UNIVERSIDAD GALILEO

IMPLEMENTACIÓN DE CALIDAD DE SERVICIO SOBRE UNA RED MPLS EN LA REGIÓN METROPOLITANA DE GUATEMALA

Autores: María Fernanda Castellanos Castellanos

José Carlos Guzmán Verbena

Ciudad de Guatemala, marzo 2008

UNIVERSIDAD GALILEO

IMPLEMENTACIÓN DE CALIDAD DE SERVICIO SOBRE UNA RED MPLS EN LA REGIÓN METROPOLITANA DE GUATEMALA

Autores: María Fernanda Castellanos Castellanos

José Carlos Guzmán Verbena

Ciudad de Guatemala, marzo 2008

UNIVERSIDAD
Galileo

Guatemala, 20 de noviembre de 2007

Señor(ita)
María Fernanda Castellanos
Jose Carlos Guzmán
Presente

Estimados alumnos:

Tengo mucho gusto en informarles que ha sido aprobado su punto de Tesis, previo a optar al diploma de **Ingeniero en Telecomunicaciones y Redes Teleinformáticas** cuyo título es **"IMPLEMENTACION DE CALIDAD DE SERVICIO SOBRE UNA RED MPLS EN EL AREA METROPOLITANA DE LA CIUDAD DE GUATEMALA".**

Al mismo tiempo le informo que ha sido aprobada la designación del **Ingeniero Marco Antonio To** , como asesor de su trabajo de graduación.

Atentamente,

FACULTAD DE INGENIERIA DE SISTEMAS,
INFORMATICA Y CIENCIAS DE LA COMPUTACION

Ing. José Eduardo Suger Castillo
Decano Fisicc
Universidad Galileo

Ing. José Eduardo Suger
Decano FISICC

vl.

UNIVERSIDAD Galileo

Guatemala, 20 de noviembre de 2007

Ingeniero
Marco Antonio To
Presente

Estimado Ingeniero To:

Tengo mucho gusto en informarle que ha sido aprobada su designación como asesor del trabajo de Tesis de los alumnos María Fernanda Castellanos y Jose Carlos Guzmán, previo a optar al diploma de **Ingeniero en Telecomunicaciones y Redes Teleinformáticas**, cuyo título es **"IMPLEMENTACION DE CALIDAD DE SERVICIO SOBRE UNA RED MPLS EN EL AREA METROPOLITANA DE LA CIUDAD DE GUATEMALA ".**

Para su información adjunto a la presente, fotocopia de la solicitud y respuesta de los alumnos María Castellanos y Jose Guzmán.

Atentamente,

FACULTAD DE INGENIERIA DE SISTEMAS,
INFORMATICA Y CIENCIAS DE LA COMPUTACION

Ing. José Eduardo Suger Castillo
Decano Fisicc
Universidad Galileo

Ing. José Eduardo Suger
Decano FISICC

vl.

UNIVERSIDAD Galileo

Guatemala, 6 de Agosto del 2008

Facultad de Ingeniería
De Sistemas, Informática y
Ciencias de la Computación.
Universidad Galileo

A quien Interese:

Por medio de la presente me dirijo a usted para informarle que he brindado asesoría a los Estudiantes Maria Fernanda Castellanos Castellanos con carné 20032059 y José Carlos Guzmán Verbena con carné 20032132 en la realización del trabajo de tesis.

IMPLEMENTACION DE CALIDAD DE SERVICIO SOBRE UNA RED MPLS EN LA REGION METROPOLITANA DE GUATEMALA

Es mi criterio que el trabajo ha sido completado de manera satisfactoria atendiendo los criterios que rigen en la facultad bajo su dirección.

Por lo anteriormente expuesto, someto a usted en mi calidad de asesor el presente proyecto para su aprobación.

Atentamente

Ingeniero Marco Antonio To
Asesor de Tesis

Ciudad de Guatemala, 13 de agosto de 2008.

Ingeniero
José Eduardo Suger Castillo
Decano FISICC
Universidad Galileo
Presente.

Señor Decano:

De manera respetuosa le informo que la tesis IMPLEMENTACIÓN DE CALIDAD DE SERVICIO SOBRE UNA RED MPLS EN LA REGIÓN METROPOLITANA DE GUATEMALA, de los alumnos María Fernanda Castellanos Castellanos y José Carlos Guzmán Verbena, ha sido objeto de revisión gramatical y estilística, por lo que pueden continuar con los trámites de graduación

Atentamente

Lic. Lizardo Porres Velásquez
Asesor Lingüístico
Universidad Galileo

Guatemala, 14 de agosto 2,008

Ing. José Eduardo Suger Castillo
Decano FISICC
Universidad Galileo
Presente

Estimado Ing.Suger:

Por medio de la presente me permito presentar el proyecto de tesis de los alumnos: María Fernanda Castellanos Castellanos (carné No. 20032059) y José Carlos Guzmán Verbena (carné No. 20032132) de la carrera de Ingeniería en Telecomunicaciones y Redes Teleinformáticas, titulada:

"IMPLEMENTACION DE SERVICIO SOBRE UNA RED MPLS EN LA REGION METROPOLITANA DE GUATEMALA"

Después de haber leído y revisado el proyecto en mención, considero que este trabajo ha sido completado en forma satisfactoria, atendiendo a los criterios que rigen esta facultad.

Atentamente,

Ing. Marco Antonio To
Director Ingeniería en Telecomunicaciones

UNIVERSIDAD
Galileo

Guatemala, 20 de agosto de 2008

Señor (ita)
María Fernanda Castellanos Castellanos
Carné 20032059
José Carlos Guzmán Verbena
Carné 20032132
Presente

Estimados Alumnos:

Tengo mucho gusto en informarles que después de que su Director de carrera ha revisado su trabajo de Tesis cuyo título es **"IMPLEMENTACION DE SERVICIO SOBRE UNA RED MPLS EN LA REGION METROPOLITANA DE GUATEMALA"** y de haber obtenido el dictamen del asesor específico; el Ingeniero Marco Antonio To, autorizo la publicación del mismo.

Aprovecho la oportunidad para felicitarlos por el magnifico trabajo realizado, el cual es de indiscutible beneficio para el desarrollo de las Ciencias en Telecomunicaciones en Guatemala.

Atentamente,

FACULTAD DE INGENIERIA DE SISTEMAS,
INFORMATICA Y CIENCIAS DE LA COMPUTACION.

Ing. José Eduardo Suger Castillo
Decano Fisicc
Universidad Galileo

Ing. José Eduardo Suger
Decano FISICC

vl.-

UNIVERSIDAD GALILEO

Facultad de Ingeniería de Sistemas, Informática
y Ciencias de la Computación

IMPLEMENTACIÓN DE CALIDAD DE SERVICIO SOBRE UNA RED MPLS EN LA REGIÓN METROPOLITANA DE GUATEMALA

Tesis presentada para obtener el
título de Ingeniería en Telecomunicaciones y Redes Teleinformáticas

Autores: María Fernanda Castellanos Castellanos
José Carlos Guzmán Verbena

Ciudad de Guatemala, marzo 2008

ÍNDICE

Introducción

La red de comunicaciones es una de las bases fundamentales para una organización exitosa. Las redes de hoy en día deben transportar gran cantidad de datos y aplicaciones, incluyendo video de alta calidad y datos sensibles que trabajan en tiempo real. Las aplicaciones utilizan mucho ancho de banda, lo que obliga a las tecnologías saber aprovechar al máximo los recursos y las capacidades de las redes. En consecuencia, ha sido necesario el desarrollo y la existencia de técnicas que permiten brindar un servicio de calidad, al maximizar la utilización de los recursos en forma eficiente. MPLS es una tecnología que permite la optimización de los recursos en una red, permite que el tráfico sea más predecible y se pueda manejar de forma sencilla, y que en conjunto con los conceptos y técnicas de calidad de servicio, se pueda garantizar una comunicación exitosa de principio a fin para todo tipo de aplicaciones.

1. MPLS (Multi Protocol Label Switching)

MPLS es una tecnología que opera al agregar etiquetas a los paquetes que recibe, para luego enviarlos a través de la red. Dichas etiquetas se agregan a los paquetes IP, de tal manera que los routers ahora son capaces de enviar datos al basarse únicamente en las etiquetas, y no en la dirección IP destino del paquete original.

La técnica de conmutar paquetes que se basa en una etiqueta no es nueva, Frame Relay y ATM lo utilizan también, al usar paquetes de tamaño variable y fijo respectivamente. En los encabezados de Frame Relay y ATM se encuentra la información del circuito virtual que los paquetes deben seguir. La similitud entre estas dos tecnologías, es que en cada salto la información de encabezado o "etiqueta" debe cambiar. En contraste, cuando un router envía un paquete IP, la dirección IP destino nunca cambia. La utilización de etiquetas en vez de direcciones IP, es lo que ayudó a aumentar la popularidad de MPLS.

1.1. Beneficios de MPLS

1.1.1. Infraestructura de red unificada

La idea consiste en etiquetar los paquetes que ingresan a la red al basarse en la dirección destino u otra información preestablecida, para luego enviar los paquetes a través de una infraestructura de red común. Esta es la ventaja de MPLS. Una de las razones por las que el Protocolo de Internet (IP) se convirtió en el protocolo dominante, es el hecho de que muchas tecnologías pueden ser transportadas sobre él.

Al utilizar MPLS en conjunto con IP, las posibilidades de transportar información aumentan. Agregar etiquetas a los paquetes permite transportar otros protocolos, similar a lo que antes era posible únicamente sobre redes Frame Relay o ATM. MPLS puede transportar IPv4, IPv6, Ethernet, HDLS, PPP y otras tecnologías de capa 2.

La capacidad de transportar cualquier tecnología de capa 2 a través de MPLS se conoce como AToM (Any Transport over MPLS), en la cual los dispositivos de red no necesitan conocer el contenido del paquete en sí. No es necesario desencapsular, sólo hace falta ver la etiqueta para conmutar el paquete. En esencia, MPLS es un simple método para transportar múltiples protocolos en una sola red.

1.1.2. Núcleo de red sin BGP

Cuando en una red es necesario enviar tráfico IP, cada router por donde pasa dicho tráfico, debe buscar la dirección IP destino del paquete. Tal es el caso de un proveedor de servicio. Si el tráfico debe ser enviado a destinos que son externos a la red del ISP, esos prefijos IP externos deben estar presentes en las tablas de enrutamiento de cada uno de los routers. BGP es el encargado de enviar dichos prefijos externos, tales como los prefijos de los clientes y los de la Internet. Esto significa que todos los routers del ISP deben utilizar BGP.

Sin embargo, MPLS permite el envío de paquetes basado en etiquetas. MPLS permite que una etiqueta sea simplemente asociada con un router de salida, en vez de una dirección IP. La etiqueta en sí contiene que router de egreso debe enviar el paquete. Los routers del núcleo ya no necesitan dicha información de destino IP, por ende, no necesitan utilizar BGP.

Los routers en la frontera aun necesitan buscar la IP destino dentro del paquete, y sí necesitan emplear BGP. Un ISP podría tener cientos de routers en su núcleo de red, todos al utilizar BGP, si MPLS fuera implementado en dicha red, únicamente los routers frontera lo necesitarían, lo cual reduce considerablemente la complejidad.

Todos los routers del núcleo están ahora enviando los paquetes al basarse en etiquetas, sin buscar en tablas de enrutamiento, libres de la tarea de utilizar BGP. El hecho de no utilizar BGP en todos los routers debe ser considerado seriamente, ya que los routers necesitan menos recursos, lo cual a su vez reduce los costos.

1.1.3. MPLS VPN

Una red virtual privada (VPN) es una red que emula una red privada en una infraestructura común. La red privada debe permitir que todos sus usuarios puedan conectarse a ella, y separarse completamente de otras redes. Los proveedores de servicio, ofrecen dos tipos principales de VPN a sus clientes:

- VPN Superpuesta
- VPN P2P

Modelo VPN superposición:

En el modelo de superposición, el proveedor de servicio ofrece uno de los enlaces punto a punto o circuitos virtuales a través de su propia red, entre los routers del cliente. Esta forma adyacencias entre ellos mismos únicamente, los routers y switches del proveedor de servicio lleva la información a través de su red, pero nunca forman adyacencias con los routers clientes.

Dichos enlaces punto a punto, podían ser de capa 1, 2 ó incluso capa 3, tales como TDM, E1, E3, SONET, SDH, X.25, ATM, o Frame Relay. Este tipo de servicio crea la ilusión de estar conectado directamente con el sitio remoto.

1.1.4. Modelo VPN P2P

En el modelo VPN P2P (peer-to-peer), igual que en el modelo anterior, los routers del proveedor de servicio transportan los datos del cliente a través del su propia red, la diferencia es que los routers del cliente sí crean adyacencias de capa 3 con los routers del proveedor de servicio. Dado el hecho de que la VPN es de naturaleza privada, dicha tarea se lograba en este modelo mediante la implementación de filtros y listas de control de

acceso, para permitir o denegar la salida desde y hacia los routers de los sitios clientes. También es posible la modificación en el proceso de publicación de rutas para lograr privacidad.

Antes del desarrollo de MPLS, el modelo de VPN por superposición utilizado con más frecuencia que el modelo P2P. El modelo P2P requería de mucha más configuración en los equipos, al elevar la complejidad relativamente. MPLS VPN es una aplicación de MPLS que convirtió la implementación de VPNs P2P más fácil.
Agregar o remover sitios clientes es mucho más fácil, ya que requiere de menor esfuerzo y tiempo de configuración.

Con MPLS VPN, el router del cliente, conocido como CER (customer edge router), crea una adyacencia de capa 3 con uno de los routers del proveedor de servicio, llamado PER (provider edge router). La privacidad se logra con la utilización de VRF (virtual routing forwarding) que asegura que la información de diferentes clientes se mantenga separada, y el hecho que el transporte de los paquetes se base en etiquetas y no en direcciones IP.

Este concepto implica que únicamente se crean adyacencias entre CER y PER. No es necesaria la configuración de circuitos virtuales como en el modelo de superposición, o la configuración de filtros de rutas, como en el modelo P2P. Este es el beneficio de MPLS VPN.

1.1.5. Ingeniería de tráfico MPLS

La idea básica detrás de la ingeniería de tráfico es usar la infraestructura de red de forma óptima, al incluir los enlaces que están siendo subutilizados por no ser las rutas óptimas o de más bajo costo. La ruta de más bajo costo es calculada por los protocolos de enrutamiento, y con ingeniería de tráfico MPLS, se puede reorientar el tráfico originado en el punto A con destino hacia el punto B, en una ruta que no es la de menor costo. Esto crea una amplia distribución ente los enlaces subutilizados, aspecto que no se puede lograr en una red puramente IP.

Otra ventaja de MPLS TE, es la posibilidad de utilizar FRR (Fast reRouting). FRR permite reenviar paquetes etiquetados por rutas alternas cuando un router no se encuentra disponible. Dicho proceso se efectúa en menos de 50ms, lo cual es considerablemente rápido incluso para los estándares de hoy en día.

1.2. Arquitectura MPLS

MPLS depende de dos componentes principales: control y envío (forwarding).
El componente de envío utiliza etiquetas acarreadas por los paquetes y la información de etiqueta-envío mantenida por los dispositivos MPLS para operar. El componente de control es responsable de mantener la información de forma coherente entre todos los dispositivos MPLS de la red.

1.2.1. Componente de envío

A continuación se describen los conceptos que conforman el componente de envío en MPLS.

1.2.1.1. Etiquetas MPLS

Una etiqueta MPLS es una estructura de 32 bits, la cual está dividida en 4 campos, cada uno con una función específica:

1. Valor de la etiqueta
   Consta de 20 bits y contiene el valor en sí de la etiqueta.

2. EXP

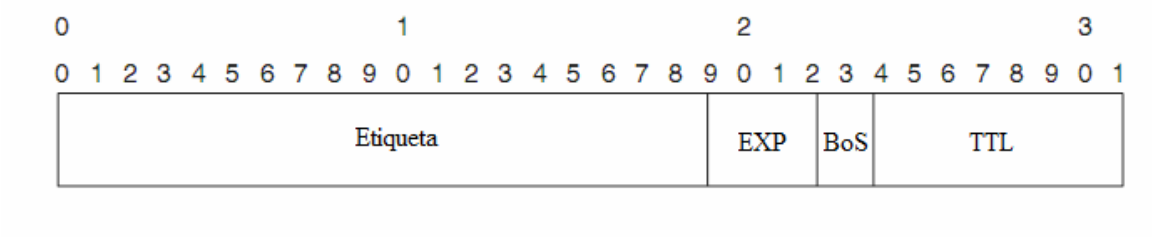
Es un campo de 3 bits que originalmente fue creado, como su nombre lo indica, para fines experimentales, pero que en la actualidad se utiliza para proveer calidad de servicio.

3. BoS

Este bit se enciende únicamente cuando la etiqueta es la última de la pila, y es cero en todas las demás etiquetas.

4. TTL

Por último se encuentran 8 bits del tiempo de vida del paquete, el cual funciona de la misma forma que el TTL de un paquete IP. Simplemente se realiza un decremento de uno, cada vez que el paquete realiza un salto. Esto evita que los paquetes queden en un bucle infinito (routing loop). Una vez que el valor TTL alcanza el 0, el paquete es descartado.



1.2.1.2.Pila de etiquetas

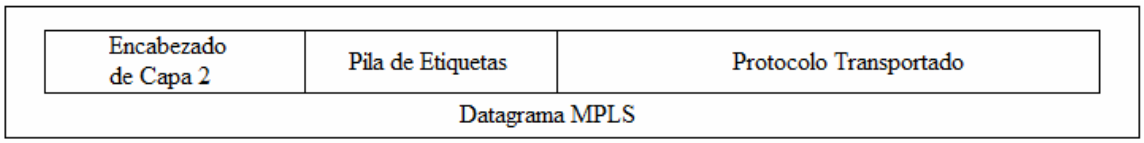
La pila es una colección de etiquetas que se encuentran “sobre” el paquete. La pila o stack puede ser una única etiqueta, o puede tener más. El número de etiquetas no tiene restricciones, aunque rara vez se llega a ver una pila con más de cuatro o más etiquetas.

Etiqueta	EXP	0	TTL
Etiqueta	EXP	0	TTL
⋮			
Etiqueta	EXP	1	TTL

Los paquetes que están destinados para ser enviados a través de una red MPLS, necesitan tener una o más etiquetas en la pila, la primera etiqueta en la pila se conoce como la etiqueta superior (top label), y al fondo de la pila se encuentra la inferior (bottom label). La última etiqueta es la única que puede tener el bit BoS encendido. La cantidad de etiquetas en la pila depende de la aplicación que las esté utilizando.

1.2.1.3.Encapsulado MPLS

La pila de etiquetas en un paquete MPLS, se encuentra entre la porción de capa 2 y capa 3 del paquete original. El encapsulado del enlace puede ser casi de cualquier tipo: PPP, HDLC, Ethernet, etc. Si asumimos que el protocolo a transportar es IPv4, y el encapsulado es PPP, la pila de etiquetas se encontraría después del encabezado PPP, pero antes del encabezado de IPv4.



Datagrama MPLS

Como resultado de esta codificación o encapsulado, MPLS puede ser implementado sobre cualquier medio, incluyendo enlaces punto a punto, multi acceso, y ATM. El componente de envío es independiente de el protocolo de capa de red.

1.2.1.4.Label Switching Router (LSR)

Un LSR es un router capaz de soportar MPLS, así como de entender las etiquetas que son recibidas y luego transmitirlas. En una red MPLS, existen tres tipos de LSR:

LSR de Ingreso: Recibe un paquete sin etiqueta, inserta la pila de etiquetas para luego lo envía por el enlace apropiado.

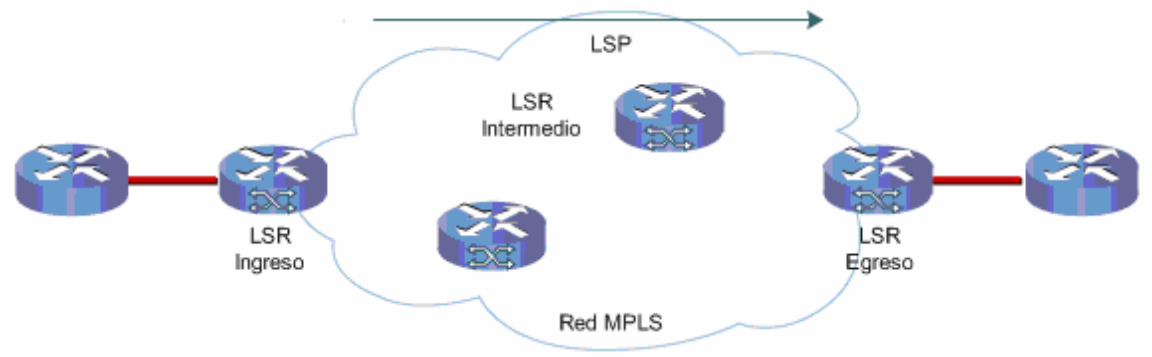
LSR de Egreso: Recibe un paquete ya etiquetado, remueve la pila de etiquetas, y luego lo envía por el enlace apropiado.

LSR Intermedio: Recibe un paquete etiquetado, realizan una operación sobre dicho paquete, luego es enviado por el enlace apropiado.

