

UNIVERSIDAD TECNICA DE COTOPAXI

CARRERA DE CIENCIAS DE LA INGENIERIA Y APLICADAS

**TESIS DE GRADO PREVIO A LA OBTENCION DEL TITULO DE
INGENIERIA EN INFORMATICA Y SISTEMAS
COMPUTACIONALES**

TEMA:

“Implantación de calidad de servicio (QoS) en redes locales virtuales (VLAN) mediante las normas 802.1D y 802.1Q en la Universidad Técnica de Cotopaxi.”

POSTULANTES:

Guanoluisa Corrales Diego Fernando

Semanate Semanate Doris Elizabeth

Tello Sevilla Guillermo Euclides

DIRECTOR:

Ing. Patricio Navas M.

Latacunga – Ecuador

CAPÍTULO I

FUNDAMENTACION TEORICA DE LAS REDES LOCALES VIRTUALES

1.1. ENTORNO DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI

1.1.1. Antecedentes históricos

La Universidad Técnica de Cotopaxi, es una institución de Educación Superior Pública, Laica y Gratuita, creada mediante Ley promulgada en el Registro Oficial N.- 618 del 24 de enero de 1995, y que forma parte del Sistema Nacional de Educación Superior Ecuatoriano. Se rige por la Constitución Política del Estado, la Ley de la Educación Superior y otras leyes conexas. Es una institución universitaria sin fines de lucro que orienta su trabajo hacia los sectores urbanos, marginales y campesinos; que busca la verdad y la afirmación de la identidad nacional, y que asume con responsabilidad el aseguramiento de la libertad en la producción y difusión de los conocimientos y del pensamiento democrático y progresista para el desarrollo de la conciencia antiimperialista del pueblo.

En nuestra institución se forman actualmente profesionales al servicio del pueblo en las siguientes áreas de especialidades: Ciencias Exactas y Naturales, Ciencias Agropecuarias y Veterinarias, Ciencias Humanísticas y del Hombre. Realizamos esfuerzos para alcanzar cada día metas superiores y más competitivas, planteándonos como retos, la formación de profesionales integrales en los ámbitos de pre y postgrado al servicio de la sociedad, el desarrollo paulatino de la investigación científica y la vinculación con la colectividad a partir de proyectos generales y específicos, con la participación plena de todos sus estamentos. Somos una Universidad con adecuados niveles de pertinencia y calidad, logrados a través de la concientización y difusión de la ciencia, cultura, arte y los conocimientos ancestrales. Contribuimos con una acción transformadora en la lucha por alcanzar una sociedad más justa equitativa y solidaria, para que el centro de atención del Estado sea el ser humano. Por ello, la Universidad Técnica de Cotopaxi asume su identidad con gran responsabilidad: "Por la vinculación

de la universidad con el pueblo”, “Por una Universidad alternativa con Visión de Futuro” Consciente de sus avances e insuficiencias, la Universidad Técnica de Cotopaxi emprende decisivamente el camino hacia la transformación plasmada en su Plan Estratégico de Desarrollo Institucional para el período 2003 – 2006.

1.1.2 Misión

La Universidad Técnica de Cotopaxi como entidad de derecho público y plena autonomía, plantea como Misión:

“Contribuir en la satisfacción de las demandas de formación y superación profesional, en el avance científico – tecnológico y en el desarrollo cultural universal y ancestral de la población ecuatoriana para lograr una sociedad solidaria, justa, equitativa y humanista. Para ello, desarrolla la actividad docente con niveles adecuados de calidad, brindando una oferta educativa alternativa en pregrado y postgrado, formando profesionales analíticos, críticos, investigadores, humanistas capaces de generar ciencia y tecnología. Asimismo, realiza una actividad científico – investigativa que le permite brindar aportes en la solución de los problemas más importantes de su radio de acción, y a través de la vinculación con la colectividad, potencia su trabajo extensionista. Se vincula con todos los sectores de la sociedad y especialmente, con aquellos de escasos recursos económicos, respetando todas las corrientes del pensamiento humano. La Universidad Técnica de Cotopaxi orienta sus esfuerzos hacia la búsqueda de mayores niveles de calidad, pertinencia y cooperación nacional e internacional, tratando de lograr niveles adecuados de eficiencia, eficacia y efectividad en su gestión. Se distingue de otras instituciones de educación superior de la provincia al ser una Universidad alternativa vinculada fuertemente al pueblo en todas sus actividades”.

1.1.3 Visión de la universidad

La Universidad Técnica de Cotopaxi plantea como Visión de Futuro los siguientes postulados que representan el estado mínimo deseable y posible de alcanzar:

- Se ha elevado la calidad de la formación integral profesional. Los graduados manifiestan satisfacción sobre la formación recibida en la mayoría de las carreras. Los

Planes de Estudios y las Mallas Curriculares están actualizados. Crece ligeramente la oferta de carreras y especialidades, así como las modalidades de estudios.

- La matrícula en todas las carreras tiene un ligero aumento. Se eleva la promoción en los primeros dos ciclos en la mayoría de las carreras. Se amplía el número de alumnos – ayudantes y se apoya adecuadamente a los estudiantes de bajo rendimiento. Existe un mejor servicio en las bibliotecas a la comunidad universitaria, creciendo además el fondo bibliográfico para el pregrado y postgrado. Se refuerza el papel del Centro Experimental y de Producción de Salache con relación a la producción agropecuaria y la captación de recursos extrapresupuestarios.

- Se avanza ligeramente en el desarrollo de la investigación científica en cada una de las carreras, creciendo el número de proyectos en ejecución y los resultados en las áreas prioritarias definidas institucionalmente. Crece ligeramente el número de convenios en el área de la investigación. Se incrementan la cantidades de eventos científicos y de artículos publicados en la Revista Alma Mater. Crece el número de estudiantes que se incorpora a la investigación. El sistema de planificación y control de la investigación funciona adecuadamente. Mejora la infraestructura para desarrollar la investigación. Aumenta ligeramente la cantidad de recursos extrapresupuestarios captados a través de la investigación.

- Mejora la calidad de las actividades de postgrado. Crece ligeramente la oferta de maestrías, diplomados y estudios de doctorados en las áreas prioritarias definidas. Crece el número de Master en la planta docente. Se establecen convenios de cooperación con Colegios Profesionales y otras Universidades para desarrollar actividades de postgrado. La actividad de postgrado se amplía a las ciudades en donde la Universidad posee Centros Asociados. La Dependencia Administrativa que atiende el postgrado en la UTC funciona eficientemente con el personal idóneo. Se logra incrementar el uso de las Nuevas Tecnologías de Información y Comunicación en las actividades de diplomados y maestrías.

- Se incrementan los Programas de Difusión Cultural, impactando favorablemente en los beneficiarios. Todas las carreras realizan actividades de extensión universitaria. El Servicio de Bienestar Universitario se amplía ligeramente y mejora la calidad de sus resultados. Se dispone de un Programa de Desarrollo de la

Extensión Universitaria actualizado, que incluye la problemática del medio ambiente. Se alcanzan buenos resultados en la proyección del deporte hacia el sector externo. Se imparte actividades de superación sobre el área de extensión a los miembros de la comunidad universitaria. Se realizan actividades de educación continua y capacitación popular con buen impacto en los beneficiarios.

- El nivel de formación pedagógica, profesional y científica de los docentes aumenta. Se eleva ligeramente el número de docentes a tiempo completo. Se eleva el nivel preparación del personal administrativo, los empleados y las autoridades a través de actividades de capacitación y profesionalización contratadas al sector externo. El sistema de reclutamiento, selección, inducción y evaluación funciona adecuadamente. Se estimulan los mejores resultados del personal a través de un sistema de reconocimientos. Se incrementa el sentido de pertenencia a la Universidad por parte del personal.
- Se eleva la cultura informática de la comunidad universitaria. El nivel de preparación del personal en ésta área aumenta. Se alcanza una mayor cobertura en la satisfacción de las demandas de equipamiento de las diferentes áreas universitarias. Se potencia el proceso de informatización de la Universidad con el aporte de los estudiantes.
- Se mejoran las relaciones con los colegios de bachillerato con mayor potencial de futuros aspirantes para la UTC, desarrollándose programas conjuntos. Se establecen alianzas estratégicas con algunas entidades productivas y de servicios y los Colegios Profesionales para realizar actividades conjuntas de mutuo beneficio. Aumenta el número de convenios con Universidades nacionales y extranjeras en áreas de interés institucional.
- Se dispone de un marco normativo actualizado y completo, que es conocido por la comunidad universitaria. Toda la base jurídica se encuentra bajo soporte automatizado.
- Mejora la gestión económica, financiera y administrativa universitaria. Se eleva el nivel de calificación del personal que trabaja en esas áreas y se automatizan una parte de los procesos, produciendo una disminución del tiempo para los trámites y una

elevación de la eficiencia del personal. Se produce un incremento paulatino en la captación de fondos extrapresupuestarios de autogestión. Existe un uso más racional de los recursos disponibles. Se mejora ligeramente la remuneración salarial del personal. La disponibilidad y uso de la infraestructura física y del equipamiento crecen. Se obtienen buenos resultados en las auditorías internas y el control estatal.

- Se dispone de un nuevo módulo adicional del proyecto de Campus Universitario. El sistema de planificación institucional se fortalece; todas las dependencias elaboran anualmente su plan operativo. Se fortalece la Dirección por Objetivos en todas áreas universitarias. Se cuenta con un Sistema de Información Estadístico que contribuye favorablemente en la toma de decisiones. El sistema de evaluación institucional funciona eficientemente. Se logra la acreditación de algunos programas académicos de pregrado y postgrado. El proceso de rendición de cuentas de las autoridades a la comunidad se desarrolla adecuadamente.

1.2. REDES LOCALES VIRTUALES

1.2.1. INTRODUCCIÓN

Las redes de área local virtuales (VLANs) han surgido de un conjunto de soluciones que los mayores distribuidores de equipamiento de redes de área local (LAN) habían propuesto para la conmutación de éstas. La mayoría de las empresas han empezado a buscar fabricantes que propongan una buena estrategia para su VLAN, así como que éstas sean incorporadas sobre las redes existentes, añadiendo funciones de conmutación y un software de gestión avanzado.

Una de las razones de que se centre la atención sobre las VLANs ha sido el rápido desarrollo de las LANs conmutadas, hecho que comenzó en 1994/1995.

Los modelos de red basados en la compartición de ancho de banda, presentes en las arquitecturas LAN de los primeros noventa, carecen de la potencia suficiente como para proporcionar los cada vez mayores anchos de banda que requieren las aplicaciones multimedia. En la actualidad se necesitan nuevos modelos capaces de proporcionar la potencia suficiente no sólo para satisfacer la creciente necesidad de ancho de banda, sino también para soportar un número mayor de usuarios en la red.

En las LAN basadas en compartición de ancho de banda, los usuarios comparten un único canal de comunicaciones, de modo que todo el ancho de banda de la red se asigna al equipo emisor de información. Quedando el resto de equipos en situación de espera. Para aumentar el ancho de banda disponible para cada usuario, se puede optar por la segmentación y anillos. Ahora bien, estas técnicas no ofrecen buenas prestaciones, debido principalmente a las dificultades que aparecen para gestionar la red. Cada segmento suele contener de 30 a 100 usuarios.

La técnica idónea para proporcionar elevados anchos de banda es la conmutación. Mediante esta técnica, cada estación de trabajo y cada servidor poseen una conexión dedicada dentro de la red, con lo que se consigue aumentar considerablemente el ancho de banda a disposición de cada usuario.

Las LANs basadas en compartición de ancho de banda se configuran mediante switches y routers. En una LAN conmutada, la función tradicional del router - encaminamiento de la información en la red- pasa a ser realizada por el conmutador

LAN, quedando aquél destinado a funciones relacionadas con la mejora de las prestaciones en lo que respecta a la gestión de la red. Con este nuevo papel del router, se pueden contener de 100 a 500 usuarios. El decremento en los precios de conmutadores Ethernet y Token Ring ha sido uno de los principales empujes a que un buen número de empresas se inclinen por una LAN conmutada.

Sin embargo, el continuo despliegue de conmutadores, dividiendo la red en más y más segmentos (con menos y menos usuarios por segmento) no reduce la necesidad de contenido de broadcast -información para gestionar la red-. Las VLANs representan una solución alternativa a los routers con función de gestores de la red. Con la implementación de switch en unión con VLANs, cada segmento de red puede contener como mínimo un usuario, mientras los dominios de broadcast pueden contener 1000 usuarios, o incluso más. Además, las VLANs pueden enrutar movimientos de las estaciones de trabajo hacia nuevas localizaciones, sin requerir de reconfigurar manualmente de las direcciones IP.

Las VLANs han sido, y son aún soluciones a nivel de propietario de cada distribuidor. Como la industria de redes de información ha demostrado, las soluciones a nivel de propietario (privadas) son una oposición a las políticas de los sistemas abiertos que se han desarrollado en la migración a estaciones de trabajo locales y el modelo cliente servidor.

Los clientes saben de los numerables costes asociados al cambio (adición y cambio de elementos, etc.) y se imaginan que las VLANs tienen sus propios costes administrativos fuertemente escondidos.

Aunque muchos analistas han sugerido que las VLANs permiten el desarrollo de servidores centralizados, los clientes han de mirar hacia implementaciones de gran empresa y ver las dificultades en habilitar un acceso completo y de alta funcionalidad a los servidores centralizados.

En este trabajo, se discuten estos conceptos con un poco más de detalle y determina las implicaciones que las VLANs tendrán en las empresas con necesidades de redes de información.

1.2.2. DEFINICIÓN DE UNA VLAN

Las LANs virtuales (VLANs) son agrupaciones de estaciones LAN que se comunican entre sí como si estuvieran conectadas al mismo cable, incluso estando situadas en segmentos diferentes de una red de edificio o de campus. Es decir, la red virtual es la tecnología que permite separar la visión lógica de la red de su estructura física mediante el soporte de comunidades de intereses, con definición lógica, para la colaboración en sistemas informáticos de redes. Este concepto, fácilmente asimilable a grandes trazos implica en la práctica, sin embargo, todo un complejo conjunto de cuestiones tecnológicas. Quizás, por ello, los fabricantes de conmutación LAN se están introduciendo en este nuevo mundo a través de caminos diferentes, complicando aún más su divulgación entre los usuarios.

Además, la red virtual simplifica el problema de administrar los movimientos, adiciones y cambios del usuario dentro de la empresa. Por ejemplo, si un departamento se desplaza a un edificio a través del campus, este cambio físico será transparente gracias a la visión lógica de la red virtual. Se reduce notablemente el tiempo y los datos asociados con los movimientos físicos, permitiendo que la red mantenga su estructura lógica al coste de unas pocas pulsaciones del ratón del administrador de la red. Puesto que todos los cambios se realizan bajo control de software, los centros de cableado permanecen seguros y a salvo de interrupciones.

Por la razón de que hay varias formas en que se puede definir una VLAN, se dividen éstas en cuatro tipos principales: basadas en puertos, basadas en MAC, VLANs de capa 3 y basada en reglas (policy based). En la figura 1 se pueden observar los elementos de la implementación de una VLAN, y en la capa 2 se encuentran los cuatro tipos posibles en que puede ser definida.

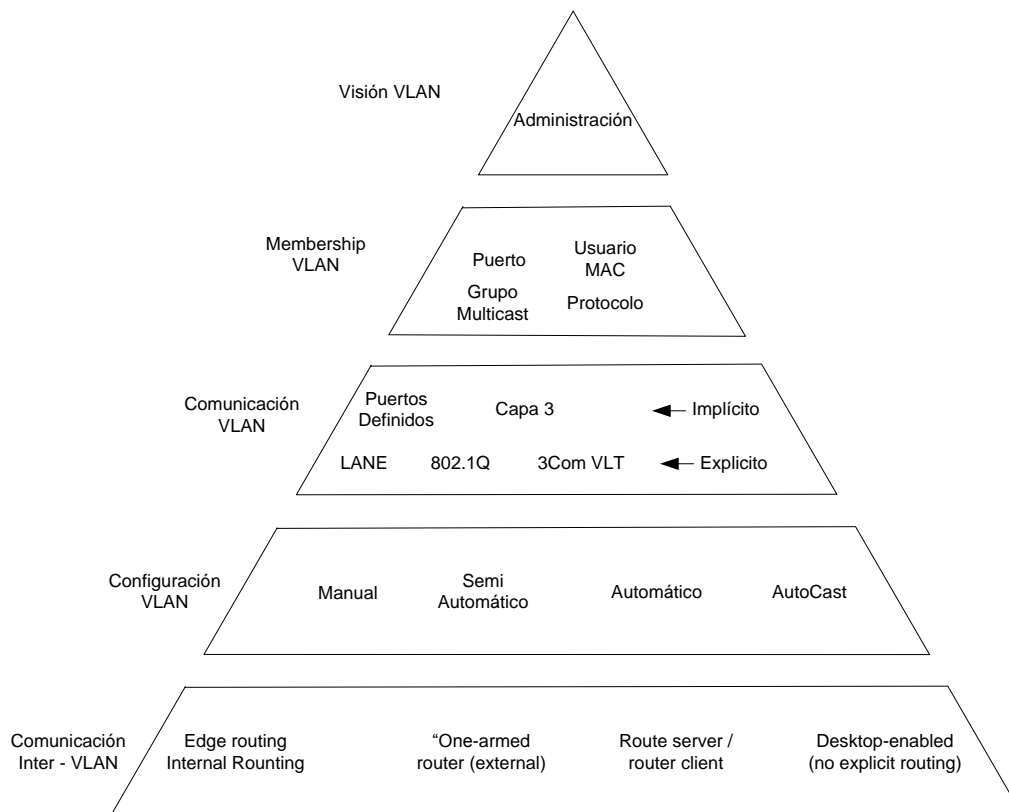


Figura 1.1.- Elementos de la implementación de una VLAN.

Fuente: www.emagister.com/public/pdf/comunidad_emagister/849677065484567-config-ciscos.pdf

1.3. CARACTERÍSTICAS

Los grupos de trabajo en una red han sido creados hasta ahora por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo concentrador o Switch. Como consecuencia directa de la forma tradicional de crear grupos de trabajo, estos grupos comparten el ancho de banda disponible y los dominios de broadcast, así como la dificultad de gestión cuando se producen cambios en los miembros del grupo. Mas aún, la limitación geográfica que supone que los miembros de un grupo determinado deben de estar situados adyacentemente, por su conexión al mismo concentrador o segmento de la red.

- a. Los esquemas VLAN (Virtual LAN, o red Virtual) proporcionan los medios adecuados para solucionar la problemática por medio de la agrupación realizada de una forma lógica, en lugar de física. Sin embargo, las redes virtuales siguen compartiendo las características de los grupos de trabajo físicos, en el sentido de que todos los usuarios comparten sus dominios de

broadcast. La diferencia principal con la agrupación física es que los usuarios de las redes virtuales pueden ser distribuidos a través de una red LAN, incluso situándose en distintos concentradores de la misma. Los usuarios pueden así atravesar la red, manteniendo su pertenencia al grupo de trabajo lógico.

- b. Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos se logra, como consecuencia directa, el incremento del ancho de banda en dicho grupo de usuarios. Además al poder distribuir a los usuarios en diferentes segmentos de red, se pueden situar bridges y routing entre ellos, separando segmentos con diferentes topologías y protocolos. Así por ejemplo, se pueden mantener diferentes usuarios del mismo grupo, unos con FDDI y otros con Ethernet, en función tanto de las instalaciones existentes como el ancho de banda que precise cada uno por su función específica dentro del grupo. Todo ello, por supuesto, manteniendo la seguridad deseada en cada configuración por el administrador de la red. Se pueden permitir o no que el tráfico de una VLAN entre y salga desde/hacia otras redes. Pero se puede llegar aun más lejos.

- c. Las redes virtuales permiten que la ubicación geográfica no se limite a diferentes concentradores o plantas de un mismo edificio, sino a diferentes oficinas intercomunicadas mediante redes WAN o MAN, a lo largo de países y continentes sin ninguna limitación, mas que la que impone el administrador de dichas redes.

1.4. SUBREDES y VLAN's

Una VLAN es también una subred, ya que si no sale de la subred mediante un router, toda la información de broadcast se queda en ella.

Cada subred necesita un direccionamiento IP y una dirección de subred.

Para transmitir los datos de una subred a otra se necesita un router.

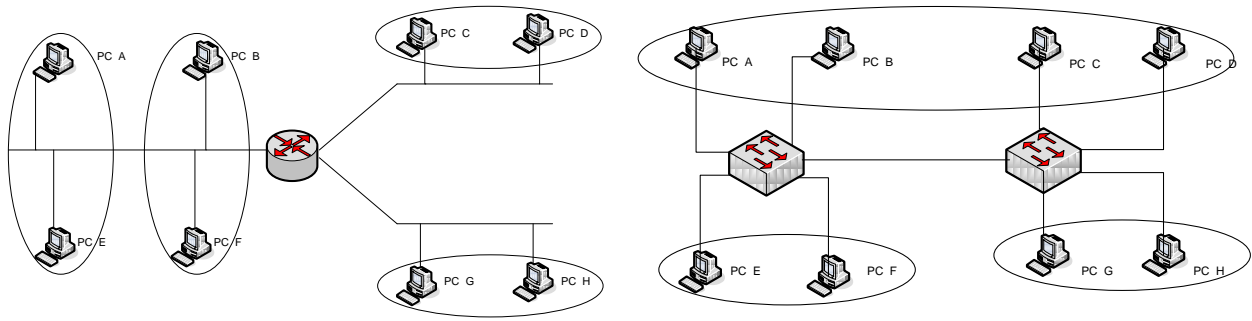


Figura 1.2.- Subredes y VLANS.

Fuente: Consultascna.com

En la figura 1.2 muestra dos redes lógicamente iguales.

Existen 3 subredes separadas con un direccionamiento diferente y que se alcanzan entre ellas mediante broadcast.

Para enviar información de una subred a otra, deben transmitir a su gateway por defecto, o sea, la interfase que los une, el router.

Una diferencia entre los bridges y los switches es que los bridges necesitan un puerto independiente del router para cada subred, mientras que un switch se basta con un puerto del router, ya que usa las subinterfaces de un mismo puerto de un router.

Cisco recomienda una cantidad de dispositivos límite para las subredes.

Protocolos	Número de Dispositivos
IP	500
IPX	300
NetBios	200
AppleTalk	200
Mixed Protocols	200

Tabla 1.1. Recomendaciones Cisco

Fuente: Cisco Networking Home Page

1.5. ESCALABILIDAD DE UNA VLAN

Mediante las VLAN's, el sistema se hace mas escalable.

Las VLAN's proveen mas flexibilidad a la hora de conectarse a la red. No se limita a una conexión en un único punto, sino que se puede conectar a la misma red desde varias posiciones. Esto hace que se deban de tener unas políticas de seguridad más estrictas.

La única limitación respecto a esta libertad de movimiento de un usuario respecto a su posición física es que siempre estará conectado a la misma subred y que para salir del nivel 3 deberá de pasar a través de un router.

Aquí vemos las limitaciones de cada switch.

Modelo de Switch	Versión de Software	Número de VLAN
1900	Entreprise IOS	64
2950	IOS Standard Image (SI)	64
2950	IOS Enhanced Image (EI)	250

Tabla 1.2. Limitaciones de Switch Cisco

Fuente: Cisco Networking Home Page

1.6. ASIGNACIÓN A UNA VLAN DINÁMICAMENTE O ESTÁTICAMENTE

Cada dispositivo de una VLAN puede ser determinado de dos maneras. Estática o dinámica. Estos dos métodos definen como un puerto de un switch se asocia a una VLAN en concreto. Se puede designar este puerto manualmente o dinámicamente. Usando la configuración de una subinterface se puede asignar un puerto a una VLAN. Este método es llamado port based VLANs. Cuando es automático, se define como dinámico. El switch asigna automáticamente el puerto a una VLAN dependiendo de quien se conecte. Esto es mediante el uso de la dirección MAC o la dirección IP de la máquina que se conecta al puerto.

El switch consulta en un servidor de políticas en un lugar llamado VLAN membership policy server (VMPS), que contiene la información necesaria para asignar al puerto a una VLAN u otra. Uno de los switches de su red debe de ser configurado como servidor.

- Las VLAN dinámicas tienen una ventaja frente las estáticas.
- Soportan la movilidad plug-and-play.

1.7.- VLANs BASADAS EN PUERTOS (MEMBERSHIP BY PORT GROUP)

Según este esquema, la VLAN consiste en una agrupación de puertos físicos que puede tener lugar sobre un conmutador o también, en algunos casos, sobre varios conmutadores. La asignación de los equipos a la VLAN se hace en base a los puertos que están conectados físicamente.

Muchas de las primeras implementaciones de las VLANs definían la pertenencia a la red virtual por grupos de puertos (por ejemplo, los puertos 1, 2, 3, 7 y 8 sobre un conmutador forman la VLAN A, mientras que los puertos 4, 5 y 6 forman la VLAN B). Además, en la mayoría, las VLANs podían ser construidas sobre un único conmutador.

La segunda generación de implementaciones de VLANs basadas en puertos contempla la aparición de múltiples conmutadores (por ejemplo, los puertos 1 y 2 del conmutador 1 y los puertos 4, 5, 6 y 7 del conmutador 2 forman la VLAN A; mientras que los puertos 3, 4, 5, 6, 7 y 8 del conmutador 1 combinados con los puertos 1, 2, 3 y 8 del conmutador 2 configuran la VLAN B). Este esquema es el descrito por la figura 1.3.

La agrupación por puertos es todavía el método más común de definir la pertenencia a una VLAN, y su configuración es bastante directa. El definir una red virtual completamente basada en puertos no permite a múltiples VLANs el incluir el mismo segmento físico (o conmutador).

La principal limitación de definir VLANs por puertos es que el administrador de la red ha de reconfigurar la VLAN cada vez que un usuario se mueve de un puerto a otro.

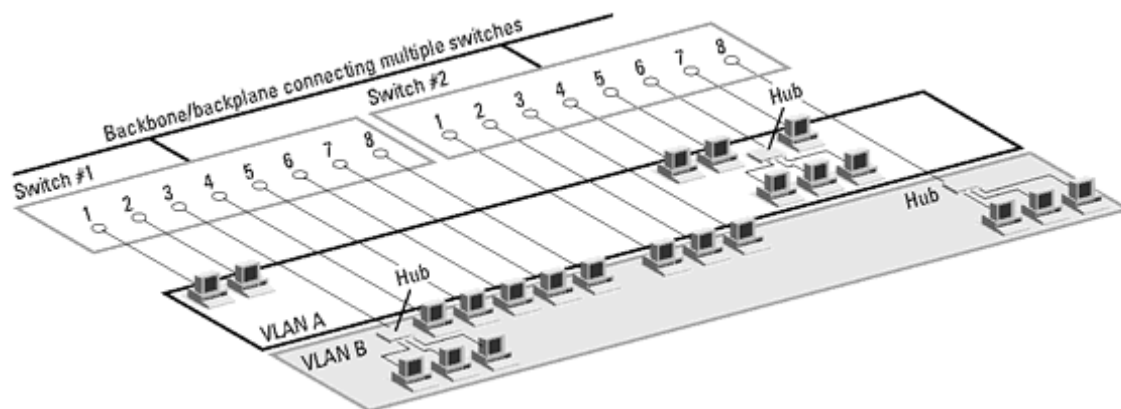


Figura 1.3.- VLANs basadas en puertos.

