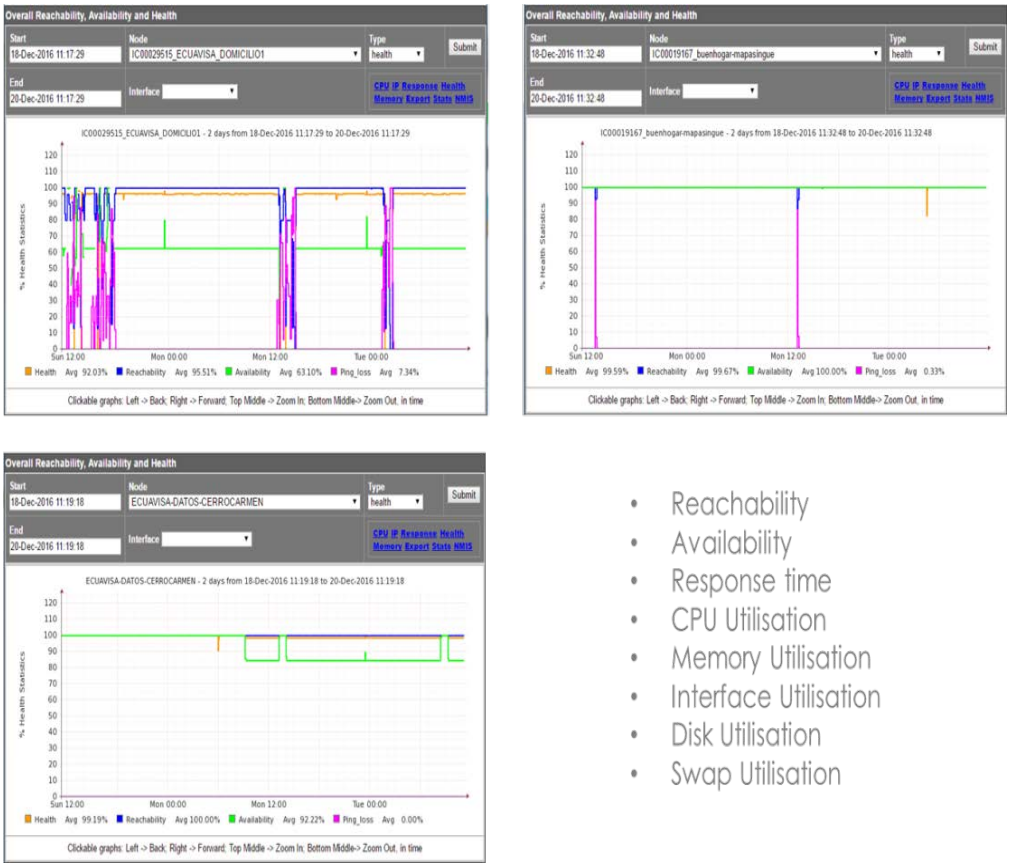

Figura 4.4: Parámetros con que se calcula la configuración “Health”

4.8 Reportes y tiempo de respuesta.

La Figura 4.5 permite visualizar los diferentes tipos de reportes que se pueden obtener.