Un LSR puede realizar cualquiera de estas tres operaciones: Push, Pop o Swap. Es decir, introducir, sacar y cambiar respectivamente. Un LSR también debe ser capaz de insertar más de una etiqueta en la pila. Si el paquete no contiene etiquetas, el LSR debe ser capaz de insertar una pila de etiquetas en el paquete, así como cambiar una etiqueta por otra, siendo esta la etiqueta superior de la pila.

1.2.1.5.Label Switched Path (LSP)

Un LSP es un camino o secuencia de routers (LSR) que conmutan un paquete etiquetado a través de toda la red MPLS, o parte de ella. Básicamente es el camino que un paquete etiquetado toma. Un LSP es equivalente a los circuitos virtuales en ATM y Frame Relay.



Un LSR de ingreso no es necesariamente el primer router que etiqueta un paquete. Dicho paquete pudo ser etiquetado con anterioridad por otro LSR, como ocurre en el caso de LSPs anidados, o LSPs dentro de otros.

1.2.1.6.Forwarding Equivalence Class (FEC)

Un FEC es una agrupación de paquetes que son enviados a través del mismo camino o ruta, y son tratados de la misma manera. Todos los paquetes pertenecientes al mismo FEC, tienen la misma etiqueta. El router que decide qué etiquetas lleva un paquete es el LSR de ingreso, es el encargado de clasificar los paquetes, por ejemplo:

- Paquetes con direcciones IP iguales a determinado prefijo
- Paquetes Multicast
- Paquetes con tratamiento basado en DSCP de IP DiffServ
- Paquetes recibidos y entregados en sub interfaces
- Paquetes con destinos IP que pertenecen a prefijos BGP.

1.2.2. Componente de Control

En MPLS es esencial crear uniones entre las rutas de capa 3 y las etiquetas. MPLS soporta una amplia gama de formas de envío para proveer características escalables y funcionalidad. El componente de control crea las relaciones de etiquetas y luego las distribuye entre LSRs al utilizar un protocolo de distribución.

1.2.2.1.Distribución de etiquetas

La distribución de etiquetas es un proceso qué se lleva a cabo entre routers. Los LSRs adyacentes deben estar de acuerdo en qué etiquetas utilizar para cada prefijo IGP. Por ende, cada LSR debe saber con que etiqueta remplazar la que ya contiene el paquete recibido. Esto implica la existencia de un mecanismo que indique a los LSRs qué etiquetas usar, para lo cual es necesario un protocolo de distribución.

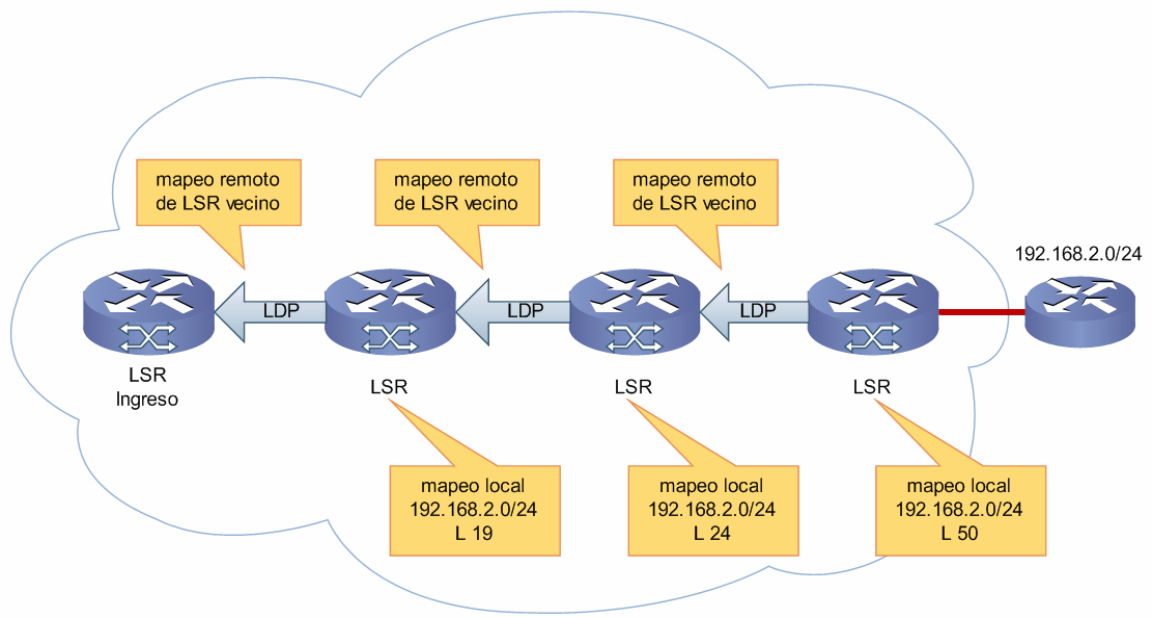
Se pueden distribuir etiquetas de dos formas:

- Agregar las etiquetas sobre un protocolo de enrutamiento ya existente
- Tener un protocolo por separado encargado únicamente de dicha tarea

1.2.2.2.Distribución de Etiquetas con LDP

Cada LSR mantiene una FIB (Forwarding Information Base) en donde se almacena la información de la capa de red. De aquí es donde se calculan las mejores rutas para ser ingresadas en la tabla de enrutamiento y distribuidas posteriormente por un IGP.

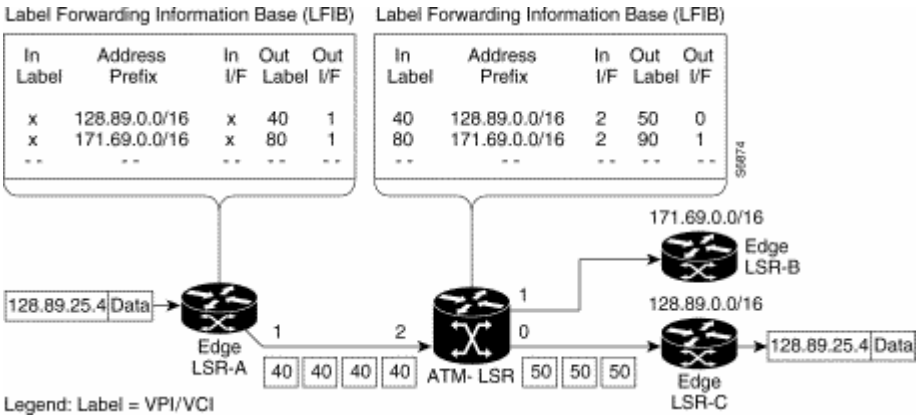
Posteriormente los LSR crean uniones o ligaduras (bindings) entre cada etiqueta y destino IP. La información de ligadura se almacena en la LFIB (Label Forwarding Information Base). El SLR distribuye las ligaduras a todos sus vecinos adyacentes, quienes a su vez repiten el proceso.



1.2.2.3.LFIB

Cuando un dispositivo MPLS recibe un paquete etiquetado, este utiliza la etiqueta como un índice en la LFIB (Label Forwarding Information Base). Como resultado de esta búsqueda, se obtiene la siguiente información:

a) El siguiente salto al cual el paquete debe ser enviado.
b) La operación que debe ser realizada a la pila de etiquetas antes de reenviar el paquete; dicha operación puede remplazar, sacar, o agregar una o más etiquetas nuevas.



2. CALIDAD DE SERVICIO (QoS)

Calidad de servicio (QoS) se refiere a la capacidad de una red de proporcionar un mejor servicio a tráfico seleccionado sobre varias tecnologías, incluyendo Frame Relay, ATM, Ethernet, redes 802.1 y SONET. La principal meta de QoS es proveer prioridad a ciertos flujos al incluir ancho de banda dedicado, jitter y latencia controlada, y mejorar la pérdida de paquetes. Algo importante es asegurar que el hecho de proporcionar prioridad a uno o más flujos, no afecte a otros flujos.

El software de CISCO permite a redes complejas controlar una variedad de servicios en una red con distintas aplicaciones y tipos de tráfico. Casi cualquier red puede tomar ventaja de la implementación de Calidad de Servicio para prestar un servicio eficiente, ya sea en una red corporativa pequeña o un proveedor de servicios. En la implementación se pueden contar con los siguientes beneficios.

- Control sobre los recursos: Se puede tener control sobre los recursos de la red como ancho de banda, equipo y facilidades que son utilizados. Por ejemplo se puede limitar el ancho de banda consumido sobre un link de transferencias FTP y dar prioridad a accesos importantes en base de datos.
- Uso más eficiente de los recursos de la red: Existen los administradores de análisis de red, los cuales nos indican para qué está siendo utilizada la red y nos muestran si estamos dando el servicio solicitado al tráfico importante en la red.

Fundamentalmente, QoS permite proveer un mejor servicio a ciertos flujos. Esto se realiza al dar prioridad a un flujo o limitar la prioridad a otros flujos. Cuando se utilizan herramientas para administrar congestiones, se trata de dar prioridad a un flujo al crear colas de distintas maneras y tipos. Las herramientas de manejo de colas para evitar congestión dan prioridad al eliminar o botar flujos de menor prioridad antes que flujos con más alta prioridad. Las políticas que proveen prioridad a flujos al limitar el ancho de banda

a otros flujos. Las herramientas para eficiencia de links limitan a flujos grandes y dan prioridad a flujos pequeños.

Las herramientas de Calidad de Servicio pueden ayudar a aliviar la mayoría de los problemas de congestión. Sin embargo, muchas veces hay demasiado tráfico muy poco ancho de banda para suplir todas las necesidades y exigencia de la red. En dicho caso, calidad de servicio sería una solución.

2.1. Arquitectura Básica de QoS

La arquitectura básica introduce tres piezas fundamentales para la implementación de Calidad de Servicio.

1. Técnicas de identificación y marcado para coordinar Calidad de Servicio de punta a punta entre los elementos de la red.
2. Calidad de Servicio dentro de un solo elemento de red. Esto incluye las colas.
3. Administrar políticas de calidad de servicio

2.1.1. Identificación y Marcado en QoS

La identificación y marcado es realizado por medio de la reservación y clasificación.

Para proveer servicio preferencial a un tipo de tráfico debe ser identificado. Segundo, el paquete puede o no ser marcado. Estas primeras dos tareas componen la clasificación. Cuando el paquete es identificado pero no marcado, la clasificación está basada en un comportamiento por salto. Esto es cuando la clasificación depende únicamente del dispositivo en el que se encuentra y no es pasado al siguiente router. Esto sucede con colas de prioridad o PQ (priority queuing) y CQ (costum queuing). Cuando los paquetes son marcados para toda la red, los bits de la IP de precedencia son establecidos.

Métodos comunes de identificación de flujos incluyen listas de control de acceso (ACLs), políticas de enrutamiento y aplicaciones para reconocimiento para redes.

2.1.2. QoS en un solo Elemento de Red

La administración de congestión, manejo de colas, eficiencia de links y herramientas de modificación de tráfico proporcionan QoS para un solo elemento de red.

2.1.2.1. Administrador de Congestiones

Debido a las distintas naturalezas del tráfico de voz, video o datos, algunas veces la cantidad de tráfico excede la velocidad del link. En este caso, qué debe hacer el router? Pondrá el tráfico en un buffer en una sola cola FIFO, opondrá los paquetes en distintas colas y antes dar servicio a ciertas colas. Las herramientas para administrar las congestiones atienden estas preguntas. Las herramientas incluyen PQ, CQ, weighted fair queuieng(WFQ) y class-based weighted fair queuing (CBWFQ).

2.1.2.2. Administrador de Colas

Debido a que las colas tienen tamaño limitado, se pueden llenar y rebalsarse. Cuado las colas están llenas ningún paquete adicional puede ingresar a la cola por lo que es descartado. Esto es lo que se conoce como "tail drop". Este problema con el tail drop es que el router no puede evitar que suceda inclusive si son paquetes de alta prioridad. Entonces es necesario un mecanismo que realice dos cosas:

1. Tratar de asegurarnos que las colas no se llenen, para que haya espacio para paquetes de alta prioridad.
2. Crear cierto criterio para botar paquetes que son de más baja prioridad antes de desechar paquetes de alta prioridad.

Weighted early random detect (WRED) provee ambos de estos mecanismos.

2.1.2.3. Eficiencia en los Enlaces

Muchas veces los enlaces de baja velocidad presentan problemás para los paquetes pequeños. Por ejemplo, el retraso del serial de un paquete de 1500 bytes en un enlace de 56-kbps es de 214 milisegundos. Si un paquete de voz se encuentra detrás de este gran paquete, el delay sería excedido antes de que el paquete dejara el router. La fragmentación e intercalación de paquetes permite a este paquete ser segmentado en paquetes pequeños e intercalarlos con el paquete de voz. La intercalación es igual de importante que la fragmentación, ya que no hay razón de fragmentar el paquete si no se intercala con otros paquetes atrás de éste.

Otra manera de hacer más eficiente un enlace es la eliminación de bits de encabezado. Por ejemplo, los paquetes de RTP (Real Time Protocol) tienen 40 bytes de encabezado. La compresión de encabezados reduce el paquete a un tamaño manejable.

2.1.2.4. Modificación de Tráfico y Políticas

La modificación es utilizada para crear un flujo de tráfico que limita el ancho de banda potencial del flujo o flujos. Esto es utilizado muchas veces para prevenir el problema del rebalse que ya fue mencionado. En este caso, el sitio central normalmente tiene un enlace de banda ancha, mientras que el sitio remoto tiene un enlace de baja capacidad. En este caso, es posible que el tráfico del sitio central sobrepase la capacidad del otro extremo. La modificación del tráfico, también llamado “Shaping”, es una manera perfecta para evitar congestiones en el link remoto. El tráfico mayor a la configuración es puesto en un buffer para la transmisión.

Las políticas son similares al shaping, pero se diferencian en algo importante. El tráfico que excede a la configuraron no es puesto en un buffer si no es descartado normalmente.

2.2. Administración De QoS

La administración de calidad de servicio ayuda a establecer y evaluar políticas y metas. Una metodología común sigue los siguientes pasos.

PASO 1: Determinar el equipo de red y realizar pruebas de tráfico. Esto ayuda a determinar las características del tráfico en la red.
PASO 2: Emplear las técnicas de calidad de servicio cuando las características del tráfico haya sido obtenido.
PASO 3: Evaluar los resultados por medio de pruebas de respuesta para ciertas aplicaciones para verificar que las metas establecidas hayan sido alcanzadas.

2.2.1. Niveles de Calidad de Servicio

Los niveles de calidad de servicio se refieren a las capacidades de inicio a fin, refiriéndose a la capacidad de una red proporcionar los servicios necesitados en una red por un tráfico de red específico de un inicio a un fin o de orilla a orilla. Los servicios difieren en el nivel de calidad de servicio en cuanto a lo estricto.

Hay tres niveles de calidad de servicio de inicio a fin, que pueden ser proporcionados a través de una red heterogénea.

- Servicio del mejor esfuerzo: es conocido como la ausencia de calidad de servicio. El mejor esfuerzo es conectividad básica sin ninguna garantía. Esto se caracteriza por las colas FIFO, las cuales no diferencian entre colas.
- Servicio Diferenciado: en este nivel algunos tráficos son tratados mejor que el resto. Este se enfoca en preferencias estadísticas, no en una severa y rápida garantía. Esto es alcanzado por medio de la clasificación de tráfico y el uso de herramientas de calidad de servicio como PQ, CQ, WFQ y WRED.

- Servicios Garantizados: en este nivel los recursos de la red son totalmente reservados para un tráfico en especial. Esto se logra a través de herramientas de QoS como RSVP y CBWFQ.

Al momento de decidir cuál es el tipo de servicio apropiado para la red, hay que tomar en cuenta varios factores.

- La aplicación o problema que el cliente está tratando de resolver. Cada uno de los tres tipos de servicios es adecuada para ciertas aplicaciones. Esto no implica que el cliente deba migrar de un servicio diferenciado a un servicio garantizado (aunque eventualmente lo hará). Un servicio diferenciado o inclusive un servicio de mejor esfuerzo puede ser apropiado, ya que depende de los requerimientos de las aplicaciones del cliente.
- El índice de transferencia al que el cliente puede realísticamente llegar con su infraestructura.
- El costo de la implementación y desarrollo de un servicio garantizado es un factor por el que se puede inclinar más por un servicio diferenciado.

2.2.1.1. Clasificación e Identificación de Flujos

Para proveer prioridad a ciertos flujos, el flujo debe de ser identificado primero y marcado si así se desea. Estas tareas son comúnmente llamadas clasificación.

Históricamente la identificación era hecha al utilizar listas de control de acceso (ACLs). Las listas de control de acceso identifican al tráfico para las herramientas de administración de congestiones como PQ y CQ. Debido a que PQ y CQ son almacenadas en los routers para su comportamiento en ese salto, la identificación de un paquete es usado solamente dentro del mismo router. En ciertas instancias, la clasificación CBWFQ es para un solo router. Esto es contrastado al declarar los bits de precedencia.

Avances como enrutamientos basados en políticas o CAR son usados para establecer precedencia basada en la clasificación por medio de listas de acceso extendidas. Esto permite una considerable flexibilidad para la asignación de precedencia, incluyendo la asignación por aplicación o por usuario, por destino o por subred origen.

Redes basadas en la identificación de aplicaciones (NBAR) son utilizadas para identificar aplicaciones de una forma más granular. Por ejemplo un URL en un paquete HTTP puede ser identificado una vez el paquete fue identificado, el paquete puede ser marcado con una precedencia establecida.

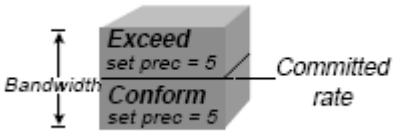
2.2.1.2. IP de Precedencia

Una de las ventajas de CAR permite clasificar el tráfico en una interfaz entrante. También permite la especificación de políticas para manejar el tráfico que excede cierto ancho de banda. CAR observa el tráfico recibido en la dirección entrante, o la subred del tráfico seleccionado por criterios de una lista de acceso, realiza una comparación de su índice de tráfico y luego toma acción basándose en el resultado, por ejemplo descartar el paquete o reescribir la ip de precedencia.

Hay alguna confusión en cuanto el uso de CAR para establecer los bits de precedencia en la IP. CAR es utilizado para supervisar el tráfico a un "Commited Access Rate". CAR realiza esto con una cubeta de tokens, que es una cubeta en la cual los tokens son representados por bytes. La cubeta se llena con tokens a un límite configurado por el usuario. Mientras los paquetes van llegando para ser entregados, el sistema verifica si hay tokens en la cubeta. Si hay suficiente tokens en la cubeta para igualar al tamaño de el paquete, los tokens son removidos de la cubeta y el paquete es enviado. Si no hay suficientes tokens en la cubeta, el paquete es descartado.

Cuando se utiliza la implementación IOS CISCO para CAR, el usuario tiene más opciones que descartar el paquete o dejarlo pasar. Una de las opciones es establecer los bits de precedencia en la IP. Cuando la aprobación de un paquete o la acción de exceso de bits

establecen los bits aún mismo valor, ya no es una política de acción sino un método para establecer los bits de precedencia en la IP, tal como se muestra en la figura.



Cuando la ip de precedencia es establecida la red del cliente, este parámetro puede ser utilizado, opcionalmente, sin embargo este puede ser reescrito por otras políticas dentro de red. La IP de precedencia permite a clases de servicio establecerse al utilizar mecanismos existentes de encolamiento, sin ningún cambio a aplicaciones existentes o complicar los requerimientos de la red.

2.2.1.3. NBAR: Identificación Dinámica de Flujos

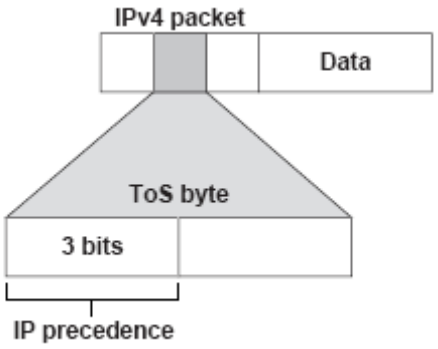
El método más nuevo de CISCO para clasificación es la identificación basada en aplicaciones de red (NBAR). Para dar claridad, NBAR es solamente una herramienta de identificación, pero se le hará referencia como una herramienta de clasificación. Para cualquier herramienta de clasificación, la parte más difícil es la identificación de tráfico. Marcar los paquetes es relativamente más fácil. NBAR realiza la parte de clasificación en otro nivel. Se necesita observar más a fondo en el paquete, la identificación puede ser realizada por ejemplo, de tipos URL o MIME de un paquete HTTP. Esto es esencial mientras más aplicaciones se convierten en aplicaciones web. Es necesario identificar entre una orden realizada o una búsqueda casual en Internet. Adicionalmente, NBAR puede identificar varias aplicaciones que usan puertos no comunes. NBAR realiza esto al observar a los paquetes de control que determinan qué puertos las aplicaciones deciden para pasar información.

NBAR adiciona un par de avances interesantes que lo hacen extremadamente valorado. Una de los avances es un protocolo con capacidad de descubrir. Esto permite a NBAR listar los protocolos en una interfaz. NBAR lista los protocolos que pueden ser identificados y

provee estadísticas de cada uno. Otro de los avances es el módulo de descripción de lenguaje de paquetes (PDLM), el cual permite protocolos adicionales ser agregados a la lista de protocolos identificables de NBAR. Cuando se trabaja con PDLM los protocolos adicionales pueden ser adicionados a las listas sin realizar una actualización a nivel de IOS o de reiniciar el router.