1.8. VLAN BASADAS EN MAC (MEMBERSHIP BY MAC ADDRESS)

Constituye la segunda etapa de la estrategia de aproximación a la VLAN, y trata de superar las limitaciones de las VLANs basadas en puertos. Operan agrupando estaciones finales en una VLAN en base a sus direcciones MAC. Este tipo de implementación tiene varias ventajas y desventajas.

Desde que las direcciones MAC (media access control -control de acceso al medio-) se encuentran implementadas directamente sobre la tarjeta de interfase de la red (NIC -network interface card-), las VLANs basadas en direcciones MAC permiten a los administradores de la red el mover una estación de trabajo a una localización física distinta en la red y mantener su pertenencia a la VLAN. De este modo, las VLANs basadas en MAC pueden ser vistas como una VLAN orientada al usuario.

Entre los inconvenientes de las VLANs basadas en MAC está el requerimiento de que todos los usuarios deben inicialmente estar configurados para poder estar en al menos una VLAN. Después de esa configuración manual inicial, el movimiento automático de usuarios es posible, dependiendo de la solución específica que el distribuidor haya dado. Sin embargo, la desventaja de tener que configurar inicialmente la red llega a ser clara en redes grandes, donde miles de usuarios deben ser asignados explícitamente a una VLAN particular. Algunos distribuidores han optado por realizar esta configuración inicial usando herramientas que crean VLANs basadas en el actual estado de la red, esto es, una VLAN basada en MAC es creada para cada subred.

Las VLANs basadas en MAC que son implementadas en entornos de medios compartidos se degradarán seriamente como miembros de diferentes VLANs coexistiendo en un mismo conmutador. Además, el principal método de compartición de información entre miembros de una VLAN mediante conmutadores en una red virtual basada en MAC también se degrada cuando se trata de una implementación a gran escala.

1.9. VLANs DE CAPA 3 (LAYER 3-BASED VLANs).

Las VLANs de capa 3 toman en cuenta el tipo de protocolo (si varios protocolos son soportados por la máquina) o direcciones de la capa de red, para determinar la pertenencia a una VLAN. Aunque estas VLANs están basadas en información de la

capa 3, esto no constituye una función de encaminamiento y no debería ser confundido con el enrutamiento en la capa de red.

Entendido lo que son las VLANs basadas en información de la capa 3 y el concepto de encaminamiento o routing, hay que apuntar que algunos distribuidores están incorporando varios conceptos de la capa 3 en sus switch, habilitando funciones normalmente asociadas al routing.

Hay varias ventajas en definir VLANs de capa 3.

- a. En primer lugar, permite el particionado por tipo de protocolo, lo que puede parecer atractivo para los administradores que están dedicados a una estrategia de VLAN basada en servicios o aplicaciones.
- b. En segundo lugar, los usuarios pueden físicamente mover sus estaciones de trabajo sin tener que reconfigurar cada una de las direcciones de red de la estación (este es un beneficio principalmente para los usuarios de TCP/IP).
- c. Y en tercer lugar, definir una VLAN de capa 3 puede eliminar la necesidad de marcar las tramas para comunicar miembros de la red mediante conmutadores, reduciendo los gastos de transporte.

Una de las desventajas de definir la VLAN de capa 3 (al contrario de lo que ocurría en las dos anteriores) es su modo de trabajo. El inspeccionar direcciones de la capa 3 en paquetes consume más tiempo que buscar una dirección MAC en tramas. Por esta razón, los conmutadores que usan información de la capa 3 para la definición de VLANs son generalmente más lentos que los que usan información de la capa 2. Esta diferencia no ocurre en todas las distintas implementaciones de cada distribuidor.

Las VLANs basadas en capa 3 son particularmente efectivas en el trato con TCP/IP, pero mucho menos efectivas con protocolos como IPX, DECnet o AppleTalk, que no implican configuración manual. Además tienen la dificultad al tratar con protocolos no enrutables como NetBIOS (estaciones finales que soportan protocolos no enrutables no pueden ser diferenciadas y, por tanto, no pueden ser definidas como parte de una VLAN).

1.10. VLANS BASADAS EN REGLAS.

Este esquema es el más potente y flexible, ya que permite crear VLANs adaptadas a necesidades específicas de los gestores de red utilizando una combinación de reglas. Estas reglas pueden ser, por ejemplo, de acceso, con objeto de alcanzar unos ciertos niveles de seguridad en la red. Una vez que el conjunto de reglas que constituyen la política a aplicar a la VLAN se implementa, sigue actuando sobre los usuarios al margen de sus posibles movimientos por la red.

1.11. TECNOLOGÍA.

Existen tres aproximaciones diferentes que pueden emplearse como soluciones válidas para proporcionar redes virtuales:

- Conmutación de puertos,
- Conmutación de segmentos con funciones de bridging,
- Conmutación de segmentos con funciones de bridging/routing.

Todas las soluciones están basadas en arquitecturas de red que emplean concentradores/conmutadores. Aunque las tres son soluciones válidas, solo la última, con funciones de bridge/router, ofrece todas las ventajas a las VLAN.

1.11.1. CONMUTADORES DE PUERTOS.

Los conmutadores de puertos son concentradores con varios segmentos, cada uno de los cuales proporciona el máximo ancho de banda disponible, según el tipo de red, compartido entre todos los puertos existentes en dicho segmento. Se diferencian de los conmutadores tradicionales en que sus puertos pueden asociarse dinámicamente a cualquiera de los segmentos, mediante comandos software. Cada segmento se asocia a un backplane (medio físico de gran velocidad que enlaza todos los puertos de los switch's), el cual equivale a su vez a un grupo de trabajo. De este modo, las estaciones conectadas a estos puertos pueden asignarse y reasignarse a diferentes grupos de trabajo o redes virtuales.

Se pueden definir los conmutadores de puertos como software patch panels, y su ventaja fundamental es la facilidad para la reconfiguración de los grupos de trabajo. Tienen, sin embargo, graves limitaciones; dado que están diseñados como dispositivos que comparten un backplane físico, las reconfiguraciones de grupo de trabajo están

limitadas al entorno de un único concentrador y por tanto, todos los miembros del grupo deben de estar físicamente próximos.

Las redes virtuales con conmutadores de puertos adolecen de conectividad con el resto de la red. Al segmentar sus propios backplanes no proporcionan conectividad integrada entre los mismos, y por tanto están separados de la comunicación con el resto de la red.

Requieren para ello un bridge/router externo. Ello implica mayores costes, además de la necesidad de reconfigurar el bridge/router cuando se producen cambios en la red. Por ultimo, los conmutadores de puertos no alivian el problema de saturación del ancho de banda de la red. Todos los nodos deben de conectarse al mismo segmento o backplane, por tanto compartirán el ancho de banda disponible en el mismo, independientemente de su número.

1.11.2. CONMUTADORES DE SEGMENTOS CON BRIDGING.

A diferencia de los conmutadores de puertos, suministran el ancho de banda de múltiples segmentos de red, manteniendo la conectividad entre dichos segmentos. Se emplean para ello los algoritmos tradicionales de los puentes (bridges), o subconjuntos de los mismos para proporcionar conectividad entre varios segmentos a la velocidad máxima que permite la topología y protocolos de dicha red.

Mediante estos dispositivos, las VLAN no son grupos de trabajo conectados a un solo segmento o backplane Sino grupos lógicos de nodos que pueden conectarse a cualquier número de segmentos de red físicos. Estas VLAN son dominios de broadcast lógicos: conjuntos de segmentos de red que reciben todos los paquetes enviados por cualquier nodo en la VLAN como si todos los nodos estuvieran conectados físicamente al mismo segmento.

Al igual que los conmutadores de puertos, se puede reconfigurar y modificar la estructura de la VLAN mediante comandos software, con la ventaja añadida de ancho de banda repartido entre varios segmentos físicos. De esta forma, según va creciendo un grupo de trabajo, y para evitar su saturación, los usuarios del mismo pueden situarse en diferentes segmentos físicos, aún manteniendo el concepto de grupo de trabajo independiente del resto de la red, con lo que se logra ampliar el ancho de banda en función del número de segmentos usados.

Aún así, comparten el mismo problema con los conmutadores de puertos en cuando a su comunicación fuera del grupo. Al estar aislados, para su comunicación con el resto de la red necesitan encaminadores, con las consecuencias que ya se han mencionado en el caso anterior, relativas al coste y la reconfiguración de la red.

1.11.3. CONMUTADORES DE SEGMENTOS CON BRIDGING/ROUTING (MULTI-LAYER SWITCHES)

Es la solución evidente de las dos soluciones anteriores. Dispositivos que comparten todas las ventajas de los conmutadores de segmentos con funciones de bridging, pero además con funciones añadidas de encaminamiento (routing), lo que les proporciona fácil reconfiguración de la red, así como la posibilidad de crear grupos de trabajo que se expanden a través de diferentes segmentos de la red. Además, sus funciones de

encaminamiento facilitan la conectividad entre las redes virtuales y el resto de los segmentos o redes, tanto locales como remotas.

Mediante las redes virtuales se puede crear un nuevo grupo de trabajo, con tan solo una reconfiguración del software del conmutador. Ello evita el recableado de la red o el cambio en direcciones de subredes, permitiendo así asignar el ancho de banda requerido por el nuevo grupo de trabajo, sin afectar a las aplicaciones de red existentes.

En las VLAN con funciones de encaminamiento, la comunicación con el resto de la red se puede realizar de dos modos distintos: permitiendo que algunos segmentos sean miembros de varios grupos de trabajo, o mediante las funciones de encaminamiento múltiprotocolo, que facilitan el tráfico incluso entre varias VLAN.

1.12. COMUNICACIÓN DE INFORMACIÓN EN UNA VLAN

Existen 3 métodos para comunicar información entre Switches a través de un Backbone: Mantenimiento de Tablas, encapsulado de tramas y TDM (Multiplexación por división de tiempo).

En el mantenimiento de tablas a través de señalización, lo que se tiene es una tabla que asocia, ya sea, direcciones MAC o número de puertos, para cada VLAN definida. Esta información es comunicada periódicamente a otros Switches de la red. Los cambios que se hagan deben hacerse manualmente por el administrador de la red, directamente en el equipo (Switch), claro esta, esto depende mucho del proveedor. El constante envío de señalización necesaria para mantener al día las tablas en los Switches causa una significativa congestión, por lo que este método no es particularmente bueno.

En el encapsulado de tramas, se agrega una cabecera con la información suficiente para identificar de manera unívoca cada VLAN definida. Esto corre el peligro de sobrepasar el tamaño máximo permitido por la subcapa MAC. Estas cabeceras adicionan una sobrecarga al tráfico de la red. Para este caso, se tienen canales reservados para cada VLAN. Esta aproximación evita problemas de sobrecarga de la señalización y del encapsulado de tramas, pero, desperdicia ancho de banda, ya que no se puede utilizar el canal asignado a otra VLAN que puede estar con baja carga.

1.13. NORMAS DE VLANS

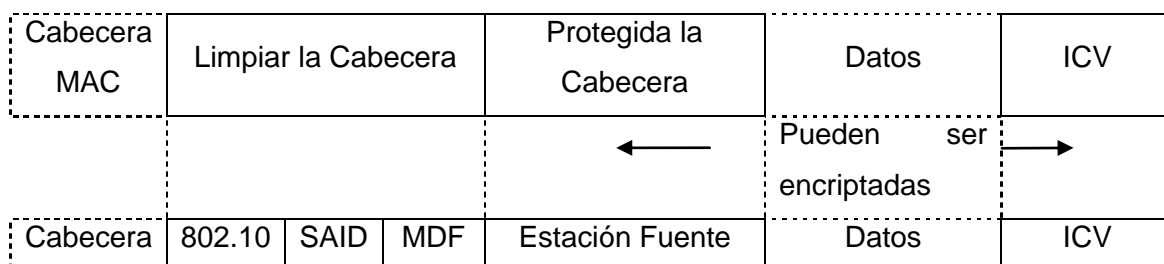
Como las tecnologías de VLAN han avanzado notablemente, es necesaria la estandarización de las VLAN.

En base a esto se originaron las siguientes normas:

- 802.10 " VLAN normal", en 1995 la CISCO Sistemas propuso el uso de IEEE 802.10 que se estableció originalmente en LAN que serviría de garantía para las VLANs. CISCO intentó tomar a la 802.10 con un título optativo de Marco de Estructura y rehusó a llevar a VLAN a la idea de etiqueta en lugar de garantizar la información.
- 802.1 "Internet Working Subcomitte", en marzo de 1996, el IEEE completó la fase inicial de investigación para el desarrollo de una VLAN normal y paso resoluciones de tres emisiones:
 - El acercamiento arquitectónico a VLAN
 - Dirección futura de regularización de VLAN
 - Regularizó el formato de marco de etiqueta.

La IEEE 802,10 incorpora técnicas de la autenticación y del cifrado para asegurar secreto e integridad de los datos a través de la red. El protocolo 802,10 permite a tráfico del LAN llevar un identificador de VLAN, así permitiendo la conmutación selectiva de paquetes.

El switch detectará la identificación de VLAN y remitirá el paquete solamente a las estaciones finales que contienen la misma identificación. Existe una sola unidad de datos de protocolo conocida como intercambio de datos seguro (SDE). Es un marco de la capa del MAC con la cabecera insertada entre la cabecera del MAC y los datos del marco según lo mostrado abajo.



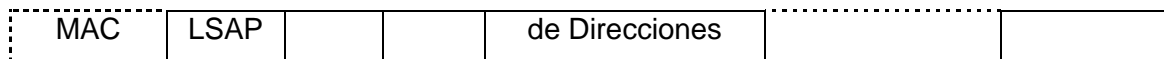


Figura 1.4.- Cabecera MAC.

Fuente: lauca.usach.cl

La cabecera clara incluye un identificador de la asociación de la seguridad (DICHO) y un campo definido gerencia opcional (MDF), que pueden llevar la información para facilitar el proceso de la PDU (Protocol Data Unit). La cabecera protegida repliega el direccionamiento de la fuente contenido en la cabecera del MAC para validar la dirección. Así evitando que otra estación sea identificada como la fuente verdadera.

Las salvaguardias del valor del cheque de la integridad (ICV) contra la modificación interna desautorizada de los datos usando un algoritmo de la seguridad. El cifrado para la cabecera 802,10 es opcional. Los gastos indirectos en la cabecera se pueden reducir al mínimo solamente incluyendo las funciones básicas, es decir, el designador de SDE y la identificación real de VLAN (DICHA).

Cuando una colección arbitraria de subnets de LAN se configura como VLAN, los paquetes nativos que originan las estaciones asociadas a estas LANs adquieren una cabecera 802,10 que contenga la identificación apropiada de VLAN mientras que los paquetes se remiten sobre el backbone.

La propagación de tales paquetes es controlada y contenida solamente por otras LANs dentro de la misma topología virtual. Esto es logrado por los otros dispositivos del establecimiento de una red en el backbone, que realizan un emparejamiento de la identificación de VLAN.

1.14. IDENTIFICACIÓN DEL PAQUETE

Los acercamientos más comunes para lógicamente agrupar a utilizadores en VLANs administrativo definido, incluyen la filtración del paquete y la identificación del paquete. La filtración del paquete es una técnica que examina la información determinada sobre cada paquete basado en definiciones del utilizador. La identificación del paquete asigna únicamente una identificación a cada paquete.

Estas técnicas examinan el paquete cuando es recibida o remitida por el switch. De acuerdo con el conjunto de reglas definidas por el administrador, estas técnicas se determinan donde será enviado el paquete, filtrado, y/o difundido.

Un vector de filtración se desarrolla para cada switch. Esto proporciona a un alto nivel del control de administración, porque puede examinar muchos atributos de cada paquete. Los encargados de red pueden agrupar a utilizadores basados sobre direccionamientos de estación del MAC, tipos del protocolo de capa de red, o tipo de la aplicación.

Las entradas del vector se comparan con los paquetes filtrados por el switch. El switch toma la acción apropiada basada en las entradas. El paquete que se filtra típicamente proporciona a una capa adicional del interruptor que procesa antes de la expedición cada paquete a otro switch dentro de la red

VLAN usa la técnica de la identificación del paquete, pone un único identificador en el título de cada paquete se reenvía en todo el tejido del switch. El identificador es detectado y examinado por cada switch, identificando los broadcast o cualquier transmisión de otros switch routers, u otros aparatos.

Cuando el paquete termina el proceso, el switch quita el identificador, después el paquete es transmitido a la estación final.

1.15. IMPLEMENTACIONES

Para tener redes virtuales que se puedan extender en diferentes ciudades incluso países se hace necesario la interconexión de los switch entre si, a esta interconexión es a lo que se le denomina el backbone, y este se puede implementar de diferentes

formas. De otro lado, es necesario resolver como se efectuará la comunicación de las VLANS entre si y qué solución será mas económica y rápida.

1.15.1. VLANS CON BACKBONE EN ATM

Combinando VLANs con redes ATM se crea una arquitectura de red que está directamente relacionada con el concepto de emular LANS en ATM denominadas ELANS, por esta razón hay que comprender éste concepto.

1.15.1.1. EMULACIÓN DE LANS (ELANS):

Cuando se tienen redes locales (LANs) los equipos funcionan con esta tecnología, al introducir tecnología ATM, la red se convierte en una mezcla de 2 tecnologías: por un lado una tecnología orientada a no conexión, que es el caso de las LANS y por el otro una orientada a conexión como en el caso de ATM. En el caso de las LANS se trabaja con direcciones MAC, mientras en ATM se usan direcciones ATM y se establecen circuitos virtuales permanentes (PVCs), por esta razón se requiere hacer cambios de direcciones MAC a ATM.

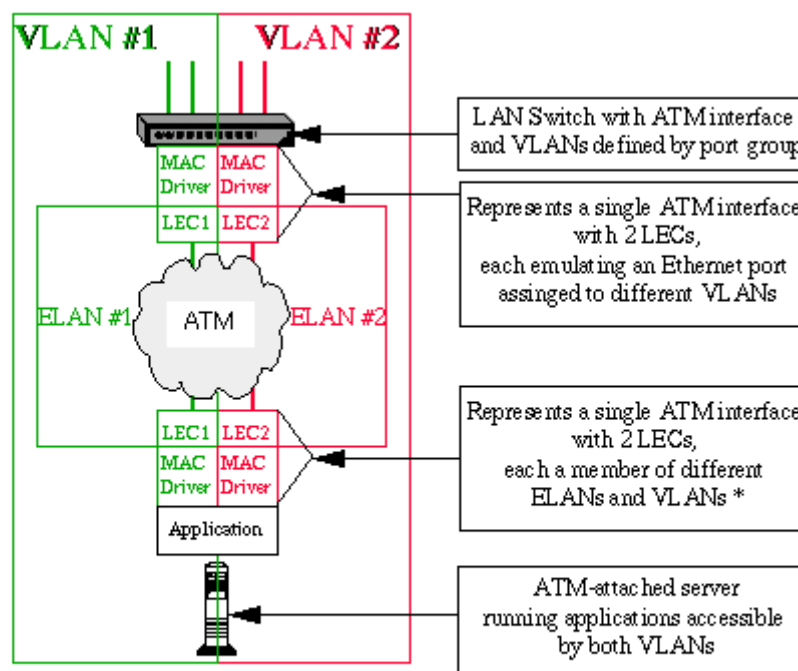
1.15.1.1.1. COMO FUNCIONA UNA ELAN

El switch LAN recibe una trama de un estación conectada a una red Ethernet, esta trama se dirige hacia otra estación Ethernet por el backbone ATM, la red Ethernet esta conectada al switch LAN, y este a su vez deberá conectarse con un switch ATM para que la trama viaje por el backbone hasta su destino, en esta conexión deberá existir un dispositivo que haga el cambio de formato de trama.

Este dispositivo que se ubica en el switch LAN se le conoce como LEC, el LEC (Emulador de Clientes LAN) envía un requerimiento a el LES (Emulador de Servidor LAN) que se ubica en el Switch ATM para conocer la dirección ATM correspondiente a la trama MAC enviada.

El LES envía una dirección Multicast a todos los otros LECS conectados a la red, preguntando a quien se dirige la trama MAC. Solamente el LEC cuya dirección corresponda, le responde al LES.

El LES envía una dirección broadcast con la respuesta, a todos los demás LECS. El LEC original reconoce esta respuesta y aprende la dirección ATM estableciendo un circuito virtual, esto es, toda la comunicación que realice con la estación lejana se hará por ese mismo circuito virtual, lo que quiere decir que se ha establecido la conexión.



* Note: Each LEC on a single ATM interface must be on separate ELANs. However, they are on separate VLANs only because their corresponding LECs on the ATM switch have been assigned explicitly to different VLANs.

Figura 1.5.- ATM Interfase

Fuente: lauca.usach.cl

Ahora, cuando se tiene una VLAN definida por puertos de switch, la interfase del switch con ATM será tratada del mismo modo que un puerto Ethernet cualquiera; es decir, en un lado de la red se conecta el switch que; manejará las VLANS, éste switch para poder conectarse al backbone ATM requerirá un LEC, uno por cada red virtual (VLAN) y al otro lado de la red podrán existir switches LAN o switches ATM.

Con ATM se obtiene una conexión donde los paquetes que van de un punto a otro usan el mismo camino. Es importante anotar que un único dispositivo ligado a la red

ATM podrá pertenecer a diferentes VLANS si cuenta con varios LECS, es decir, se presenta superposición.

La superposición permite que diferentes VLANS accedan a un mismo recurso por ejemplo una impresora sin necesidad de comunicarse entre ellas, así pues con un backbone ATM diferentes VLANS podrán acceder a un mismo servicio solamente usando switches (ya se sabe que ATM se basa en conmutación de switches) y no se requerirán routers, sino, en algunos casos donde las VLANS tengan que estar completamente separadas.

1.16. EL BENEFICIO DE IMPLEMENTAR UNA VLAN

Entre las ventajas de esta topología virtual están las siguientes:

- Reducción de costos de cambios y movimientos de los usuarios.
- Grupos de trabajo virtuales.
- Reducción del enrutamiento

1.16.1. REDUCCIÓN DE COSTOS DE CAMBIOS Y MOVIMIENTOS DE LOS USUARIOS.

La principal excusa para implementar una VLAN es la reducción en el coste de los cambios y movimientos de usuarios. Desde que estos costes son bastante sustanciales, este argumento es suficientemente obligatorio para la implementación de una VLAN.

Muchos fabricantes están prometiendo que la implementación de una VLAN resultará más conveniente a la hora de habilitar la administración de redes dinámicas, y que esto supondrá bastante ahorro. Esta promesa se puede aplicar con buenos resultados a redes IP, ya que, normalmente, cuando un usuario se mueve a una diferente subred, las direcciones IP han de ser actualizadas manualmente en la estación de trabajo.

Este proceso consume gran cantidad de tiempo que podría ser aprovechado para otras tareas, tales como producir nuevos servicios de red. Una VLAN elimina ese hecho, porque los miembros de una red virtual no están atados a una localización física en la red, permitiendo que las estaciones cambiadas de sitio conserven su dirección IP original.

Sin embargo, cualquier implementación de VLAN no reduce este coste. Una VLAN añade una nueva capa de conexión virtual que ha de ser administrada al mismo tiempo que la conexión física. Esto no quiere decir que no se puedan reducir los costes hablados anteriormente. Sólo que no hay que precipitarse a la hora de implementar una VLAN y es mejor estar bien seguro de que la solución no genera más trabajo de administración de red que el que se pueda ahorrar.

1.16.2. GRUPOS DE TRABAJO VIRTUALES.

Uno de los objetivos más ambiciosos de una red virtual es el establecimiento del modelo de grupos de trabajo virtuales. El concepto es que, con una completa implementación de una VLAN a través de todo el entorno de red del campus, miembros del mismo departamento o sección puedan aparentar el compartir la misma red local, sin que la mayoría del tráfico de la red esté en el mismo dominio de broadcast de la VLAN. Alguien que se mueva a una nueva localización física pero que permanezca en el mismo departamento se podría mover sin tener que reconfigurar la estación de trabajo.

Esto ofrece un entorno más dinámicamente organizado, permitiendo la tendencia hacia equipos con funciones cruzadas. La lógica del modelo virtual por grupos de trabajo va la siguiente forma: los equipos pueden estar conectados virtualmente a la misma LAN sin necesidad de mover físicamente a las personas para minimizar el tráfico a través de una red troncal colapsada. Además, estos grupos serán dinámicos: un equipo destinado a un proyecto puede ser configurado mientras dure ese proyecto, y ser eliminado cuando se complete, permitiendo a los usuarios retornar a sus mismas localizaciones físicas.

1.16.3. SEGURIDAD.

El único tráfico de información en un segmento de un sólo usuario será de la VLAN de ese usuario, por lo que sería imposible "escuchar" la información si no nos es permitida, incluso poniendo el adaptador de la red en modo promiscuo, porque ese tráfico de información no pasa físicamente por ese segmento.

1.17. VLANs Y ATM. PROBLEMAS Y SOLUCIONES.

Aunque el concepto de VLAN fue originado a partir de la conmutación LAN, su empleo puede también ser extendido a entornos donde están presentes redes ATM (modo de transferencia asíncrono - asynchronous transfer mode -); eso sí, siempre que se esté dispuesto a hacer frente a nuevos problemas, como las relaciones entre VLAN y LAN emuladas ATM (ELAN - emulated local área network -) y la determinación de dónde situar la función de encaminamiento o routing.

En una red troncal con VLAN que afectan a varios conmutadores LAN, éstos determinan dónde han sido originadas las tramas, En un entorno donde ATM sólo está presente en la troncal (es decir, no hay estaciones finales conectadas a ATM), es posible establecer circuitos virtuales permanentes ATM (PVC -permanent virtual circuit) en una malla lógica para transportar tráfico interno de la VLAN entre esos múltiples conmutadores LAN. En estos escenarios, cualquier técnica propietaria empleada por el fabricante resulta transparente a la troncal ATM, pues los conmutadores ATM no precisan estar capacitados explícitamente para soportar VLAN.

Pero la verdad es que el escenario arriba descrito refleja la realidad de muy pocos entornos. En general, las organizaciones que implantan troncales ATM también desean conectar directamente a ellas estaciones de trabajo, o más probablemente, servidores. Y en cuanto una estación final lógica se conecta vía ATM, aparece un mayor nivel de complejidad: para permitir la comunicación entre estaciones finales conectadas a ATM y no conectadas a ATM es preciso introducir LAN Emulation (LANE).

Con la introducción de estaciones finales a ATM, la red se convierte en un verdadero entorno mixto, con redes LAN no orientadas a conexión, como Ethernet, Token Ring o FDDI, y ATM orientado a conexión. Este entorno deja en el lado ATM de la red la responsabilidad de emular las características de broadcast (envío) y se encarga de la conversión de direcciones de MAC a ATM.

La especificación LANE, detalla cómo se efectúa la emulación en un entorno multifabricante. LANE especifica un servidor de LANE (LES-LAN emulation server) que puede ser incorporado a uno o más conmutadores o a una estación de trabajo para proporcionar conversión de direcciones MAC - ATM en conjunción con clientes LANE (LEC - LAN emulation client), los cuales son incorporados a los conmutadores de extremo y tarjetas de red ATM.