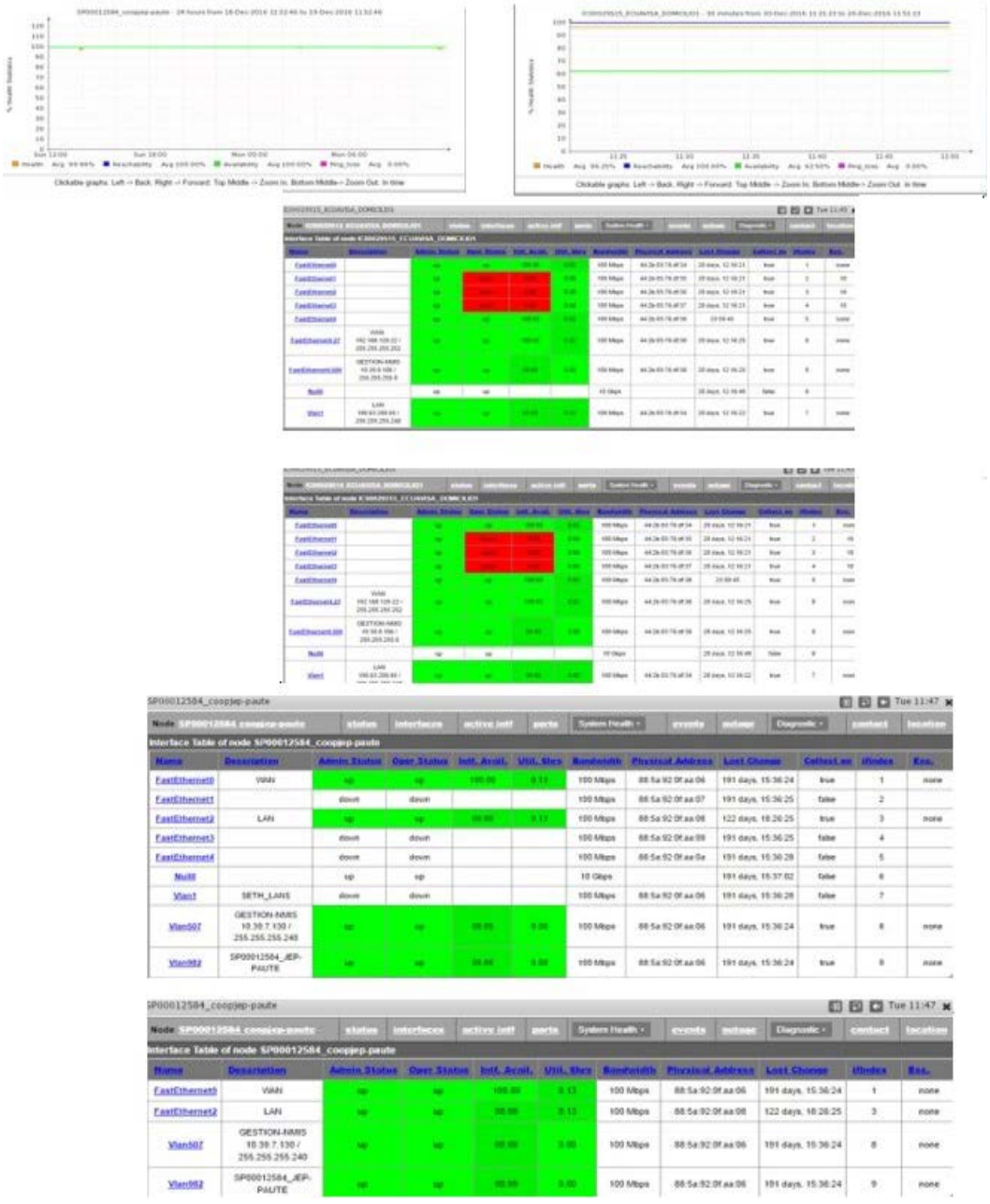

Figura 4.5: Gráficos de reportes que se obtienen del NMIS

4.9 Revisión del consumo de BW una interfaz

La Figura 4.6 muestra una interfaz de revisión del consumo BW.