2.2.1.4.IP de Precedencia: QoS DIFERENCIADO

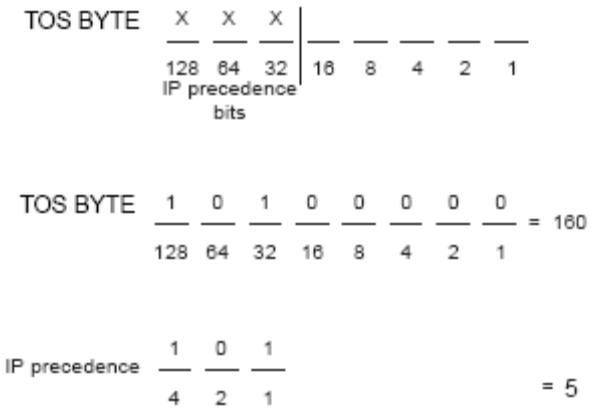
La ip de precedencia utiliza 3 bits de precedencia en el encabezado de IP versión 4 del campo llamado tipo de Servicio (ToS) para especificar el tipo de servicio para cada paquete. Se puede partir el tráfico en hasta seis clases al utilizar la IP de precedencia (otros dos son utilizados para uso interno de la red). Las tecnologías de encolamiento dentro de la red puede usar esta señal para proporcionar el debido tratamiento.



Los bits más significativos (los bits correlativos 32, 64 y 128) de el campo de ToS en el encabezado IP constituyen los bits que son utilizados para la IP de precedencia. Estos bits son usados para proveer prioridad de 0 a 7 (los valores de 6 y 7 están reservados y no deben ser establecidos por ningún administrador de red) para el paquete IP.

Debido a que solamente hay 3 bits para el uso de ToS, es necesario diferenciar estos bits del resto de los bytes de ToS. Como se muestra en la figura, un número 1 en el primer y tercer bit (observándolo de izquierda a derecha) corresponde a un IP de precedencia

número 5, pero cuando se observa el byte de ToS tiene un valor de 160. Es necesario que se haga una traducción de estos valores.



El tráfico que es identificado puede ser marcado con la IP de precedencia, de esta manera solamente necesita ser clasificado una sola vez. RFC 2475 extiende el número de bits utilizado en el campo de ToS de 3 a 6. Los 6 bits más significativos van a ser utilizados para los valores de la IP de Precedencia, los 2 bits más significativos se reservan para uso futuro. Esta especificación es comúnmente conocida como DiffServ.

2.2.2. Herramientas para el Manejo de Congestiones

Una manera que los elementos de la red manejan un rebalse de tráfico entrantes es utilizar un algoritmo de colas para repartir el tráfico, y así determinar algún método para priorizarlo. Software de CISCO incluye las siguientes herramientas de encolamiento:

- Colas FIFO
- Priority Queuing (PC)
- Costume Queuing (CQ)
- Flow-based weighted fair queuing (WFQ)
- Class-based weighted fair queuing (CBWFQ)

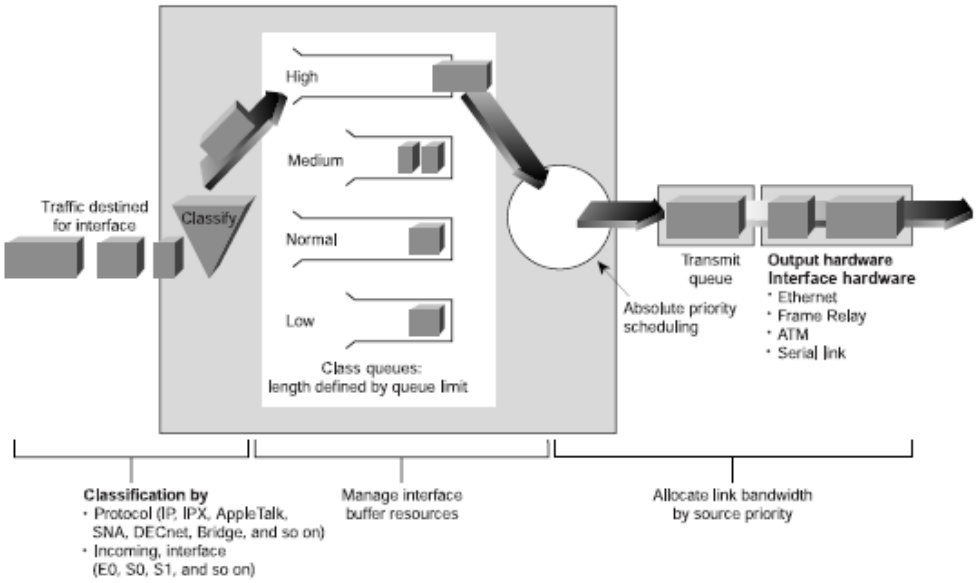
Cada algoritmo de encolamiento es diseñado para resolver un problema específico de tráfico de la red y tiene un efecto particular en el desempeño de la red.

2.2.2.1.Capacidades de Envío y Almacenamiento

En su forma más sencilla, el encolamiento FIFO incluye almacenamiento de paquetes cuando la red se encuentra congestionada y envío de los mismos en el orden de llegada cuando la red ya no se encuentra congestionada. FIFO es el algoritmo de encolamiento pre establecido para algunas instancias y no requiere configuración. FIFO no toma ninguna decisión acerca de prioridad de paquetes, el orden de llegada determina ancho de banda y su ubicación en el buffer. El encolamiento FIFO era necesario al principio para controlar el tráfico de la red, hoy en día, las redes inteligentes necesitan algoritmos más sofisticados. Adicionalmente, una cola llena provoca pérdida de paquetes, esto es indeseable debido a que el paquete perdido pudo ser un paquete de alta prioridad. El router no pude prevenir que el paquete sea descartado debido a que ya no había espacio para él en la cola.

2.2.2.2. PQ: Priorizar el Tráfico

PQ asegura qué tráfico importante obtenga un manejo más rápido en cada punto donde es usado. Fue diseñado para obtener una prioridad estricta del tráfico importante. PQ puede priorizar de manera flexible de acuerdo al protocolo de la red, la interfaz entrante, el tamaño del paquete, dirección origen o destino, etc. En PQ, cada paquete es colocado en una de cuatro colas – alta, mediana, normal o baja- basándose en la prioridad asignada. Paquetes que no son clasificados con ninguna de estas prioridades caen en la cola de prioridad normal. Durante la transmisión, el algoritmo da a la cola de alta prioridad un tratamiento preferencial sobre las colas de baja prioridad.

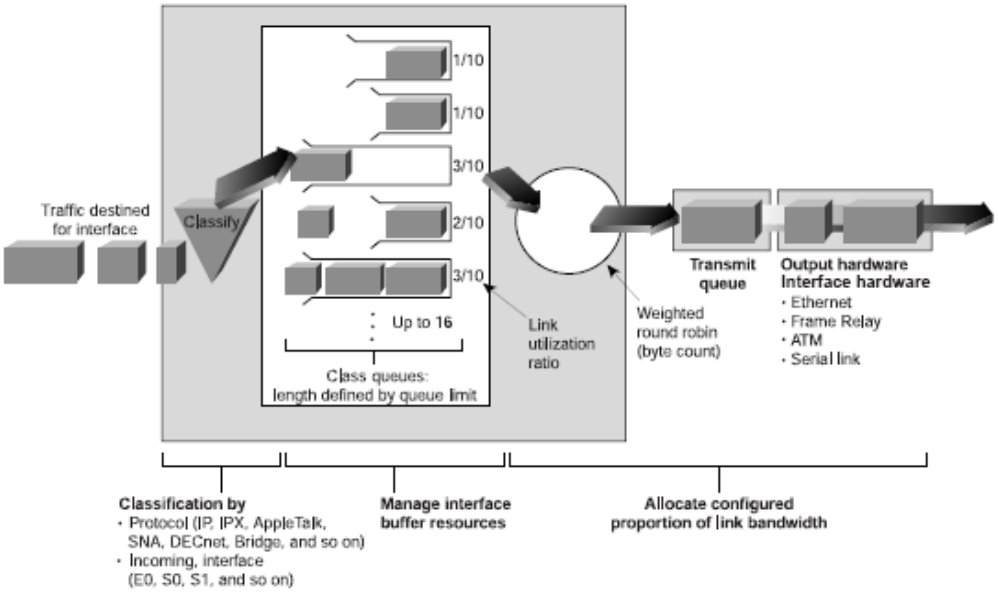


.

PQ es útil para asegurar qué tráfico crítico al atravesar varios links WAN pueda obtener prioridad. Actualmente PQ utiliza configuración estática, por lo que no se adaptan automáticamente a cambios en la red.

2.2.2.3.CQ: Garantizando Ancho de Banda

CQ fue diseñado para permitir a varias aplicaciones u organizaciones compartir la red con aplicaciones de ancho de banda mínimos. En estos casos, el ancho de banda puede ser compartido proporcionalmente entre aplicaciones y usuarios. Se pude utilizar la herramienta de CISCO CQ para proporcionar garantías de ancho de banda en un punto de congestión, al asegurar el tráfico específico una porción establecida de ancho de banda y dejar disponible el resto para el tráfico restante. CQ maneja tráfico al asegurar una cantidad de espacio en la cola para cada tráfico y luego darle servicio a la cola de manera round robin.



Se puede reservar la mitad del ancho de banda para una aplicación, y el resto para otros protocolos como IP.

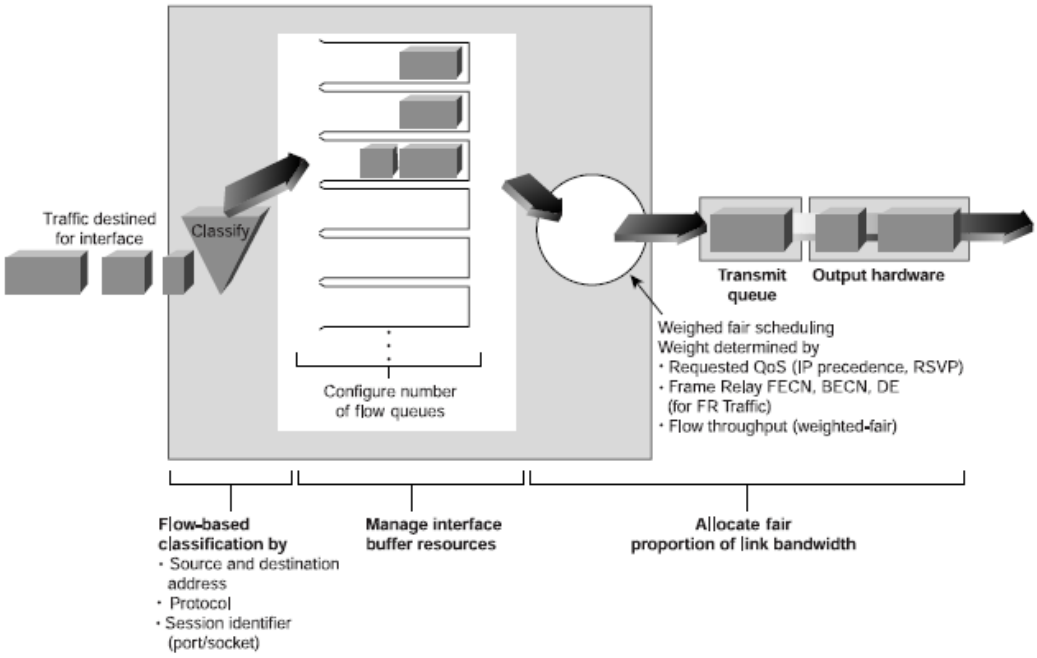
Los algoritmos de encolamiento coloca a los mensajes en una de las 17 colas (la cola 0 tiene mensajes del sistema como señalización y keepalives), las cuales son vaciadas en prioridad de peso. El router da servicio a las colas de la 1 a la 16 en orden round robin, al sacar de la cola una cantidad de bytes contabilizados en cada ciclo. De la misma manera que PQ, CQ es configurado estadísticamente y no se actualiza automáticamente adaptándose a los cambios en la red.

2.2.2.4.Flow-Based WFQ

Para las situaciones en las cuales es deseable proporcionar tiempos de respuesta consistentes, tanto para usuarios livianos como para usuarios pesados sin agregar excesivo ancho de banda, la solución es flow-based WFQ. WFQ es una de las técnicas principales de CISCO. Está basado en un algoritmo de encolamiento basado en el flujo que crea justicia, ya que permite que cada cola sea atendida de una manera justa en cuanto a conteo de bytes. Por ejemplo, si una la cola 1 tiene un paquete de 100bytes y la cola 2 tiene 2 paquetes de 50bytes, el algoritmo WFQ tomaría dos paquetes de la cola 2 por cada paquete de la cola 1.

Esto hace que el servicio sea justo para cada cola: 100 bytes cada vez que la cola da servicio.

WFQ asegura que a las colas no les faltara ancho de banda y que el tráfico obtenga un servicio predecible. Las tramas de bajo volumen, las cuales comprometen a la mayoría del tráfico, reciben un mayor servicio, ya que transmiten la misma cantidad de bytes que un paquete de gran volumen. El resultado de este comportamiento pareciera ser preferencial para el tráfico de bajo volumen, cuando realmente está creando un sistema justo.



WFQ es diseñado para minimizar la configuración, y se adapta automáticamente a cambios en la red. De hecho, WFQ realiza tan buen trabajo para la mayoría de aplicaciones que ha sido el mecanismo de colas preestablecido en la mayoría de interfaces seriales configuradas para correr a velocidades menores a un E1 (2Mbps).

Flow-based WFQ crea flujos basado en un número de características en los paquetes. A cada flujo le es dado su propia cola con buffer, por si experimentan congestión.

La parte de peso en WFQ está dado por los bits de la IP de precedencia para proporcionar un gran servicio a ciertas colas. Utilizando valores de 0 a 5, WFQ usa su algoritmo para determinar cuánto servicio hay que proporcionar a qué cola.

WFQ es eficiente ya que usa cualquier ancho de banda disponible para enviar tráfico, desde baja prioridad hasta flujos de alta prioridad. WFQ trabaja con ambos IP de precedencia y el protocolo de reserva de recursos (RSVP).

2.2.2.5.Class-Based WFQ

Class-based WFQ (CBWFQ) es la herramienta para el manejo de congestiones más nuevo de CISCO, el cual provee mayor flexibilidad. Cuando se quiere proveer la menor cantidad de ancho de banda hay que utilizar CBWFQ. CAR y la modificación de tráfico son utilizados en este caso.

CBWFQ permite al administrador de red crear una garantía de mínimo de ancho de banda a las clases. En lugar de proveer una cola para cada flujo individual, una clase es definida, la cual consiste en uno o más flujos. Se puede garantizar una cantidad mínima de ancho de banda a cada clase.

Un ejemplo en el cual CBQWF puede ser utilizado, es para prevenir que múltiples flujos de baja prioridad detengan a un solo flujo de alta prioridad. Por ejemplo, una trama de video que necesita la mitad del ancho de banda de un T1 va a ser proporcionado por WFQ si hay dos tramas. Mientras más flujos son adicionados, la trama de video obtiene menos ancho de banda debido al mecanismo de WFQ para crear justicia entre los flujos. Si hay 10 flujos, la trama de video obtendría únicamente 1/10 de el ancho de banda, lo cual no es suficiente. Aunque la ip de precedencia sea 5, esto no resuelve el problema.

Ya que (1*9)+ 6= 15, por lo que la trama de video obtendría 6/15 de el ancho de banda, lo cual es menos de lo que el video necesita. Un mecanismo debe ser invocado para proporcionar la mitad del ancho de banda que el video necesita. CBWFQ provee esto. El

administrador de red define una clase, se la coloca a la trama de video y le dice al router que provee la mitad de un T1 a esta clase. De esta manera el video está recibiendo la cantidad de ancho de banda que necesita. Una clase predeterminada es utilizada para el resto de los flujos. Esta clase es servida al usar esquemas flow-based WFQ para alojar el restante de ancho de banda.

Adicionalmente, una cola de baja latencia (LLQ) puede ser designada, la cual es esencialmente una cola de alta prioridad. Notar que este avance también le hace referencia como una cola de prioridad basada en la clase (PQCBWFQ)

La baja latencia en las colas permite a una clase ser servida como una clase de alta prioridad. El tráfico en esta clase va a ser servida antes que cualquier cola. Se realiza una reserva de una cantidad de ancho de banda. Cualquier tráfico con requerimientos arriba de este ancho de banda es descartado.

2.2.3. MANEJO DE LAS COLAS (HERRAMIENTAS PARA EVITAR CONGESTIONES)

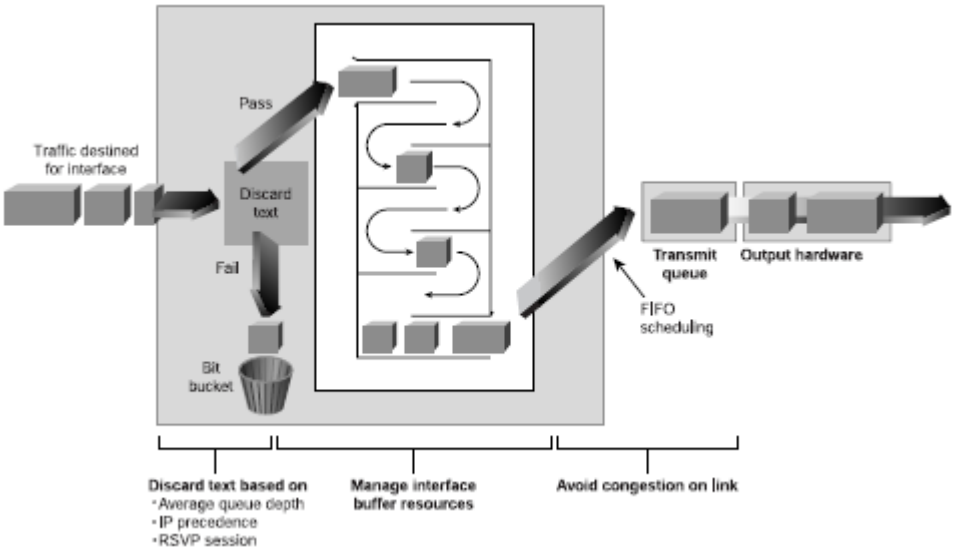
Evitar congestiones es una manera de manejar las colas. Las técnicas para evitar congestión en la red monitorea la carga de tráfico para evitar y anticipar los cuellos de botella, de manera opuesta que las técnicas de manejo de congestiones que operan una vez la congestión ha ocurrido. La principal herramienta de CISCO para evitar congestiones es la "weighted random early detection (WRED)".

2.2.3.1 WRED: EVITANDO CONGESTIONES

Los algoritmos de la detección temprana al azar (RED) son diseñados para evitar cogestiones en una red antes que se convierta en un problema. RED trabaja al monitorear las cargas de tráfico en puntos de la red en donde descarta paquetes al azar si la congestión empieza a aumentar. El resultado del descarte de un paquete es que la fuente detecte la

pérdida de tráfico y realiza la transmisión de una manera más pausada RED, que es principalmente diseñado para TCP en una red IP.

WRED combina las capacidades del algoritmo de RED con la IP de precedencia. Esta combinación proporciona la preferencia por el manejo del tráfico de mayor prioridad. Puede selectivamente descartar los paquetes de baja prioridad cuando la interfaz empieza a estar congestionada, también puede mostrar distintos tipos de desempeños para las diferentes clases de servicio. WRED también detecta RSVP y pude proveer un servicio integrado de carga controlada de QoS.



Dentro de cada cola, un número finito de paquetes pueden ser almacenados. Una cola que se encuentra llena pueda causar pérdida de paquetes también llamado como tail drop. El tail drop es la pérdida de paquetes debido a una cola llena. Esto es indeseable porque el paquete que es botado pudo o no haber sido de alta prioridad, y el router no tuvo la oportunidad de ponerlo en la cola para verificar. Si la cola no está llena, el router puede ver la prioridad de todos los paquetes entrantes y deshacerse de los paquetes de baja prioridad, al permitir a los paquetes de alta prioridad en la cola. Por medio del manejo de la profundidad de la cola (la cantidad de paquetes que soporta la cola), al botar varios paquetes, el router puede tomar la mejor decisión de qué paquetes botar cuando la cola empiece a llenarse. WRED también ayuda a prevenir la congestión en la intrarred. WRED usa un la ip de precedencia para determinar cuándo los paquetes son descartados.

3. Calidad de Servicio en MPLS

La calidad de servicio puede ser implementada en MPLS con leves modificaciones a la arquitectura MPLS y DiffServ. MPLS no introduce nuevos conceptos al condicionamiento de tráfico ya existentes en DiffServ. Un router MPLS (SLR) utiliza los mismos mecanismos para implementar los diferentes comportamientos (PHB) del tráfico MPLS.

Una red MPLS podría implementar DiffServ para soportar diversos requerimientos de calidad de servicio en una forma escalable, MPLS DiffServ no es específico para transportar tráfico IP sobre MPLS. Una red MPLS podría estar transportando tráfico para el cual DiffServ no aplica (por ejemplo, ATM o FR). La implementación de DiffServ en MPLS se preocupa únicamente de soportar el comportamiento por salto (PHB) para satisfacer los requerimientos de calidad de servicio para el tráfico que transporta. Además, una red MPLS puede aumentar de tamaño sin tener que introducir cambios significativos a la implementación de DiffServ. Dichas características juegan un papel importante en la implementación de redes MPLS de gran escala.