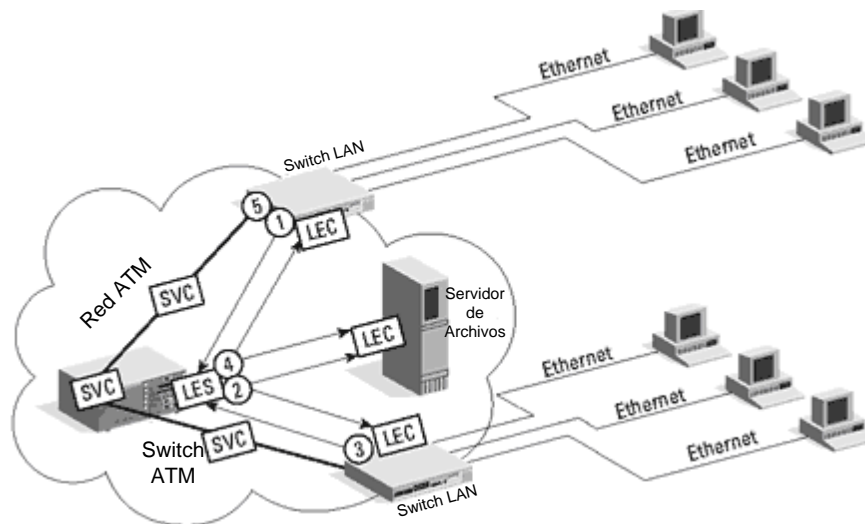


Figura 1.6.- LAN Emulation

Fuente: Emagister.com

Teniendo en cuenta el camino que ha de seguir el tráfico entre un cliente conectado a Ethernet y un servidor conectado a ATM, la sección controlada por LANE se extiende desde el LEC de la interfaz ATM del conmutador LAN al LEC residente en la tarjeta ATM del servidor. Desde el punto de vista de cualquiera de los dos controladores MAC, las tramas pasan directamente entre ellos como si estuvieran conectados por una troncal no ATM.

Las VLAN definidas por grupos de puertos tratan la interfaz ATM del conmutador LAN justo como otro puerto Ethernet, y, por tanto, todos los dispositivos conectados a ATM son miembros de esa VLAN. De esta manera, las VLAN podrían ser desplegadas con independencia de cuál sea el fabricante de los conmutadores ATM de la troncal. Sin embargo, desde una perspectiva administrativa, es posible que muchas organizaciones no deseen emplear software de gestión diferente para la troncal ATM por lo que se decantarán por adquirir tanto los conmutadores LAN como los ATM al mismo proveedor.

LANE permite, además, crear múltiples ELAN mediante el establecimiento de más de un LEC en las interfaces ATM de los dispositivos, así como un LES distinto para cada ELAN. Cada LEC de la interfaz ATM del conmutador LAN es tratado como un puerto Ethernet lógico distinto, y cada LEC de un dispositivo conectado a ATM es visto como una distinta estación final conectada a Ethernet. En consecuencia, múltiples LEC de un dispositivo conectado a ATM pueden ser miembros de diferentes VLAN,

permitiendo a estas VLAN solapar los dispositivos conectados a ATM. Como LANE soporta sólo los dispositivos conectados a ATM, mientras que las VLAN son definidas tanto por los dispositivos de red ATM y no ATM, éstas pueden ser vistas como superconjuntos de ELAN.

Existen cuatro distintas soluciones para tratar el routing entre VLANs en entornos mixtos ATM/LAN. Las diferencias entre ellas se encuentran en la funcionalidad de routing:

- Edge Routing (encaminamiento de extremo o periférico). Básicamente, este enfoque establece que la función de encaminamiento a través de la troncal ATM recaer en el conmutador LAN situado en el extremo de la misma. El tráfico entre VLAN puede ser conmutado a través de la troncal ATM con un retardo mínimo, mientras que los paquetes entre VLAN son procesados por la función de encaminamiento integrada en el conmutador.
- One-armed router. Este concepto elimina la función de routing de los caminos de datos primarios, que consumen mayor procesamiento y tienen una mayor latencia. Un one-armed router se establece fuera del conmutador de la troncal ATM con un solo enlace ATM, permitiendo a los paquetes que no necesitan atravesar el router pasar a través de la troncal ATM sin impedimentos.

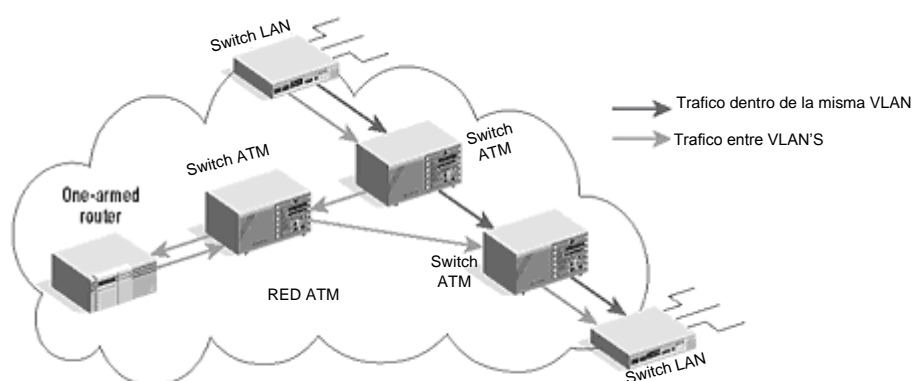


Figura 1.7.- One-armed router.

Fuente: Emagister.com

- Route Server. Este modelo es "físicamente" similar al anterior, pero "lógicamente" difiere en que divide la función de encaminamiento en partes distribuidas. En una configuración one-armed router, un paquete de una VLAN A que se dirige a una VLAN B es enviado al router, donde espera para resolver

la conversión de direcciones, el cálculo de ruta, establecimiento de conexión a través de la troncal ATM y, finalmente, transmisión. En un esquema de servidor de ruta, el mismo paquete espera en el caché del conmutador LAN del extremo de la troncal ATM antes de la transmisión. En este proceso, el paquete por sí mismo nunca atraviesa un router. El único tráfico es la señalización para establecer una conexión entre conmutadores LAN a través de la troncal ATM.

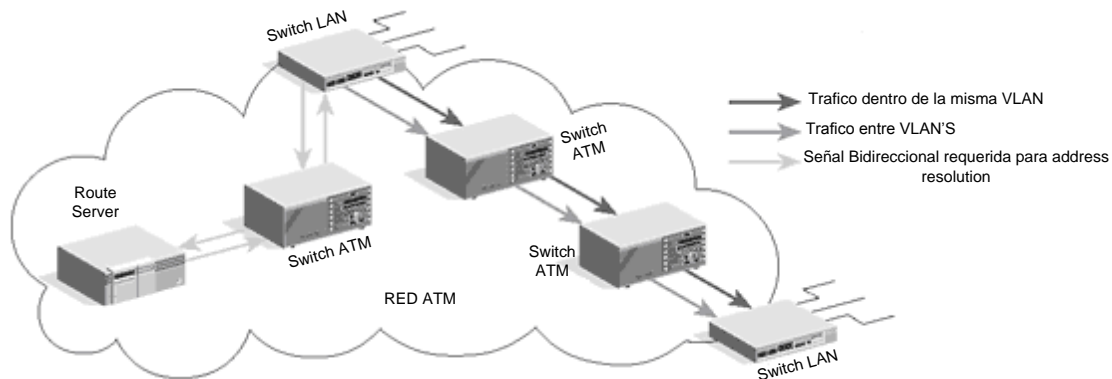


Figura 1.8.- Route server.

Fuente: Emagister.com

- Multiprotocol over ATM (MPOA). Actualmente se está trabajando en el diseño de un modelo de implementación para servicios MPOA que proporcione circuitos virtuales directos entre dispositivos conectados ATM que pueden pertenecer a diferentes subredes de routing. Como las ELAN son subconjuntos de VLAN, MPOA permitirá a una troncal ATM conectar VLAN sin la necesidad de un router externo.

1.18. FUTURO DE LAS ARQUITECTURAS VLAN

Existen dos futuros inmediatos para las VLANs: Implementaciones infraestructurales de VLANs e Implementaciones de VLAN basadas en el servicio.

1.18.1. IMPLEMENTACIONES INFRAESTRUCTURALES DE VLANS

Se basa en la estrategia tradicional de las VLANs, el formar grupos de trabajo de acuerdo a como están distribuidas las organizaciones. Cada grupo, departamento o

sección tiene unívocamente definida su VLAN, basado a en la regla del 80/20, es decir, se asume que la mayoría de tráfico se da dentro de la VLAN.

Normalmente existirán sobrelapamientos al acceder fuentes comunes a todas las VLAN, lo cual se resolverá al ubicar estos recursos en servidores; esto evita que se empleen Routers para poder controlar el tráfico al acceder estos recursos.

Esto incluye todas las ventajas que pueda tener este tipo de implementación: Administración sencilla y centralizada, permite mantener fronteras organizacionales discretas, Bajo costo de desarrollo, Buen grado de privacidad y Permite alcanzar una alta eficiencia de la red.

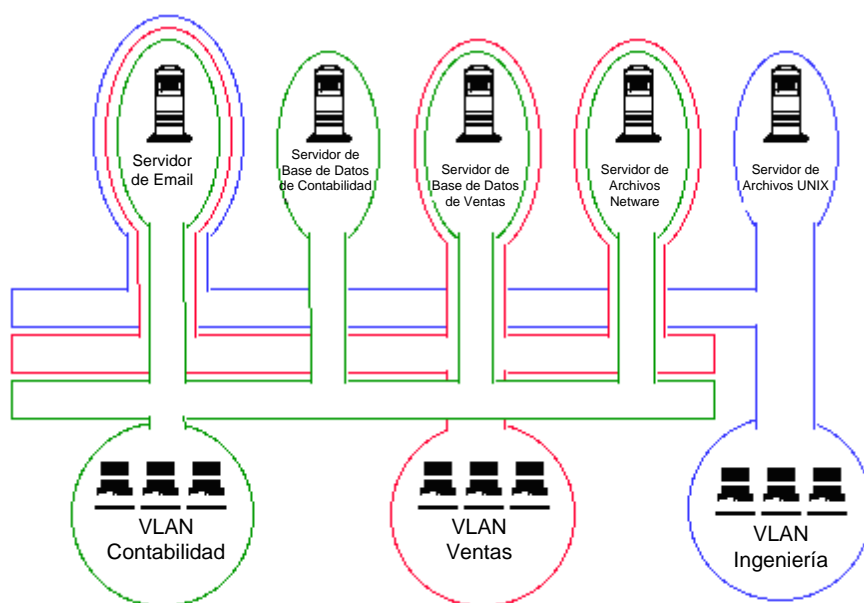


Figura 1.9.- Implementaciones Infraestructurales De Vlans.

Fuente: lauca.usach.cl

1.18.2. IMPLEMENTACIÓN BASADA EN EL SERVICIO

En esta clase de aproximación, no se tienen grupos o algo similar, cada VLAN presta un servicio, es responsable de administrar un recurso específico y ningún servidor podrá pertenecer a múltiples VLANs.

A diferencia de los usuarios que accederán a servicios de correo, bases de datos, aplicaciones, etc. a través de una VLAN independiente. Por naturaleza, esta clase de

implementación, más dinámica que la anterior, posee serios inconvenientes para administrar la memoria a cada VLAN.

Esto conlleva a un alto grado de automatización en la configuración de las VLANs. Las VLANs perderán la característica estática o semi-estática de dominios previamente definidos, para cambiar a canales a los cuales suscribirse. Los usuarios, simplemente ejecutarán determinada aplicación por cierto tiempo, el cual será limitado dependiendo de si la persona posee una cuenta o habilita a pagar por ello. Véase la Figura 1.10

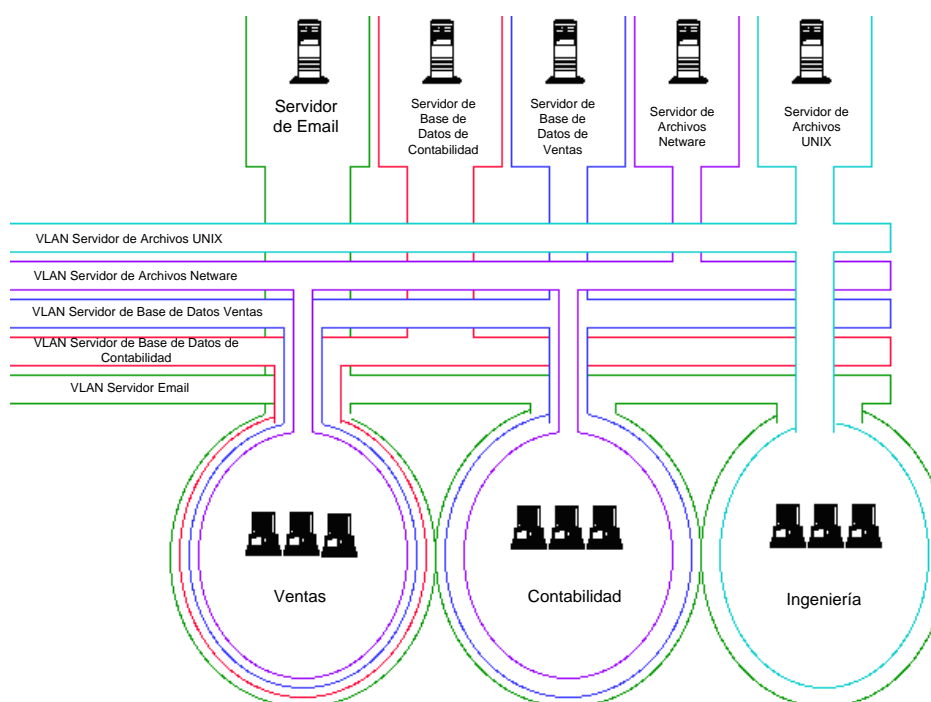


Figura 1.10.- Implementación Basada En El Servicio.

Fuente: lauca.usach.cl

1.19. ENCAPSULACIÓN DE VLAN (ISL INTER SWITCH LINK)

ISL es un protocolo de propiedad de Cisco para interconectar múltiples switches manteniendo la información del viaje de tráfico de VLAN a través de los enlaces truncados.

ISL esta conformado por 3 componentes muy importantes: una cabecera, el frame original de Ethernet y un frame verificador de secuencias (FCS frame check sequence) al final. Con ISL, un frame de Ethernet es encapsulado con una cabecera que transporta la ID de la VLAN entre los switches y los routers. Los 26 bytes de la

cabecera contienen 10 bits de ID de la VLAN es añadido a cada frame. Adicionalmente una cola de 4 bytes es añadido a un frame al funcionamiento de una redundancia cíclica (CRC). Este CRC está verificando que el frame de Ethernet funcione además con cualquier frame. Véase en la Figura 1.11

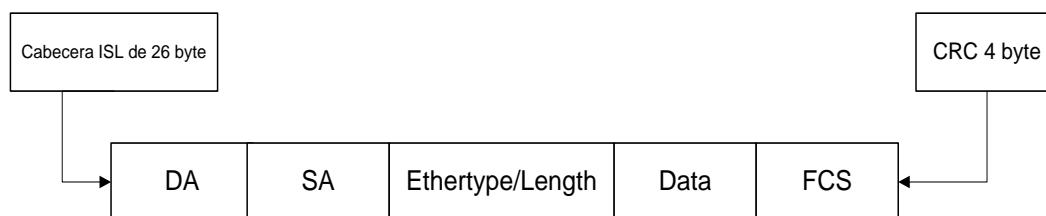


Figura 1.11.- El frame ISL identificación técnica añadiendo 30 Bytes a frame de Ethernet Estándar

Fuente: Cisco Company

- DA = Dirección del destinatario
- SA = Origen de Dirección
- FCS = Frame de Verificación de secuencias

Una ID de una VLAN es añadido solo si el frame es enviado fuera del puerto configurado como un enlace troncado. Si el frame es enviado fuera de un puerto configurado como enlace de acceso, la encapsulación ISL es removida.

En la Figura 1.11 se presenta los 30 bytes adicionales al frame de Ethernet por la encapsulación de ISL. Esto es importante para notar que el frame de Ethernet no es modificado en una sola vía. Los FCS al final de la encapsulación ISL en la Figura 1.12 es una adición al FCS original del frame de Ethernet.

40 Bits	4 Bits	4 Bits	48 Bits	16 Bits	24 Bits	24 Bits	15 Bits	1 Bit	16 Bits	16 Bits	Variable length	32 Bits
DA	TYPE	USER	SA	LEN	SNAP/LLC	HSA	VLAN ID	BDPU/CDP	INDX	Reserved	Encapsulated Frame	FCS (CRC)

Tabla 1.3.- Formato del Frame ISL

Fuente: Cisco Company

La siguiente sección provee las descripciones de los campos de la encapsulación ISL de la Figura 1.12.

Dirección del Destinatario (DA).- La dirección de destinación multicast y se fija en 01.00.0c.00.00. Los primeros 40 bits del campo de DA señalan el receptor que este es un frame ISL.

Tipo Frame.- El campo tipo indica el tipo de frame que es encapsulado y puede ser usado en el futuro para indicar un tipo de encapsulamiento alternativo. Los siguientes son definiciones de diversos códigos de TIPO:

- 0000 Ethernet;
- 0001 Token Ring;
- 0010 FDDI;
- 0011 ATM.

Usuario definido por bits (USER).- Los bits del usuario se utilizan para ampliar el significado del campo TIPO. Por ejemplo, los frame token ring pueden tener más de un tipo. El USER por defecto tiene valores de 0000. Para los frames de Ethernet, 2 campos ya han sido definidos. Para los frame de Ethernet los bits son "0" y "1" indicando la prioridad del paquete a través del switch. Siempre que el tráfico se pueda manejar de una manera que permita que sea remitido más rápidamente, los paquetes que tienen un bit ya definido puede tomar ventaja de una trayectoria más rápida. No se requiere que tales trayectorias sean suministradas.

Código	Significado
XX00	Prioridad normal
XX01	Prioridad 1
XX10	Prioridad 2
XX11	Alta prioridad

Tabla 1.4.- Prioridad para los códigos de USER

Fuente: Cisco Company

Dirección de la Fuente (SA).- El campo del SA es el campo de dirección de la fuente del paquete del ISL. Puede ser fijado por el MAC Address "802.3" del puerto de transmisión del frame del switch. Este es un valor 48 bit. El dispositivo de recepción puede no hacer caso del campo del SA.

LEN - Longitud.- El campo de LEN almacena el tamaño del paquete verdadero del paquete original como valor 16 bit. El campo de LEN representa la longitud del paquete en bytes excepto los campos de DA, TIPO, USER, SA, LEN, y del FCS. La longitud total de los campos excluidos son 18 bytes, así que el campo de LEN representa la longitud total menos 18 bytes.

SNAP/LLC.- El campo SNAP tiene un valor constante de 24 bits 0xAAAA03

HSA - Bits altos de la dirección de la fuente.- El campo de HSA tiene un valor de 24 bit. Este campo representa los tres bytes superiores (fabrica la porción de la identificación) del campo SA. Debe contener el valor "0x00-00-0C."

VLAN - Identificación VLAN.- El campo de VLAN es el paquete virtual de la ID LAN. Es un valor de 15 bit que es usado para distinguir frames de diferentes VLANs. Este campo se refiere a menudo como el "color" del paquete.

BPDU Bridge Protocol Data Unit (BPDU) and Cisco Discovery Protocol (CDP) Indicator.- El bit en el campo de BPDU se fija para todos los paquetes de BPDU que sean encapsulados por el frame del ISL. El BPDUs es usado por el algoritmo Spanning Tree para determinar la información que atraviesa la topología de la red.

INDX - Índice.- El campo de INDX indica el puerto index de origen del paquete cuando sale del switch. Se utiliza para el propósito de diagnóstico solamente, y se pueden fijar a cualquier valor por otros dispositivos. Tiene un valor 16 bit y se no hace caso en paquetes recibidos.

Reservado para Token Ring y el Fiber Distributed Data Interface (FDDI).- El campo RES tiene un valor 16 bit. Se utiliza este campo cuando los paquetes del token ring o del FDDI se encapsulan con un frame del ISL. En el caso de los frames de token ring, el control de acceso (CA) y el campo frame de control (FC) son colocados aquí. En el caso de FDDI, el campo de FC es colocado en el byte menos significativo (LSB) de este campo (como en un FC de "0x12" podría tener un campo del RES de "0x0012"). Para los paquetes de Ethernet, el campo RES puede ser fijado todos los ceros.

Frame Encapsulados.- El campo del frame Encapsulado es el paquete de datos encapsulado, incluyendo su propio valor de control por redundancia cíclica (CRC),

totalmente sin modificar. El frame interno debe tener un valor del CRC que sea válido una vez que el campo de encapsulación del ISL sea removido. La longitud de este campo puede ser de 1 a 24575 bytes de largo para acomodar Ethernet, Token Ring y frame de FDDI. Un switch de recepción puede dismantelar los campos de la encapsulación de ISL, y utiliza el campo frame de encapsulamiento como frame es recibido (asociando la VLAN apropiada y otros valores con el frame recibido como indica los propósitos del switch).

FCS - Secuencia Del Cheque Del Marco.- El campo del FCS consta de cuatro bytes. Esta secuencia contiene un valor 32 bit de CRC, que es creado para transmitir MAC y es recalculado por el MAC de recepción para comprobar si hay frame dañados. El FCS se generado sobre el DA, SA, Tipo/Longitud, y campo de datos. Cuando la cabecera ISL es ajuntada, un nuevo FCS es calculado sobre el paquete ISL entero y agregado al final del frame.

Nota: La adición del nuevo FCS no altera el FCS original que se contiene dentro del frame encapsulado.

CAPÍTULO II

CALIDAD DE SERVICIO EN UNA RED

2.1. INTRODUCCIÓN

La calidad del Servicio (QoS) se refiere a la capacidad de una red para proporcionar mejor servicio al tráfico escogido de la red sobre varias tecnologías, inclusive Frame Relay, Modo de Transferencia Asíncrono (ATM), Ethernet, redes 802,1, SONET, y las redes IP-Router que pueden utilizar cualquier o todas estas tecnologías. La meta primaria de QoS deberá proporcionar la prioridad inclusive ancho de banda dedicada, la inestabilidad y estado latente controlados (requerido por algún tiempo real y el tráfico recíproco), y características mejoradas de pérdida. También es importante cerciorarse de proporcionar la prioridad para uno o más flujos para que los otros flujos no fallen. Las tecnologías de QoS proporcionan los componentes elementales que se utilizarán para aplicaciones futuras de negocio en el campus, WAN, y las redes de proveedor de Internet. Este capítulo resume las características y los beneficios del QoS proporcionado por el IOS QoS.¹

El software IOS QoS permite a redes complejas controlar y atender previsiblemente una variedad de aplicaciones y tipos de tráfico. Casi cualquier red puede aprovecharse de QoS, si es una red corporativa pequeña, un proveedor de servicios Internet, o una red de la empresa. El software IOS QoS proporciona estos beneficios:

El control sobre recursos

Usted tiene el control sobre los recursos (ancho de banda, el equipo, las facilidades de ancho-área, etcétera) son utilizados. Por ejemplo, usted puede limitar el ancho de banda consumida sobre una conexión de elemento principal por transferencias de FTP o da la prioridad a un acceso importante de la base de datos.

- **El uso más eficiente de la administración del análisis de la red de recursos.** Usando una red e instrumentos de contabilidad, usted sabrá lo que en su red se utiliza y estará preparado para atender el tráfico más importante de la red.

¹ **Nota:** El flujo se puede definir de varias maneras. Cualquier paquete de una cierta aplicación o de una comunicación entrante. Los instrumentos recientes de identificación han permitido la definición de un flujo para ser realizada más precisamente (por ejemplo al URL o de tipo MIMO dentro de un paquete de HTTP). Dentro de este capítulo, las referencias a un flujo podrían ser cualquiera de estas definiciones

- **Atender hecho a la medida.** El control y la visibilidad proporcionados por QoS permiten a proveedores de servicios de Internet a ofrecer grados de seguridad hechos a la medida de la diferenciación del servicio a sus clientes.
- **La coexistencia de aplicaciones de misión crítica.** QoS se asegura de que su WAN sea utilizada eficientemente por las aplicaciones de misión crítica que es muy importante en su negocio, esas demoras de ancho de banda, tiempo mínimo sensible requerido para multimedia, las aplicaciones de voz estén disponible, y que otras aplicaciones que utiliza la conexión obtiene su servicio justo sin intervenir con el tráfico de misión crítica.
- **La base para una red completamente integrada en el QoS futuro.** Implementación de tecnología en su red puede ser ahora un primer paso hacia la red multimedia completamente integrada necesaria a un futuro próximo.

2.2. DEFINICIÓN DE QOS

Para establecer una correcta definición del término QoS, calidad de servicio, debemos acudir primero a estudiar la asignada por el Diccionario de la Lengua de la Real Academia Española. Según éste, la Calidad es el “Valor intrínseco de una cosa y el valor relativo resultante de compararla con otras de su misma categoría”. Así mismo Servicio es “La acción y el efecto de servir. Estar hecho para algo concreto”. Las dos definiciones llevan contenidas de forma inherente la propiedad de comparación; por lo tanto, para determinar si un servicio ofrece mayor o menor calidad será necesario establecer una comparación con el resto de servicios de ese nivel.

Al tratarse la anterior de una descripción demasiado genérica, son múltiples las definiciones concretas que actualmente se realizan sobre el término QoS, si bien difieren en significados dependiendo del ámbito de aplicación de tales siglas. En el ámbito de las telecomunicaciones, desde la publicación en 1984 del documento E-800 de la UIT, no debería existir discusión posible ante su definición: “el efecto colectivo del rendimiento de un servicio que determina el grado de satisfacción del usuario de dicho servicio”. Es una definición comúnmente aceptada, que no deja ninguna duda de que se trata de una percepción del usuario, pues es éste quién, al final, establece unos requerimientos mínimos para cualificar.

En el ámbito de la telemática, QoS es la capacidad de un elemento de red (bien una aplicación, un servidor, un router, un switch, etc.) de asegurar que su tráfico y los

requisitos del servicio previamente establecidos puedan ser satisfechos. Habilitarla requiere además la cooperación de todas las capas de la red, así como de cada elemento de la misma. Desde este punto de vista, la QoS también suele ser definida como un conjunto de tecnologías que permiten a los administradores de red manejar los efectos de la congestión del tráfico usando óptimamente los diferentes recursos de la red, en lugar de ir aumentando continuamente capacidad. En este punto es necesario prestar una atención especial al hecho de que la QoS no crea ancho de banda.

La QoS tiene, básicamente, cuatro variantes estrechamente relacionadas:

- La QoS que el usuario desea,
- La que el proveedor ofrece,
- La que el proveedor consigue realmente y la que,
- Finalmente, percibe el usuario.

En cualquiera de ellas existen algunos parámetros que están muy condicionados por las características técnicas de la red soporte, y por eso el primer Informe técnico que publicó, en 1994, el ETSI fue la ETR-003, "General Aspects of Quality of Service (QoS) and Network Performance (NP)", atendiendo a las inquietudes surgidas en el seno de FITCE, que tuvieron su reflejo oficial en los acuerdos de la reunión de Estrasburgo, de 1991, poniendo en marcha los estudios que permitiesen definir los parámetros técnicos de la red, a partir de los requisitos de los usuarios. La metodología resultante es la que se refleja en el documento de ETSI, antes citado.

2.2.1. QoS, CoS y ToS

Son varios los acrónimos terminados en "oS" que hacen referencia a la obtención de calidad de servicio en redes, llevando en ocasiones a situaciones equívocas por el mal uso de los mismos, si bien QoS es el único que refiere completamente a la Calidad de Servicio, englobando todas las técnicas que se encuentran en torno a ella, mientras que CoS (clase de servicio) y ToS (tipo de servicio) son, sencillamente, dos de las técnicas utilizadas para su obtención. Veamos pues, una diferenciación más exhaustiva

2.2.2. QoS: CALIDAD DE SERVICIO

Recoge varios parámetros o atributos que describen un servicio, tales como:

- Reserva ancho banda
- Retardo extremo a extremo
- Jitter
- Tasa de error

2.2.3. CoS: CLASE DE SERVICIO

Este término implica, a su vez, dos procedimientos: en primer lugar la priorización de los distintos tipos de tráfico claramente definidos a través de la red y, en segundo lugar, la definición de un pequeño número de clases de servicio.