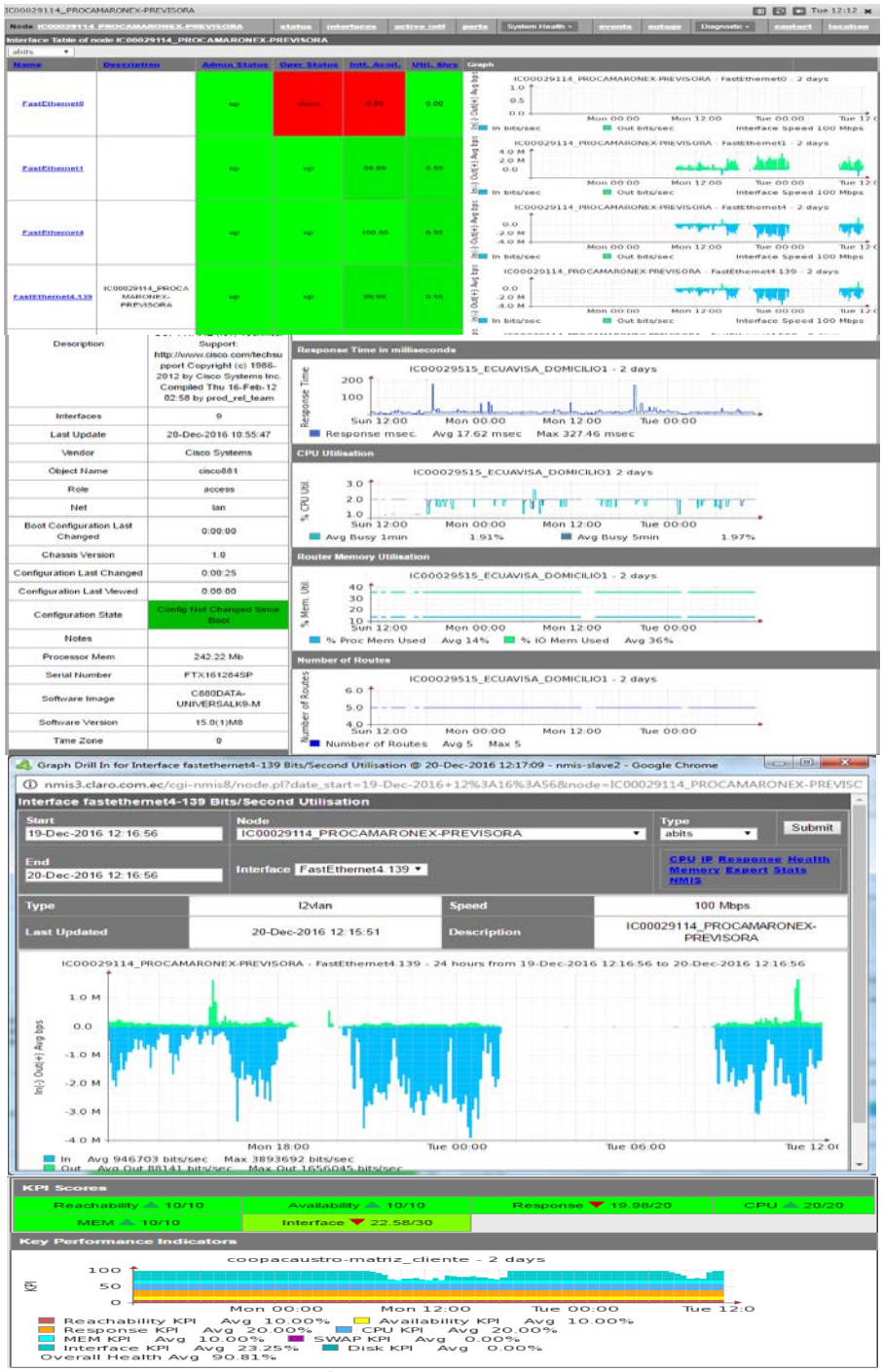

Figura 4.6: Revisión del consumo de BW una interfaz

4.10 KPI – Key Performance Indicators

KPI Item	Configuration Item	Configured Weighting	Maximum KPI Score
Reachability	weight_reachability	0.1	10 (10%)
Availability	weight_availability	0.1	10 (10%)
Response	weight_response	0.2	20 (20%)
CPU	weight_cpu	0.2	20 (20%)
Memory	weight_mem	0.1 x 50%	5 (5%)
Swap	weight_mem	0.1 x 50%	5 (5%)
Interface	weight_int	0.3 x 50%	15 (15%)
Disk	weight_int	0.3 x 50%	15 (15%)

KPI Item	Configuration Item	Configured Weighting	Maximum KPI Score
Reachability	weight_reachability	0.1	10 (10%)
Availability	weight_availability	0.1	10 (10%)
Response	weight_response	0.2	20 (20%)
CPU	weight_cpu	0.2	20 (20%)
Memory	weight_mem	0.1	10 (10%)
Interface	weight_int	0.3	30 (30%)

Tabla 2: Indicadores KPI

4.11 Fórmula de cálculo de indicadores KPI

100 - (0.02+2.96+0.25+4.5) = 92.27% (4.1)

En la Tabla 2 y la Figura 4.7 se puede visualizar los diferentes indicadores KPI que muestra la interfaz.