3.1. Arquitectura de servicios diferenciados en MPLS

La implementación de calidad de servicio en redes MPLS no introduce nuevas arquitecturas, sino que utiliza la arquitectura de servicios diferenciados que ya han sido definidos para la implementación de calidad de servicio para el Protocolo de Internet (IP).

3.1.1. MPLS DiffServ vs. IP DiffServ

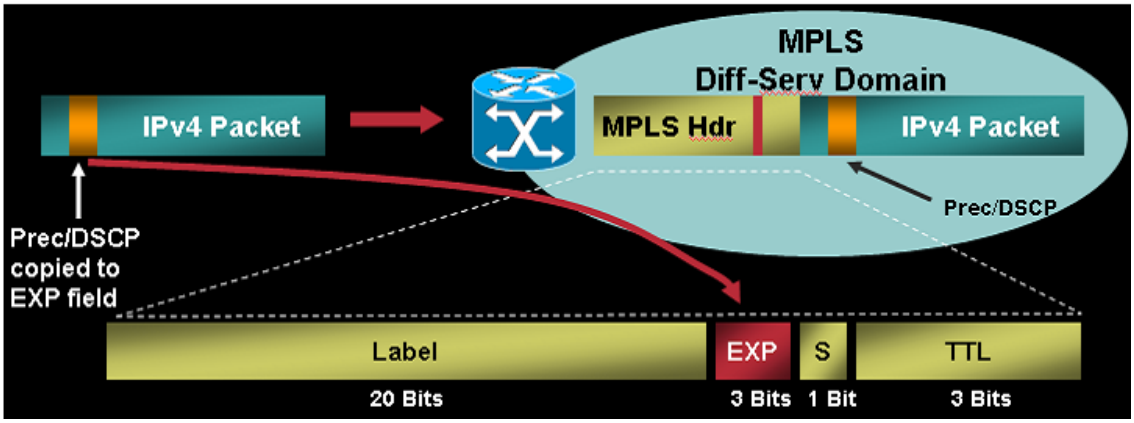
Si comparamos las dos formas de implementación, nos podemos dar cuenta que sólo existen unas pequeñas diferencias entre ambas formas, ya que todos los componentes que conforman la calidad de servicio, proveen la misma funcionalidad y en los mismos puntos

donde es requerido. El condicionamiento, marcado, formación, políticas de tráfico, colas y demás mecanismos para manejar de tráfico son los mismos que los utilizados para IP.

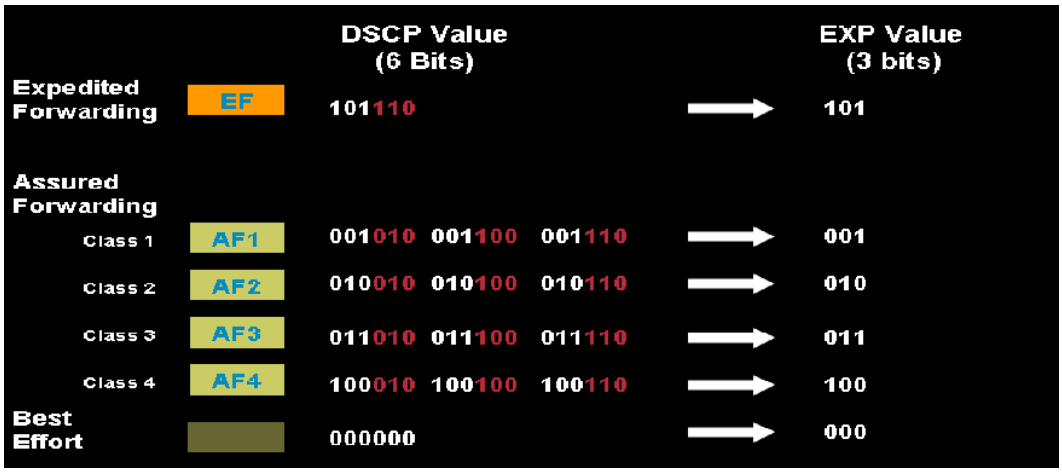
3.1.2. Mapeo DSCP a EXP

Las diferencias en la implementación son mínimas, ya que MPLS trabaja con base en etiquetas, los LSRs no pueden examinar el contenido del encabezado IP y el valor DSCP como es requerido en la especificación original de DiffServ. Esto significa que el PHB adecuado debe ser determinado por la información contenida en la etiqueta, como todo lo demás en MPLS.

A medida que los paquetes entran al dominio DiffServ MPLS a través de un router frontera, los bits de precedencia IP o los primeros bits del DSCP, son copiados al campo experimental (EXP) que fue previamente definido como parte de la etiqueta MPLS.



Esto deja el encabezado IP intacto y disponible para el uso del cliente. La clase de servicio que ha sido configurada por el cliente no cambia a medida que el paquete atraviesa el dominio MPLS. El mapeo de la información de DSCP a los bits experimentales de la etiqueta MPLS, no ha sido estandarizado, así que en cada dominio MPLS se puede implementar de forma diferente.



3.1.3. Tipos de LSPs

El hecho que el campo EXP de la etiqueta MPLS sólo tenga espacio para 3 bits crea el siguiente problema. ¿Qué sucede si en el dominio DiffServ MPLS se necesitan más de las 8 clases de tráfico que permite el campo experimental?

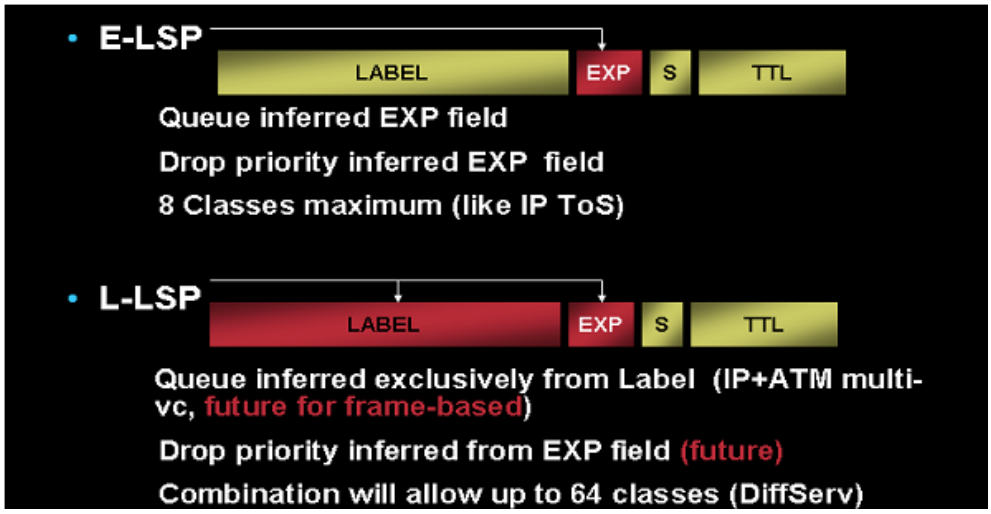
El problema existe debido a que el campo que se utiliza para la implementación de DiffServ en IP, tiene un tamaño de 6 bits. Para solucionar dicho problema, DiffServ en MPLS introduce dos tipos de LSPs con distintas características. El primer tipo, E-LSP, es capaz de transportar simultáneamente múltiples tipos de tráfico. El segundo tipo es L-LSP, transporta sólo una clase de tráfico. Ambos tipos dependen de diferentes mecanismos para codificar el marcado de paquetes requerido por DiffServ.

3.1.3.1. E-LSP

DiffServ en MPLS define un E-LSP, el cual es un tipo de LSP capaz de transportar simultáneamente múltiples clases de tráfico. Los routers (LSR) utilizan el campo EXP del encabezado MPLS para determinar el PHB requerido para dicho paquete. Dicho campo EXP contiene tres bits, lo cual implica que un E-LSP puede transportar hasta 8 clases de servicio diferentes. Las especificaciones no definen los valores recomendados de EXP para PHB existentes.

3.1.3.2.L-LSP

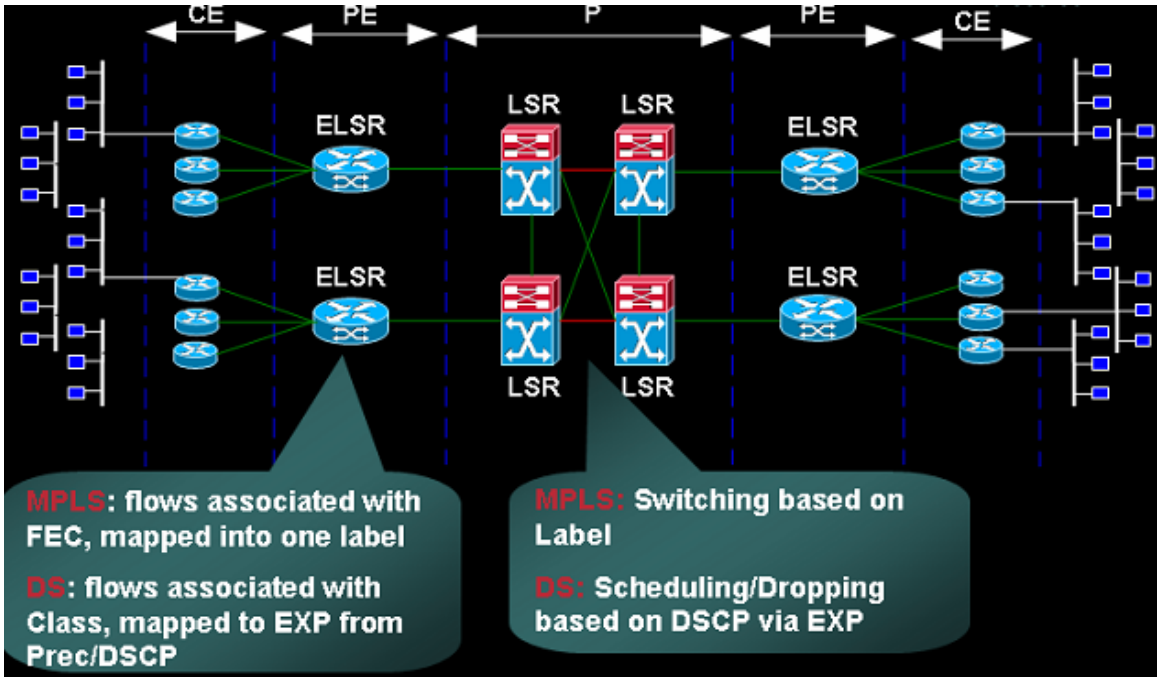
MPLS DiffServ define L-LSPs como un tipo de LSP capaz de transporte únicamente una clase de tráfico. Los LSRs conocen la clase de tráfico asociada con el paquete por medio de la etiqueta, y determinan el PHB exacto al usar una combinación de la etiqueta y el campo EXP.



EL uso de E-LSPs y L-LSPs en una red MPLS no es mutuamente exclusivo. Los LSRs operan dentro del contexto de etiquetas DiffServ. Dicho contexto indica el tipo de LSP (E-LSP o L-LSP), el PHB que el LSP soporta, y el mapeo entre el encapsulado del paquete y el PHB.

Los E-LSPs son más eficientes que los L-LSPs, ya que el primer modelo es similar al modelo DiffServ estándar. Múltiples PHBs pueden ser soportaos sobre un único E-LSP.

E-LSP	**L-LSP**
Una o más clases de LSP	Una clase de LSP
PHB por medio de EXP	PHB por medio de etiqueta y EXP
Señalización opcional	Señalización requerida



Topología de Ejemplo

3.2.Modelos de Túnel en MPLS DiffServ

En DiffServ MPLS han sido definidos tres modelos de interacción entre el marcado de paquetes DiffServ en diferentes capas de encapsulado. Un ejemplo sencillo es el de un paquete IP que ha sido encapsulado para MPLS. Existe un marcado de PHB en el encapsulado MPLS, y también un marcado PHB en el campo DiffServ IP del paquete original. Existen tres modelos que manejan la interacción entre múltiples tipos de dichos marcados: modelo de tubería (pipe), modelo de tubería corta (short-pipe), y el modelo uniforme. Dichos modelos definen procedimientos que los routers MPLS (LSR) pueden aplicar cuando un paquete con una marca PHB existente entre y sale de un LSP.

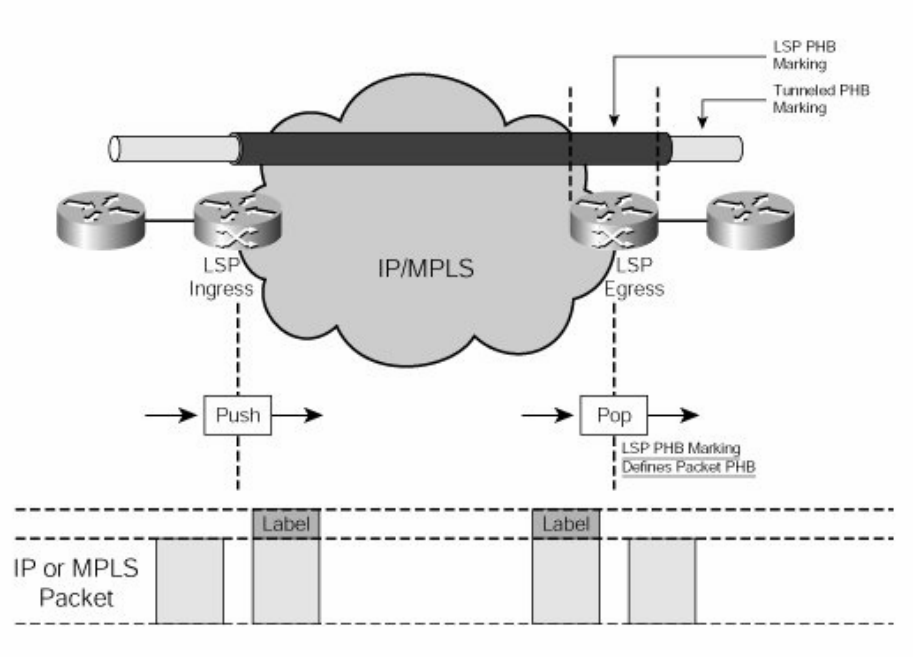
Estos modelos no introducen cambios en el comportamiento de intercambio de etiquetas de un LSR, y se aplican por igual a E-LSPs y L-LSPs.

3.2.1. Modelo de Tubería

Este modelo esconde el previo marcado PHB entre los LSPs de ingreso y egreso. El modelo de tubería garantiza que no se realizarán cambios al marcado PHB original, cuando el paquete atraviese el LSP; incluso si un LSR realiza condicionamientos y remarca el tráfico. Todos los LSR por los cuales el LSP pase utilizan el PHB perteneciente a LSP e ignoran el PHB original. Este modelo es útil cuando una red MPLS se conecta con otros dominios DiffServ. La red MPLS puede implementar DiffServ en su propia manera y al mismo tiempo ser transparente para los dominios contiguos.

A continuación se muestra el funcionamiento del modelo de tubería. El LSR de ingreso determina cuál será el PHB para el LSP correspondiente en el encapsulado MPLS. Para esto puede ser considerado también el PHB ya existente del paquete.

El PHB original se conserva, ya que uno nuevo es agregado con el encapsulado MPLS. Cabe destacar que el paquete entrante puede ser un paquete tanto IP como MPLS. El LSR de egreso maneja el paquete de acuerdo al PHB del LSP, luego realiza la operación de extracción de la última etiqueta o des-encapsulado y el paquete sale del dominio. De esta forma se logra que el PHB que ha pasado a través del túnel no haya sido modificado.

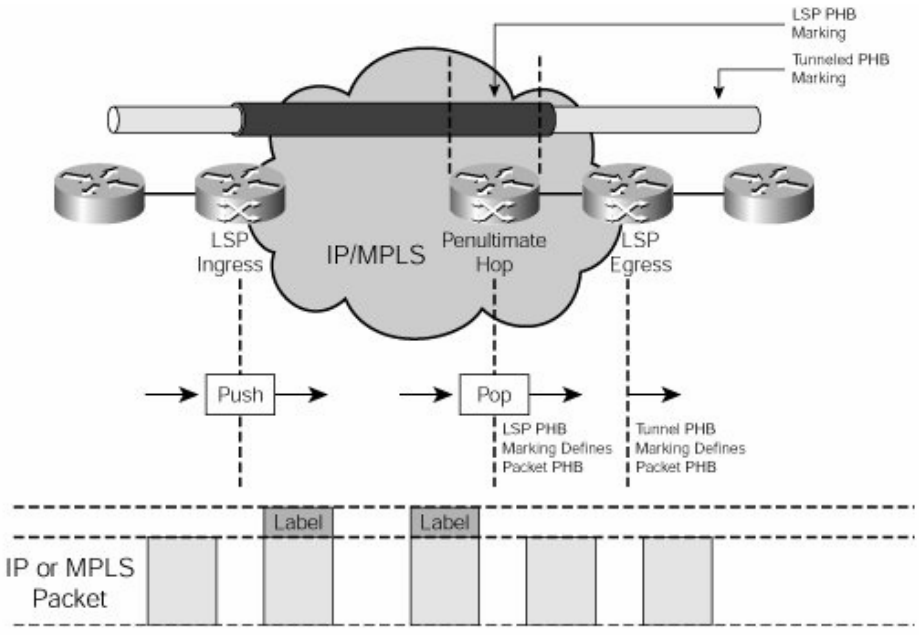


3.2.2. Modelo de Tubería Corta

El modelo de tubería corta representa una pequeña variación del modelo anterior. Este modelo también garantiza que no habrá cambios al PHB que pasa a través del túnel, incluso cuando un LSR vuelve a marcar el paquete. El modelo de tubería también tiene la habilidad de ser transparente desde el punto de vista DiffServ. Sin embargo, la diferencia está en la forma en la cual el LSR de egreso determina el PHB del paquete. El LSR de egreso si utiliza el PHB dentro del túnel para darle el tratamiento debido al paquete.

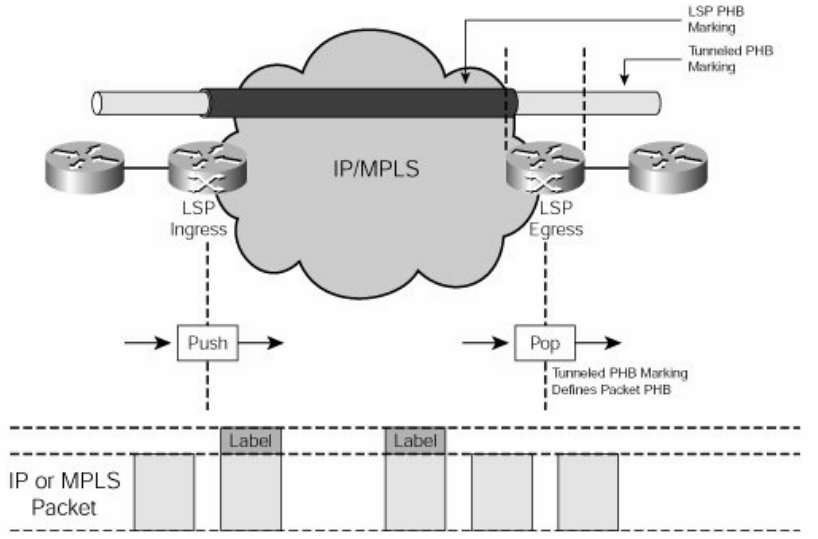
Dada esta diferencia con el modelo de tubería normal, una red MPLS puede implementar LSPs al utilizar el modelo de tubería corta sin importar si los LSR usan PHP (penultimate-hop-popping). En el modelo anterior, el LSR de egreso no puede hacer uso PHP ya que este nunca llega a examinar esa porción del paquete antes de reenviarlo.

La siguiente figura ilustra los detalles del funcionamiento del modelo de túnel corto al utilizar PHP. El LSR de ingreso debe determinar el LSP PHB que va a codificar en la etiqueta MPLS. El LSR puede considerar el PHB ya existente para tomar la decisión. EL LSR de ingreso también preserva los datos originales del PHB cuando introduce una nueva etiqueta.



Los modelos de túnel y túnel corto comparten el mismo procedimiento que realiza el LSR de ingreso, la diferencia radica en el hecho que, si se utiliza PHP, el penúltimo LSR realiza la operación de quitar la última etiqueta y remover el PHB del LSP sin modificar el PHB del cliente, de esta forma el LSR de egreso determina la información PHB del paquete original.