Priorizar es importante en los puntos de congestión de la red, donde las decisiones de priorización pueden ser realizadas por puentes y encaminadores.

Las aplicaciones que requieren distinguir clases de servicio incluyen procesos transaccionales, el vídeo y cualquier otro tráfico sensible al tiempo.

No se debe confundir CoS con QoS, pues, a diferencia de QoS, CoS no garantiza ancho de banda o latencia, en cambio permite a los administradores de red solicitar prioridad para el tráfico basándose en la importancia de éste.

Independientemente de la diferenciación, tanto CoS como QoS categorizar el tráfico para asegurar que el tráfico considerado crítico siempre fluya por la red, a pesar del ancho de banda demandado o de las aplicaciones de menor importancia.

Existen muchas posibles definiciones de tipos de calidad de servicio, pero la mayoría de las empresas definen las clases de tráfico por tipo de aplicación, tipo de dispositivo o por tipo de usuario. Hoy es además posible definir clases separadamente en routers o puentes individuales, pero suele ser poco práctico.

Un claro ejemplo de tecnología que usa CoS es el estándar **IEEE 802.1p**

2.2.4. TOS: TIPO DE SERVICIO.

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

ToS está incluido como uno de los campos en la tecnología de QoS denominada Diffserv (servicios diferenciados), dónde también es conocido como DiffServ codepoint (DSCP o punto de código Diffserv). Es un campo de 8 bits, estando los dos últimos reservados. Con los otros 6 bits restantes es posible obtener 64 combinaciones o 'codepoint', de ellas, 48 son utilizadas para diréccionar el espacio global y 16 son para uso local.

Parte del protocolo IP Versión 4 reserva un campo en el paquete IP para el tipo de servicio (IP TOS). En este campo se pueden especificar los atributos de fiabilidad, capacidad de procesamiento y retardos del servicio.

2.3. ARQUITECTURA BÁSICA DE QoS

La arquitectura básica introduce las tres partes fundamentales para la implementación de QoS:

- **Clasificación.** Estas técnicas identifican qué aplicaciones han generado qué paquetes. Sin clasificación, la red no puede determinar qué hacer con un paquete determinado.
- **Marcación.** Tras su identificación, el paquete se "marca" de modo que otros dispositivos de la red puedan a su vez identificarlo fácilmente. Como este proceso puede resultar intensivo y complejo, sólo debería realizarse una vez.
- **Priorización.** Puesto que la red es capaz de diferenciar, por ejemplo, una conversación telefónica de una navegación Web, la priorización asegura que una gran descarga desde Internet no interrumpa la conversación telefónica.

Todo el tráfico debe ser identificado en la troncal de la red para asegurar la priorización. Un hacker podría marcar deliberadamente un tráfico convencional de una organización como de alta prioridad, sustrayendo ancho de banda al tráfico crítico y causando el caos. Esto es conocido como ataques de denegación de servicio o DoS (Denialof-Service).Analizando todo el tráfico a

medida que entra en la red, los ataques de seguridad pueden ser detectados y detenidos inmediatamente, antes de que causen problemas.

2.4. LOS PROBLEMAS

Se entiende por calidad de servicio la posibilidad de asegurar una tasa de datos en la red (ancho de banda), un retardo y una variación de retardo (jitter) acotados a valores contratados con el cliente. En las redes Frame Relay o ATM la calidad de servicio se garantiza mediante un contrato de CIR (Committed Information Rate) con el usuario. Para disponer de una calidad de servicio aceptable en redes soportadas en protocolo IP se han diseñado herramientas a medida como ser los protocolos de tiempo real RTP y de reservación RSVP. Por otro lado, un problema evidente es que cuando se soporta un servicio de voz sobre IP (VoIP) por ejemplo, los paquetes son cortos y el encabezado es largo comparativamente. En este caso se requiere un encabezado reducido y un proceso de fragmentación e intercalado LFI. Mediante QoS (Quality of Service) se tiende a preservar los datos con estas características.

Los servicios tradicionales de la red Internet (SMTP o FTP) disponen de una calidad denominada "best effort"; es decir que la red ofrece el mejor esfuerzo posible para satisfacer los retardos mínimos; lo cual no es mucho pero es suficiente para servicios que no requieren tiempo-real como el web. Para servicios del tipo "real-time" (voz y vídeo) se requiere una latencia mínima.

LATENCIA JITTER. Se denomina latencia a la suma de los retardos en la red. Los retardos están constituidos por el retardo de propagación y el de transmisión (dependiente del tamaño del paquete), el retardo por el procesamiento "store and forward" (debido a que los switch o router emiten el paquete luego de haber sido recibido completamente en una memoria buffer) y el retardo de procesamiento (necesario para reconocimiento de encabezado, errores, direcciones, etc.). Un tiempo de latencia variable se define como jitter (fluctuación de retardo) sobre los datos de recepción.

La solución al jitter es guardar los datos en memorias buffer, lo cual introduce un retardo aun mayor. Se han implementado diversas formas de buffer garantizados mediante software:

- Cola prioritaria: donde el administrador de la red define varios niveles (hasta 4) de prioridad de tráfico.
- Cola definida: donde el administrador reserva un ancho de banda para cada tipo de protocolo específico.
- Cola ponderada: mediante un algoritmo se identifica cada tipo de tráfico priorizando el de bajo ancho de banda. Esto permite estabilizar la red en los momentos de congestión.

2.5. VARIANTES DE SERVICIOS.

Los servicios de datos y multimediales tienen distintos requerimientos de calidad referido a latencia y jitter. Para satisfacer los requerimientos de calidad se acude al manejo de las colas de paquetes, la reservación de ancho de banda y la gestión del tráfico. Para obtener estos objetivos en diversos ámbitos se han definido variantes de servicios.

En La Tabla 2.1 se encuentran las siguientes variantes de servicios: clase de servicio en redes LAN, tipo de servicio sobre protocolo IP y calidad de servicio sobre redes IP. Por otro lado se han definido las características de la calidad de servicio que se entregan en la misma Tabla: servicio garantizado (mediante reservación de ancho de banda), diferenciado (mediante prioridad de tráfico) y el "mejor esfuerzo".

VARIANTES Y CLASIFICACIÓN: VARIANTES EN CAPA 2, 3 Y 4	
CoS	(Class Of Service) Se logra mediante 3 bits que se ingresan en un campo adicional de 4 Bytes (etiqueta denominado Tag o Label) dentro del protocolo MAC. Estos 3 bits permite definir prioridades desde 0 (máxima) a 7 (mínima) y ajustar un umbral en el buffer de entrada y salida del Switch LAN para la descarga de paquetes. Para más detalles ver el servicio VLAN que es soportado por esta versión de funcionamiento para servicios de capa 2. Se ocupa la IEEE 802.x en los siguientes estándares
IEEE 802.1p	Determina el uso de un Tag en el encabezamiento de MAC con 3 bits de precedencia. Se define el protocolo para registración de CoS GARP (Generic Attribute Registration Protocol). Las aplicaciones específicas del GARP son la registración de direcciones multicast GMRP (Multicast GARP) y de usuarios VLAN con protocolo GVRP

	(LAN GARP).
IEEE 802.1Q	Servicio VLAN para realizar enlaces troncales punto a punto en una red de switch.
IEEE 802.3x	Este estándar examina el control de flujo en enlaces Ethernet del tipo full – duplex. Se aplica en enlaces punto a punto (Fast Gigabit Ethernet). Si existe congestión se hace axial atrás un paquete llamado “pause frame” que detiene la emisión por un periodo de tiempo determinado. Una trama denominada “time to wait zero” permite reiniciar la emisión de paquetes
IEEE 802.1D	Define el protocolo STP (Spanning-Tree Protocol). Se diseñó para permitir que en una red de bridge y switch de muchos componentes se formen enlaces cerrados para protección de caminos. Se intercambia información de la topología de la red que permiten construir el árbol. De esta forma se crean puertas redundantes en el cableado, el protocolo STP deshabilita automáticamente una de ellas y la habilita en caso de falla de la otra. Cada puerto tiene una ponderación en costo (el administrador de la red puede modificar el costo para dar preferencia a cierta puerta).
ToS	(Type of Service). Es sinónimo de CoS en la capa 3. Sobre el protocolo IP se define el ToS con 3 bits (del segundo byte del encabezado IP) para asignar prioridades. Se denomina señal de precedencia.
QoS	(Quality of Service). En redes IP se define la tasa de acceso contratada CAR (Committed Access Rate) en forma similar al CIR de Frame Relay y ATM. La calidad QoS se ve garantizada mediante protocolos de reservación RSVP y de tiempo real RTP que se describen en este mismo capítulo.
CLASIFICACIÓN DE LA QoS	
Guaranteed	El servicio garantizado es utilizado para requerir un retardo máximo extremo a extremo. Se trata de un servicio análogo al CBR (Constant Bit Rate) en ATM. Se puede aplicar un concepto de reservación de tasa de bit (utiliza RSVP) o el método Leaky bucket. Al usuario se le reserva un ancho de banda dentro de la red para su uso exclusivo aún en momentos de congestión. Se lo conoce como Hard QoS.
Differentiated	El servicio diferenciado utiliza la capacidad de particionar el tráfico

	<p>en la red con múltiples prioridades o ToS (Type of Service). Se dispone de 3 bits de precedencia para diferenciar las aplicaciones sensibles a la congestión (se brindan mediante el encabezado del protocolo IPv4). Es por lo tanto un Soft QoS. El control de aplicación es del tipo leaky-bucket. Se puede soportar la función CAR permite un management del ancho de banda (política de tráfico). La primer línea de defensa frente a la congestión es el uso de buffer de datos; lo cual implica el armado de una cola de espera y el retardo correspondiente dependiendo de la prioridad asignada en dicha cola.</p>
Best-effort.	<p>Este es un servicio por default que no tiene en cuenta las modificaciones por la QoS. Se trata de una memoria buffer del tipo FIFO. Por ejemplo, el software Microsoft NetMeeting para aplicaciones multimediales utiliza la norma H.323 (E.164); trabaja sobre redes LAN y redes corporativas. Esta norma no tiene previsto garantizar la calidad de servicio QoS.</p>

Tabla 2.1. Variantes y Clasificación: Variantes en capa 2, 3 Y 4

Fuente: Grupo Investigativo

2.6. IDENTIFICACIÓN DE QoS Y MARCAR

Identificación y marcar se alcanzan por la clasificación y la reservación.

2.6.1. CLASIFICACIÓN

Todas las aplicaciones dejan huellas sobre los paquetes que pueden ser utilizadas para identificar la aplicación fuente.

El proceso de clasificación examina estas huellas y discierne qué aplicación ha generado el paquete.

Los cuatro métodos de clasificación son:

- **Protocolo.** Algunos protocolos, especialmente los utilizados por algunos de los dispositivos más antiguos, son extremadamente “charlatanes” y su sola presencia origina retardos de tráfico; pero estos retardos se pueden minimizar identificando y priorizando datos en función del protocolo. Las aplicaciones pueden ser identificadas por su EtherType. Por ejemplo, AppleTalk utiliza 0x809B e IPX utiliza 0x8137. La priorización basada en este mecanismo representa una buena manera de controlar o detener estos protocolos “charlatanes”.
- **TCP y UDP Socket Number.** Muchas aplicaciones utilizan ciertos sockets UDP para comunicar. Por ejemplo, HTTP utiliza TCP Port 80. Examinando el número de socket del paquete IP, la red inteligente determina qué tipo de aplicación ha generado el paquete. Esta función es conocida como conmutación de Nivel 4 debido a que TCP y UDP pertenecen a la capa 4 del modelo OSI.
- **Source IP Address.** Muchas aplicaciones son identificadas por su dirección Source IP (fuente IP). Como a veces algunos servidores están dedicados exclusivamente a soportar una sola aplicación -correo electrónico, por ejemplo-, el análisis de la dirección Source IP de un paquete permite identificar qué aplicación lo ha generado.

Esto resulta particularmente útil cuando el conmutador identificante no está directamente conectado al servidor de la aplicación y llegan a él diferentes corrientes de datos.

- **Physical Port Number.** Como las direcciones Source IP, el Physical Port Number (número de puerto físico) puede indicar qué servidor está enviando los datos. Esta técnica, que se basa en el mapeado de los puertos físicos en un conmutador a un servidor de aplicación, es la forma más simple de clasificación, pero exige que el servidor esté conectado directamente al conmutador, sin hubs ni conmutadores intermedios.

2.6.2. MARCACIÓN

Una vez identificada la aplicación, el paquete debe ser marcado para asegurar que los conmutadores de la red son capaces de darle prioridad. Para ello se pueden utilizar alguno de estos métodos:

- IEEE 802.1p. Ahora integrado en el estándar de bridging IEEE 802.1D, el esquema IEEE 802.1p asigna a cada paquete un nivel de prioridad entre 0 y 7. Aunque es el método de priorización más utilizado en el entorno LAN, cuenta con varios inconvenientes, como el requerimiento de una etiqueta adicional de 4 bytes. Esta etiqueta viene definida en el estándar IEEE 802.1Q, pero es opcional en redes Ethernet. Además, sólo puede ser soportado en una LAN, ya que las etiquetas 802.1Q se eliminan cuando los paquetes pasan a través de un router.
- Differential Services Code Point (DSCP). DSCP es un esquema de marcación de Nivel 3 que usa la cabecera IP para almacenar la prioridad del paquete. Las principales ventajas de DSCP sobre IEEE 802.1p son que no se precisan etiquetas extras puesto que el paquete usa la cabecera IP y que la prioridad queda preservada a través de Internet. DSCP utiliza 64 valores para definir distintos niveles de servicio en función del usuario.
- IP TOS (Type Of Service). Opera de una manera similar a 802.1p, pero, como DSCP, a Nivel 3, introduciendo tres bits en un subcampo de la cabecera IP para marcar la prioridad, que podrá ser preservada en las WAN.

Cuando se ha de elegir un Switch, es necesario asegurarse que el equipo es capaz de reconocer tanto el esquema de marcación 802.1p como DSCP. Aunque es muy probable que este último acabe reemplazando a 802.1p en la LAN, su despliegue todavía es limitado. Por ello, la interoperatividad con dispositivos 802.1p será esencial aún durante algún tiempo. Conviene, por tanto, decantarse por conmutadores que permitan la conversión entre ambos esquemas como herramienta de migración.

2.7. QoS DENTRO DE UN SOLO ELEMENTO DE LA RED

La administración de la congestión, la administración de la cola, la eficiencia de la conexión, e instrumentos de formar/custodiando proporcionan QoS dentro de un solo elemento de la red.

2.7.1. ADMINISTRACIÓN DE CONGESTIÓN

A causa de la naturaleza de bursty de voz/video/datos, a veces la cantidad del tráfico excede la velocidad de una conexión. ¿En este momento, qué haría el router? ¿Protegerá el tráfico del búfer en una sola cola y permitirá que el primer paquete sea el primer paquete en salir? O, ¿pondrá paquetes en colas diferentes y atenderá ciertas colas más a menudo? Los instrumentos de la administración de congestión dirigen estas preguntas. Los instrumentos incluyen la prioridad haciendo cola (PQ), la custom queuing (CQ), compensado justo haciendo cola (WFQ), y clase-basado compensado justo haciendo cola (CBWFQ).

2.7.2. ADMINISTRACIÓN DE COLA

Porque las colas no son del tamaño infinito, ellos pueden llenar y poder derramarse. Cuando una cola está repleta, un paquete adicional no pueden entrar en la cola y se dejará caer. Esto es una gota en la cola. El asunto con gotas de cola es que el router no puede prevenir que este paquete pueda ser dejado caer (incluso si fuera un paquete de la alta prioridad). Así, un mecanismo es necesario para hacer dos cosas:

1. La prueba para cerciorarse que la cola no esta llena, es que hay el espacio para paquetes de alta prioridad,

2. Permite los criterios de algún tipo para dejar caer paquetes que son de prioridad más baja antes de dejar caer paquetes de más alta prioridad,

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

2.7.3. ENLACE DE EFICIENCIA

Muchas veces las conexiones de baja velocidad presentan un problema para los paquetes más pequeños. Por ejemplo, la demora de la serialización de un paquete de 1500 byte en una conexión de 56 kbps es 214 milisegundos. ¡Si un paquete de voz debía ir detrás de un paquete grande, el presupuesto de retardo para la voz se excedería aún antes que el paquete deje el router. Fragmentación de conexión e interpolación permite que paquetes grandes sean divididos en paquetes más pequeños que interpolan el paquete de voz. Interpolación es tan importante como la fragmentación. No hay razón de fragmentar el paquete y tener el paquete de voz que vaya atrás de los paquetes fragmentados.

La demora de la Serialización es el tiempo que toma para poner un paquete en la conexión. Para el ejemplo dado, se aplican estas matemáticas aplican:

El tamaño del paquete: paquete de 1500 byte * 8 bytes/bits = de 12.000 bits

Línea de tasa: 56.000 bps

El resultado: $12.000 \text{ bits} / 56,000 \text{ bps} = 0,214 \text{ sec}$ o 214 msec

Otra eficiencia es la eliminación de demasiados bits de overhead. Por ejemplo, encabezamientos de RTP tienen un encabezamiento de 40 byte. Con una carga útil de tan poco 20 byte, los gastos indirectos pueden ser dos veces de la carga útil en algunos casos. La compresión de encabezamiento de RTP (conocido también como protocolo de compresión en tiempo real) reduce el encabezamiento a un tamaño más manejable.

2.7.4. FORMACIÓN DE TRÁFICO Y POLÍTICAS

Se utiliza para formar o para crear un flujo del tráfico que limita el potencial del ancho de banda de los flujos. Esto es usado muchas veces para prevenir el problema de capacidad excesiva mencionado en la introducción. Por ejemplo muchas topologías de red utilizan Frame Relay en un hub y un diseño spake. En este caso, el sitio central tiene normalmente una alta conexión de ancho de banda (T1), mientras los sitios remotos tienen una baja conexión de ancho de banda en comparación (384 Kbps). En este caso, es posible para el tráfico del sitio central rebasar el enlace bajo de ancho de banda al final. Formar es una manera perfecta de establecer el tráfico más cercano a 384 Kbps para evitar el desbordamiento de la capacidad excesiva de la conexión remota. El tráfico sobre la tarifa configurada se protege para la transmisión para mantener luego la tasa configurada.

Las Políticas es semejante a formar, pero difiere en una manera muy importante: el Tráfico que excede la tasa configurada no es buffered (y es desechado normalmente).²

2.8. ADMINISTRACIÓN DE QoS

La administración de QoS ayuda a poner y evaluar las políticas y metas de QoS. Una metodología común trae consigo los pasos siguientes:

Paso 1 La Línea base de la red con dispositivos tales como RMON probes. Esto ayuda a determinar las características del tráfico de la red. También, las aplicaciones dirigidas para QoS se deben a la línea base (generalmente en términos del tiempo de respuesta).

Paso 2 Despliegan las técnicas de QoS cuando las características del tráfico se han obtenido y una aplicación (es) ha sido concentrada en QoS aumentado.

Paso 3 Evalúan los resultados probando la respuesta de las aplicaciones dirigidas para ver si las metas de QoS se han alcanzado.

² **Nota:** La implementación de custodiar (CAR) permite un numero de acciones desechar para el performance. Sin embargo, custodiando se refiere normalmente al desecha del tráfico encima de una tasa configurada

Para la comodidad, usted puede utilizar las Políticas de Administración de Calidad (QPM) y la Administración de Dispositivos de Calidad del Servicio (QDM). Para la comprobación de niveles de servicio, usted puede utilizar el Monitor del Desempeño de Internetwork (IPM).

Usted debe considerar que en un ambiente siempre variable de la red, QoS no es un despliegue anterior, es una parte progresiva y esencial del diseño de la red.

2.9. NIVELES DE QoS DE EXTREMO A EXTREMO

Los niveles del servicio se refieren a fin de determinar verdaderamente las capacidades de QoS, significando la capacidad de una red para entregar el servicio necesitado por el tráfico específico de la red de extremo a extremo o borde a borde. Los servicios difieren en su nivel de la severidad de QoS, que describe cuán apretadamente el servicio puede ser atado por el ancho de banda especificado, por la demora, por la inestabilidad, y por las características de pérdida.

Tres niveles básicos de QoS de extremo a extremo se pueden proporcionar a través de una red heterogénea, como mostrado en la Figura 2.1:

- El servicio Best – Effort. También conocido como falta de QoS, el servicio de Best – Effort es conectividad básica con ninguna garantía. Esto es caracterizado mejor por colas FIFO, que no tiene diferenciación entre flujos.
- El servicio diferenciado (llamado también QoS soft). Algo de tráfico se trata mejor que los demás (el manejo más rápido, ancho de banda de promedio y baja la tasa media de pérdida). Esto es una preferencia estadística, no es una garantía inalterable. Esto es proporcionado por la clasificación del tráfico y el uso de instrumentos de QoS tales como PQ, CQ, WFQ, y WRED (todo discutido luego en este capítulo).
- El servicio garantizado (llamada también QoS hard). Esta es una reservación absoluta de recursos de red para el tráfico específico. Esto se proporciona por instrumentos de QoS RSVP y CBWFQ (discutió luego en este capítulo).

Decidir cuál tipo del servicio es apropiado a desplegarse en la red depende de varios factores:

- La aplicación o el problema que el cliente trata de resolver. Cada uno de los tres tipos del servicio son apropiados para ciertas aplicaciones. Esto no implica que un cliente debe emigrar diferenciado el servicio protegido (aunque muchos probablemente se hagan finalmente). Un servicio diferenciado o aún un servicio de best effort puede ser apropiado, dependiendo de los requisitos de la aplicación del cliente.
- La tasa en cuál los clientes pueden mejorar prácticamente sus infraestructuras. Hay un sendero natural del aumento de la tecnología necesitada de proporcionar los servicios diferenciados que necesitan para proporcionar los servicios garantizados, que es un sobre conjunto de que necesitan para servicios diferenciados.
- El costo de aplicar y desplegar garantiza que el servicio es probable de ser más que eso para un servicio diferenciado.

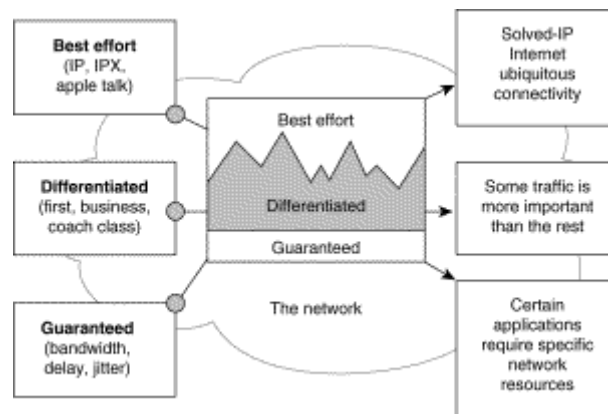


Figura 2.1. Los tres niveles de QoS de extremo a extremo son los servicios del Best – Effort, el servicio diferenciado, y el servicio garantizado.

Fuente: Cisco Networking Academy.

2.10. CLASIFICACIÓN IDENTIFICACIÓN DE FLUJOS

Para proporcionar la prioridad a ciertos flujos, el flujo debe ser identificado primero y (si se desea) marcado. Estas dos tareas son referidas comúnmente como apenas la clasificación.

Históricamente, la identificación es usada en las listas de Control de Acceso (ACLs). ACLs identifica el tráfico para las herramientas de congestión tales como PQ y CQ. Porque PQ y CQ son colocados en routers en una base de hop by hop (eso es, los escenarios de prioridad para QoS pertenecen sólo a ese router y no son pasados a subsiguientes routers en la red), identificación del paquete se utiliza sólo dentro de un solo router. En algunos casos, la clasificación de CBWFQ es para sólo un solo router. Esto es contrastado poniendo los bits de IP precedence.

Las características tales como políticas basadas en routeo y (CAR) puede ser utilizado para poner la prioridad basada en la clasificación prolongada de la lista del acceso. Esto permite la flexibilidad considerable para la tarea de la precedencia, inclusive la tarea por la aplicación o el usuario, por subred de destino y fuente, etcétera. Típicamente esta funcionalidad se despliega al cierre como a la orilla de la red (o el dominio administrativo) como es posible para que cada elemento subsiguiente de la red pueda proporcionar el servicio basado en la política determinada.

El reconocimiento de la aplicación de red base (NBAR) se utiliza para identificar el tráfico más granularmente. Por ejemplo, URLs en un paquete de HTTP se pueden identificar. Una vez que el paquete se ha identificado, se puede marcar con una colocación de precedencia.

2.10.1. CONFIGURACIONES DE POLÍTICAS DE QoS CON POLÍTICAS BASADAS EN ROUTING

Las Políticas Base de Roteo (PBR) le permiten clasificar el tráfico basado en criterios extendidos de lista de acceso, configurando la prioridad de bits de la IP y una ruta específica para reingeniar senderos que podían ser requeridos para admitir QoS específicos a través de la red. Poniendo la precedencia niveles en el tráfico entrante y los usos en combinación con la cola de instrumentos descritos anteriormente en este capítulo, usted puede crear el servicio diferenciado. Estos instrumentos proporcionan opciones poderosas, sencillas y flexibles para aplicar las políticas de QoS en su red.

Utilizando políticas base de routing, mapas de routing hacen emparejar en ciertos criterios del flujo y después para fijar bits de precedencia cuando se emparejan ACLs.

La capacidad de configurar bits de IP Precedence no se deben confundir con la capacidad primaria de PBR: (dirigir paquetes basados en políticas configuradas). Algunas aplicaciones o el tráfico se pueden beneficiar a QoS específico en transferir registros en una oficina corporativa (por ejemplo, en un alto ancho de banda, alto es el costo de conexión para un tiempo corto), al transmitir los datos rutinarios de la aplicación tales como correo electrónico sobre un bajo ancho de banda, a un costo de conexión baja.

También los mapas de las rutas disponibles que utilizan la capacidad de identificar paquetes basados en el Protocolo (BGP) atribuyen tal como las listas de la comunidad y paths AS. Esto es conocido como QoS policy propagation via Border Gateway Protocol.

2.10.2. CAR: CONFIGURADO IP PRECEDENCE

Semejante en algunas maneras a PBR, la característica de CAR le permite clasificar el tráfico en un interfaz entrante. Permite también la especificación de políticas para manejar el tráfico que excede una cierta asignación de ancho de banda. CAR mira el tráfico recibido en una comunicación, o un subconjunto de ese tráfico escogido por criterios de lista de acceso, compara su tasa a que de un bucket configurado de muestra, y entonces toma medidas basado en el resultado (por ejemplo, deja caer o reordena la IP precedence).

Hay alguna confusión con utilizar CAR de configuración de bits de IP precedence. Una tentativa para aclarar cualquier confusión sigue. Descrito en este capítulo. CAR (como su nombre describe) es utilizado para custodiar los flujos del tráfico a una tasa cometida del acceso. CAR hace esto con un bucket de muestra. Un bucket de muestra es un bucket con muestras en ello que representa los byte (1 token = 1 byte). El bucket es llenado de muestras en una tasa de usuario configurado. Cuando los paquetes llegan a ser entregados, el sistema verifica el bucket de muestra. Si hay suficientes muestras en el bucket en el tamaño del paquete, esas muestras son retiradas y el paquete se pasa (este paquete ajustado). Si no hay suficientes muestras, el paquete es dejado caer (este paquete excede).