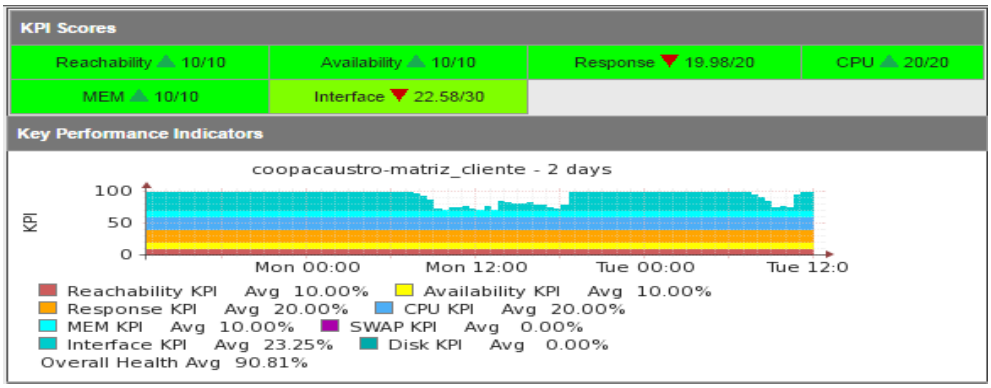

Figura 4.7: Interfaz de indicadores KPI

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

A pesar de estar en etapa de integración de los equipos, de los resultados obtenidos se ha logrado tener un mayor y más ágil diagnóstico de los eventos que se suscitan con los CPEs de los clientes, entre ellos por ejemplo:

Se puede obtener graficas de consumo del servicio, gracias a este beneficio se pueden descartar los problemas reportados como lentitud de servicio ya que mayormente estos se deben a problemas internos por la generación de tráfico que llega a saturar el ancho de banda contratado.

Históricos de caídas de las interfaces de los CPEs: así se puede determinar o visualizar más eficazmente reportes de caída de servicios que están relacionados con problemas en la red interna del cliente como desconexión problemas de negociación con sus equipos.

Soportes de primer nivel más efectivos: puesto que ahora se cuenta con la gestión de los equipos CPEs del cliente y esto no solo implica la gestión de enrutadores sino de los enlaces de UM asociadas a los servicios, se pueden resolver problemas de interferencia a partir de alarmas generadas en el Gestor, de manera remota.

Información de BCKUP: ahora es posible programar el gestor y tener información de la configuración de los CPEs, gracias a esta característica se reducirán los tiempos de afectación ya que la logística en caso de daño será reducida.

Información del equipo CPE: en el reporte de la herramienta implementada se cuenta con un histórico de los números de serie de los equipos asociados a ese punto de monitoreo, por lo que se puede determinar situaciones en las que el usuario reemplazara los CPEs de la compañía.

Geolocalización de elementos: Con la implementación de la nueva herramienta es posible asociar por coordenadas que deben ser configurados en los CPEs la ubicación de cada equipo mediante el motor de posicionamiento googlemaps.

RECOMENDACIONES:

El problema a nivel empresarial en la implementación de soluciones de gestión deberían ser estándares más sin embargo muchas de las soluciones tienen integradas ya su propio de sistema de gestión por lo que luego se deberá de trabajar con desarrollos muy particulares para su integración con el Gestor de Gestores.

Con respecto a la aplicación analizada, la interfaz gráfica por donde se adicionan los nuevos elementos no es lo bastante intuitiva y se complica al momento de su visualización.

Debería poseer una asociación de grupos para los elementos, así sería más fácil de identificar por regiones y ciudades.

La aplicación actualmente no puede ingresar a los elementos a nivel de líneas de comando si no es ingresando a través de su servidos primero.

BIBLIOGRAFÍA

[1] CISCO. (2010, Enero) CISCO WEB. [Online]. http://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/4649-mpls-faq-4649.html#anc1

[2] A. Barba, "Gestión de Red". Cataluña: Edicions, UPC, 1999.

[3] W. Stallings, SNMP, SNMPv2, SNMPv3 and RMON 1 and 2 (3rd Edition). Massachusetts: Addison-Wesley Professional, 1999.

[4] Greg Shields. realtimepublishers.com. [Online]. http://www.realtimepublishers.com/sgnmm.php

[5] SNMP: VERSIONES DE SNMP. (2011, JUNIO) http://protocolo-snmp.blogspot.com/2011/06/versiones-de-snmp.html.

[6] PANDORAFMS:Monitorizacion_traps_SNMP, teoría de traps en SNMP. (2014, ENERO) http://wiki.pandorafms.com/index.php?title=Pandora:Monitorizacion_traps_SNMP.

[7] CISCO WEB. (2014, ENERO) http://www.cisco.com/cisco/web/psa/default.html?mode=tech.

[8] James Reagan, CISCO CCIP Study guide. San Francisco: SYBEX, 2002.

[9] DATATRACKET. (2014) https://datatracker.ietf.org/.

[10] J. Witters, G. van Kersen, J. De Clerq, S. Khandekar, "Claves para desplegar con éxito el VPLS" TUTORIAL TÉCNICO DEL VPLS," Revista de Telecomunicaciones de Alcatel, pp. 439-443 (este número), 4º trimestre de 2004.