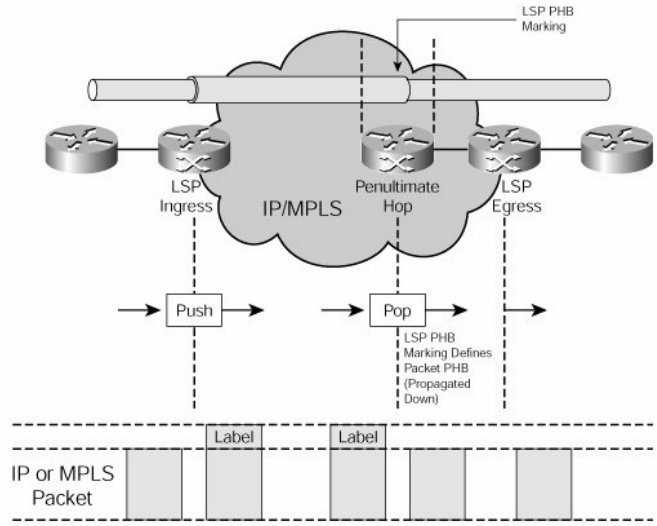
La siguiente figura muestra el funcionamiento del modelo de túnel corto, sin experimentar PHP. La operación en el LSR de ingreso permanece igual que en el caso anterior. El penúltimo salto realiza el intercambio de etiquetas y maneja el paquete de acuerdo a los procedimientos correspondientes en el E-LSP o L-LSP. EL LSR de egreso determina la información PHB del paquete original. Esta acción implica que el LSR de egreso determina la información después de realizar la extracción (pop) de la última etiqueta. Como sucede con los modelos anteriores, este nodo reenvía el paquete original con la información PHB del cliente de forma intacta.



3.2.3. Modelo Uniforme

El modelo uniforme convierte al LSP en una extensión del dominio original del paquete encapsulado. En este modelo, el paquete sólo tiene un único marcado PHB (el cual reside en el último encapsulado). Los LSRs propagan el PHB del paquete expuesto cuando realizan la operación pop. Dicha propagación implica que cualquier re marcado del paquete, se verá reflejado en el paquete cuando salga del LSP. El LSP se convierte en una parte integral del dominio DiffServ del cliente, en contraste con la transparencia en el transporte que proveen los modelos de túnel y túnel corto. Este modelo es útil cuando una red MPLS conecta otros dominios DiffServ y todas las redes deben comportarse como un único dominio DiffServ.

La siguiente figura muestra la operación del modelo uniforma con PHP. El LSR de ingreso codifica el PHB existente en la etiqueta MPLS. Cuando el paquete recibe un nuevo encapsulado, el marcado PHB original se vuelve irrelevante. El penúltimo salto determina el PHB del paquete antes de realizar la extracción y luego lo codifica en el paquete expuesto.



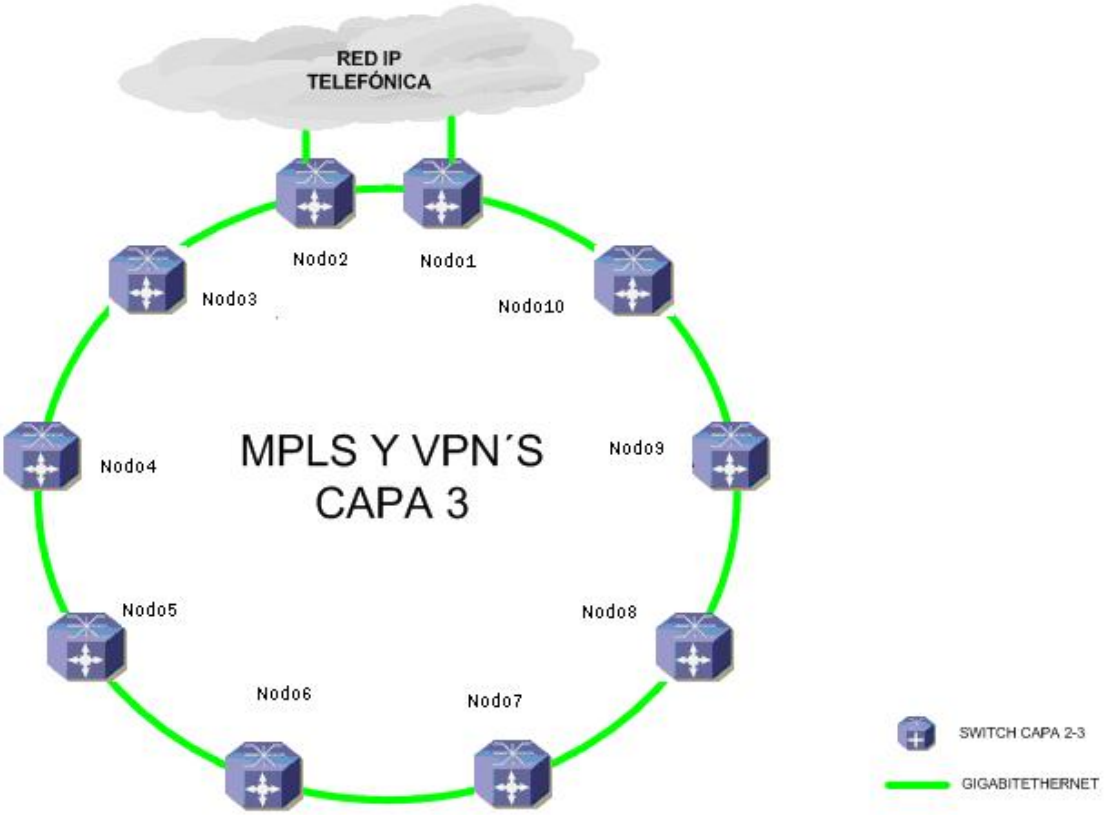
La figura muestra los detalles del modelo uniforme sin PHP. La operación del SLR de ingreso permanece igual. El penúltimo salto realiza el intercambio habitual de etiquetas. El LSR de egreso siempre determina el PHB antes de hacer la operación pop y propaga el

PHB en el paquete expuesto. El modelo uniforme ofrece el mismo comportamiento externo, no importando si se utiliza PHP. A continuación se presenta un resumen de la operación de los tres modelos de túnel con PHP y sin PHP, respectivamente.

Modelo	**LSR ingreso**	**Penúltimo salto**	**LSR egreso**
Tubería	No es posible	No es posible.	No es posible.
Tubería Corta	Se preserva el PHB del cliente, y se agrega otro al encapsulado.	Se determina el PHB antes de la extracción.	Se determina el PHB usando paquete original.
Uniforme	Copiar el PHB existente al Nuevo encapsulado.	Determinar PHB antes de hacer pop y se propaga.	Se Determina el PHB usando la información recibida.

Modelo	**LSR ingreso**	**LSR egreso**
Tubería	Se preserva el PHB del cliente, y se agrega otro al encapsulado.	Se determina el PHB antes de la extracción.
Tubería Corta	Se preserva el PHB del cliente, y se agrega otro al encapsulado.	Se determina el PHB después de la extracción, usando paquete original.
Uniforme	Copiar el PHB existente al Nuevo encapsulado.	Se determina el PHB antes de la extracción y se propaga.

4. **TOPOLOGÍA DE RED**



La topología de red cuenta con 10 routers localizados en la capital Metropolitana de Guatemala. Se encuentran posicionados en una topología de anillo, en donde los enlaces son de punto a punto. Toda la información de la red pasa a través de cada nodo hasta que es tomado por el nodo apropiado. La convergencia de esta topología depende del protocolo de enrutamiento que se tenga configurado.

Se manejan enlaces de GigabitEthernet ópticos debido al volumen de datos que se manejan. En la topología se tienen dos modelos de routers marca CISCO, los cuales son el Catalyst 6504 y Cisco 7606.

A continuación se describe el equipo y cantidad de puertos que posee cada nodo:

NODO	EQUIPO	PUERTOS 10/100/1000 ELÉCTRICOS	PUERTOS GigabitEthernet ÓPTICOS
Nodo1	7606	48	26
Nodo2	7606	48	26
Nodo3	6504	48	9
Nodo4	6504	48	9
Nodo5	6504	48	9
Nodo6	6504	48	9
Nodo7	6504	48	9
Nodo8	6504	48	9
Nodo9	6504	48	9
Nodo10	6504	48	9

4.1.DIRECCIONAMIENTO

Para el anillo metro se define el siguiente direccionamiento:

DIRECCIONAMIENTO PRIVADO	
Bloque	10.145.0.0/16
Direcciones para Equipos	10.145.0.0/17
Direcciones para Clientes	10.145.128.0/17

El direccionamiento privado se seleccionó de un rango que no se está usando actualmente en la Red Ip de Telefónica Móviles Guatemala y está destinada para usarse tanto en enlaces de clientes como en enlaces con otros equipos. Como su nombre lo indica, estas redes no son anunciadas en Internet, por lo tanto su uso está limitado sólo a conectividad.

DIRECCIONAMIENTO PÚBLICO	
Clientes IPCP	190.10.100.0/23
Clientes IPCP	190.10.101.0/23
Clientes ADSL	190.10.102.0/23

El direccionamiento público es utilizado para el servicio de Internet. Este se puede clasificar en dos grupos que son los IPCP´s que son los clientes corporativos y los clientes de servicio ADSL, que serán los clientes que anteriormente se daban con servicios de ISDN.

DIRECCIONAMIENTO PRIVADO PARA GESTIÓN DE CPE´S	
Rango	10.11.128.0/17

El direccionamiento privado para la gestión de CPE´s se seleccionó de un rango que no se está usando, ya que aunque la gestión se llevará por VRF´s en el anillo MetroEthernet, en algún momento se conectará con la red de gestión que ya está montada y se hace necesario que no exista conflicto de direccionamiento.

4.1.1. Direccionamiento Loopbacks

A continuación se listan las direcciones Loopback empleadas para la identificación de los equipos, procesos de enrutamiento y gestión.

Loopback 0		NODO
Dirección IP	**Mascara**	
66.119.95.40	255.255.255.255	Nodo1
66.119.95.41	255.255.255.255	Nodo2

66.119.95.42	255.255.255.255	Nodo3
66.119.95.43	255.255.255.255	Nodo4
66.119.95.44	255.255.255.255	Nodo5
66.119.95.45	255.255.255.255	Nodo6
66.119.95.46	255.255.255.255	Nodo7
66.119.95.47	255.255.255.255	Nodo8
66.119.95.48	255.255.255.255	Nodo9
66.119.95.49	255.255.255.255	Nodo10

4.1.2. Direccionamiento Interfaces GigabitEthernet

Las interfaces que interconectan los equipos del anillo se configuran en nivel 3 con subredes de 30 bits consecutivas.

NODO	INTERFACE	DIRECCION IP	MASCARA
Nodo1	GE 1/1	10.145.0.42	255.255.255.252
	GE 5/1	10.145.0.1	255.255.255.252
	GE 5/2	10.145.0.5	255.255.255.252
Nodo2	GE 1/1	10.145.0.9	255.255.255.252
	GE 5/1	10.145.0.2	255.255.255.252
	GE 5/2	10.145.0.6	255.255.255.252
Nodo3	GE 1/1	10.145.0.13	255.255.255.252
	GE ½	10.145.0.10	255.255.255.252
Nodo4	GE 1/1	10.145.0.17	255.255.255.252
	GE ½	10.145.0.14	255.255.255.252
Nodo5	GE 1/1	10.145.0.21	255.255.255.252
	GE ½	10.145.0.18	255.255.255.252
Nodo6	GE 1/1	10.145.0.25	255.255.255.252
	GE ½	10.145.0.22	255.255.255.252

Nodo7	GE 1/1	10.145.0.29	255.255.255.252
	GE ½	10.145.0.26	255.255.255.252
Nodo8	GE 1/1	10.145.0.33	255.255.255.252
	GE ½	10.145.0.30	255.255.255.252
Nodo9	GE 1/1	10.145.0.37	255.255.255.252
	GE 1/2	10.145.0.34	255.255.255.252
Nodo10	GE 1/1	10.145.0.41	255.255.255.252
	GE 1/2	10.145.0.38	255.255.255.252

4.1.3. Direccionamiento Gestión de Equipos de Acceso

Se define un direccionamiento específico para la gestión de los equipos Teledata (Central Unit - CU) configurando una interfaz Vlan 2000 en cada nodo con las direcciones designadas en la tabla como "IP Gestion CUs (Vlan 2000)".

Los equipos Teledata poseen una tarjeta principal (Dirección IP CU Nodo) y una tarjeta secundaria (Dirección IP Tarjeta Adicional CU Nodo), cada una de las cuales posee un direccionamiento asignado dentro del rango de la VLAN 2000.

También se define un direccionamiento de gestión para los CPEs xDSL en el rango privado 10.11.128.0/25 subdividiéndolo para otorgar 8 subredes Clase C a cada nodo. Estas 8 subredes por nodo son transportadas por la Vlan 2002 de Gestión de CPE´s.

Nodo	IP Gestión CUs (Vlan 2000)	Dirección IP CU Nodo	Dirección IP Tarjeta Adicional CU Nodo	Red de Gestión CPEs (Vlan 2002)
Nodo1	10.145.1.1/24	10.145.1.2/24	10.145.1.3/24	10.11.136.1-
Nodo2	10.145.2.1/24	10.145.2.2/24	10.145.3.3/24	10.11.143.254

Nodo3	10.145.3.1/24	10.145.3.2/24	10.145.3.3/24	10.11.144.1-10.11.151.254
Nodo4	10.145.4.1/24	10.145.4.2/24	10.145.4.3/24	10.11.152.1-10.11.159.254
Nodo5	10.145.5.1/24	10.145.5.2/24	10.145.5.3/24	10.11.160.1-10.11.167.254
Nodo6	10.145.6.1/24	10.145.6.2/24	10.145.6.3/24	10.11.168.1-10.11.175.254
Nodo7	10.145.7.1/24	10.145.7.2/24	10.145.7.3/24	10.11.176.1-10.11.183.254
Nodo8	10.145.8.1/24	10.145.8.2/24	10.145.8.3/24	10.11.184.1-10.11.191.254
Nodo9	10.145.9.1/24	10.145.9.2/24	10.145.9.3/24	10.11.192.1-10.11.199.254
Nodo10	10.145.10.1/24	10.145.10.2/24	10.145.10.3/24	10.11.200.1-10.11.207.254

Adicionalmente se asignó una Vlan para el servidor que tiene el programa Cisco Works que es el gestor de la red MetroEthernet.

DIRECCIONAMIENTO PARA SERVIDOR CISCO WORKS		
Red	**Servidor**	**Vlan**
10.145.0.48/28	10.145.0.50/28	2003

4.1.4. Direccionamiento VLANS ADSL

Los usuarios de ADSL serán configurados con una ip pública en el CPE la cual hará NAT a las redes internas del cliente. Estos usuarios son agrupados en Vlans con subredes consecutivas de 27 bits (32 direcciones por VLAN) con el fin de limitar el dominio de Broadcast.

DIRECCIONAMIENTO PARA VLANS DE ADSL	
Nodo	**Vlan101**
Nodo1	190.10.102.0/27
Nodo2	
Nodo3	190.10.102.32/27
Nodo4	190.10.102.64/27
Nodo5	190.10.102.96/27
Nodo6	190.10.102.128/27
Nodo7	190.10.102.160/27
Nodo8	190.10.102.192/27
Nodo9	190.10.102.224/27
Nodo10	No tendrá equipo de acceso

Cada Vlan de ADSL en cada nodo tendrá una red de 32 ip´s lo que da una capacidad de 29 clientes. Al momento que alguna Vlan en algún nodo se llene, se deberá proceder a configurar la siguiente agregándole otra red de 32 IP´s.

4.1.5. Direccionamiento de Interfaces de Conexión del Anillo Metro a la Red

El Anillo Metro se conecta a la red de Telefónica por medio de 2 interfaces FastEthernet en cada equipo Cisco 7606. Estas interfaces pertenecen al proceso OSPF 10 empleado en la

red de Telefónica y a través del cual los equipos 7606 aprenden las diferentes rutas de la red incluyendo la ruta por defecto. A continuación se listan las interfaces y el direccionamiento.

Equipo 7606	Puerto Local	Dirección local del puerto	Dirección Remota
Nodo1	2/47	66.201.183.242/30	66.201.183.241/30
	2/48	66.201.183.246/30	66.201.183.245/30
Nodo2	2/47	66.201.183.250/30	66.201.183.249/30
	2/48	66.201.183.254/30	66.201.183.253/30

4.1.6. Distribución de VLAN´S por Nodo.

Para manejar un estándar en el uso de Vlan´s se tomará como referencia la siguiente tabla que indica los rangos de Vlan´s a utilizar.

DISTRIBUCIÓN DE VLANS POR NODO	
Rango	**Asignación**
1 - 100	Pruebas
101 - 200	Clientes ADSL
201 - 1000	Clientes Corporativos
1001 - 1010	Reservadas
1011 - 1999	Clientes Corporativos
2000	Gestión de CU´s
2002	Gestión de CPE´s
2003	Gestión Cisco Works
2004 - 2050	Gestión
2051 – 4096	Reservado Distribución Futura

4.2.ENRUTAMIENTO

Las interfaces que interconectan el anillo se configuran a nivel 3 con direccionamiento privado. Cada equipo posee una interfaz Loopback 0 con direccionamiento público empleado para las labores de gestión y de enrutamiento. La información de estas rutas y el enrutamiento global del anillo es controlado por el protocolo ospf configurado en cada equipo.

El anillo también posee configurado en cada equipo el protocolo BGP, quien es el encargado de transportar la información de enrutamiento de las VPNs L3 configuradas gracias a las funcionalidades de MPLS de la red.

4.2.1. Configuración Ospf

Cada equipo Cisco del anillo posee configurado el proceso OSPF 1 quien se encarga de controlar la tabla de enrutamiento global del equipo.

Comandos empleados:

```
Router(config)# router ospf 1
```

Este proceso OSPF1 se encargará directamente de controlar el transporte de los accesos a Internet, por lo cual cada subred asignada al cliente deberá ser matriculada en el proceso.

Comandos empleados:

```
Router(config-router)# network x.x.x.x y.y.y.y area 0
```

También este proceso ospf 1 se encarga de enrutar los paquetes entre las interfaces de los equipos permitiendo la conectividad básica y a su vez estableciendo las rutas dinámicas necesarias para la correcta operación de BGP.

Este proceso se encuentra configurado para que todas las interfaces del equipo se encuentren por defecto en modo pasivo:

Comandos empleados:

```
Router(config-router)# passive-interface default
```

Únicamente las interfaces que conectan el anillo se encuentran configuradas en modo activo dentro del proceso.

Comandos empleados:

```
Router(config-router)# no passive-interface GigabitEthernet x/y
```

El proceso ospf 1 configurado en los equipos 7600 se encarga de anunciar a estos equipos como la ruta por defecto hacia Internet al interior del anillo.

Comandos empleados:

```
Router(config-router)# default-information originate
```

Debido a que los routers 7606 no deben obtener su ruta por defecto desde el proceso ospf 1 a menos que no exista otra ruta, se filtra la ruta 0.0.0.0 aprendida por el proceso ospf1 en los equipos.

Comandos empleados:

```
Router(config-router)# distribute-list ospf1-in in

Router(config)# ip access-list standard ospf1-in
 deny   0.0.0.0
 permit any
```

Para asegurar que cada enrutador 7606 aun tenga una ruta de salida a la red de telefónica a través de del Router 7606 restante se configura una ruta estática con forma flotante (alta métrica) la cual únicamente será empleada en caso que ambas interfaces de interconexión a telefónica fallen.

Comandos empleados:

En Nodo1 :

```
Router(config)# ip route 0.0.0.0 0.0.0.0 10.145.0.1 250
```

En Nodo2 :

```
Router(config)# ip route 0.0.0.0 0.0.0.0 10.145.0.2 250
```

Con el fin de proteger el anillo ante inyecciones de rutas de OSPF desde equipos no autorizados, el proceso ospf 1 se configura con contraseña y seguridad MD5.

Comandos empleados:

```
Router(config-router)# area 0 authentication message-digest
```

Sobre las interfaces individuales activas en ospf 1 :

```
Router(config-interface)# ip ospf message-digest-key 100 md5 XXXXXX
```

Los equipos 7606, poseen un segundo proceso de ospf identificado como ospf 10 y que incluye activamente a las interfaces fastethernet que conectan a estos equipos a la red de telefónica.

Comandos empleados:

En Nodo1:

```
Router(config)# router ospf 10
Router(config)# no passive-interface GigabitEthernet2/47
Router(config)# no passive-interface GigabitEthernet2/48
Router(config)# network 66.201.183.242 0.0.0.0 area 0
Router(config)# network 66.201.183.246 0.0.0.0 area 0
```

En Nodo2:

```
Router(config)# router ospf 10
Router(config)# no passive-interface GigabitEthernet2/47
Router(config)# no passive-interface GigabitEthernet2/48
Router(config)# network 66.201.183.250 0.0.0.0 area 0
Router(config)# network 66.201.183.254 0.0.0.0 area 0
```

Este proceso ospf 10 permite que los Router cisco 7606 obtengan dinámicamente las rutas de la red de Telefónica, incluyendo el Default Gateway hacia Internet. También ofrecen las características de balanceo de carga y protección contra fallas, entre los 4 enlaces FastEthernet actuales.

4.2.2. Configuración Áreas de Ospf y Redistribución

Tanto el proceso OSPF 1 como el proceso OSPF 10 configurado en los equipos poseen una única área 0. Dado que cada área 0 pertenece a procesos diferentes no se presentan conflictos y operan independiente.

Comandos empleados:

```
Router(config-router)# network x.x.x.x y.y.y.y area 0
```

En los equipos Cisco 7606 , El proceso Osp1 es redistribuido en el proceso OSPF 10 con una distancia de 200, la cual es configurada sobre los equipos Cisco 7600 en el proceso OSPF 10 como la distancia de redistribución externa.