Cuando se usa implementación de CAR de IOS, usted tiene más opciones que apenas de paso o cae. Una opción es fijar bits de IP precedence. Cuándo las acciones de conforma y excede ambos dicen poner los bits de precedencia al mismo ajuste, entonces no son más largos que la característica de la política, pero meramente un método de bits ponientes de IP precedence.

La Figura 2.2 muestra una proporción comprometida que se decide. Cualquier paquete que está debajo de la tasa se conforma. Los paquetes encima de la tasa exceden. En este ejemplo, la acción para ambos condiciona deberá poner prec = 5. En este caso, lo que la tasa no importa y el CAR se utiliza simplemente poner los bits de la precedencia.

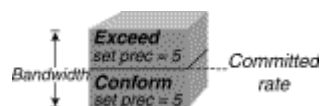


Figura 2.2. La tasa cometida que se decide sobre.

Fuente: Cisco Networking Academy.

Cuándo IP Precedence es configurada en el host o cliente de red, esta configuración puede ser usada opcionalmente; sin embargo, esto puede ser hecho caso omiso por las políticas dentro de la red. La prioridad de IP permite las clases de servicio a ser estableciendo usando mecanismos de cola en la red (por ejemplo, WFQ o WRED), con ningún cambio a aplicaciones existentes o requisitos complicados de red. Note que este mismo enfoque es extendido fácilmente a IPv6 que utiliza su campo de la Prioridad.

El software IOS se aprovecha de la naturaleza de punta a punta de IP para encontrar este desafío recubriendo la Capa 2. QoS señala tecnología específica a las soluciones con la Capa 3 IP QoS que señala los métodos de RSVP y la IP precedence.

2.10.3. NBAR: IDENTIFICACIÓN DINÁMICA DE FLUJOS

El método más nuevo de la clasificación es la Red el Reconocimiento Basado en la Aplicación (NBAR). Para la claridad, NBAR es realmente sólo un instrumento de identificación, pero será referido aquí como un instrumento de clasificación. Con cualquier herramienta de clasificación, la parte dura es la identificación el tráfico. Marcado el paquete es luego relativamente fácil. NBAR toma la identificación de la porción de la clasificación a otro nivel. Examinando con más detalle el paquete, la identificación se puede realizar, por ejemplo, la URL o de tipo MIME de un paquete de HTTP. Esto llega a ser esencial con más aplicaciones que llegan a ser Web Based. Usted necesitaría diferenciar entre una orden para ser colocado y hojear casualmente la Web. Además, NBAR puede identificar varias aplicaciones que utilizan los puertos efímeros. NBAR hace esto para mirar los paquetes de control para determinarse sobre que puertos la aplicación decide pasar los datos en adelante.

NBAR añade un par de características interesantes que lo hacen sumamente valiosas. Una característica es una capacidad del descubrimiento de protocolo. Esto deja a NBAR en la cola de fondo los protocolos en una interfase. NBAR lista los protocolos que lo puede identificar y proporcionar estadísticas en cada uno. Otra característica es el Módulo de Idioma de Descripción de Paquete (PDLM), que permite a protocolos adicionales ser añadidos fácilmente a la lista de NBAR de protocolos identificables. Estos módulos se crean y son cargados en la memoria Flash, donde luego es cargada en la RAM. Usando PDLMs, adiciona protocolos a la lista sin que se actualicen el nivel IOS o reiniciar el router.³

2.11. IP PRECEDENCE: DISTINGUIENDO QoS

IP Precedence utiliza los 3 bits de la precedencia en la cabecera de IPv4 de tipo de Servicio (ToS) especificando la clase del servicio para cada paquete, como se muestra en la Figura 2.3. Usted puede dividir el tráfico en superior a seis clases de servicio usando la IP Precedence (otros dos se reservan para el uso interno de la red). Las

³ **Nota:** Aunque NBAR sólo identifique paquetes, estos paquetes se pueden marcar también con una colocación de la IP precedence.

tecnologías de Cola a través de la red pueden utilizar esta señal para proporcionar el apropiado fácil manejo.

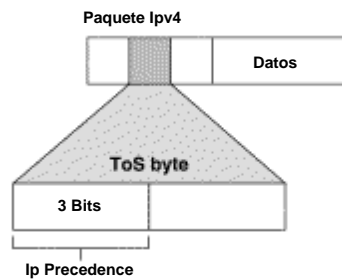


Figura 2.3. Este esquema muestra la IP Precedence para sortear en un encabezamiento paquete de IP.

Fuente: Cisco Networking Academy.

Los 3 bits mas significativos (relacionando a las configuraciones binarias 32, 64, y 128) del Tipo de Servicio (TOS) en el encabezamiento de IP constituye los bits usados para la IP precedence. Estos bits se utilizan para proporcionar una prioridad de 0 a 7 (los escenarios de 6 y 7 son reservados y no deberán ser puestos por un administrador de la red) para el paquete de IP. Porque sólo 3 bits de los ToS Byte se utilizan para la IP precedence, usted necesita diferenciar estos bits del resto del ToS byte. En la Figura 2.4, un 1 en el primer y tercer bit posicionado (viendo de izquierda a derecha) pone en correlación a una IP Precedence que pone 5, pero al ver el ToS byte en un sniffer trace, mostrará 160. Usted necesita ser capaz de traducir estos escenarios.

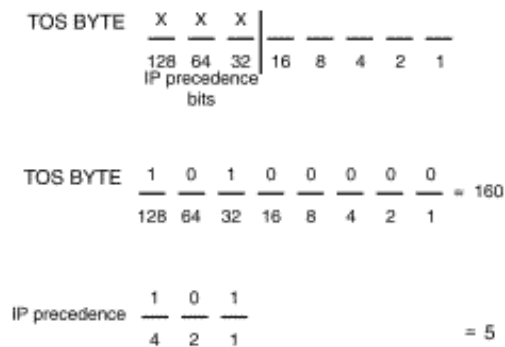


Figura 2.4. IP Precedence.

Fuente: Cisco Networking Academy.

El Tráfico que es identificado puede ser marcado por poner bits de IP Precedence. Así, necesita ser clasificado sólo una vez.

RFC 2475 extienden el número de bits utilizados en el ToS byte de 3 a 6. El 6 MSBs se utilizará para escenarios de precedencia (conocido como codepoints), con los 2 bits

menos significativos (2 bits de la derecha) reservados para usos futuros. Esta especificación es referida comúnmente como DiffServ.

2.12. HERRAMIENTAS DE ADMINISTRACIÓN DE CONGESTIÓN

Los elementos unidireccionales de la red manejan un desbordamiento del tráfico que llega en el cual es utilizado un algoritmo que hace cola para clasificar el tráfico, y después determinan un cierto método de darle la prioridad sobre un acoplamiento de la salida. El software IOS incluye las siguientes herramientas:

- Primero en entrar, primero en salir (FIFO)
- La prioridad haciendo cola (PQ)
- Custom queuing (CQ)
- Flow - Based cargó justo haciendo cola (WFQ)
- Class-based weighted fair queuing (CBWFQ)

En cada cola el algoritmo fue diseñado para resolver un problema específico del tráfico de la red y tiene un efecto particular en el desempeño de la red, como es descrito en las secciones siguientes.⁴

2.12.1. FIFO: ALMACENAMIENTO BÁSICO Y CAPACIDAD DELANTERA

En su forma más sencilla, la cola FIFO involucra los paquetes almacenados cuando la red esta congestionada y remitiéndose en el orden de llegada cuando la red ya no esta congestionada. FIFO es el algoritmo de la información de colas de espera predefinidos en algunos casos, así no requieran configuración, pero tiene varios defectos. La más importante, la cola FIFO no toma decisión acerca de la prioridad de paquete; la orden de la llegada determina el ancho de banda, la prontitud, y la asignación del búfer. Ni proporciona la protección contra aplicaciones (fuentes) ill-behaved. Las fuentes de Bursty pueden causar largos retrasos de entrega en tiempo sensible en el tráfico de aplicaciones, potencializar el control de red y los mensajes que señalen. En la cola FIFO era necesario el primer paso al contratar el tráfico de la red, pero las redes inteligentes actuales necesitan los algoritmos más sofisticados. Además, una cola

⁴ **Nota:** En la cola los algoritmos surten efecto cuando la congestión es experimentada. Por definición, si la conexión no se congestionada, entonces no hay necesidad de hacer cola paquetes. En ausencia de congestión, todos los paquetes son entregados directamente la interfaz.

repleta causa gotas de cola. Esto es indeseable porque el paquete dejado caer podría haber sido un paquete de alta prioridad. El router no podría prevenir que el paquete pueda ser dejado caer porque no hay sitio en la cola (además del hecho de que FIFO no puede decidir si un paquete es de alta o de baja prioridad). Las herramientas del software IOS implementan algoritmos de colas para evitar los defectos de FIFO.

2.12.2. PQ: PRIORIZANDO EL TRÁFICO

PQ asegura que el tráfico importante obtenga el manejo más rápido en cada punto donde se lo utiliza. Se diseñó para dar la prioridad estricta al tráfico importante. Priorizando las colas pueden priorizar flexiblemente según un protocolo de red (por ejemplo IP, IPX, o AppleTalk), interfaz entrante, el tamaño de paquete, la dirección del fuente/destino, etcétera. En PQ, cada paquete se coloca en uno de cuatro colas, alto media o normal basado en una prioridad asignada. Los paquetes que no son clasificados por esta prioridad cae hacia la lista normal (véase la Figura 2.5). Durante la transmisión, el algoritmo da la más alta prioridad hacia la de absolutamente preferencial tratamiento sobre las colas de baja prioridad.

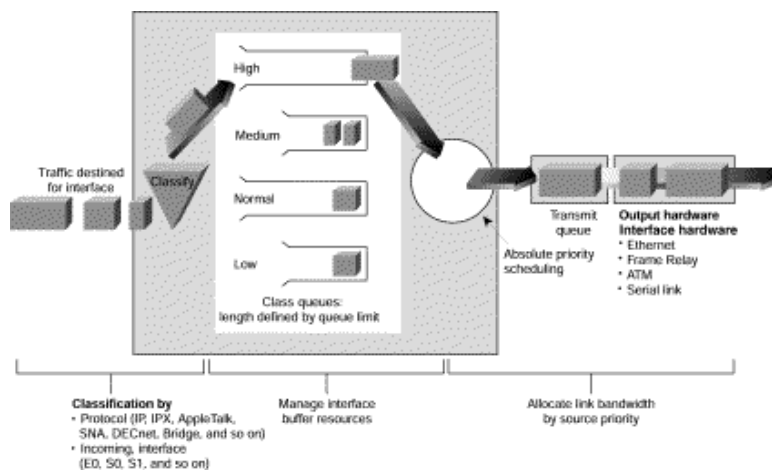


Figura 2.5. Prioridad de cola los datos de lugares en cuatro niveles de colas: Alto, Medio, Normal, y Bajo

Fuente: Cisco Networking Academy.

PQ es útil para cerciorarse que el tráfico crítico atraviesa varias conexiones WAN obteniendo la prioridad de tratamiento. PQ actualmente usa configuraciones constantes y así no se adapta automáticamente a requisitos cambiantes de red.

2.12.3. CQ: GARANTIZANDO ANCHO DE BANDA

CQ fue diseñado para permitir que varias aplicaciones pueda compartir la red entre aplicaciones con requisitos mínimos específicos de ancho de banda o estado latente.

En estos ambientes, el ancho de banda se debe compartir proporcionalmente entre aplicaciones y los usuarios. Usted puede utilizar la característica de CQ para proporcionar ancho de banda garantizada en un punto potencial de la congestión, asegurando que el tráfico especificado a una porción fija de ancho de banda este disponible y dejando el ancho de banda restante a otro tráfico. El trafico encargado de la formación de colas de espera personalizadas asigna una cantidad especificada de espacio de la cola a cada clase de paquetes y ellos sirven las colas en un round – robin fashion (véase la Figura 2.6).

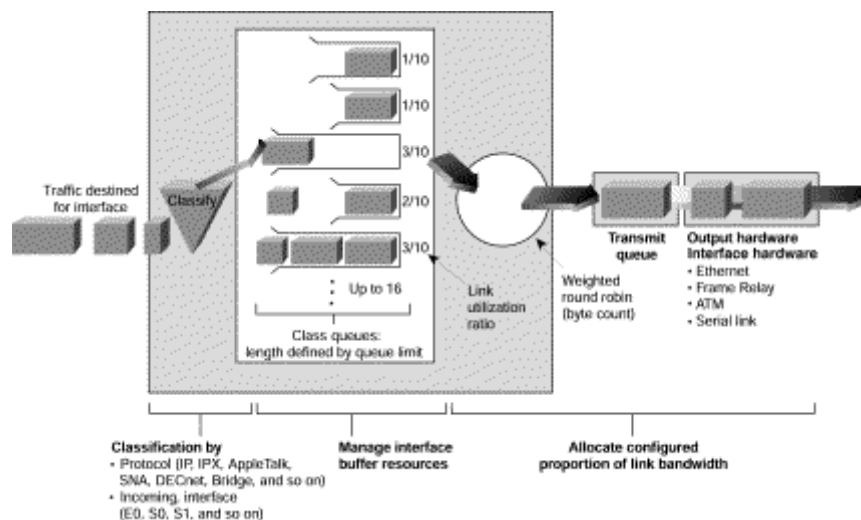


Figura 2.6. Costumbre formación de colas de espera encargadas del tráfico asignado una cantidad especificada de espacio de la cola a cada clase de los paquetes y ellos sirven las colas en un Round – Robin Fashion.

Fuente: Cisco Networking Academy.

En un ejemplo, Los Sistemas de Arquitectura de red encapsulada (SNA) requiere un nivel mínimo garantizado del servicio. Usted podría reservar la mitad de ancho de banda disponible para datos de SNA y permitir la mitad restante ser utilizada por otros protocolos tales como IP e (IPX).

El algoritmo de formación de colas de espera pone los mensajes en una de 17 colas (cola 0 tiene mensajes de sistemas tales como keepalives, señales, etcétera) y se vacía la prioridad pesada. El router atiende a las colas 1 por 16 en la orden de round - robin, dequeuing configurando una cuenta byte cada cola en cada ciclo. Esta característica asegura que ninguna aplicación (o grupo específico de aplicaciones) consigue más de una proporción predeterminada de la capacidad en conjunto cuando la línea está bajo tensión. Como PQ, CQ se configura constantemente y no se adapta automáticamente a las condiciones cambiantes de red.

2.12.4. FLOW - BASED WFQ: CREANDO LA IMPARCIALIDAD ENTRE FLUJOS

Para situaciones en la cual es deseable proporcionar el tiempo de respuesta coherente a usuarios pesados y ligeros de red semejantes sin agregar ancho de banda excesivo, la solución es Flow – Based WFQ (comúnmente referido como apenas WFQ). WFQ es una de las técnicas de formación de colas de espera Premier. Es un algoritmo de formación de colas de esperas que crea la justicia bit-wise permitiendo que cada cola pueda ser atendida en términos de byte count. Por ejemplo, si en la cola 1 tiene paquetes de 100 byte y la cola 2 tienen paquetes de 50 byte, el algoritmo de WFQ tomará dos paquetes de la cola 2 para cada paquete de la cola 1. Esto hace el servicio justo para cada cola: 100 byte cada vez la cola es atendida.

WFQ asegura que las colas no starve para el ancho de banda y ese tráfico obtiene el servicio previsible. El tráfico de bajo volumen que comprende la mayoría del tráfico que recibe el servicio aumentado, transmitiendo el mismo número de byte como corrientes de alto volumen. Esta conducta tiene como resultado lo que parece ser el tratamiento preferente para el tráfico de bajo volumen, cuando en la realidad crea la justicia, como mostrado en la Figura 2.7.

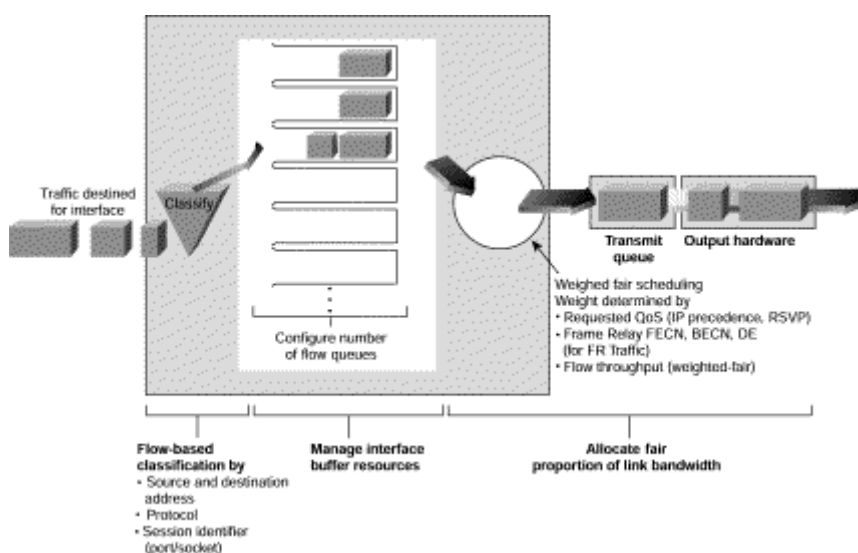


Figura 2.7. Con WFQ, si las conversaciones de alto volumen son activas, sus tasas de transferencia y períodos de interarriual se hacen mucho más previsible.

Fuente: Cisco Networking Academy.

WFQ se diseña para aminorar el esfuerzo de configuración, y adapta automáticamente a condiciones cambiantes de tráfico de red. De hecho, WFQ hace un trabajo tan bueno para la mayoría de las aplicaciones que se lo ha hecho por defecto en la mayoría de las interfaces seriales configuradas para correr o bajar una velocidad E1 (2,048 Mbps).

Flow - Based WFQ crea los flujos basados en un número de características en un paquete. Cada flujo (también referido como una conversación) es dado su propia cola para el buffering si la congestión es experimentada. Las descripciones siguientes utilizan el flujo, la conversación, y la cola intercambiabilmente.

La porción compensada de WFQ viene del uso de bits de IP Precedence a proporcionar el servicio más grande para ciertas colas. Utilizando los escenarios 0 a 5 (6 y 7 son reservados), WFQ utiliza su algoritmo para determinar cuánto más servicio a proporcionar a una cola. Vea la próxima sección "La Cooperación Entre WFQ y QoS señalando las Tecnologías," para más detalles.

WFQ es eficiente al utilizar cualquier ancho de banda que este disponible para remitir tráfico de flujos de baja prioridad si no hay tráfico de flujos de alta prioridad presente. Esto es diferente en la Multiplexación por división de tiempo (TDM), cual simplemente divide el ancho de banda y la deja ir si no hay tráfico presente para un tipo particular del tráfico. Los trabajos de WFQ con la reservación de la precedencia IP y el protocolo de reservación de recursos (RSVP), descrito más adelante en este capítulo ayuda a proporcionar distinguido QoS así como servicios garantizados.

El algoritmo de WFQ dirige también el problema de la variabilidad de la demora de round – trip delay. Si múltiples conversaciones de alto volumen son activas, sus tasas de transferencia y períodos de interarrival se hacen mucho más previsibles. Esto es creado por la justicia bit - wise. Si las conversaciones son atendidas en una manera coherente con cada enfoque del round - robin, la variación de demora (o jitter) estabiliza. WFQ aumenta mucho los algoritmos tales como SNA el Control Lógico de Enlace (LLC), el Protocolo de Control de Transmisión (TCP) y las características del show-start. El resultado es rendimiento y tiempo de respuesta más previsible para cada flujo activo, como se muestra en la Figura 2.8.

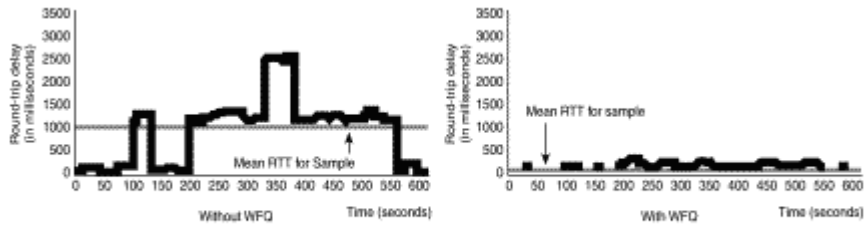


Figura 2.8- Este diagrama muestra un ejemplo del tráfico interactivo de demora (128 - kbps frame relay enlace WAN)

Fuente: Cisco Networking Academy.

2.12.4.1. COOPERACIÓN ENTRE WFQ Y QOS SEÑALANDO LAS TECNOLOGÍAS

Mencionado previamente, WFQ es IP Precedence consciente; Es decir, es capaz de detectar paquetes de más alta prioridad marcados con precedencia para la IP forwarder y los puede planificar más rápido, proporcionando el tiempo de respuesta superior para este tráfico. Esto es la porción compensada de WFQ. El campo de la IP Precedence tiene los valores entre 0 (por default) y 7 (6 y 7 son reservados y normalmente no son puestos por administradores de red). Cuando el valor de la precedencia aumenta, el algoritmo asigna más ancho de banda a esa conversación para cerciorarse que se sirve más rápidamente cuándo ocurre congestión. WFQ asigna un peso a cada flujo, que determina el orden de la transmisión para cada cola de los paquetes. En este esquema, se proporcionan los más bajos pesos. IP Precedence sirve como un divisor a este factor del aumento. Por ejemplo el tráfico con un valor de campo de IP Precedence de 7 obtiene un peso más bajo que el tráfico con un valor de campo de IP Precedence de 3, y así tiene la prioridad en el transmite la orden.

Un peso es un número calculado de la IP Precedence que pone para un paquete en el flujo. Este peso se utiliza en el algoritmo de WFQ para determinar cuando el paquete será atendido.

$$\text{Peso} = (4096 / (\text{IP Precedence} + 1)).$$

$$\text{Peso} = (32384 / (\text{IP Precedence} + 1)).$$

El numerador de la ecuación cambia de 4096 a 32384 en una liberación de la conservación v12.0.

Los escenarios del peso se pueden ver utilizando la cola de la exposición comando <interfaz>.

El efecto de Escenarios de IP Precedence

El efecto de escenarios de IP Precedence se describe aquí:

Si usted tiene un flujo en cada nivel de la precedencia en un interfaz, cada flujo obtendrá la precedencia + 1 partes de la conexión, de la siguiente manera:

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 = 36$$

Los flujos obtendrán 8/36, 7/36, 6/36, y 5/36 de el enlace, etcétera. Sin embargo, si usted tiene 18 prioridades: 1 flujo y 1 de cada uno de los otros la formula se parece:

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 = 36 - 2 + 1 * 2 = 70$$

Los flujos obtendrán 8/70, 7/70, 6/70, 5/70, 4/70, 3/70, 2/70, y 1/70 del enlace, y 18 de los flujos pueden aproximadamente conseguir 2/70 del enlace.

WFQ está también RSVP-AWARE; RSVP utiliza WFQ para asignar el espacio del búfer, paquetes de horario, y garantiza el ancho de banda para flujos reservados. Adicionalmente, en una red de Frame Relay, la presencia de la congestión es señalada por la notificación de congestión explícita delantera (FECN) y las notificaciones de congestión explícita hacia atrás (BECN) bits. Las pesas de WFQ son afectadas por el Frame Relay descartada elegible (DE), FECN, y los bits de BECN cuando el tráfico es cambiado por el módulo de la conmutación del Frame Relay. Cuando la congestión se marca, las pesas usadas por el algoritmo son alterados para que la conversación que encuentre la congestión transmita con menos frecuencia.

2.12.4.2. CLASS-BASED WFQ: ASEGURANDO ANCHO DE BANDA DE RED

WFQ (CBWFQ) de class-based es una de las herramientas más nuevas para la Administración de Congestión de Cisco para proporcionar mayor flexibilidad. Cuando usted quiere proporcionar una cantidad mínima de ancho de banda, use CBWFQ. Esto está con respecto a un deseo de proporcionar una cantidad máxima de ancho de banda. CAR y formación de tráfico se utiliza en ese caso.

CBWFQ permite a un administrador de la red cree el mínimo de las clases garantizadas de ancho de banda. En vez de proporcionar una cola para cada flujo individual, una clase se define como uno o más flujos. Cada clase puede garantizar una cantidad mínima de ancho de banda.

Además, una cola de bajo estado latente (LLQ) se puede designar, esencialmente en una cola de prioridad. Note que esta característica es referida también como una cola de prioridad class-based compensada justo la cola (PQCBWFQ).

Bajo estado latente hace que la cola deje una clase para ser atendida como una cola de prioridad estricta. El tráfico en esta clase será atendido antes de cualquiera de las otras clases. Una reservación para una cantidad de ancho de banda se hace. Cualquier tráfico encima de esta reservación se desecha. Fuera de CBWFQ, usted puede utilizar la prioridad de IP RTP (también conocido como PQWFQ) o la reserva de IP RTP para proporcionar el servicio semejante para el tráfico de RTP sólo.⁵

2.13. ADMINISTRACIÓN DE COLAS (HERRAMIENTAS PARA LA ANULACIÓN DE CONGESTIÓN)

Evitar la congestión es una forma de administración de la cola. Las técnicas de anulación de la congestión controlan las cargas del tráfico de la red en un esfuerzo de anticipar y evitar la congestión en embotellamientos comunes de red, en comparación con las técnicas de administración de la congestión que operan para controlar la congestión después que ocurre. El instrumento primario para evitar la congestión del IOS es (WRED).

2.13.1. WRED: EVITANDO LA CONGESTIÓN

Descubrimiento aleatorio temprano (Random Early Detection RED) diseñan los algoritmos para evitar la congestión en el internetworks antes que llegue a ser un problema. RED trabaja controlando la carga del tráfico en puntos en la red y

⁵ **Nota:** CBWFQ, una cantidad mínima de ancho de banda se puede reservar para una cierta clase. Si más ancho de banda está disponible, esa clase puede utilizar. La key garantiza una cantidad mínima de ancho de banda. También, si una clase no utiliza su ancho de banda garantizado, otras aplicaciones pueden utilizar el ancho de banda

desechando estocásticamente paquetes si la congestión comienza a aumentar. El resultado del goteo es que la fuente detecta el goteo de tráfico y retarda su transmisión. RED es diseñado principalmente para trabajar con TCP en ambientes de internetwork de IP.

2.13.2. LA COOPERACIÓN DE WRED CON TECNOLOGÍAS DE SEÑALAR DE QoS

WRED combina las capacidades del algoritmo RED con la IP precedence. Esta combinación mantiene tráfico preferencial para paquetes de más alta prioridad. Puede desechar selectivamente el tráfico de la más baja prioridad cuando la interfaz empieza a congestionarse y pueden proporcionar características diferenciadas de desempeño para clases diferentes del servicio (véase la Figura 2.9). WRED está también RSVP-AWARE y puede proporcionar un servicio integrado de carga controlada de servicios QoS.

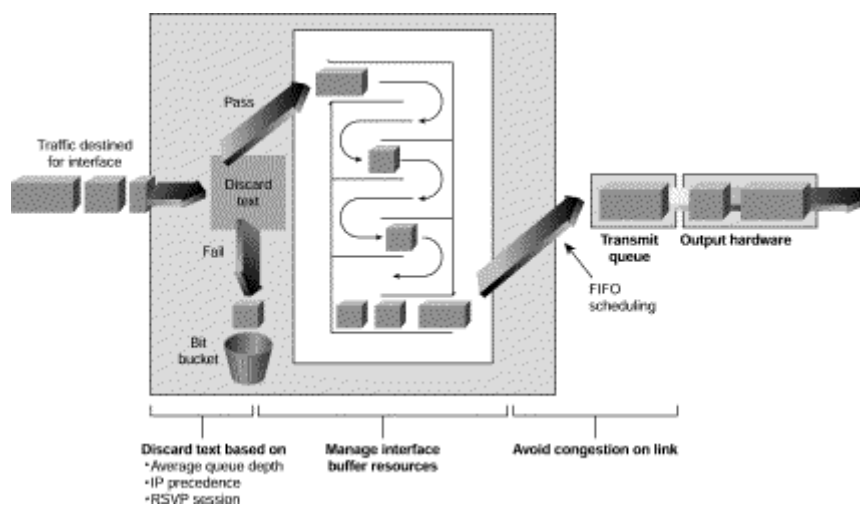


Figura 2.9. WRED proporciona un método que desecha estocásticamente paquetes si la congestión comienza a aumentar.

Fuente: Cisco Networking Academy.

Dentro de cada cola, un número finito de paquetes se puede albergar. Una cola repleta causa goteo de paquetes de la cola. Los paquetes de la cola dejados caer no podrán encajar en la cola porque esta llena. Esto es indeseable porque el paquete desechado puede haber sido un paquete de alta prioridad y el router no tiene una oportunidad de hacer cola. Si la cola no está repleta, el router puede mirar la prioridad de todos los paquetes que llegan y dejan caer los paquetes de más baja prioridad, permitiendo que

los paquetes de alta prioridad queden en la cola. A través de la administración de la profundidad de las colas (el número de paquetes en la cola) dejando caer varios paquetes, el router puede cerciorarse mejor que la cola no este llena y esas gotas de cola no son experimentadas. Esto permite al router tomar la decisión de cuál paquete deja caer cuando la profundidad de la cola aumenta. WRED ayuda también a prevenir la congestión general en un internetwork. WRED utiliza un umbral mínimo para cada nivel de la IP Precedence para determinar cuando un paquete se puede dejar caer. (El umbral mínimo se debe exceder para WRED para considerar un paquete como un candidato para ser dejado caer.)

Eche una mirada a este ejemplo de WRED:

La profundidad de la cola: 21 paquetes

El umbral mínimo de la gota para la IP Precedence = 0: 20

El umbral mínimo de la gota para la IP Precedence = 1: 22

Porque el umbral mínimo de gota para la IP Precedence = 0 ha excedido, los paquetes con una IP Precedence = 0 pueden ser dejados caer. Sin embargo, el umbral mínimo de gota para la IP Precedence = 1 no ha excedido, así que esos paquetes no se dejarán caer. Si la profundidad de la cola ahonda y excede 22, entonces los paquetes con la IP Precedence = 1 puede ser dejado caer también. WRED utiliza un algoritmo que levanta la probabilidad que un paquete pueda ser dejado caer como las subidas de profundidad de cola del umbral de gota mínimo a umbral de gota máximo. Encima del umbral máximo de gota, todos paquetes se dejan caer.

2.13.3. FLUJO RED: RED PARA FLUJOS NO COMPATIBLES CON TCP.

WRED se usado principalmente para los flujos de TCP que recortarán la transmisión si un paquete se deja caer. Hay flujos no compatibles con TCP que no se recorta cuando los paquetes se dejan caer. Flujo RED es utilizado para tratar con tales flujos. El enfoque deberá aumentar la probabilidad de dejar caer un flujo si excede un umbral.

Flow - Based WRED depende de estos dos enfoques principales para remediar el problema de descarga lineal del paquete:

- Clasifica el tráfico entrante en flujos basados en parámetros tales como las direcciones del destino, la fuente y puertos.

- Mantiene el estado acerca de flujos activos, que es los flujos que tienen paquetes en las colas de salida.

Flow - Based WRED utiliza esta clasificación y el estado de la información para asegurar que cada flujo no consuma más que su acción permitida de los recursos de salida del búfer. Flow - Based WRED determina cuáles flujos monopolizan los recursos, y castigan estos flujos penalizándolos.

Esto es cómo Flow - Based WRED asegura la imparcialidad entre flujos: mantiene una cuenta de número de flujos activos que existen a través de una interfaz de salida. Dado el número de flujos activos y el tamaño de salida de la cola, Flow - Based WRED determina el número de búferes disponibles para el flujo.

Para tener en cuenta algún burstiness, WRED Flow - Based escala el número de búferes disponibles para el flujo por un factor configurado y permite que cada flujo activo tenga un cierto número de paquetes en la cola de salida. Este factor de escala es común a todos los flujos. El resultado del número escalado de búferes se vuelve el límite de flujo. Cuando un flujo excede el límite de flujos, la probabilidad que un paquete de esa circulación pudiera ser dejado caer aumenta.

2.14. FORMACIÓN DE TRÁFICO Y HERRAMIENTAS POLÍTICAS

Las soluciones del software QoS incluye dos herramientas para el tráfico genérico: Forma Genérico de Tráfico (GTS) y forma de tráfico de Frame Relay (FRTS) para manejar el tráfico y la congestión de la red. Las herramientas Políticas de IOS del Contestador Automático en Red (CAR). Esto se describió brevemente en la sección de la "Clasificación", anteriormente.

2.14.1. CAR: ADMINISTRANDO LAS POLÍTICAS DE ACCESO DE ANCHO DE BANDA Y LAS POLÍTICAS DE DESEMPEÑO

Descrito con anterioridad, fundamentalmente, QoS proporciona la prioridad o elevando la prioridad de un flujo o limitando la prioridad de otro. CAR se utiliza para limitar el ancho de banda de un flujo para favorecer otro flujo.

En la sección de la "Clasificación", anteriormente revisada, un bucket genérico fue descrito. En esa descripción, los paquetes que conforman son pasados, y los paquetes que exceden se dejan caer.

Con la implementación de IOS de CAR, un número de acciones se pueden realizar. Estas acciones consisten en transmitir, dejar caer, configurando los bits de IP precedence, y continuando (esto se refiere a caer en cascada las declaraciones de CAR). Esta flexibilidad tiene en cuenta varias maneras de afectar el tráfico. Aquí están algunos escenarios:

- Conformando el tráfico puede ser clasificados con una IP Precedence de 5, y exceder el tráfico se puede ser dejado caer.
- Conformando el tráfico se puede transmitir con una IP Precedence proponiendo un valor de 5, al exceder el tráfico se puede transmitir también, pero con una IP Precedence con un valor de 1.
- Conformando el tráfico se puede transmitir, y si excede el tráfico puede ser vuelto a clasificar a una precedencia más baja de IP y después enviando la próxima declaración del CAR para condiciones adicionales.

La puesta en práctica de CAR de IOS proporciona un bucket de explosión de exceso no encontrado en un token bucket genérico. En este bucket se adiciona un tokens sobre el original (o normal) el burst bucket. Cuando se utiliza este token, los paquetes tiene la posibilidad de ser drenados (incluso si la acción es transmitir). Un algoritmo RED-Like se usado como se dice, "cuanto más token usted use en este bucket, más alta prioridad que el siguiente paquete pueda ser dejado caer." Esto permite que el flujo sea escalado lentamente como en WRED, mientras consigue la oportunidad de enviar sobre el bucket normal.

2.14.2. GTS: CONTROL DE FLUJO DE SALIDA DE TRÁFICO

GTS proporciona un mecanismo para controlar el tráfico de flujo en una interfaz particular. Esto reduce el flujo de tráfico de salida para evitar la congestión forzando el tráfico especificado a una tasa particular del bit (utiliza también un enfoque de bucket) al hacer cola los bursts del tráfico especificado. Así, cualquier tráfico encima de la tasa configurada es hecho cola. Esto difiere del CAR, en el cuál los paquetes no son hechos cola. Así, el tráfico se adhiere a un perfil particular para reunir los requisitos de un stream, eliminando los embotellamientos en topologías con incompatibilidades de date-rate. Figura 2.10 ilustran GTS.

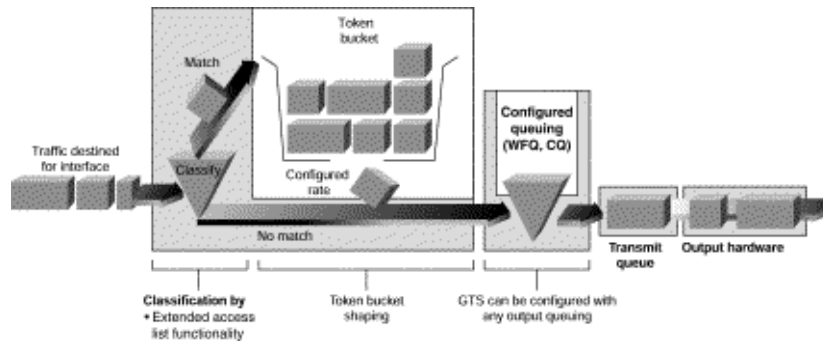


Figura 2.10. Formando tráfico genérico es aplicado en una base Per Interfase

Fuente: Cisco Networking Academy.

GTS aplica en una base de per-interfaz puede utilizar las listas de acceso para escoger el tráfico para formar, y para trabajar con una variedad de tecnología de Capa 2, inclusive Frame Relay, ATM, Switched Multimegabit Data Service (SMDS), y Ethernet.

En una subinterfaz del Frame Relay, GTS puede prepararse para adaptar dinámicamente al ancho de banda disponible integrando las señales BECN, o puede prepararse para formar simplemente especificando primero un tasa. GTS se puede configurar también en un procesador de interfaz ATM (ATM/AIP) la tarjeta de interfaz responde a RSVP señalando sobre la configuración estática ATM los circuitos virtuales permanentes (PVCs).

2.14.3. FRTS: MANEJANDO EL TRÁFICO DE FRAME RELAY

FRTS proporciona los parámetros que son útiles para manejar la congestión del tráfico de la red. Estos incluyen la tasa cometida de información (CIR), FECN y BECN, y el bit DE. Durante un tiempo, Cisco ha proporcionado apoyo para FECN de DECnet, BECN para el tráfico de SNA que utiliza la encapsulación LLC2 vía RFC 1490, y soporte DE bit. La característica de FRTS construye en este apoyo de Frame Relay con las capacidades adicionales de mejora la escalabilidad y el desempeño de una red de Frame Relay, incrementando la densidad de circuitos virtuales y mejora el tiempo de respuesta.

Por ejemplo, usted puede configurar la aplicación de la tarifa con una tarifa máxima configurada para limitar tráfico de salida al CIR o un cierto otro valor definido, tal como exceso de la tarifa de la información (EIR), en un per circuito virtual (VC) básico.

Usted puede también definir la prioridad y la costumbre de la cola en el VC o el nivel de sub interfase. Esto permite una granularidad más fina en la priorización, cola del tráfico, y proporciona más control sobre el flujo del tráfico en un VC individual. Si usted combina CQ con el per-VC que hace cola y valora las capacidades de la aplicación, usted habilita Frame Relay VCs a llevar múltiples tipos del tráfico tales como IP, SNA, e IPX, con ancho de banda garantizado para cada de tipo tráfico.

FRTS puede eliminar los embotellamientos en redes de Frame Relay con conexiones de gran velocidad en las conexiones del sitio central y conexiones de baja velocidad en las sucursales. Usted puede configurar la aplicación de la tasa para limitar que los datos se envían en el VC al sitio central. Usted puede utilizar también la aplicación con la existencia de identificador de conexión de DataLink (DLCI) priorizando las características de mejora del desempeño en esta situación. FRTS aplica sólo Frame Relay PVCs y swiched circuitos virtuales (SVCs).

Usando la información contenida en los paquetes de BECN-tagged recibidos de la red, FRTS puede también regular dinámicamente tráfico. Con BECN-based regula, los paquetes que se sostienen en los buffers del router's para reducir los flujos de los datos del router en el red Frame Relay. El regular se hace en un per VC básico, y se ajusta la tarifa de la transmisión basado en el número de paquetes de BECN-tagged recibidos.

FRTS también proporciona un mecanismo para compartir medios por múltiples VCs. La característica de la aplicación de la tarifa se puede también utilizar para reservar ancho de banda a cada VC, creando una red virtual de TDM. Finalmente, con la característica de FRTS, usted puede integrar StrataCom ATM previniendo en control de circuito cerrado de congestión para adaptar activamente a las condiciones downstream de congestión.

2.15. MECANISMOS DE ENLACES EFICIENTES

Actualmente, el software del IOS ofrece 2 mecanismos de enlaces eficientes: enlaces de fragmentación e interpolación (LFI) y protocolo de tiempo real - comprensión de Titulo (RTP-HC) el cual trabaja con colas y formando tráfico para mejorar la eficacia y la previsibilidad de los niveles de servicio de las aplicaciones.

2.15.1. LFI: FRAGMENTANDO E INTERPOLANDO EL TRÁFICO DE IP

El tráfico interactivo (Telnet, voz sobre IP, y similares) es susceptible al incremento de latencia y a inquietudes crecientes cuando la red procesa los paquetes grandes (por ejemplo, LAN a LAN Transferencias FTP a través de un enlace WAN), especialmente se hacen cola en acoplamientos más lentos. La característica del IOS, LFI reduce el retardo y la inestabilidad en enlaces de velocidad reducida por encima de los datagramas grandes e interpolando bajo tráfico de paquetes con el resultado de más pequeños paquetes (véase la Figura 2.11).

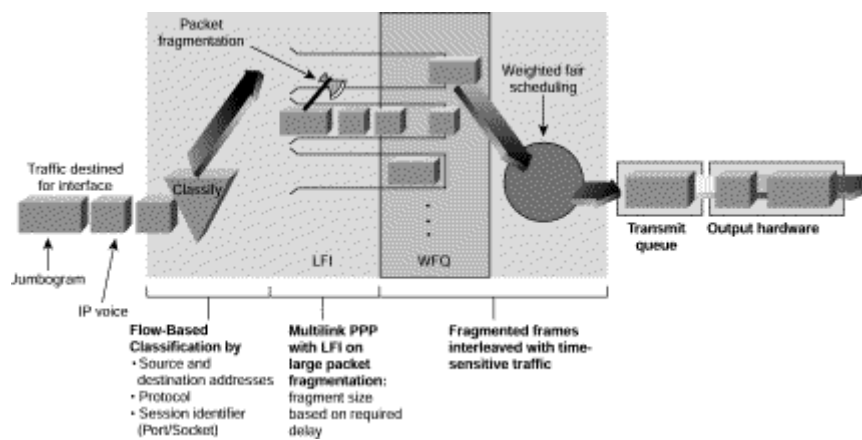


Figura 2.11. Divide datagramas grandes con la característica de LFI, la demora es reducida en conexiones de baja velocidad.

Fuente: Cisco Networking Academy.

LFI se diseñó especialmente para conexiones de baja velocidad en las que la demora de la serialización es significativa. LFI requiere de multienlaces del Protocolo Punto a Punto (PPP) configurados en la interfaz con interpolación girada. Un giro relacionado de IETF, llamado "Multiclass Extensions to Multilink PPP (MCML)," implementados casi de la misma función de LFI.

Cabe anotar que para la implementación de fragmentación sobre Frame Relay, usted debe utilizar las características de FRF.12, que proporciona los mismos resultados.

2.15.2. PROTOCOLO DE TIEMPO-REAL (RTP) (REAL-TIME TRANSPORT PROTOCOL).

El protocolo RTP tiene como objetivo asegurar una QoS para servicios del tipo tiempo

real. Incluye la identificación del payload, la numeración secuencial, la medición de tiempo y el reporte de la calidad (protocolo RTCP). Entre sus funciones se encuentran la memorización de datos, la simulación de distribución interactiva, el control y mediciones de aplicaciones.

Este protocolo RTP es de transporte (capa 4) y trabaja sobre UDP de forma que posee un checksum para detección de error y la posibilidad de multiplexación de puertos (port UDP). Las sesiones de protocolo RTP pueden ser multiplexadas. Para ello se recurre a un doble direccionamiento mediante las direcciones IP y el número de port en UDP. Sobre RTP se disponen de protocolos de aplicación del tipo H.320/323 para vídeo y voz (H.32x forma una familia del ITU-T de normas para videoconferencia). El protocolo de H.323 se detalla entre los servicios de las redes IP. Junto a RTP se dispone del protocolo de control RTCP.

El RTP funciona en conjunto con RSVP (capa 3) para la reservación de ancho de banda y asegurar de esta forma la calidad del servicio QoS del tipo Garantizada. La QoS del tipo Diferenciada se logra mediante la priorización de tráfico que puede adoptar dos alternativas. En IP se pueden asignar diversas alternativas de prioridad para formar una cola de espera en routers. Un algoritmo particular de gestión de prioridad de tráfico es el WFQ (Weighted Fair Queuing) que utiliza un modelo de multiplexación TDM para distribuir el ancho de banda entre clientes. Cada cliente ocupa un intervalo de tiempo en un Round-Robin. El ToS (Type of Service) en IP puede determinar un ancho de banda específico para el cliente. Un servicio sensible al retardo requiere un ancho de banda superior. En IP además del ToS se puede utilizar la dirección de origen y destino IP, tipo de protocolo y número de socket para asignar una ponderación.

RTP además provee transporte para direcciones unicast y multicast. Por esta razón, también se encuentra involucrado el protocolo IGMP para administrar el servicio multicast. El paquete de RTP incluyen un encabezado fijo y el payload de datos; RTCP utiliza el encabeza del RTP y ocupa el campo de carga útil. Los campos del encabezado fijo del protocolo RTP se muestran en la Tabla 2.2.

OH	2 Bytes de encabezado fijo para aplicaciones de identificación.
VRS	2 bits. Es la versión del protocolo. Actualmente se utiliza la versión 2 (RFC-1889).

PAD	1 bit. El bit de padding activo informa que luego del encabezado existen bytes adicionales (por ejemplo para algoritmos de criptografía).
X	1 bit. Con el bit de extensión activado existe solo una extensión del encabezado.
CC	4 bits. (CSRC Count). Identifica el número de identificadores CSRC al final del encabezado fijo.
M	1 bit de Marker. La interpretación está definida por el perfil.
PT	7 bits. (Payload Type). Identifica el formato de payload y determina la interpretación de la aplicación.
SN	2 Bytes. (Sequence Number). Numera en forma secuencial los paquetes de RTP y permite la identificación de paquetes perdidos
TS	4 Bytes. (TimeStamp). Refleja el instante de muestreo del primer Byte en el paquete RTP. Permite el cálculo del tiempo y jitter en la red. Por ejemplo, en una aplicación de audio que comprime cada 160 muestras, el reloj se incrementa en 160 en cada bloque
SSRC	4 Bytes. (Synchronization Source). Identifica la fuente de sincronismo de forma que dos sesiones del mismo RTP tengan distinta SSRC.
CSRC	Nx4 Bytes. (Contribution Source). Identifica la fuente que contribuye al payload contenido en el paquete. El valor de N lo da el campo CC.

Tabla 2.2. Protocolos para Tiempo-Real RTP (Real-Time Protocol).

Fuente: Grupo Investigativo

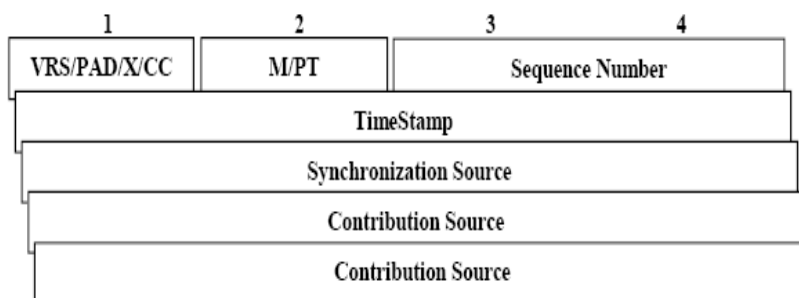


Figura 2.12. Protocolos para Tiempo-Real RTP (Real-Time Protocol).

Fuente: Grupo Investigativo

2.15.3. RTP HC (REAL-TIME PROTOCOL-HEADER COMPRESSION).

La compresión del encabezado permite mejorar la eficiencia del enlace en paquetes de corta carga útil. Se trata de reducir los 40 bytes de RTP/UDP/IP a una fracción de 2 a 5 bytes, eliminando aquellos que se repiten en todos los

datagramas. (RTP). Como los servicios de tiempo real generalmente trabajan con paquetes pequeños y generados en forma periódica se procede a formar un encabezado de longitud reducida que mejore la eficiencia de la red.

2.15.4. RSVP: GARANTIZANDO QoS

RSVP es un protocolo estándar del Internet del IETF (RFC 2205) para permitir que un uso reserve dinámicamente ancho de banda de la red. RSVP permite solicitar un QoS específico para un flujo de datos, según lo demostrado en la Figura 2-13. La implementación de Cisco también permite que RSVP sea iniciado dentro de la red, usando configuraciones Proxy RSVP. Los Administradores de las redes pueden aprovecharse de tal modo de las ventajas de RSVP en la red, incluso para no permitir usos RSVP y host. Los hosts y los routers utilizan RSVP para entregar las peticiones de QoS a los routers a lo largo de las trayectorias de las secuencias de datos y mantener el estado de router y del host para proporcionar el servicio solicitado, generalmente ancho de banda y estado latente. RSVP utiliza un índice de datos malos, la cantidad más grande de los datos que el router mantendrá en la cola, y QoS mínimo para determinar la reservación de ancho de banda.

WFQ o WRED actúa como un burro de carga para RSVP, estableciendo la clasificación de los paquetes y planificando los requisitos para los flujos reservados. Usando WFQ, RSVP puede entregar un servicio integrado y garantizado. Usando WRED, puede entregar un servicio controlado de carga. WFQ continúa proporcionando su manejo ventajoso sobre el tráfico no reservado facilitando el tráfico recíproco y compartiendo el ancho de banda restante entre flujos de alto ancho de banda; WRED proporciona sus ventajas proporcionadas para flujo de tráfico no RSVP. RSVP se puede desplegar en redes existentes con una mejora del software.

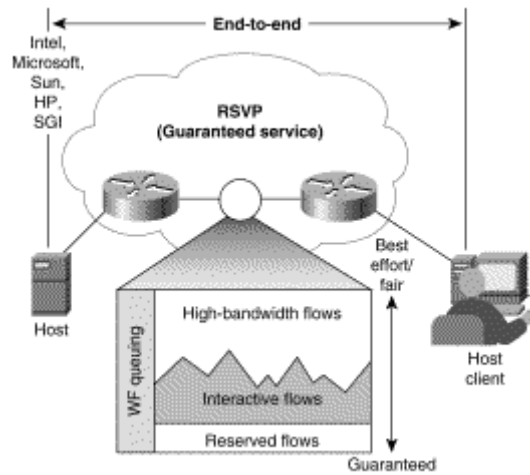


Figura 2.13. Esta figura muestra RSVP puesta en ejecución en una red basada en un router Cisco

Fuente: Cisco Networking Academy.

2.16. QoS EN LA ETHERNET

En la línea de Catalyst de Switches de multicapas tiene la capacidad de proporcionar QoS en Capa 2. En la Capa 2, el frame utiliza la clase del servicio (CoS) en 802.1p e Interconecta la Conexión Switch (ISL). CoS usas 3 bits, justo como IP Precedence, y mapas de capa 2 a capa 3 y viceversa. Los switches tienen la capacidad de diferenciar frames basados en configuraciones CoS. Si múltiples colas están presentes, los frames pueden ser colocados en diversas colas y mantener vía weighted round robin (WRR). Esto permite que cada cola tenga diversos niveles de servicios. Dentro de la cola, se fijan los umbrales de WRED. Estos umbrales son similares a los umbrales mínimos fijados en WRED en la capa 3. Actúan como el punto de partida para la probabilidad que un paquete será caído

La figura 2-14 explica el uso de WRR con WRED usando dos colas con dos umbrales cada una. Esto es referido como 2Q2T. En este caso, los escenarios 4 a 7 son puestos en la cola 1. Los escenarios 0 a 3 son puestos en la cola 2. La cola 1 se fija para conseguir el servicio de 70 por ciento del tiempo, y en la cola 2 obtienen el servicio del 30 por ciento del tiempo. En la cola 1, cuando la cola tiene el 30 por ciento lleno, los escenarios 4 y 5 pueden ser dejados caer. No hasta que la cola tenga el 85 por ciento lleno pueden los escenarios 6 y 7 ser dejados caer. En la cola 2, cuando la cola tiene un 20 por ciento lleno, los escenarios 0 y 1 pueden ser dejados caer. No hasta que la cola tenga el 60 por ciento lleno pueden los escenarios 2 y 3 ser dejados caer.

Muchas implementaciones proporcionaron la cartografía de ToS (o IP precedence) a CoS. En este caso, una configuración frame Ethernet CoS puede ser trazada el byte ToS del paquete de IP, y viceversa. Esto proporciona la prioridad de extremo a extremo para el flujo del tráfico.

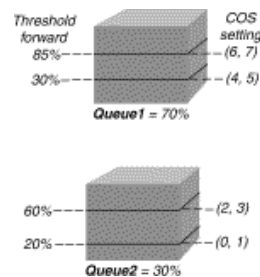


Figura 2.14. WRR con WRED usa dos colas con dos umbrales cada una.

Fuente: Cisco Networking Academy.

2.17. CONMUTACIÓN DE LA ETIQUETA DE MULTIPROTOCOL: PERMITIENDO LA INGENIERÍA FLEXIBLE DEL TRÁFICO

La característica de MPLS de Cisco (también conocida como tag switching) contiene los mecanismos de interoperabilidad con y toma las ventajas de ambos RSVP e IP precedence. La cabecera tag switching contiene 3 bit que pueden ser utilizados como señal de priorización del tráfico. Puede también ser utilizado en mapas particulares de flujos y clases de tráfico a lo largo de las trayectorias tag switching para obtener el QoS requerido a través de una porción de tag switching de una red.

2.18. POLÍTICAS DE CONTROL DE QoS

La arquitectura del control de políticas de QoS se desarrollo primeramente como una clave inicial de la iniciativa del establecimiento de políticas de una red de CiscoAssure. Esta iniciativa proveer estándares basados en protocolos de control de política de QoS y mecanismos de implementación de políticas de QoS para una sola consola.

En el nivel de la infraestructura, la clasificación de paquete es una capacidad clave para cada política técnica que permite que los paquetes apropiados atraviesen un elemento de la red o una interfaz particular ha ser escogida por QoS. Estos paquetes pueden ser entonces marcados por la apropiada IP precedence en algunos casos, o pueden ser identificados como un RSVP. El control de la política también requiere la integración con tecnologías de red subyacentes de la capa de transmisión de datos o no protocolos de IP.

2.19. QoS PARA VOZ DE PACKETIZED

Una de las aplicaciones más prometedoras para las redes de IP es permitir compartir el tráfico de voz con los tradicionales datos y el tráfico LAN a LAN. Típicamente, esto puede ayudar a reducir costos de transmisión reduciendo el número de conexiones de red que comparten conexiones e infraestructura existentes, etcétera.

En Cisco hoy tiene una amplia gama de productos y tecnologías, incluyendo un número soluciones de Voz sobre IP (VoIP), para proporcionar la calidad de voz requerida, sin embargo, la capacidad de QoS debe ser agregado a la red de datos tradicional. Las características de QoS de software de IOS de Cisco dan al tráfico de VoIP el servicio necesario, mientras proporciona los datos tradicionales circulan con el servicio que necesita también.