Comandos empleados:

```
Router(config-router)# redistribute ospf 1 subnets route-map ospf1-to-
ospf10
Router(config-router)# distance ospf external 200
```

Dado que la distancia por defecto de ospf es de 110, el proceso OSPF 10, siempre preferirá una ruta propia a una ruta inyectada desde el anillo en caso de conflicto.

La redistribución configurada en cada equipo Cisco 7606 es controlado por un route-map enlazado a listas de acceso de dirección IP, con el fin de permitir la redistribución de únicamente las redes necesarias y no todas las redes que pudieran estar contenidas en el proceso OSPF1. Esto permite ofrecer la seguridad que una red no será enrutada fuera del anillo, así sea anunciada al interior de este por el proceso OSPF 1**.**

Comandos empleados:

```
Router(config-router)# redistribute ospf 1 subnets route-map ospf1-to-
ospf10
```

La activación y el mantenimiento de estos route-maps son herramientas de control que se dejan al alcance de Operación y Mantenimiento de Telefónica, quienes según su criterio determinarán la necesidad y la mejor forma de uso de estos. Por esta razón los route-maps configurados en los equipos se enlazan con listas de acceso abiertas, preparadas para el uso y modificación por parte del personal de O & M. La recomendación es sólo permitir las redes necesarias.

Comandos empleados:

```
Router(config)# ip access-list extended ospf1-to-ospf10
Router(config-access)# permit ip any any
```

En el proceso de redistribución desde el proceso OSPF 1 al proceso OSP10 , se tiene configurado la sumarización de las subredes pertenecientes al anillo con el fin de reducir las tablas de enrutamiento al máximo y optimizar los recursos de la red.

Comandos empleados:

```
Router(config-router)# summary-address 10.145.0.0 255.255.0.0
Router(config-router)# summary-address 66.201.182.176
255.255.255.240
Router(config-router)# summary-address 66.119.95.40 255.255.255.248
```

4.2.3. Configuración BGP

El anillo MetroEthernet posee una configuración de BGP al emplear un único sistema autónomo AS 65100. Estableciendo vecindades iBGP únicamente.

Comandos empleados:

```
Router(config)# router bgp 65100
```

Con el fin de hacer la configuración más compacta y administrable se determina un Peer-Group para incluir todos los Switches Cisco 6504 y aplicar los comandos de BGP a todo el grupo, en vez de aplicarlos individualmente.

Comandos empleados:

```
Router(config-router)# neighbor peers-anillo peer-group
```

```
      Router(config-router)# neighbor 66.119.95.42 peer-group peers-
anillo
      Router(config-router)# neighbor 66.119.95.43 peer-group peers-
anillo
      Router(config-router)# neighbor 66.119.95.44 peer-group peers-
anillo
      Router(config-router)# neighbor 66.119.95.45 peer-group peers-
anillo
      Router(config-router)# neighbor 66.119.95.46 peer-group peers-
anillo
      Router(config-router)# neighbor 66.119.95.47 peer-group peers-
anillo
      Router(config-router)# neighbor 66.119.95.48 peer-group peers-
anillo
      Router(config-router)# neighbor 66.119.95.49 peer-group peers-
anillo
```

Los equipos Cisco 7606 quienes son los Getway del resto del anillo hacia Internet , se configuran como Route Reflector de BGP para un mismo Cluster 10 en el cual se incluyen todos los equipos Cisco 6504. El hecho que existan 2 Route Reflector en el mismo cluster, permite que si uno de estos falla las rutas sigan siendo reflejadas por el restante al ofrecer redundancia en caso tal de la falla de uno de los enrutadores 7606. Esta configuración únicamente es requerida en los enrutadores 7606.

Comandos empleados:

```
router bgp 65100
 bgp cluster-id 10
   !
 address-family ipv4
  neighbor peers-anillo route-reflector-client
  exit-address-family
 !
 address-family vpnv4
  neighbor peers-anillo route-reflector-client
  exit-address-family
```

Esto permite que los equipos Cisco 6504 únicamente requieran poseer configurada una vecindad con cada uno de los Cisco 7606 y no requieran de la configuración de vecindades individuales con cada nodo, al reducir la complejidad de la configuración en los equipos 6504 y también reducir la carga de BGP en estos.

Comandos empleados:

En el equipo Nodo1:

```
neighbor peers-anillo remote-as 65100
neighbor peers-anillo update-source Loopback0
neighbor 66.119.95.41 remote-as 65100
neighbor 66.119.95.41 update-source Loopback0
```

En el equipo Nodo2

```
neighbor peers-anillo remote-as 65100
neighbor peers-anillo update-source Loopback0
neighbor 66.119.95.41 remote-as 65100
neighbor 66.119.95.41 update-source Loopback0
```

En los equipos 6504:

```
neighbor 66.119.95.40 remote-as 65100
neighbor 66.119.95.40 update-source Loopback0
neighbor 66.119.95.41 remote-as 65100
neighbor 66.119.95.41 update-source Loopback0
```

También esta configuración genera una simplificación que prepara la red para la interacción a redes futuras que empleen otros Sistemas autónomos los cuales únicamente deberían establecer una vecindad eBGP a los Router cisco 7606 y no una a cada equipo.

Con el fin de proteger el anillo ante inyecciones de rutas de BGP desde equipos no autorizados, cada vecindad se configura con una contraseña de verificación. El listado de

las contraseñas empleadas en la configuración de los equipos del anillo se adjunta al presente documento.

Comandos empleados:

```
Router(config-router)# neighbor X.X.X.X password 7 YYYYYYYY
```

4.2.4. Redistribución de Rutas

El proceso de BGP 65100 configurado se destina a transportar la información de las VRFs configuradas en los diferentes nodos. Por esta razón cada VRF configurada redistribuye sus redes en el Address Familly VPNv4 de la VRF específica, del proceso de BGP del nodo permitiendo que estas rutas sean transportadas a través del anillo hasta el nodo de destino.

Comandos empleados:

```
address-family ipv4 vrf internet
 redistribute ospf 300 vrf internet
  exit-address-family
```

Nota: "internet" es el nombre de una vrf de prueba configurada en la red. Esta VRF puede ser eliminada

Igualmente en los protocolos dinámicos de enrutamiento dentro de las VRFs , se deberá redistribuirse el proceso de BGP 65100 dentro de ellos para permitir la inyección de las rutas remotas.

Comandos empleados:

```
router ospf 300 vrf internet
 redistribute bgp 65100 metric 100 subnets
```

Nota: "internet" es el nombre de una vrf de prueba configurada en la red. Esta VRF puede ser eliminada

4.2.5. MPLS

Los equipos del anillo metro se encuentran configurados con MPLS con el fin de permitir la fácil implementación de VPNs de nivel 3 (VRFs) dentro de un mismo nodo y entre diferentes nodos.

as VRFs estarán enfocadas a brindar un servicio de conectividad punto a punto y multipunto entre diferentes redes de clientes.

Dada la independencia de cada tabla de enrutamiento de cada VRF, es posible generar VRFs sin estar limitado por el direccionamiento global o por el direccionamiento de otros clientes. Las rutas de una VRF no son vistas por otras VRFs, ni por la tabla de enrutamiento Global proporcionado.

El servicio de conexión Internet a través de la red metro se configura para ser prestado por medio del enrutamiento global (OSPF) y no empleando VRFs las cuales se reservan para la conectividad entre redes de clientes, por lo cual estas deben permanecer independientes y no deben ser redistribuidas en la tabla global.

4.2.5.1. Activación MPLS

Para preparar los equipos pertenecientes al anillo metro y activar la utilización de MPLS, emplean los siguientes comandos en modo global.

Comandos empleados:

```
Router(config)# ip cef distributed
Router(config)# mpls label protocol ldp
```

4.2.6. Configuración de Tag-Switching

Las interfaces que conectan cada equipo Cisco de la red Metro entre ellos, son las únicas interfaces que se encuentran configuradas para pasar los Tags de MPLS entre sí, por lo cual se encuentran marcadas para esta labor y no serán usadas para el forwarding.

Comandos empleados:

```
Router(config-interf)# tag-switching ip
```

Dado que cada TAG de MPLS aumenta en 4 bits el tamaño del paquete, es necesario amentar el MTU de las interfaces configuradas para pasar los TAGs, para evitar el descarte de los paquetes que superen el valor máximo predeterminado 1500.
Comandos empleados:

```
Router(config-interf)# mtu 1600
```

Las VRFs se establecerán inicialmente en su mayoría para equipos SHDSL conectados desde los equipos Multiservicio Teledata. Cada VRF tendrá asignada una Vlan que estará configurada para hacer el forwarding de la VRF específica configurada para cada cliente.

Las Vlans serán transportadas por las interfaces Trunk dot1q las cuales estarán a nivel 2 y no requerirán ser configuradas como forwarding ni tampoco para el traspaso de los TAGs de MPLS. Estas interfaces son conectadas a los equipos Multiservicio Teledata.

4.2.7. Definición de VRFs

Cada VRF a crear debe ser definida en cada equipo que va a participar en la VRF, indicando el nombre quedeberá concordar en todos los equipos.

Cada vez que se define una VRF en un quipo, esta debe ser identificada por un numero compuesto RD, el cual se ha seleccionado como la dirección Loopback0:X, donde X es un número diferenciador que puede aumentar en dígitos. Cada RD debe ser diferente, inclusive cuando se trata de la misma VRF configurada en distintos equipos para permitir que un nodo de la VRF sea identificado completamente.

Comandos empleados:

```
Router(config)# vrf XXXXX
 rd w.x.y.z:X
```

Posteriormente es necesario definir de cuáles puntos remotos de la VRF se van a importar las rutas y exportar las rutas propias a los demás puntos. Esta labor se realiza especificando con los comandos las funciones de importación para cada punto en específico al emplear su RD y especificar el propio RD para la función de exportación.

Comandos empleados:

```
route-target export w.x.y.z:1
route-target import a.b.c.d:1
route-target import l.m.n.ñ:1
```

4.2.8. Inclusión de Redes en cada VRF.

El poceso de enrutamiento de cada VRF es independiente de las demás VRFs y de la tabla global. Esto implica que por defecto, desde una VRF no se observan las rutas ni se tiene

comunicación a los elementos manejados por la tabla global de enrutamiento, ni por las demás VRFs y únicamente se tiene acceso a las redes incluidas a la VRF.

Para poder comunicar la VRF hacia el exterior del enrutador se debe incluir una internfaz Nivel 3 en la VRF , tras lo cual la interfase será removida de la tabla de enrutamiento global y será adicionada a la tabla de enrutamiento de la VRF configurada.

Comandos empleados:

```
interface XXX
  ip vrf forwarding VRF-NAME
  ip address a.b.c.d w.x.y.z
```

El enrutamiento para cada VRF en cada enrutador permite que sea configurado independientemente, pudiendo emplear los protocolos OSPF, BGP, RIP y enrutamiento estático.

Para definir el enrutamiento se emplean las mismas reglas de cada protocolo pero adicionando el nombre de la VRF al crear el proceso, identificarlo y separarlo de la tabla global.

Comandos empleados:

```
router ospf XXX vrf YYY
 redistribute bgp ...
 network ...
```

Para comunicar la VRF hacia dentro de la red y permitir que las rutas sean transportadas y vistas desde otro nodo de la VRF, es necesario que se realice una redistribución de las rutas de la VRF al proceso de BGP que comunica la red. Este procedimiento es descrito en el numeral 6.4.

4.3. Parámetros de Seguridad

Se define un aseguramiento básico de la plataforma y de los equipos los cuales dividimos en 3 grupos de comandos dependiendo de su funcionalidad para su explicación. El primero de estos se enfoca a la seguridad misma del enrutador, al limitar su acceso desde el exterior, eliminando servicios no necesarios y vulnerables. El segundo grupo de comandos se enfoca al aseguramiento de nivel 2 que se debe tener para los puertos de clientes que ingresan al equipo, quitando variables que pudieran llegar a ser explotadas. El tercer grupo se enfoca al aseguramiento de nivel 3 de los puertos que conectan a los clientes, eliminando protocolos, filtrando flujos y aplicando procesos de validación adicionales.

Esta configuración se presenta como una recopilación de las mejores practicas del fabricante y de la experiencia de implementación de Italtel, como una herramienta para la implementación de esquemas de seguridad de la red Metro. Sin embargo la correcta definición, e implantación de las políticas completas de seguridad y sus resultados es un proceso evolutivo que será controlado por Operación y Mantenimiento.

4.3.1. Aseguramiento de elementos de red.

Con el fin de poder identificar los servicios generados desde los equipos de una forma fácil y única, y poder definir procesos de filtrado y autenticación externos, es necesario que estos se identifiquen siempre con la misma dirección fuente. Para esto se define específicamente en cada equipo que la dirección fuente sea la dirección Loopback 0 que es la dirección empleada para la gestión local e identificación única de cada equipo

Comandos empleados:

```
ip ftp source-interface Loopback0
ip tftp source-interface Loopback0
```

```
snmp-server trap-source Loopback0
logging source-interface Loopback0
```

Para evitar que la configuración de las Vlans sea modificada por el protocolo VTP, se especifica el modo transparente de este.

Comandos empleados:

```
vtp mode transparent
```

Para evitar que el password de enable sea visto directamente se configura la encriptación no reversible de éste.

Comandos empleados:

```
no enable password
enable secret password
```

También se habilita la encriptación para las demás contraseñas configuradas en el equipo.

Comandos empleados:

```
service password-encryption
```

Se define un mensaje de aviso desplegable en el momento de conexión al equipo, con el fin de informar los requerimientos de autorización y las sanciones, el cual puede ser posteriormente empleado en procesos legales contra intrusos detectados. Este mensaje es un mensaje de muestra y debe ser modificado por el personal de O & M según lo que se ha configurado hasta el momento.

Comandos empleados:

```
banner log c La Conexion a este dispositivo esta extrictamente
restringida y es monitoreada Constantemente. Si no esta
especificamente autorizado desconectese inmediatamente. c
```

Muchos servicios actualmente innecesarios se encuentran activos en los equipos de red, con el fin de proporcionar compatibilidad con aplicaciones y equipos antiguos. Lamentablemente, muchos de estos servicios son fácilmente explotables y se convierten en una vulnerabilidad potencial de seguridad.

En la configuración de los equipos de la red Metro Ethernet se han desactivado los siguientes servicios, (recomendados en las "best practice" del fabricante, e igualmente analizados uno a uno por los ingenieros de Italtel) por no ser necesarios para los procesos actuales de la red Metro.

Comandos empleados:

```
no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
```

En caso tal que posteriormente estos servicios sean requeridos en los equipos, bastará con ser habilitados por el personal de O & M en la configuración, al eliminar el parámetro "no" al inicio del comando.

Según la definición del protocolo TCP, es posible que un cliente abra sesiones TCP y estas se queden inconclusas, permitiendo la utilización de recursos innecesariamente y eventualmente generar un ataque de DoS. Para evitar esto se activa la verificación de actividad de los servicios TCP por medio de keepalives.

Comandos empleados:

```
service tcp-keepalives-in
service tcp-keepalives-out
```

El acceso a los equipos es uno de los puntos de seguridad más críticos por lo cual inicialmente se restringe el acceso, se elimina el acceso vía telnet y únicamente se permite el acceso SSH y se configuran la autenticación según los usuarios definidos localmente. Después de la entrega de la red Operación y Mantenimiento, deberán proceder a integrar la red al sistema actual de verificación de usuarios.

Comandos empleados:

```
Username italtel password YYYY
aaa authentication login local_auth local

line con 0
 exec-timeout 5 0
 logging synchronous
 login authentication local_auth
 transport output none

line vty 0 4
 access-class acceso-ssh in
 timeout login response 300
 password 7 <removed>
 logging synchronous
 login authentication local_auth
 transport input ssh
 transport output ssh
```

Adicionalmente se restringe este acceso a los equipos por medio de una lista de acceso para permitir únicamente orígenes conocidos.

Comandos empleados:

```
ip access-list extended acceso-ssh
permit ip host 10.145.0.50 any log
permit ip host 10.145.128.32 any log
permit ip 10.145.0.0 0.0.0.63 any log
permit ip host 66.119.95.48 any log
permit ip host 66.119.95.49 any log
permit ip 66.119.95.40 0.0.0.7 any log
deny   tcp any any range 0 65535 log
deny   ip any any log
```

También se modifican los parámetros de almacenamiento de logs y de envío de traps, para asegurar que se capture la información crítica con los datos de fecha y hora específicos y adicionalmente que los mensajes críticos sean enviados correctamente.

Comandos empleados:

```
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec


logging facility local2
logging trap debugging
service sequence-numbers

logging console critical
logging buffered
```

4.3.2. Aseguramiento nivel 2 para puertos

Para cada interfaz GigaEthernet se configuran los siguientes parámetros de seguridad de nivel 2:

Inicialmente se especifica el tipo de puerto, la vlan, la encapsulación en caso que se emplee modo Trunk y se elimina la auto negociación para evitar que los equipos externos (clientes) influyan en las decisiones de configuración propias del equipo. También se cambia la vlan nativa, la cual es por defecto la vlan 1 por la vlan 99.

Comandos empleados:

```
interface GigabitEthernet X/Y
 switchport
 switchport access vlan XXX
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport trunk allowed vlan none
 switchport mode access
 switchport nonegotiate
```

Se deshabilita el servicio de CDP en los puertos que conectan a los usuarios, dado que este servicio sólo debe estar activo en las interfaces que conectan el anillo por razones de gestión.

Comandos empleados:

```
interface GigabitEthernet X/Y
 no cdp enable
```

Finalmente se deshabilita el envío y la recepción de mensajes del protocolo Spanning Tree (STP) en las inveraces hacia los clientes, dado que los procesos de STP no deben ser influenciados por estos. También se asegura la elección de la raíz de STP y se configuran los equipos para que deshabiliten el puerto cuando este detecte un mensaje de STP y evitar la conexión de switches no autorizados. Esta última es una medida de seguridad que deberá ser removida cuando se requiera conectar switches con STP habilitado.

Comandos empleados:

```
interface GigabitEthernet X/Y
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable (! No permite switches con STP)
 spanning-tree guard root
```

4.3.3. Aseguramiento nivel 3 para interfaces

A nivel 3 se configuran los siguientes parámetros de seguridad en cada uno de las interfaces L3 de los equipos del Anillo Metro Ethernet.

Se desactivan los siguientes servicios de nivel 3, que por defecto se encuentran activos y que no son necesarios para la red actual, pero que sí dejan latente una posible vulnerabilidad altamente explotable u ofrecen información de la red que ayudan a descubrir la topología interna a un atacante. En caso de ser requeridos estos servicios en el futuro, basta que se activen invocando los mismos comandos al eliminar el parámetro "no" que se antepone a estos.

Comandos empleados:

```
interface ZZZZ X/Y
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no mop enabled
```

Con el fin de minimizar los riesgos de ip Spoofing en los cuales un cliente conectado a un puerto, inyecta tráfico con una dirección ip origen falsa y obtener acceso a recursos no autorizados. Se activa la funcionalidad de verificación de dirección fuente, la cual compara la IP origen de la información originada de un puerto contra la información de la tabla de

enrutamiento para ese puerto específico, y si no concuerda, descarta el tráfico evitando que direcciones origen inválidas o válidas en otros puertos sean inyectadas.

Comandos empleados:

```
interface ZZZZ X/Y
 ip verify unicast source reachable-via rx
```

Finalmente se realiza un filtrado de direcciones fuente y destino por medio de un listas de acceso aplicadas diferentes aplicadas a las interfaces de entradas desde los clientes en todos los equipos y a las interfaces de salida hacia Internet en los equipos 7606.

Estos filtros están encaminados a impedir las comunicaciones por definición inválidas en relación a su dirección de flujo. Por ejemplo se filtran las comunicaciones iniciadas desde Internet con direcciones origen privadas y también se filtran las comunicaciones originadas desde Internet y desde los clientes con direcciones IP origen asignadas a dispositivos propios del anillo como las direcciones Loopback. Normalmente tampoco se debe permitir el tráfico de protocolos de enrutamiento como ospf o bgp desde los clientes dado que estos pudieran estar encaminados a interferir en los propios procesos de enrutamiento de la red Metro Ethernet.

Comandos empleados:

```
interface ZZZZ X/Y
 ip access-group desde-clientes in

interface GigabitEthernet2/47
ip access-group desde-inernet in
!
interface GigabitEthernet2/48
 ip access-group desde-inernet in

ip access-list extended desde-clientes
 deny   tcp any any eq bgp
 deny   ospf any any
 deny   ip host 66.201.183.250 any
 deny   ip host 66.201.183.254 any
```

```
 deny   ip host 66.201.183.242 any
 deny   ip host 66.201.183.246 any
 deny   ip 66.119.95.40 0.0.0.7 any
 deny   ip 66.119.95.48 0.0.0.3 any
 deny   ip 66.119.94.0 0.0.0.15 any
 deny   ip 66.201.182.176 0.0.0.15 any
 deny   ip 10.145.0.0 0.0.0.127 any
 permit ip any any

ip access-list extended desde-inernet
 permit ospf host 66.201.183.241 any
 permit ospf host 66.201.183.245 any
 deny   ospf any any
 deny   ip 0.0.0.0 0.255.255.255 255.0.0.0 0.255.255.255
 deny   ip 10.0.0.0 0.255.255.255 255.0.0.0 0.255.255.255
 deny   ip 127.0.0.0 0.255.255.255 255.0.0.0 0.255.255.255
 deny   ip 169.254.0.0 0.0.255.255 255.255.0.0 0.0.255.255
 deny   ip 172.16.0.0 0.15.255.255 255.240.0.0 0.15.255.255
 deny   ip 192.0.2.0 0.0.0.255 255.255.255.0 0.0.0.255
 deny   ip 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255
 deny   ip 224.0.0.0 31.255.255.255 224.0.0.0 31.255.255.255
 deny   ip any 255.255.255.128 0.0.0.127
 deny   ip 10.145.0.0 0.0.255.255 any
 deny   ip host 66.119.95.48 any
 deny   ip host 66.119.95.49 any
 deny   ip 66.119.95.40 0.0.0.7 any
 deny   ip 66.201.182.176 0.0.0.15 any
 deny   tcp any any eq bgp
 permit ip any any
```

La depuración, complemento y aplicación de estas listas de acceso y demás herramientas de seguridad y sus resultados en los entornos de producción específicos que se desarrollen en la red, son un proceso evolutivo del cual deberá estar a cargo el personal de Operación y Mantenimiento para garantizar el correcto funcionamiento y aseguramiento óptimo de los elementos de la red y sus servicios.