La Figura 2.15 presenta un negocio que fue escogido para reducir algunos de los costos de voz combinando el tráfico de voz en una red existente de IP. El tráfico de Voz en cada oficina es digitaliza en módulos de voz en 3600 procesos. Este tráfico entonces es dirigido al router vía protección H.323, el cual también requiere especificaciones de QoS para el tráfico de voz. En este caso, IP Precedence es configurado en alta para el tráfico de voz. WFQ es habilitado en toda la interfaz del router para esta red. WFQ facilita automáticamente adelantar el tráfico de voz de alta precedencia fuera de cada interfase, reduciendo la demora y la inestabilidad para este tráfico.

Porque la red IP manejada originalmente el tráfico LAN a LAN, muchos datagramas que atraviesan la red son grandes paquetes de 1500 bytes. En acoplamientos lentos (debajo de las velocidades T1/E1), los paquetes de voz pueden ser forzados ha esperar detrás de uno de estos paquetes grandes, agregando decenas o aún más centenares de milisegundos de retraso. LFI se utilizado conjuntamente con WFQ para romper estos enormes paquetes e interpolar el tráfico de voz para reducir los retrasos o bien la inestabilidad.

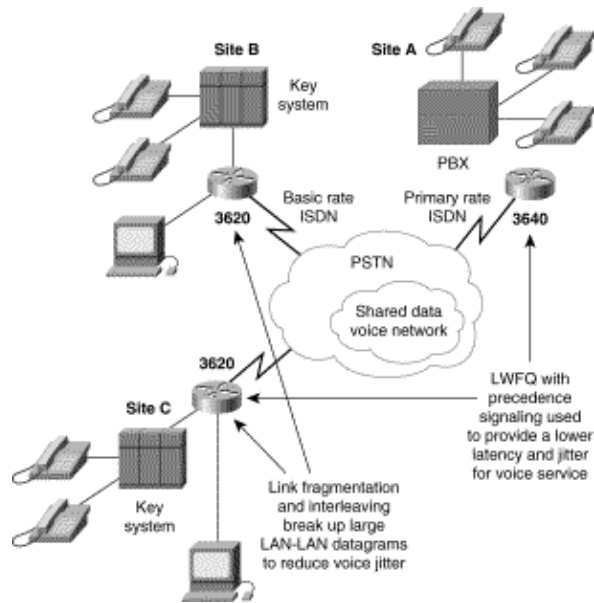


Figura 2.15. Esta figura proporciona una vista general de una solución de QoS en VoIP.

Fuente: Cisco Networking Academy.

2.20. QoS PARA EJECUTAR VIDEO

Uno de los desafíos más significativos para redes basadas en IP, que ha proporcionado tradicionalmente sólo servicio de best-effort, ha sido de proporcionar algún tipo de garantías de servicio para diferentes tipos de tráfico. Esto ha sido un desafío particular para ejecutar aplicaciones de video, que a menudo requieren una cantidad significativa de ancho de banda reservada para ser utilizadas.

En la red presentada en la Figura 2.16, RSVP se utiliza en conjunción con ATM PVCs para proporcionar ancho de banda garantizado a una malla de ubicaciones. RSVP es configurado dentro del IOS para proporcionar trayectoria a las redes del router, en los bordes, y a través de ATM core. El tráfico de la simulación entonces utiliza estas trayectorias garantizadas para resolver los apremios de la simulación en tiempo real geográficamente distribuida. La habilitación de video en las máquinas de varios sitios que también utilizan la red puede realizar videoconferencias en vivo.

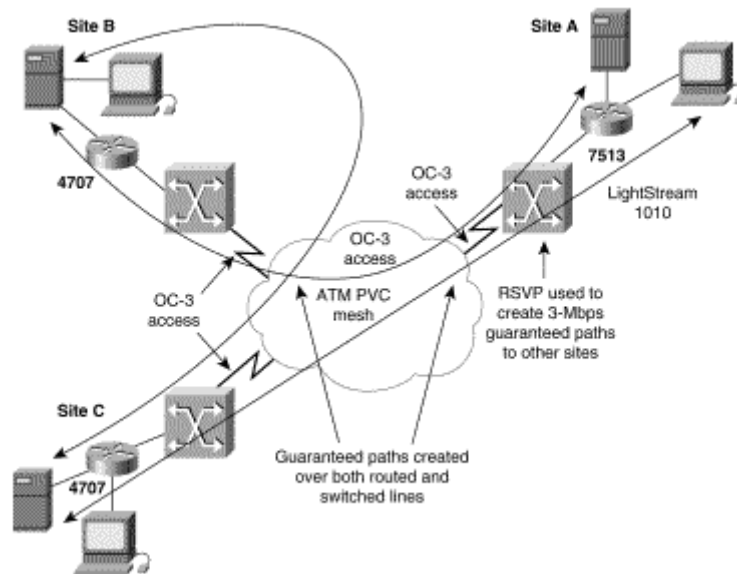


Figura 2.16. El esquema de la red muestra el uso de RSVP en un ambiente engranado de ATM

Fuente: Cisco Networking Academy.

En este caso, los enlaces de ATM OC-3 son configurados con múltiples 3 Mbps de PVCs que conecta a varios sitios remotos. RSVP asegura que QoS para este PVC sea extendido a la aplicación apropiada a través de la red local del router. En el futuro, IOS podría extender esta capacidad de RSVP para establecer dinámicamente ATM SVCs. Esto podría reducir la complejidad de configuración y agregará un gran grado de configuración automática.

2.21. ESTÁNDARES IEEE

Los documentos de los estándares de IEEE se desarrollan dentro de las sociedades de IEEE y los comités de coordinación de estándares de la Asociación de Estándares de la IEEE (IEEE-SA). IEEE desarrolla sus estándares a través de consensos, estos son aprobados por el American National Standards Institute, el cual reúne a voluntarios que representan puntos de vista e intereses variados para alcanzar el producto final. Los voluntarios no son necesariamente miembros del instituto. Mientras que IEEE administra el proceso y establece reglas para promover la imparcialidad en el proceso del desarrollo de consensos, la IEEE no evalúa, prueba, o verifica independientemente la exactitud de cualquiera de la información contenida en sus estándares.

El uso de un estándar de IEEE es enteramente voluntario.

2.22.- IEEE 802.1P, Q - QOS SOBRE EL NIVEL DE MAC

2.22.1.- INTRODUCCIÓN

Esta información explica el uso de los estándares IEEE 802.1P y Q, Q es el protocolo de Calidad de Servicio (QoS) sobre el nivel de Mac. Hoy la Internet provee solamente el servicio de Best Effort. Debido a que la Ethernet es la tecnología de acceso de red de área local más utilizada, la importancia de proporcionar un mecanismo de calidad de servicio no debe ser descuidada.

Primero, relacionemos los estándares de IEEE 802.1p, 802.1D y 802.1Q. El estándar de 802.1p se encarga de las clases de tráfico y multicast dinámico que filtran parte del Control del Medio de Acceso (MAC), que en la actualidad es conocida como el estándar IEEE 802.1D. IEEE 802.1Q forma parte del estándar IEEE 802.1D, definiendo una arquitectura para Redes Virtuales LAN y servicios proveídos en Redes Virtuales LAN.

Luego, la expresión de calidad de servicio puede ser definida de acuerdo con el estándar IEEE 802.1p los parámetros siguientes son esenciales para suministrar QoS.

1. Disponibilidad del servicio
2. Pérdida de frame
3. Frame Misordering
4. Duplicación de frames
5. Retardo de tránsito
6. Tiempo de vida del frame
7. Tasa de error del frame no detectado
8. Tamaño de unidad de datos del servicio máximo
9. Prioridad
10. Throughput

Los parámetros de QoS serán expuestos con mayor detalle en una sección posterior.

2.23.- IEEE 802.1Q⁶

⁶ Tomado de : <http://standards.ieee.org/getieee802/download/802.1Q-2003.pdf>

El estándar IEEE 802.1Q fue desarrollado para proporcionar un mecanismo que permita a múltiples redes con switch compartir información transparentemente en el mismo medio físico sin problemas de interferencia entre las redes que comparten el medio (Trunking).

Ningún mecanismo de Calidad de Servicio es definido en este estándar, pero un importante requisito para suministrar QoS es incluido en este estándar, por ejemplo. Habilidad para regenerar prioridades de usuario de los frames recibidos usando prioridades de la información contenida en el frame y regeneración de la tabla de prioridades de usuario para el puerto de recepción.

2.23.1.- ESTRUCTURA DEL PROTOCOLO - VLAN Y LA IEEE 802.1Q

Preamble	SFD	DA	SA	TPID	TCI	Tipo de Longitud	DATOS	FCS
7	1	6	6	2	2	2	42-1496	4

Tabla 2.3.- IEEE 802.1Q frame etiquetado para Ethernet

Fuente: Implementing Cisco Quality of Service (QoS) v2.0

- Preamble (PRE) - 7 bytes. PRE es un patrón alterno de unos y ceros el cual es enviado para permitir que el receptor pueda sincronizarse con la transmisión que llega y ubicar el inicio de la trama.
- Delimitador de inicio del frame (SFD) - 1 byte. El delimitador del inicio de la trama inicia al comienzo de la trama MAC. El cual es un octeto con la secuencia 10101011.
- Dirección del destinatario (DA) - 6 bytes. El campo de DA identifica qué estación (es) puede recibir el frame.
- Direcciones de la fuente (SA) - 6 bytes. El campo del SA identifica la estación que envía.
- TPID - valor definido de 8100 en hexadecimal. Cuando un frame tiene el EtherType igual a 8100, este frame lleva la etiqueta IEEE 802.1Q/802.1P.
- TCI – Control de etiqueta de información con etiqueta de control incluyendo prioridad del usuario, indicador canónico del formato y la identificación de VLAN.
-

PRI	CFI	VLAN ID
3 bits	1 bit	12 bits

Tabla 2.4.- IEEE 802.1Q parte del frame de Ethernet
Fuente: Implementing Cisco Quality of Service (QoS) v 2.0

- Prioridad del usuario – Define la prioridad del usuario, dando ocho niveles de la prioridad (valores 0 – 7). IEEE 802.1P define la operación para estos 3 bits de prioridad del usuario.
- CFI - El indicador canónico del formato se configura siempre a cero para los switchs de Ethernet. CFI es usado por razones de compatibilidad entre el tipo de red Ethernet y del tipo token ring. Si un frame es recibido en un puerto de Ethernet tiene un CFI configurado en 1, después ese frame no debe ser remitido mientras que está en el puerto no etiquetado.
- VID – VID ID es la identificación de VLAN, donde es básicamente usado por el estándar 802.1Q. Tiene 12 bits y permite la identificación de 4096 (2^{12}) VLANs. De las 4096 VIDs posibles, un VID de 0 es usado para identificar prioridad de frames y el valor 4095 (FFF) es reservado, así que las configuraciones posibles máximas de VLAN es 4.094.
- Tipo de Longitud - 2 bytes. Este campo indica cualquier el número de bytes de datos del cliente MAC que son contenidos en el campo datos del frame, o del tipo ID del frame si el frame es ensamblado usando un formato opcional.
- Los datos - Es una secuencia de n bytes ($42 \leq n < 1496$) de cualquier valor. El mínimo total del frame es 64 bytes.
- Secuencia de Control cíclico (FCS) - 4 bytes. Esta secuencia contiene un valor de 32 bits de control de redundancia cíclica (CRC), cual fue creado por el MAC que envía y recalculado por el MAC de recepción para comprobar que no haya frames dañados.

2.24.- IEEE 802.1D⁷

La actualización de la IEEE 802.1D: ISO/IEC 15802-3(bridge de Mac) el estándar cubre toda las partes de las clases de trafico y el filtrado dinámico de multicast descrito en el estándar IEEE 802.1p. Todos estos asuntos de QoS serán expuestos en la sección de IEEE 802.1p

2.24.1.- ESTRUCTURA DEL PROTOCOLO

2.24.1.1.- DISPONIBILIDAD DEL SERVICIO

⁷ Mayor información se encuentra en <http://standards.ieee.org/getieee802/download/802.1D-2004.pdf>

La disponibilidad del servicio es medida durante el servicio MAC esta disponible y no disponible. Para incrementar el servicio puede ser reconfigurado automáticamente.

2.24.1.2.- PÉRDIDA DE FRAME

El servicio Mac no provee una entrega garantizada de unidades de datos del servicio, pero la probabilidad es alta. La pérdida de frame podría ocurrir:

- Frames dañados en la capa física
- Es descartado el frame por el bridge debido:
 - El frame ha rebasado el tiempo de vida
 - Sobrepasado la capacidad del buffer interno
 - El tamaño de la unidad de datos de servicio que es transportada es muy grande para la LAN.
 - El bridge de la LAN es forzado a descartar el frame para mantener otros aspectos de QoS

2.24.1.3.- FRAME MISORDERING

El Servicio Mac no permite reordenar frames con la misma prioridad de usuario para direcciones de origen y destino.

2.24.1.4.- DUPLICACIÓN DE FRAMES

El servicio de Mac no permite la duplicación de frames.

2.24.1.5.- RETARDO DE TRÁNSITO

El retardo de tránsito de los frame es un lapso de tiempo transcurrido entre un MA_UNITDATA.request y MA_UNITDATA.indication correspondiente sobre una transferencia de satisfactoria.

2.24.1.6.- TIEMPO DE VIDA DEL FRAME

Si los retardos máximos de un frame fueran impuestos por todos los bridges en las redes de área local excede el tiempo de vida del frame deseado debe ser descartado.

2.24.1.7.- TASA DE ERROR DEL FRAME NO DETECTADO

Para usar los cálculos de FCS para cada frame, la tasa de error no detectado es muy baja.

2.24.1.8.- TAMAÑO DE UNIDAD DE DATOS DEL SERVICIO MÁXIMO

El tamaño de unidad de datos del servicio máximo está en función de los medios de acceso usados. Un bridge entre dos LAN tiene el tamaño de unidad de datos del servicio máximo del que tiene el más pequeño.

2.24.1.9.- PRIORIDAD

Servicio Mac cuenta con prioridades de usuario como un parámetro de QoS.

2.24.1.10.- THROUGHPUT

El throughput total de una Bridged LAN puede ser significativamente más grande que el de una LAN equivalente.

2.25.- IEEE 802.1P⁸

Dentro del estándar IEEE 802.1p se encuentran: Tipos de tráfico y prioridades de usuario. Describe importantes métodos para suministrar QoS en el nivel de Mac.

2.25.1.- TIPOS DE TRÁFICO

- a. Control de red; Alto requerimiento para conseguir mantener y respaldar la infraestructura de la red.
- b. Voz; El retardo debe ser menor a 10 milésima de segundos.
- c. Video; El retardo debe ser menor a 100 milésima de segundos.
- d. Carga controlada; Para algunas aplicaciones importantes.

<http://standards.ieee.org/getieee802/download/802.1D-2004.pdf>, Anexo G

- e. Excelente Esfuerzo (Excellent Effort); Best Effort por importancia de usuario.
- f. Mejor esfuerzo (Best Effort); La prioridad ordinaria de LAN
- g. Background; Transferencia Bulk, juegos etc.

Refiérase a la tabla 2.5 y 2.6

Prioridad de Usuario	Acrónimo	Tipo de tráfico
1	BK	Background
2	–	Spare
0	BE	Best Effort
3	EE	Excelente Effort
4	CL	Controlled Load
5	VI	Video
6	VO	Voz
7	NC	Control de la red

Tabla 2.5.- Tipos de Tráfico y Prioridad de Usuario según IEEE 802.1p.

Fuente: IEEE 802.1D Versión 2004 Anexo G.

Número de colas	Tipos de tráfico
1	BE, EE, BK, VO, CL, VI, NC.
2	BE, EE, BK, VO, CL, VI, NC.
3	BE, EE, BK, CL, VI, VO, NC.
4	BK, BE, EE, CL, VI, VO, NC.
5	BK, BE, EE, CL, VI, VO, NC.
6	BK,

	BE, EE, CL, VI, VO, NC.
7	BK, BE, EE, CL, VI, VO, NC.

Tabla 2.6.- Asignación de Colas y Tipos de Tráfico según IEEE 802.1p.

Fuente: IEEE 802.1D Versión 2004.

CAPÍTULO III

PROPUESTA DE IMPLEMENTACION DE QoS

3.1. ANALISIS DE LA SITUACION ACTUAL (Características Técnicas)

En la actualidad la Dirección de Servicios Informáticos cuenta con tecnología de punta la misma que está siendo subutilizada ya que sus servidores y los concentradores no se encuentran trabajando para lo que fueron diseñados esto por el escaso numero de computadores que trabajan en la Universidad y mientras no se habilite nuevos laboratorios y mas usuarios de computadores no podría mejorar el panorama, a continuación detallamos con los equipos y el mapa de ubicación de equipos con el que cuenta la Universidad en la actualidad, al momento de desarrollar la presente aplicación, teniendo en cuenta que el campus se encuentra en pleno funcionamiento forma física sus instalaciones mas no la parte tecnológica.

3.1.1. SERVIDORES

3.1.1.1. SERVIDOR COMPAQ PROLIANT

Información General

Tipo	Servidor
Uso recomendado	Empresarial
Factor de Forma	Torre
Cantidad de Compartimentos Frontales	4
Cantidad de compartimentos de Hot Swap	4
Anchura	27 cm
Profundidad	57.6 cm
Altura	47.3 cm
Peso	28.3 Kg.

Color Blanco

Procesador

Tipo Intel Pentium III 1 Ghz

Cantidad Instalada 1

Cantidad Máxima Soportada 2

Velocidad de bus de datos 133 Mhz

Capacidad de Actualización Actualizable

Tipo conjunto de chips ServerWorks ServerSet III LE

Memoria Cache

Tipo L2- Advanced Transfer Cache

Tamaño Instalado 256KB (Instalados) / 512 KB(max)

Memoria RAM

Tamaño Instalado 256 MB /4 GB (max)

Tecnología SDRAM – ECC

Velocidad de memoria 133 Mhz

Factor de Forma DIMM 166 PIN

Características Registrado

Norma de Actualización Max. 1 GB módulo

Controlador de Almacenamiento

Tipo 1 x SCSI – integrado – PCI

Tipo de Controlador Interfaz	Ultra2 Wide SCSI
Nº canales	2
Almacenamiento	
Unidad de disquete	Disquete de 3.5 " de 1.44 MB
Disco Duro	2 x 18.2 GB hot swap – Ultra2 Wide SCSI
Conexión de Redes	
Conexión de Redes	Adaptado de red v- PCI – Integrado
Protocolo de Interconexión de datos	Ethernet, Fast Ethernet
Red / Protocolo de Transporte	TCP/IP
Cumplimiento de Normas	IEEE 802.3, IEEE 802. 3U
Alimentación	
Tipo de dispositivo	Fuente de alimentación
Cantidad Instalada	1
Cantidad Máxima Soportada	2
Voltaje Necesario	CA 100/240 ± 100% (50/60 Hz.)
Potencia Suministrada	325 vatios
Cumplimiento de normas	EPA Energy Star
Sistemas Operativos	
OS proporcionado	Controladores y utilidades, Compaq Insight Manager, Compaq SmartStart
Software	
Parámetros de Entorno	

Temperatura mínima de funcionamiento	10° C
Temperatura máxima de funcionamiento	35°C
Ámbito de humedad de funcionamiento	20 – 80 %
Emisión de sonido	44 dB

3.1.1.2. SERVIDOR Dell PowerEdge 1800

Factor de Forma	Tore
Procesadores	2 Microprocesadores Intel Xeon, con tecnología de 64 bits de Memoria Ampliada hasta a 3, 4 Ghz.
Bus Frontal	800 Mhz
Cache	1 MB L2
Chipset	Intel E7250
Memoria	2048 MB en DDR2 de 400 con disponibilidad de ampliar hasta 12 GB en un único bastidor de “Gb DIMM”
Canales de E/S	Seis en total de dos ranuras PCI Express (1 * 8 vías y 1 * 4 vías) dos ranuras PCI- X (64bits/100 Mhz); una PCI(32bits/33Mhz, 5v) y una PCI (64 bits/66Mhz)
Controlador de Unidad	Canal simple incorporado Ultra320 SCSI y controlador SATA de dos canales
Controlador RAID	CERC SATA de 6 canales opcional, CERC SATA 2S, PERC 4/DC, PERC4/SC y PERC4a/DC
Capacidad de Unidades de Disco	Seis unidades SCSI conectables en caliente Ultra320 de 1 “o seis de SATA de conexión por cable

Almacenamiento Interno máximo	SCSI; hasta 1,8 TB con soporte para y disponibilidad de disco duro de 300GB; SATA: hasta 1,5 TB
Unidades de disco duro	Originalmente cuenta con dos discos duros de 76 GB, el equipo es expandible a seis de diferentes capacidades y velocidades estos pueden ser SATA o SCSI
Almacenamiento Interno	Unidades de 10K / 15K RPM SCSI, unidades 7200 RPM SATA
Almacenamiento externo	SCSI de PowerVault de Dell y almacenamiento de canal de fibra de DEII/EMC
Opciones de copia de seguridad en cinta	Interno; PowerVault 100T, 110T; unidades de cinta de altura ½ soportadas internamente
Tarjeta de Interfaz de Red	Externo: PowerVault 114T, 122T y 132T Incorporado simple Intel 10/100/1000Gigabit NIC, Intel PRO/1000MT Gigabit NIC(cobre), Intel PRO/1000 MF Gigabit NIC (fibra)
Fuente de Alimentación	650 W no redundante o alimentación redundante conectable en caliente a 675W
Disponibilidad	Memoria ECC, Corrección de Datos de dispositivo simple(SDDC), conexión en caliente opcional Unidades de disco duro SCSI, alimentación redundante de conexión en caliente opcional, chasis sin necesidad de herramientas, soporte para canal de fibra de alta disponibilidad y cluster SCSI, hardware o software RAID opcional ; Active ID
Video	ATI Radeon 7000-M incorporado con SDRAM de 16MB
Gestión Remota	Controlador de gestión de placa base con

Gestión de Sistemas	soporte IPMI 1.5, accesible mediante red o puerto serie, tarjeta PCI DRAC 4/P opcional
Soporte de Rack	OpenManage de DELL
Sistemas Operativos	4 postes (bastidor Dell) y otros fabricantes Microsoft, Linux, Solaris , Novell Netware

3.1.1.3. PC SERVER

En la actualidad por el crecimiento a nivel tecnológico de la Dirección de Servicios Informáticos se ha visto en la necesidad de adaptar momentáneamente algunos computadores normales, para que hagan las funciones de servidores, en total se dan con 3 computadores que hacen de servidores Web, Bases de Datos y Respaldos.

PLACA BASE

Tipo	Torre
Procesador	Intel Pentium 4, 2800 MHz.(21 * 133)
Reloj externo	533 MHz.
Velocidad de reloj Máxima	3200 MHz.
Velocidad de reloj actual	2800 MHz.
Voltaje	1.5 V
Identificación del socket	XU1 Processor
Placa Base	Hewlett-Packart HP dc5000 uT(PB642A)
Chipset de la Placa Base	Intel Morgan Hill i865GV
Memoria del Sistema	503 MB DDR SDRAM
Tipo de BIOS	Compaq(02/12/2004)

Puerto de Comunicación	Puerto de Comunicaciones (COM1)
Puerto de Comunicación	Puerto de Comunicaciones (LPT1)

Almacenamiento

Controlador IDE	Controladora de almacenamiento Intel(r) 82801EB Parallel Ultra ATA-24DB
Disquetera de 3 1/2	Unidad de disquete
Disco Duro	Maxtor 6Y080L0 (80 GB, 7200 RPM, Ultra – ATA/133)
Lector Óptico	HL- DT –ST CD – RW GCE – 8526B (52x/32x/52x CD-RW)
Lector Óptico	SAMCUNG CD-ROM SC- 152L (52x CD ROM)

3.1.2. SWITCH

En lo que tiene que ver a los concentradores la Dirección de Servicios Informáticos cuenta con la siguiente infraestructura la misma que se detalla a continuación:

Switch 3COM OfficeConnect Dual Speed de 16 Puertos

Información del Producto:

Clave de Artículo: 55015

Garantía: 1 año

Modelo del Fabricante: 3C16792A



Este switch básico y económico acelera las aplicaciones de base de datos, contabilidad y multimedia, así como el intercambio de archivos. Idóneo para servidores de alta velocidad, troncales o estaciones de trabajo de usuarios que requieren un alto rendimiento. O use este switch para añadir más hubs Fast Ethernet a un grupo de trabajo. El Auto MDI-MDIX en cada puerto simplifica la expansión de red al eliminar los errores de cableado más comunes, tanto si el puerto está conectado a un servidor, a un PC o a otro switch o hub.

Especificaciones

- Con instalación plug-and-play y sin necesidad de configuración, el switch encaja fácilmente en su red sin administración
- El Auto MDI/MDIX en cada puerto simplifica la expansión de red al eliminar los errores de cableado más comunes
- Dieciséis puertos con auto-detección identifican automáticamente la velocidad del dispositivo conectado para maximizar el rendimiento de la red
- Con instalación plug-and-play y sin necesidad de configuración, encaja fácilmente en su red sin administración
- La función full-duplex soporta la transferencia de datos en los dos sentidos, duplicando así el ancho de banda efectivo de la red
- El diseño compacto, sin ventiladores, garantiza un funcionamiento silencioso en espacios de pequeñas oficinas
- Los conectores en la parte trasera ayudan a reducir la acumulación de cables enredados

Especificaciones de producto Puertos totales:

- 16 puertos 10/100 Ethernet con detección automática
- Interfaces con los medios:

10/100BASE-TX/RJ-45

Características de switching Ethernet:

Store-and-forward; autonegociación full/half dúplex

Altura: 54,6 mm

Anchura: 228 mm

Fondo: 185,4 mm

Switch 3Com® SuperStack® 3 Baseline 10/100 de 24 puertos



Información del Producto:

Clave de Artículo: 30559

Modelo del Fabricante: 3C16471

Características y ventajas

Switching simple y rico en funcionalidad para usuarios diversos

El Switch 3Com® SuperStack® 3 Baseline 10/100 de 24 puertos es un switch sin bloqueo y sin necesidad de administración diseñado para oficinas pequeñas a medianas. Este switch de clase empresarial, que se puede instalar en rack, puede colocarse en el armario de cableado o como unidad autónoma.

El switch viene pre-configurado para una instalación rápida y fácil, utilizando económicos cables de cobre. Su auto-negociación ajusta la velocidad del puerto con la del dispositivo de comunicación. Cualquiera de los 24 puertos del switch pueden ofrecer Ethernet 10BASE-T para usuarios con requerimientos promedio de ancho de

banda, o Fast Ethernet 100BASE-TX para usuarios de potencia con conexiones de red más nuevas.

Además, la detección automática del tipo de cable Ethernet (MDI/MDIX) simplifica las conexiones del cable. Y el establecimiento integrado de prioridades IEEE 802.1p con dos filas de prioridades facilita la administración del tráfico en redes de empresas más grandes.

Al igual que todos los productos 3Com SuperStack 3 Baseline, este switch ofrece una practicidad poderosa y rica en funcionalidad en un robusto paquete diseñado para brindar fiabilidad, larga vida y un bajo coste total de propiedad.