5. IMPLEMENTACIÓN DE CALIDAD DE SERVICIO

5.1. Análisis Previo a Configuración de Calidad de Servicio

Se procede a configurar las siguientes interfaces MPLS con calidad de servicio. Solamente se toma un enlace de el anillo metropolitano para menor afectación de servicio en caso haya inconvenientes con la configuración

Las interfaces de interconexión entre los routers es la **GigabitEthernet5/1** por lo que las demás interfaces se dejarÁn trabajando con MPLS pero sin Calidad de Servicio Aplicada.

```
NODO1#show mpls interfaces
Interface              IP           Tunnel   Operational
GigabitEthernet1/1     Yes (ldp)    No       Yes
GigabitEthernet2/33    Yes (ldp)    No       Yes
GigabitEthernet2/34    Yes (ldp)    No       Yes
GigabitEthernet2/35    Yes (ldp)    No       Yes
GigabitEthernet2/36    Yes (ldp)    No       Yes
GigabitEthernet5/1     Yes (ldp)    No       Yes
```

```
NODO2#show mpls interfaces
Interface              IP           Tunnel   Operational
GigabitEthernet1/1     Yes (ldp)    No       Yes
GigabitEthernet2/33    Yes (ldp)    No       Yes
GigabitEthernet2/34    Yes (ldp)    No       Yes
GigabitEthernet2/35    Yes (ldp)    No       Yes
GigabitEthernet2/36    Yes (ldp)    No       Yes
GigabitEthernet5/1     Yes (ldp)    No       Yes
```

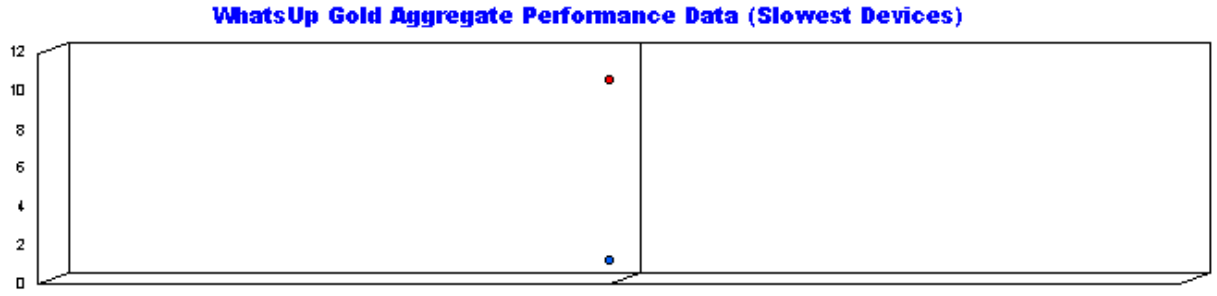
Por medio de un SNMP llamado WHATSUP se monitorea el comportamiento de las interfaces indicadas para ver los tiempos de respuesta.

Se monitorean durante cuatro días del 23 al 26 de Febrero del 2008 el comportamiento de ese enlace para tener un punto de comparación.

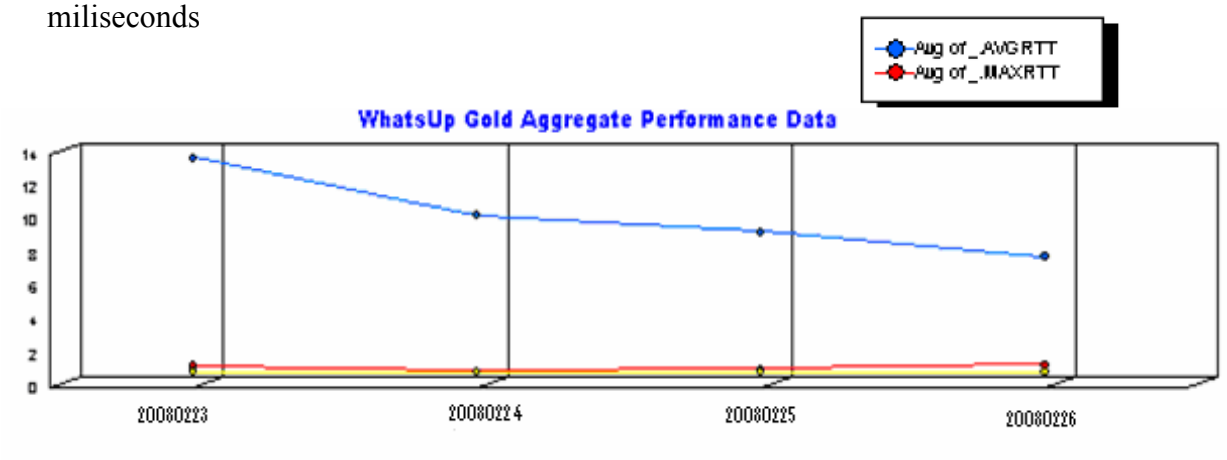
Performace Report

February 23, 2008 - February 26,2008

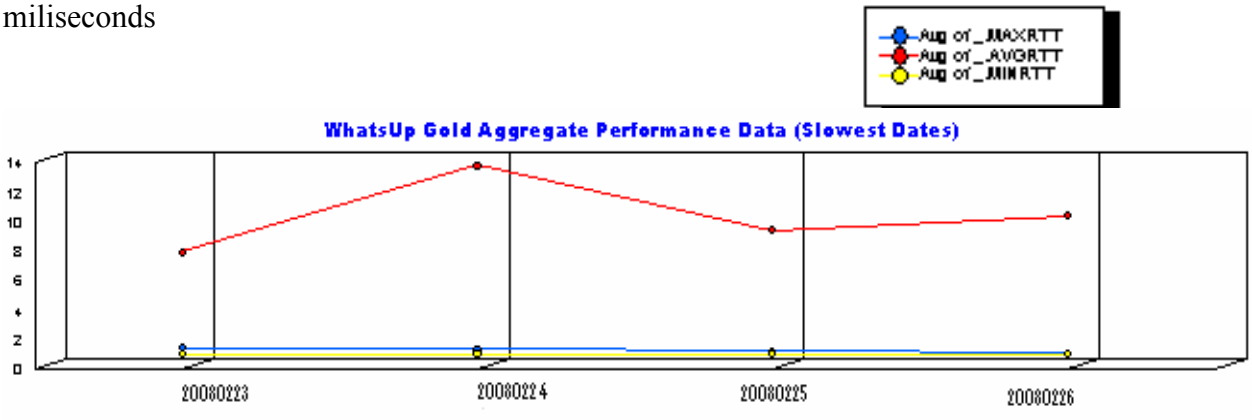
Last Command Line



miliseconds

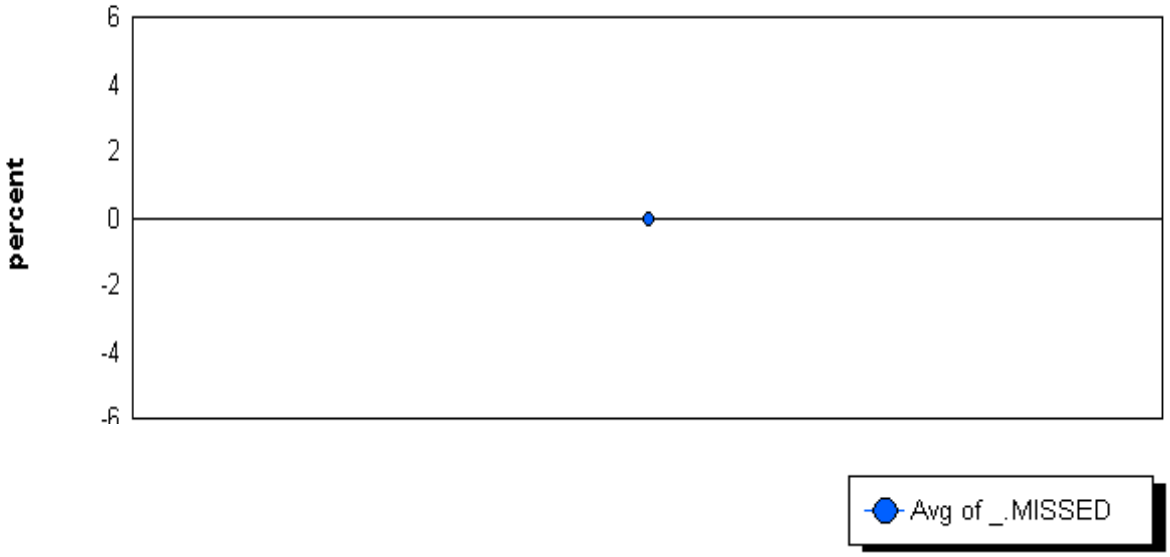


miliseconds

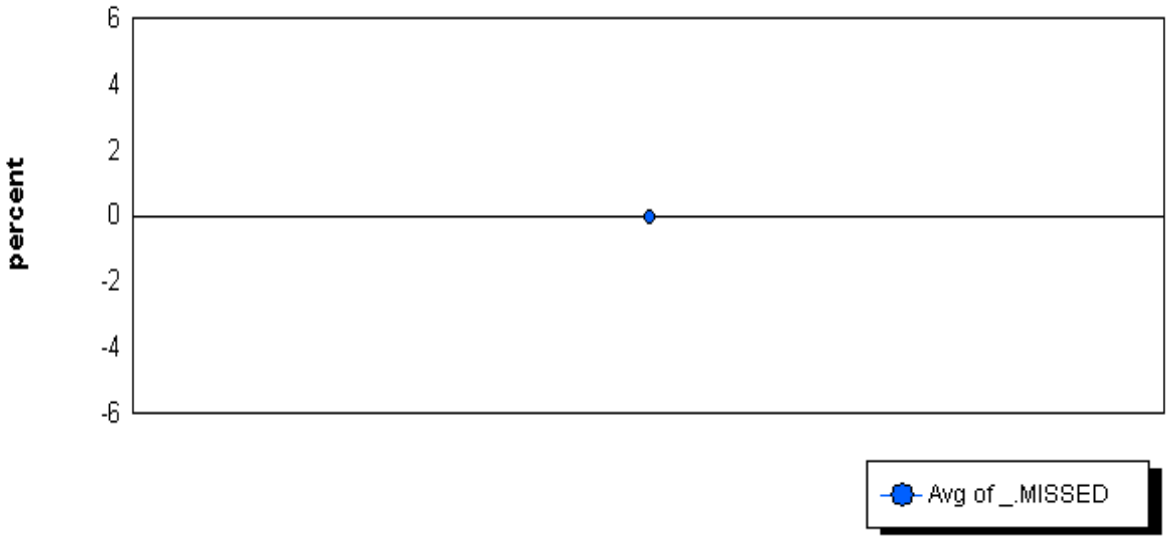


miliseconds

WhatsUp Gold Performance Data (Highest Average of Missed Polls)



WhatsUp Gold Performance Data (Lowest Average of Missed Polls)



AVGRTT	AVGMAXRTT	AVGMINRTT	Percent Missed
1.36	10.63	1.00	0%

AVGRTT: Average Round Trip Time
AVGMAXRTT: Average Maximum Round Trip Time
AVGMINRTT: Average Minimum Round Trip Time
Percent Missed: Porcentaje de pérdida
Round Trip Time: Poleo de una hora

5.2.CONFIGURACIÓN PARA CALIDAD DE SERVICIO

5.2.1. Política de Calidad de Servicio

La política de calidad de servicio tiene como objetivo darle uniformidad a la clasificación del tráfico y al tratamiento del mismo en todos los nodos del anillo metropolitano. Este es uno de los requerimientos para ofrecer el servicio de VPN MPLS a nivel de WAN. En su versión más reciente, se detalla la política de calidad de servicio, divide la clasificación del tráfico en 6 clases para que de manera ideal, esta se aplique en equipos que soporten 6 colas lógicas. Debido a que no todos los equipos habilitados en las redes soportan la configuración de 6 colas, se tiene un mapeo para 4 colas, el cual sÍ es aplicable en la mayoría de los equipos.

5.2.2. Mapeo para 6 colas

Como se mencionó anteriormente, el mapeo de 6 colas está diseñado para aplicarse en equipos de alta densidad. A continuación se muestra una tabla que ilustra dicho mapeo.

COLA	Nombre	EXP	Drop profile
q5	Control de red	7	No Drops
		6	No Drops
q4	Real Time	5	Tail Drop
q3	Video	4	Tail Drop
q2	Datos críticos	3	WRED LOW
		2	WRED HIGH
q1	Datos no críticos	1	WRED
q0	Best Effort	0	WRED

5.2.3. Mapeo para 4 colas

Este es el mapeo que se utilizará para la configuración en los equipos de la red, ya que los mismos sólo soportan 4 colas. A continuación se muestra una tabla con el mapeo.

COLA	Nombre	EXP	Drop profile
q3	Control de red	7	No Drops
		6	No Drops
q2	Real Time	5	Tail Drop
q1	Datos	4	WRED LOW
		3	WRED LOW
		2	WRED LOW
		1	WRED HIGH
q0	Best Effort	0	WRED

5.3. Configuración para interfaces troncales

La Red MetroEthernet utiliza interfaces ópticas de 1 Gbps para interconectarse tanto a nivel troncal, como interconexiones a equipos de acceso.

5.3.1. Configuración para interfaces troncales del anillo

Configuración del clasificador de tráfico

```
class-map match-any CONTROL-RED
  match mpls experimental 6 7
  match ip precedence 6 7

class-map match-any VOZ
  match mpls experimental 5
  match ip precedence 5

class-map match-any VIDEO
  match mpls experimental 4
  match ip precedence 4

class-map match-any DATOS-CRITICOS
  match mpls experimental  2 3
  match ip precedence 2 3

class-map match-any DATOS-NO-CRITICOS
  match mpls experimental 1
  match ip precedence 1

class-map match-any BEST-EFFORT
  match mpls experimental 0
  match ip precedence 0
```

Configuración del Policy-Map

```
policy-map QOS_BACKBONE
  class VOZ
    priority percent 20
    queue-limit 1574
    police cir percent 15
     conform-action transmit
     exceed-action drop
  class CONTROL-RED
    bandwidth percent 3
  class VIDEO
    bandwidth percent 20
    queue-limit 9766
  class DATOS-CRITICOS
    bandwidth percent 30
    random-detect precedence-based
    random-detect precedence 2 8030 24414
    random-detect precedence 3 12913 29297
  class DATOS-NO-CRITICOS
    bandwidth percent 15
    random-detect precedence-based
    random-detect precedence 1 17796 34180
  class class-default
    bandwidth remaining percent 100
    random-detect precedence-based
    random-detect precedence 0 32120 97656
```

Aplicación del Policy-Map en la interfaz

```
interface GigabitEthernetX/Y
 description TRONCAL BB
 ip address aa.bb.cc.dd 255.255.255.252
 mpls label protocol ldp
 tag-switching ip
 service-policy output QOS_BACKBONE
```

5.3.2. Configuración para interfaces troncales con tarjetas WS-65xxx

Para el caso en que se usen tarjetas WS-X6724-SFP se utiliza la configuración encolamiento wrr directamente sobre la interfaz. A continuación se muestra el mapeo para la configuración de encolamiento 1p3q8t,

Mapeo de colas de salida:

Queue	Trheshold	cos-map
1	1	0
1	2	1
2	1	2
2	2	3
2	3	6 7
3	1	4
Pq	--	5

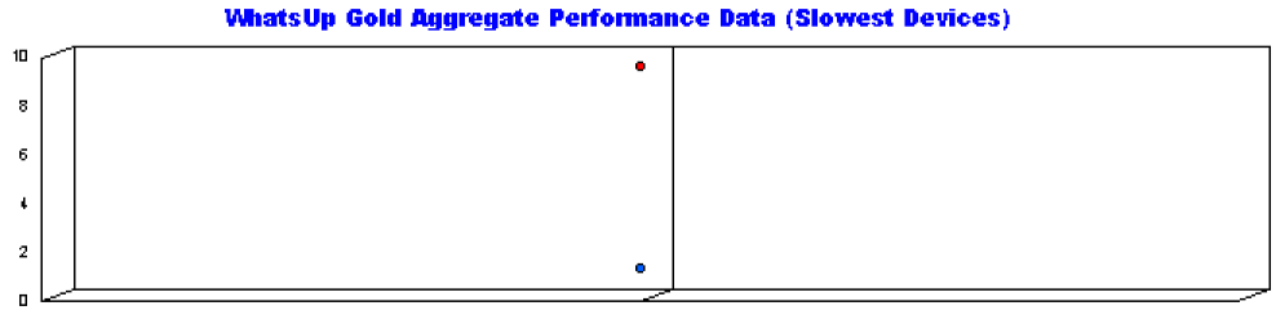
```
interface GigabitEthernetX/Y
 description TRONCAL BB
 ip address aa.bb.cc.dd 255.255.255.252
 mpls label protocol ldp
 tag-switching ip
 wrr-queue bandwidth percent 53 27 20
 wrr-queue queue-limit 53 27 20
 wrr-queue random-detect min-threshold 1 40 60 1 1 1 1 1 1
 wrr-queue random-detect min-threshold 2 70 80 100 1 1 1 1 1
 wrr-queue random-detect min-threshold 3 100 1 1 1 1 1 1 1
 wrr-queue random-detect max-threshold 1 70 80 1 1 1 1 1 1
 wrr-queue random-detect max-threshold 2 90 100 100 1 1 1 1 1
 wrr-queue random-detect max-threshold 3 100 1 1 1 1 1 1 1
 wrr-queue cos-map 1 1 0
 wrr-queue cos-map 1 2 1
 wrr-queue cos-map 2 1 2
```

```
wrr-queue cos-map 2 2 3
wrr-queue cos-map 2 3 6 7
wrr-queue cos-map 3 1 4
priority-queue cos-map 1 5
priority-queue queue-limit 25
mls qos trust cos
```

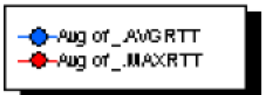
Performace Report

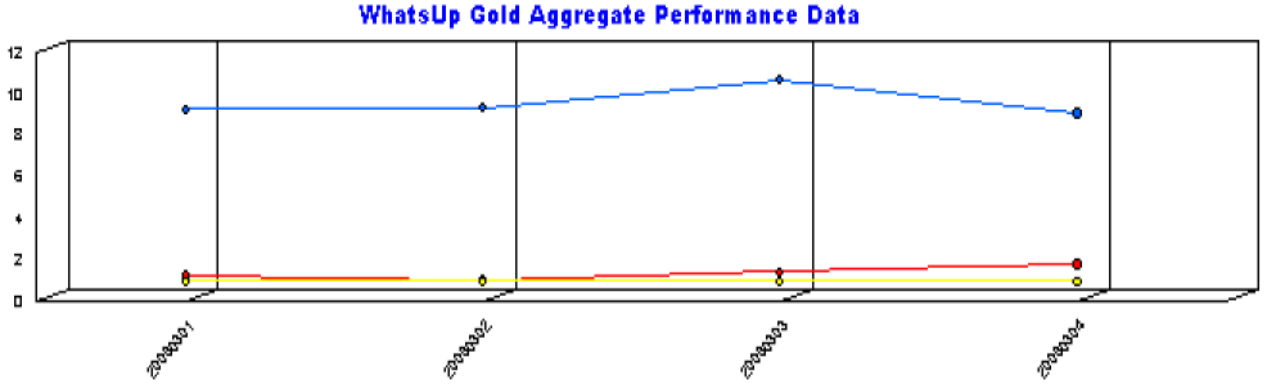
March 1, 2008 - March 4,2008

Last Command Line

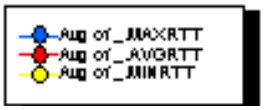


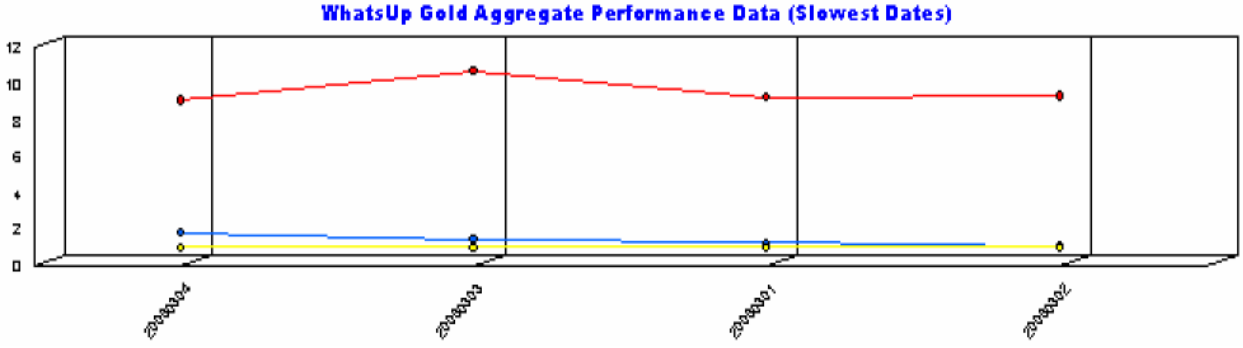
miliseconds





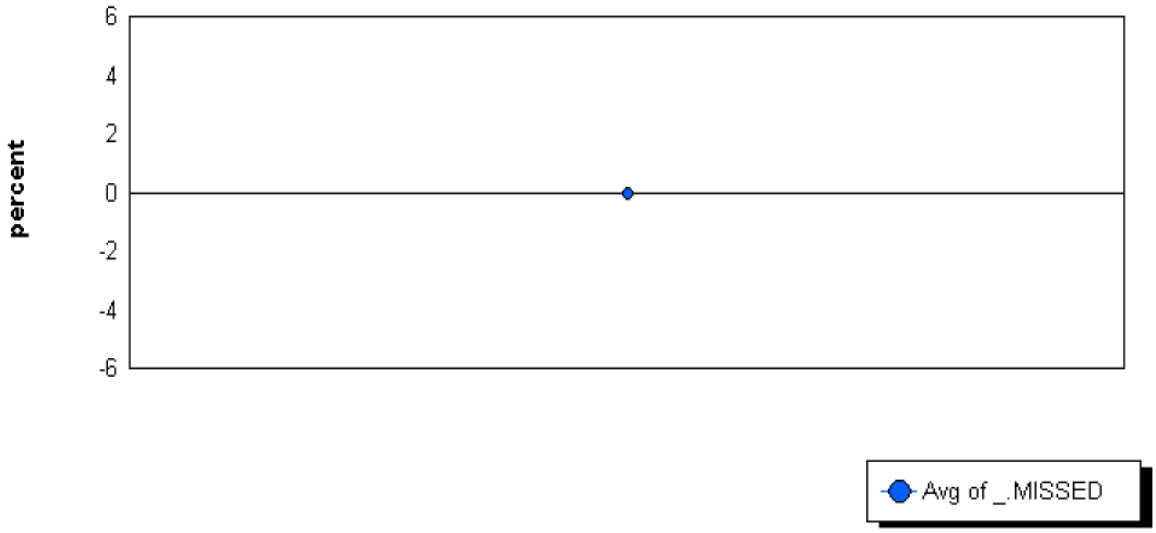
miliseconds



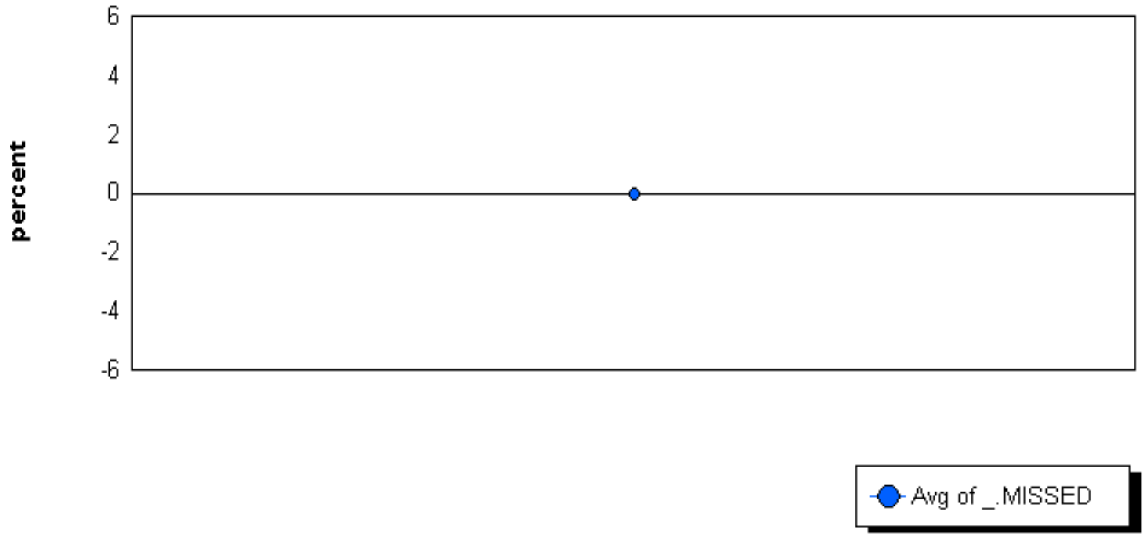


miliseconds

WhatsUp Gold Performance Data (Highest Average of Missed Polls)



WhatsUp Gold Performance Data (Lowest Average of Missed Polls)



AVGRTT	AVGMAXRTT	AVGMINRTT	Percent Missed
1.23	9.67	1.00	0%

6. CONCLUSIONES

1. Se logró verificar al momento de realizar la implementación por medio de protocolo, la funcionalidad en tiempo real de Calidad de Servicio sobre el enlace, haciendo énfasis en la prioridad de paquetes notando los siguientes datos:
    a. Se mantuvo establecida la sesión MPLS en el enlace
    b. La transferencia de datos sobre el enlace se mantuvo al 100%, ya que como se muestra en la gráfica de resultados no se tuvo pérdida de paquetes durante el período de la prueba.
    c. Se realizó la observación del etiquetamiento de los paquetes, los cuales mostraban, según el analizador de protocolos, en el campo llamado Differentiated Services Field: el número de DSCP y el Class Sector. Esta fue la prueba más sustancial para dar validez al funcionamiento correcto de esta implementación. En esta prueba se tuvo evidencia de la categorización de los paquetes dentro del enlace en prueba.

2. En el enlace no se observa latencia que pudiera afectar algún servicio en ningún momento. Debido a que la implementación de calidad de servicio a esta red se está realizando de manera preventiva, se planea introducir una cantidad de tráfico considerable, lo cual hace necesaria esta implementación.

3. Al momento de implementar la calidad de servicio en un enlace del anillo se observa lo siguiente:
    a. Los tiempos promedio de respuesta tienen una baja de 0.13 milisegundos.
    b. Los tiempos promedio máximos de respuesta tienen una baja de 0.96 milisegundos.
    c. El tiempo promedio mínimo se mantiene a 1 milisegundo.
    d. No se observan pérdidas de paquetes, tanto antes de implementar calidad de servicio como después.

4. Debido a que la red analizada es de un Proveedor de Servicio, se obtiene un beneficio económico, ya que los enlaces de WAN son bastante costosos y muy limitados en ancho de banda. Muchas aplicaciones críticas como voz sobre IP, servidores remotos de aplicaciones, información crítica requieren de ancho de banda definido y garantizado. Sin una priorización de los servicios y una repartición adecuada del ancho de banda estos servicios no responderían de una manera ademada. Utilizando QoS el ancho de banda se puede garantizar durante los periodos de alta congestión, sin necesidad de una inversión.

5. Mediante el control de acceso basados en identificación, filtrado y eliminación de paquetes, se puede garantizar la seguridad de la red y los servicios de acceso remoto y de esta manera protegerlos contra intrusiones de cualquier tipo.

6. A partir de la implementación de QoS en la red, la empresa puede garantizar a sus clientes un ancho de banda mínimo y asegurar así también que no tendrán pérdida de paquetes en momentos de saturación en la red.

7. RECOMENDACIONES

Durante la creación de esta implementación se pudo observar el crecimiento del tráfico dentro del anillo metropolitano, tanto de clientes como ADSL, red EVDO, Corporativos (IPCP) e Info-Internet ha ido creciendo como se espera en una red de servicios.

Actualmente se ha observado la migración de equipos de acceso como DIAMUX, los cuales son equipos terminales remotos los que normalmente están unidos a la central por medio de fibra óptica. Estos equipos dan servicio de Internet ADSL y líneas de teléfono normales llamadas POTS.

La tendencia actual en los equipos terminales remotos es la migración a red ip. Ejemplo claro de esto es que actualmente sobre la red se han adicionado los equipos conocidos como BROADACCESS que en este caso es el reemplazo de DIAMUX. El Broad Acces es un equipo en donde se pueden dar servicios de ADSLs, POTS, PRAs y Clear Channels. Todos estos servicios se pueden proporcionar en un mismo equipo, el cual utiliza como red de transporte al Anillo Metropolitano.

Conforme los equipos y usuarios de los equipos Broad Access vayan aumentando será necesario proporcionar alguna prioridad en la calidad de servicio y de esta manera garantizar a los usuarios que soliciten Calidad de Servicio.

Una vez ya establecido sobre toda la red QoS, sería interesante explorar la opción de poder garantizar en distintos niveles calidad de servicio a usuarios finales de la red. Con esta implementación realizada sobre el anillo metropolitano estamos garantizando servicio dentro de nuestra red, por lo que la implementación de QoS sobre las VPN de clientes corporativos como bancos.

8. BIBLIOGRAFIA

1. Alwayn, Vivek. Advanced MPLS Design and Implementation. Cisco Press, 2002

2. Osborne, Erick y Ajay Simha. Traffic Engineering with MPLS. Cisco Press, 2002

3. Alvarez, Santiago. QoS for IP/MPLS Networks. Cisco Press, 2006

4. Srinivas, Vegesna. IP Quality of Service. Cisco Press, 2001

5. Reagan James, CCIP: MPLS Study Guide. Sybex, Inc. 2002

6. Pignataro, Carlos, Ross Kazemi y Bil Dry. Cisco Multiservice Switching Networks. Cisco Press, 2003

7. Lobo, Lancy. MPLS Configuration on Cisco IOS Software. Cisco Press, 2005

8. De Ghein, Luc. MPLS Fundamentals, Cisco Press. 2006

9. F. Le Faucheur. MPLS Support of Differentiated Services (RFC3270), Axiowave Networks, PMC-Sierra Inc, 2002

10. S. Blake. An Architecture for Differentiated Services (RFC2475), Sun Microsystems, Lucent Technologies, 1998

11. E. Rosen. Multiprotocol Label Switching Architecture (RFC3031), Juniper Networks, Inc, Force10 Networks, Inc. 2001.

GLOSARIO

ACL

Access Control List; es una lista de reglas que detallan accesos a puertos de servicio en redes que están disponibles en una terminal u otro dispositivo de capa de red.

ADSL

Asymmetric Digital Subscriber Line. Tecnología de comunicación por medio de módems y utiliza como medio el par trenzado para transmisión asimétrica de datos.

ATM

Asynchronous transfer mode; es una arquitectura de red que divide los datos en celdas de igual tamaño y establece una entre la estación de origen y la estación de destino.

AToM

Any transfer over MPLS, es la capacidad de transportar cualquier tecnología de capa 2 a través de MPLS.

AS

Autonomous System, sistema autónomo, es un conjunto de dispositivos de capa de red administrados bajo una misma política.

AVGMAXRTT

Average maximum round trip time, tiempo máximo promedio de respuesta de un paquete.

AVGMINRTT

Average minimum round trip time, tiempo mínimo promedio de respuesta de un paquete.

AVGRTT

Average round trip time, tiempo promedio de respuesta de un paquete.

BGP

Es un protocolo de enrutamiento entre dominios o sistemas autónomos, permite el intercambio de actualizaciones de enrutamiento.

BIT

Binary Digit, Dígito binario o unidad mínima de información con la que trabajan los computadores. Es un dígito del sistema binario que puede tener el valor 0 o 1

BoS

Bit que se utiliza en MPLS para indicar que la etiqueta es la ultima de la pila.

Byte

Unidad básica de almacenamiento de información, generalmente equivalente a ocho bits.

CBWFQ

Class-based weighted fair queueing; es una extensión de WFQ estándar, esta variación permite la definición de clases para criterios de protocolos, control de acceso e interfaces de entrada.

CDP

Cisco Discovery Protocol; protocolo de capa 2 propietario de Cisco, el cual utilizado para el descubrimiento de dispositivos vecinos.

CPE

Customer Premises Equipment; cualquier Terminal o equipo que se encuentre ubicado del lado del cliente. Es el punto donde termina la responsabilidad del proveedor del servicio.

CQ

Custom Queuing; tecnica que permite reservar cierto porcentaje de ancho de banda según el tipo de protocolo utilizado.

DiffServ

Differentiated Services; modelo de Calidad de Servicio en Internet basado en Servicios Diferenciados

DoS

Un DoS o ataque de denegación de servicio es un incidente en el cual un usuario o una organización se ven privados de sus recursos informáticos.

Dot1Q

Estándar de la IEEE desarrollado para permitir a múltiples redes compartir redes virtuales de forma transparente en el mismo medio físico, sin problemas de interferencia entre ellas (*Trunking*).

DSCP

Differenciated Services Code Point; hace referencia al segundo byte en el header de los paquetes IP que se utiliza para diferenciar la calidad de servicio en la comunicación de los datos que se transportan.

E1

Canal digital con un ancho de banda de 2,048 kbps o 2 Mbps.

E3

Es un circuito con capacidad de transmisión de 34.368 Mbps.

EXP

Es un campo de 3 bits que originalmente fue creado, como su nombre lo indica, para fines experimentales, pero que en la actualidad se utiliza para proveer calidad de servicio.

FEC

Forwarding Equivalent Class; es un termino utilizado en MPLS para describir un conjunto de paquetes con características idénticas o similares que deben ser enviadas por el mismo camino.

FIB

Forwarding information base; también conocida como tabla de encaminamiento, es utilizada para encontrar la interfaz apropiada para enviar los paquetes.

FIFO

First In, First Out; EL primero en entrar es el primero en salir. Es una regla para proporcionar servicios en el orden en que entran las peticiones en un sistema de colas.

FRR

Fast reroute; es un mecanismo que provee el re encaminamiento del tráfico de forma automática dentro de un LSP en el evento de que un LSR llegara a fallar.

FTP

File transfer protocol; protocolo estándar en Internet para transferencia de archivos.

HDLC

High-Level Data Link Control; control de Enlace de Datos de Alto Nivel.

HTTP

Hypertext transfer protocol; protocolo de Transmisión Hipertexto. Protocolo de comunicaciones utilizado por los programas clientes y servidores en el Internet para comunicarse entre si.

IGP

Interior Gateway Protocol; protocolo utilizado para enviar información entre dispositivos de capa de red dentro de un domino o sistema autónomo.

IOS

Internetworking Operative System; sistema operativo de red propietario de Cisco Systems.

IP

Internet Protocol; el protocolo que manipula la entrega de paquetes en las redes TCP/IP.

IPCP

IP Control Protocol; protocolo que establece la comunicación IP sobre PPP.

IPv6

Es la nueva version de protocolo IPv4, la cual extiende la cantidad actual de 32 bits a 128bits.

ISDN

Integrated Services Digital Network; sistema para transmisión telefónica digital.

ISP

Internet Sevice Provider o proveedor de servicio de Internet.

Jitter

Variación en la cantidad de latencia entre paquetes de datos recibidos.

Kbps

Kilobits por segundo. Medida de velocidad de transmisión. KiloByte: KB. Unidad de medida de memoria. Equivalencia: 1 KByte = 10 Bytes = 1.024 Bytes.

LDP

Label Distribution Protocol; protocolo utilizado para la distribución de etiquetas.

LFIB

Label Forwarding information base, es una tabla que mantienen los routers MPLS, la cual almacena la información de envió de etiquetas.

LLQ

Low Latency Queuing; técnica de encolado que le da prioridad y trato preferencial a aplicaciones de tiempo real, tales como voz y video.

LSP

Label Switching Path; es el camino que recorren los paquetes dentro de una infraestructura de red MPLS, el cual es determinado por protocolos de señalización como LDP y RSVP.

LSR

Label Switching Router; es un tipo de router que se utiliza para conmutar paquetes dentro de una red MPLS. Es el responsable por manejar las etiquetas en los paquetes.

MD5

Es un algoritmo de reducción criptográfico MD5 (acrónimo de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5)

MIME

Multi-purpose Internet Mail Extensions; un estándar que permite enviar ficheros de cualquier tipo adjuntos a un mensaje de texto a través de Internet.

MPLS

Multiprotocol Label Switching; protocolo que opera entre la capa 2 y capa 3 del modelo de referencia OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Opera por medio de etiquetas.

MPLS TE

Multi Protocol Label Switching Traffic Engineering; Ingeniería de tráfico en MPLS.

MTU

Maximum Transfer Unit ; la unidad máxima de transferencia.

Multicast

Comunicación entre un único emisor y múltiples receptores en una red.

NBAR

Network Based Application Recognition; mecanismo que se utiliza para reconocer un flujo de datos por medio del primer paquete que es enviado.

OSPF

Open Shortest Path First; protocolo de enrutamiento avanzado y escalable basado en el algoritmo de Dijkstra.

P2P

Acrónimo de peer-to-peer, designa la modalidad de compartir información entre iguales, así como el software que facilita tales intercambios.

PHB

Per-Hop Behaviour; término utilizado en MPLS para definir la política o prioridad que se le da a un paquete cuando atraviesa cada salto una red con calidad de servicio.

PHP

Penultimate Hop Popping; es una función que realizan algunos routers MPLS. Se refiere al proceso de extracción de la última etiqueta de la pila, la cual es extraída por el penúltima LSR, antes de que el paquete sea enviado al router frontera.

POTS

Plain Old Telephone Services; infraestructura antigua que se utilizaba para la realización de llamadas telefónicas.

PPP

Point to Point Protocol. Protocolo que encapsula una conexión hacia una red TCP/IP a través de un módem y una línea telefónica.

PQ

Priority Queuing; técnica que se utiliza para asegurar que el tráfico mas importante reciba el trato mas rapido en cada salto.

QoS

Quality of Service; conjunto de técnicas y políticas que se aplican en una red para garantizar que los servicios sean prestados de forma adecuada a los usuarios.

RIP

RIP son las siglas de Routing Information Protocol. Es un protocolo estándar utilizado por routers para intercambiar información de capa de red.

RSVP

Resource Reservation Protocol; protocolo utilizado para reservar recursos en la red, destinado para brindar calidad de servicio en aplicaciones que lo requieran.

RTP

Real Time Protocol; un protocolo que permite especializar aplicaciones tales como llamadas telefónicas, vídeo y audio a través de Internet que están teniendo lugar a tiempo real.

SDH

Synchronous digital hierarchy; protocolo de transmisión utilizado en telecomunicaciones para el manejo de los anchos de banda.

SNMP

Simple Network Management Protocol; protocolo simple de gestión de redes, es aquel que permite la gestión remota de dispositivos de red, tales como switches, routers y servidores.

SONET

Synchronous Optical Network; estándar para el transporte de telecomunicaciones en redes de fibra óptica.

SSH

Secure Shell; este protocolo sirve para acceder a máquinas remotamente a través de una red, de forma similar a como se hacía con telnet. SSH usa técnicas de cifrado durante toda la sesión.

STP

Spanning tree protocol; es utilizado en dispositivos de capa 2 para eliminar la existencia de bucles de comunicación.

TCP

Protocolo de redes, orientado a conexión y confiable, que forma parte del conjunto de protocolos de TCP/IP.

TDM

Time Division Multiplex; es una técnica de multipexion en la cual los distintos canales se transmiten en distintos instantes de tiempo utilizando todo el ancho de banda asignado.

Telnet

Protocolo estándar en Internet que permite mantener una sesión en un sistema remoto.

TFTP

Versión del protocolo FTP de TCP/IP que utiliza UDP y no dispone de capacidades de directorio ni de contraseña.

ToS

Type of Service; es un campo de un byte que se encuentra en el encabezado de un paquete IP, el cual es utilizado para especificar el nivel de calidad de servicio requerido para dicho paquete.

TTL

Time To Live; tiempo de Vida de un paquete.

UDP

Acrónimo de User Datagram; protocolo de transporte clasificado como de mejor esfuerzo perteneciente a la familia de protocolos TCP/IP.

URL

El URL es la cadena de caracteres con la cual se asigna dirección única a cada uno de los recursos de información disponibles en Internet.

VLAN

Virtual Local Area Network; es una red de computadoras que aparenta estar conectada en la misma área físicamente, cuando en realidad pueden estar ubicadas en distintos segmentos.

VPN

Acrónimo de Virtual Private Network, permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

VRF

Virtual Routing and Forwarding; tecnología que permite la existencia de múltiples instancias de una tabla de ruteo dentro de un mismo router y al mismo tiempo.

VTP

VTP son las siglas de VLAN Trunking Protocol, un protocolo usado para configurar y administrar VLANs en equipos Cisco.

WFQ

Weighted Fair Queuing; es una técnica de encolamiento que proporciona calidad de servicio en redes convergentes. Trata de evitar la congestión.

WRED

Weighted random early detection; algoritmo para el manejo de colas utilizado para la prevención de congestionamiento, de tal forma que se puede efectuar diferenciación de servicios y se priorizan los paquetes que requieren mas recursos.

X.25

Protocolo de transmisión de datos. Establece circuitos virtuales, enlaces y canales. Es considerada una tecnología antigua.