- El switch trabaja "al sacarlo de su caja" - no se necesita configuración o software de administración
- El rendimiento sin bloqueo se traduce en un mejor acceso a los recursos de la red
- La auto-negociación 10/100 determina automáticamente la velocidad correcta para el puerto
- MDI/MDIX automático en todos los puertos simplifica la instalación al permitir una conexión directa a otro dispositivo, utilizando cables directos o entrecruzados
- Establecimiento de prioridades- IEEE 802.1p con dos filas de prioridad por puerto; libera las redes para las aplicaciones en tiempo real y otras aplicaciones de alta prioridad
- Su sólido diseño y calidad de construcción aseguran una operación fiable y larga vida.
- Se puede usar junto con otros switches y hubs 3Com® SuperStack® 3 Baseline para expandir su capacidad
- Se puede instalar en un rack o apilarse para maximizar el espacio disponible; su tamaño estándar 1RU simplifica la planificación del espacio

Puertos: 24 puertos 10BASE-T/100BASE-TX con auto-detección y auto-configuración MDI/MDIX

Interfaces para medios: RJ-45

Funciones de switching Ethernet: Velocidad total sin bloqueo en todos los puertos Ethernet, auto-negociación y control de flujo bidireccional / semi-dúplex, establecimiento de prioridades de tráfico, 802.1p

Direcciones MAC que se soportan: 4,000

Alto: 4.36 cm (1.7 pulgadas)

Ancho: 44 cm (17.3 pulgadas)

Profundidad: 23.5 cm (9.3 pulgadas)

Peso: 3 kg

Switch 3Com® Baseline Switch de 16 Puertos 10/100Mbps



Información del Producto:

Clave de Artículo: 54257

Modelo del Fabricante: 3C16470

Información Adicional:

3Com Baseline Switch

Características y ventajas Switching simple y rico en funcionalidad para usuarios diversos

El Switch 3Com® SuperStack® 3 Baseline 10/100 de 16 puertos es un switch sin bloqueo y sin necesidad de administración diseñado para oficinas pequeñas a medianas. Este switch de clase empresarial, que se puede instalar en un rack, puede colocarse en el armario de cableado o como unidad autónoma.

El switch viene pre-configurado para una instalación rápida y fácil, utilizando económicos cables de cobre. Su auto-negociación ajusta la velocidad del puerto con la del dispositivo de comunicación. Cualquiera de los 16 puertos del switch pueden ofrecer Ethernet 10BASE-T para usuarios con requerimientos promedio de ancho de

banda, o Fast Ethernet 100BASE-TX para usuarios de potencia con conexiones de red más nuevas.

Además, la detección automática del tipo de cable Ethernet (MDI/MDIX) simplifica las conexiones del cable. Y el establecimiento integrado de prioridades IEEE 802.1p con dos filas de prioridades facilita la administración del tráfico en redes de empresas más grandes.

Al igual que todos los productos 3Com SuperStack 3 Baseline, este switch ofrece una practicidad poderosa y rica en funcionalidad en un robusto paquete diseñado para brindar fiabilidad, larga vida y un bajo coste.

- El switch trabaja al sacarlo de su caja-no se necesita configuración o software de administración
- El rendimiento sin bloqueo se traduce en un mejor acceso a los recursos de la red
- La auto-negociación 10/100 determina automáticamente la velocidad correcta para el puerto
- MDI/MDIX automático en todos los puertos simplifica la instalación al permitir una conexión directa a otro dispositivo, utilizando cables directos o entrecruzados
- Establecimiento de prioridades- IEEE 802.1p; con dos filas de prioridad por puerto- libera las redes para las aplicaciones en tiempo real y otras aplicaciones de alta prioridad
- Su sólido diseño y calidad de construcción aseguran una operación fiable y larga vida
- Se puede usar junto con otros switches y hubs 3Com® Baseline para expandir su capacidad
- Se puede instalar en rack o apilarse para maximizar el espacio disponible; su tamaño estándar 1RU simplifica la planificación del espacio

Especificaciones de producto

- Puertos: 16 puertos 10BASE-T/100BASE-TX con auto-detección y auto-configuración MDI/MDIX
- Interfaces para medios: RJ-45

- Funciones de switching Ethernet: Velocidad total sin bloqueo en todos los puertos Ethernet, auto-negociación y control de flujo bidireccional / semi-dúplex, establecimiento de prioridades de tráfico, 802.1p
- Direcciones MAC que se soportan: 4,000

Alto: 4.36 cm (1.7 pulgadas)

Ancho: 44 cm (17.3 pulgadas)

Profundidad: 23.5 cm (9.3 pulgadas)

• Peso: 3 kg

HUB 3COM Office Connect, Dual Speed, 8 Puertos, 10/100Mbps.



Información del Producto:

Modelo del Fabricante: 3C16701

Características y ventajas

Conectividad asequible en red de alta velocidad para las pequeñas empresas

Este flexible y fiable conmutador 'plug and play' ha sido diseñado específicamente para ofrecer a las pequeñas empresas o a las oficinas en el hogar, una vía de migración suave al rendimiento Fast Ethernet, con soporte para los ordenadores y los dispositivos de red adaptados a Ethernet.

Sus ocho puertos 'autosensing' 10/100 se adaptan a la velocidad de cualquier dispositivo para optimizar el rendimiento. Su conmutador integrado conecta sin obstáculos a los usuarios de 10/100 Mbps.

- Soporta hasta ocho usuarios o dispositivos
- Su conmutador interno integra segmentos de 10 y de 100 Mbps
- Sus indicadores luminosos de estado y colisión simplifican las tareas de monitorización

- Su puerto MDI/MDIX ofrece una conexión sencilla con otro concentrador o conmutador OfficeConnect® de 3Com®, o con un servidor o PC
- Ocupa muy poco espacio gracias a su reducido tamaño Su sistema de anclaje de una sola pieza facilita la ampliación
- Presenta un diseño muy ergonómico con un claro panel frontal que facilita la solución de problemas
- Su fuente de alimentación externa y su diseño de auto enfriado, eliminan la necesidad de un ruidoso ventilador
- Su garantía limitada sin fecha de vencimiento, proporciona una gran tranquilidad

Especificaciones de producto

- Puertos por concentrador: Ocho Ethernet 10/100 Mbps
- Soportes: Ocho conectores RJ-45 10BASE-T/100BASE-TX
- Indicadores luminosos del sistema: Colisión, energía
- Indicadores luminosos de puertos: Velocidad de la red (10 ó 100 Mbps)
- Sistemas op. que soporta: Novell NetWare, Windows 2000/98/95/NT 4.0
- Tipo de concentrador: Novell NetWare, Windows 2000/98/95/NT 4.0
- Requisitos de alimentación: 3 VA

Alto: 4,2 cm (1,6 in)

Ancho: 22,8 cm (9,1 in)

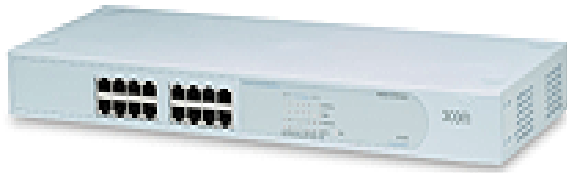
Fondo: 13,5 cm (5,3 in)

Contenidos del paquete

- Concentrador
- Adaptador de corriente de 11 vatios
- Soportes de goma
- Sistema de apilación de un solo anclaje
- Guía del usuario

3Com® Baseline Switch 2016

3C16470



Características y ventajas

Switching simple y rico en funcionalidad para usuarios diversos

El 3Com® Baseline Switch 2016 es un switch 10/100 de 16 puertos, sin bloqueo y sin administración diseñado para oficinas pequeñas a medianas. Este switch de clase empresarial, que se puede instalar en un rack, puede colocarse en el armario de cableado o como unidad autónoma.

El switch viene pre-configurado para una instalación rápida y fácil, utilizando económicos cables de cobre. Su auto-negociación ajusta la velocidad del puerto con la del dispositivo de comunicación. Cualquiera de los 16 puertos del switch pueden ofrecer Ethernet 10BASE-T para usuarios con requerimientos promedio de ancho de banda, o Fast Ethernet 100BASE-TX para usuarios de potencia con conexiones de red más nuevas. Para simplificar la conexión de cables, los 26 puertos detectan automáticamente el tipo de cable Ethernet (MDI/MDIX).

Al igual que todos los productos 3Com SuperStack 3 Baseline, este switch ofrece una practicidad poderosa y rica en funcionalidad en un robusto paquete diseñado para brindar fiabilidad, larga vida y un bajo coste.

El switch trabaja al sacarlo de su caja-no se necesita configuración o software de administración

El rendimiento sin bloqueo se traduce en un mejor acceso a los recursos de la red

La auto-negociación 10/100 determina automáticamente la velocidad correcta para el puerto

MDI/MDIX automático en todos los puertos simplifica la instalación al permitir una conexión directa a otro dispositivo, utilizando cables directos o entrecruzados

Su sólido diseño y calidad de construcción aseguran una operación fiable y larga vida

Se puede instalar en rack o apilarse para maximizar el espacio disponible; su tamaño estándar 1RU simplifica la planificación del espacio

3.2. DESCRIPCIÓN DEL ENTORNO

3.2.1. ELEMENTOS DE RED

En la Universidad Técnica de Cotopaxi en la actualidad existen 3 Centros de Datos los cuales dan servicios a las diferentes áreas de la institución. Los Centros de Datos se encuentran interconectados por cable utp 5e y cuya configuración es la EIA/TIA 568^a(CD 1 se encuentra en la Dirección de Servicios Informático en el segundo piso de la Universidad) y por cable UTP interconectado el (CD2 y el CD3) el CD2 se encuentra en el laboratorio 1 y 2.El CD3 se encuentra ubicada en el laboratorio 3.

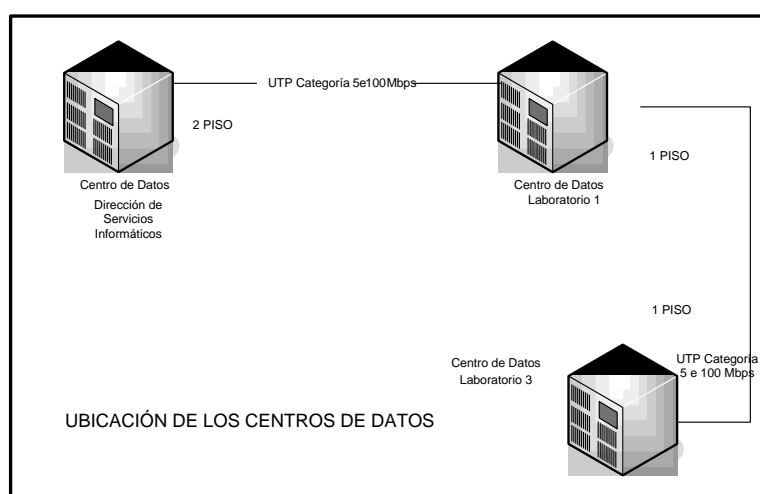


Figura 3.1. Distribución de los Centros de Datos UTC.

Fuente: Grupo Investigador

Como podemos observar en la grafica anterior el Centro de datos 1 es el que se encarga de distribuir las comunicaciones en toda la Universidad, este a su vez se comunica con los Centros de datos 2 y 3 los mismos que abastecen a los laboratorios y las oficinas que se encuentran en la Planta Baja del edificio antiguo de la UTC.

En la presenta grafica no encontramos el Edificio Verde como Centro de datos ya que es una red independiente la misma que por el numero de usuarios y la arquitectura planteada no cumple para ser tomado todavía como Centro de datos, sino más bien como un canal de datos, el mismo que llega a un concentrador y se encarga únicamente de distribuir la información.

3.2.1.1.- CENTRO DE DATOS 1

En el centro de Datos 1 se encuentra equipado de un Rack el mismo que se encuentra distribuyendo las redes a todos los estamentos universitarios.

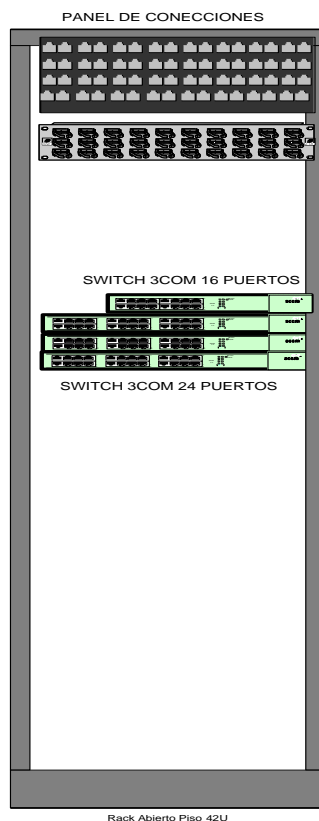


Figura 3.2. Distribución de los Centros de Datos UTC.

Fuente: Grupo Investigador

El Centro de Datos 1 es el distribuidor principal de servicios la institución al cual todos los demás centros de Datos deben conectarse para lo cual se ha venido utilizando cable UTP categoría 5e el cual está interconectados con los Centros de Datos 2 y el Centro de Datos 3.

A continuación detallamos como en la actualidad distribuye el enlace mediante las redes el mismo que parte del Centro de Datos1 a los Centros de Datos 2 y 3, y las dependencias más próximas a la oficina de Dirección de Servicios Informáticos que se le ha llamado Centro de Datos 1.

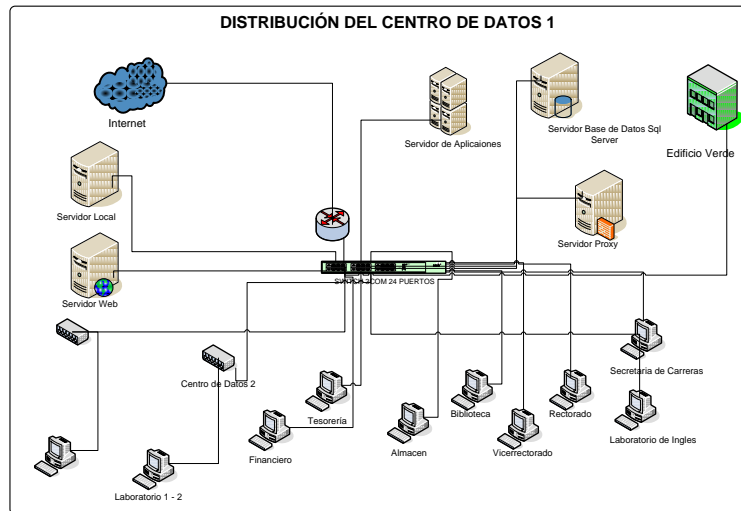


Figura 3.3.: Distribución de Equipos y segmento de Red UTC – Noviembre 2006

Fuente: Grupo Investigador

3.2.1.2. CENTRO DE DATOS 2

En el Centro de Datos 2 encontramos la siguiente distribución la misma que comprende los laboratorios informáticos 1 y 2 que se encuentran distribuidas 19 computadores por laboratorio. Refiérase a la figura 3.4.

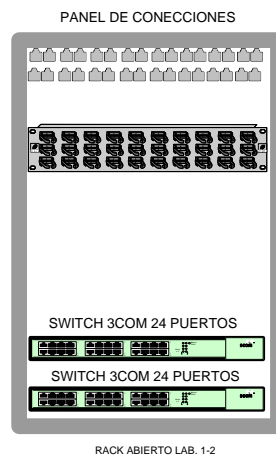


Figura 3.4.: Rack del Centro de datos 2– Noviembre 2006

Fuente: Grupo Investigador

La distribución se lo hace a través de dos switch los mismos que son interconectados a través de un patch panel que se encuentran todos estos componentes por medio de un patch cord, formando una red académica.

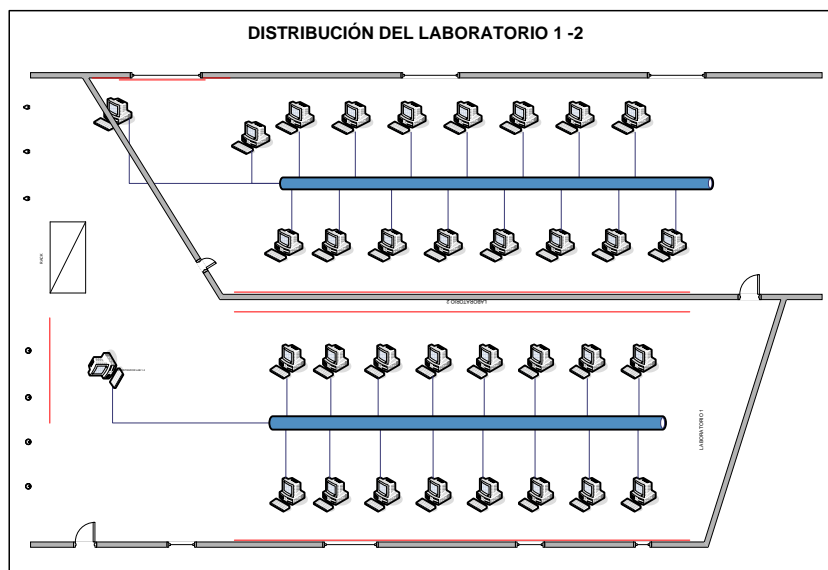


Figura 3.5.: Distribución de Equipos y segmento de Red de los Laboratorios 1 y 2 de la UTC – Noviembre 2006

Fuente: Grupo Investigador

3.2.1.3.- CENTRO DE DATOS 3

En el Centro de Datos 3 encontramos 1 switch y un hub los mismos que distribuyen la señal en los laboratorios 3 y 4 adicionalmente a la oficina de la FEUE – C.

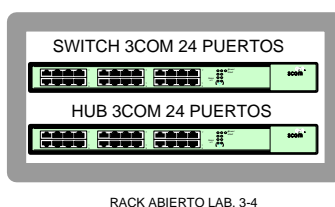


Figura 3.5.: Centro de Datos 3 de la UTC – Noviembre 2006

Fuente: Grupo Investigador

El Centro de Datos 3 como se puede observar al contar con un HUB, tiene algunos problemas de pérdida de información por las colisiones que se dan al no tener un switch que realice la distribución ordenada de la señal.

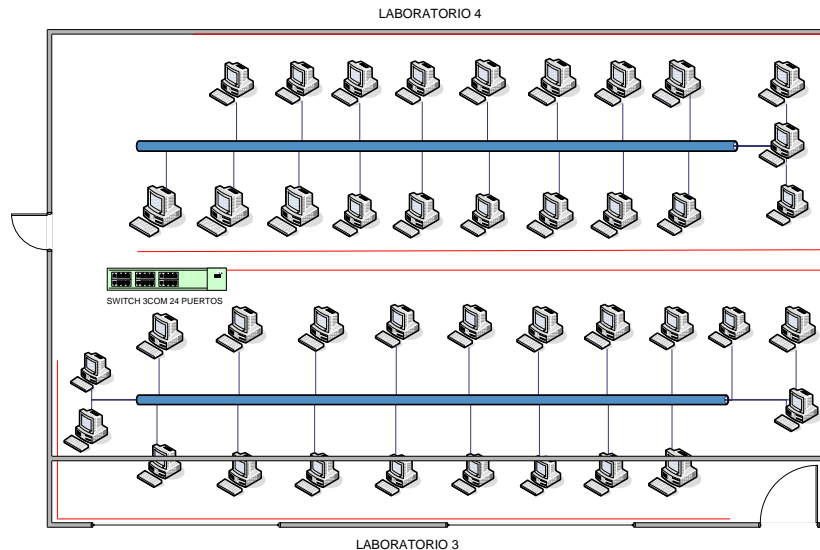


Figura 3.6.: Centro de Datos 3 de la UTC – Noviembre 2006

Fuente: Grupo Investigador

3.2.1.4.- TOPOLOGÍA DE RED

La topología de red implementada en la Red de la Universidad Técnica de Cotopaxi es Estrella.

3.2.1.5.- CABLEADO

En la actualidad la Universidad Técnica de Cotopaxi cuenta con un cableado estructurado bajo la norma EIA/TIA 568 A.

Para la comunicación entre las estaciones de trabajo y los switches se utiliza cable UTP categoría 5e. Además interconectan los centros de datos de la Universidad.

3.2.1.6.- ESTACIONES DE TRABAJO

El número de estaciones de trabajo que existen en la Universidad Técnica de Cotopaxi están repartidas de la siguiente manera:

- 100 Estaciones de Trabajo en el Área Administrativa.

En los cuales están instalados:

- Windows XP
- Antivirus McAfee 10, Panda Titanium
- Microsoft Office 2003
- Winzip
- Adobe Acrobat Reader
- Aplicaciones de Negocios dependiendo del perfil del usuario

3.2.1.7.- SERVIDOR

Existen 6 Servidores: 2 PowerEdge™ 1800 de Dell™, 2 Compaq Proliant, 2 Computadores Hp con procesador Core Duo.

- El Primer Servidor cumple la función de Controlador de Dominio en el cuál esta instalado Microsoft Windows 2000 Advanced Server. Realiza las funciones de Controlador de Dominio.
- El Segundo Servidor “Base de Datos” esta instalado con Microsoft Windows 2000 Advanced Server. En el cual está las Bases de Datos de las aplicaciones que en la Universidad se encuentran funcionando, que son en su mayoría en Microsoft SQL Server 2000
- El Tercer equipo es el “Servidor Web” el cual almacena la aplicación o pagina WEB, de la Universidad Técnica de Cotopaxi.
- El Cuarto Servidor es el Proxy, el mismo que reparte el Internet a toda la Universidad.
- El Quinto es de Servidor de la aplicación del departamento financiero el mismo que almacena las Bases de Datos del Olimpo.
- Existe un Sexto servidor el mismo que son de respaldos o en ocasiones hace las veces de servidor de pruebas.

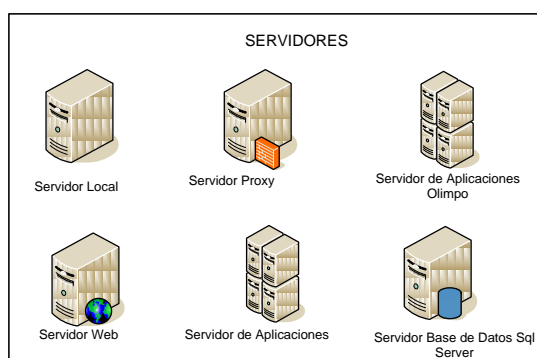


Figura 3.6.: Cuadro detallado de Servidores de la UTC – Noviembre 2006

Fuente: Grupo Investigador

3.2.1.8.- VLANS

- En la actualidad la Universidad Técnica de Cotopaxi no cuenta con VLAN alguna ya que el número de PC no alcanza aun a los 240 equipos, por lo que no se hace urgente la implementación de este tipo de tecnología
- Con el constante incremento de estudiantes y de personal administrativo como docente, el número de equipos por laboratorio y oficinas va incrementándose por lo que adoptar este tipo de tecnología justifica ya la implementación de las mismas.
- Con la implementación de las VLAN la infraestructura tecnológica de telecomunicaciones de la Universidad van a estar mejor organizadas y el rendimiento va a estar optimizado de mejor manera.

3.2.1.9.- ESTÁNDARES DE ETIQUETACIÓN

Por lo anteriormente expuesto y al no contar con un cableado estructurado certificado, se etiqueta de acuerdo al nombre del departamento en el que funciona, en otros casos de acuerdo al laboratorio, al nombre de usuario, en fin dependiendo la ubicación física del equipo.

3.2.1.10.- DIRECCIONES IP

Las Direcciones IP que han sido utilizadas dentro de la Red de la Universidad Técnica de Cotopaxi, ha sido la Clase A que comprenden entre 0 a 127 excluyendo 0 y 127 porque son direcciones reservadas. Esta clase de Direcciones IP son implementadas en la red Interna.

La dirección adoptada para la distribución de la red de la Universidad Técnica de Cotopaxi es el 10.10.1.0 con una máscara de Subred 255.255.255.0, ya que el número de equipos no exceden de 240, y trabaja un solo tipo de red sin distribución de subredes.

3.3.- RESUMEN DE LA SITUACIÓN ACTUAL

Vamos a detallar en un cuadro, la situación tratando de tomar todos los aspectos que caracterizan el área de tecnología de la Universidad Técnica de Cotopaxi.

ACTIVIDAD	CAUSA	IMPACTO	RECOMENDACIONES
No está implementado un cuarto frío, el cual centralizaría todos los equipos.	Despreocupación de las autoridades universitarias.	No existe un buen desempeño de los servidores y de los concentradores.	Se busque un espacio para poder construir un adecuado cuarto de maquinas informáticas en el cual puedan ser ventilados los servidores y concentradores y que puedan rendir de mejor manera.
Falta de seguridades físicas de los equipos de hardware de redes	Despreocupación de los integrantes del Departamento de Servicios Informáticos y autoridades de la Universidad	Al mal utilizarlos o al ser alterados, o substraídos, puede ocasionar un gran perjuicio a la Universidad por cuanto se perdería información y alteraría el normal desempeño de las actividades	Implementar un plan de contingencia en caso de daños de los equipos, perdidas, o robos de cualquiera de los equipos informáticos.
La universidad no cuenta con una adecuada distribución de equipos y espacios para los ambientes de redes y equipos de concentración.	Despreocupación de las autoridades de la Universidad	No existe un buen desempeño de los equipos y en caso de daños existe demasiado retardo en arreglar los equipos.	Asignar espacios que cuenten con seguridades y que estén en sitios estratégicos de la universidad.
Todavía en los	Despreocupación	Perdida de señal	A corto plazo se debe

Centros de Datos de la Universidad existen HUB, lo cual está propenso a causar colisiones con la información.	de los Técnicos del Departamento de Servicios Informáticos	en las interconexiones, sobre todo cuando la señal tiene que pasar por este tipo de concentrador	intercambiar los HUB por SWITCH ya que se pierde la señal en ocasiones, al producirse colisiones.
No existen seguridades de tipo lógicas al no existir un servidor de Firewall o un IPS o IDS	Despreocupación de los Técnicos de la Dirección de Servicios Informáticos	Puede ocasionar pérdida de información o adulteración en los registros de notas.	Adquirir equipos que ayuden en la seguridad de la información, tal como IPS, IDS o un servidor
Los equipos de los centros de datos se encuentran saturados, cuando se incrementa equipos se hace necesario desconectar otros causando malestar a los usuarios de la red	Despreocupación de los Técnicos de la Dirección de Servicios Informáticos	Que la universidad no pueda adquirir mas equipos de computo para expandirse de mejor manera	Adquirir nuevos SWITCH que guarden un mismo estándar
No existe una adecuada etiquetación de los concentradores, servidores, y equipos que acceden al servidor	Despreocupación de los Técnicos de la Dirección de Servicios Informáticos	Puede ocasionar confusión al momento de pasar información entre equipos.	Se debe etiquetar todos los equipos bajo un estándar de instituciones que rigen las comunicaciones

3.4. IMPLEMENTACIÓN DE CONTROL DE CALIDAD DE SERVICIO (QoS) EN REDES LOCALES VIRTUALES (VLAN) EN LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

3.4.1.- VLANS

La implementación de las VLANS que se va a aplicar en la Universidad Técnica de Cotopaxi son de tipo estáticas las cuales son los puertos en un switch que se asignan estáticamente a una VLAN. Esta configuración está regida por una de las normas en este proyecto de investigación planteadas como es la norma IEEE 802.1D p. Estos puertos mantienen sus configuraciones de VLANS asignadas hasta que se cambien. Aunque las VLAN estáticas requieren que el administrador haga los cambios, este tipo de red mantiene muchas seguridades, de fácil configuración y monitoreo. Las VLANS estáticas funcionan bien en las redes en las que el movimiento se encuentra controlado y administrado, que para el momento y para la Universidad todavía no es el caso.

Para el agrupamiento de las VLANS se realizará por Puertos por las siguientes razones: el agrupamiento de puertos se ha mantenido como el más común de los métodos para la definición de los miembros de una VLAN, y su configuración es bastante directa. Al definir las así no se permite que varias VLANs se incluyan en el mismo segmento físico (o puerto del conmutador).

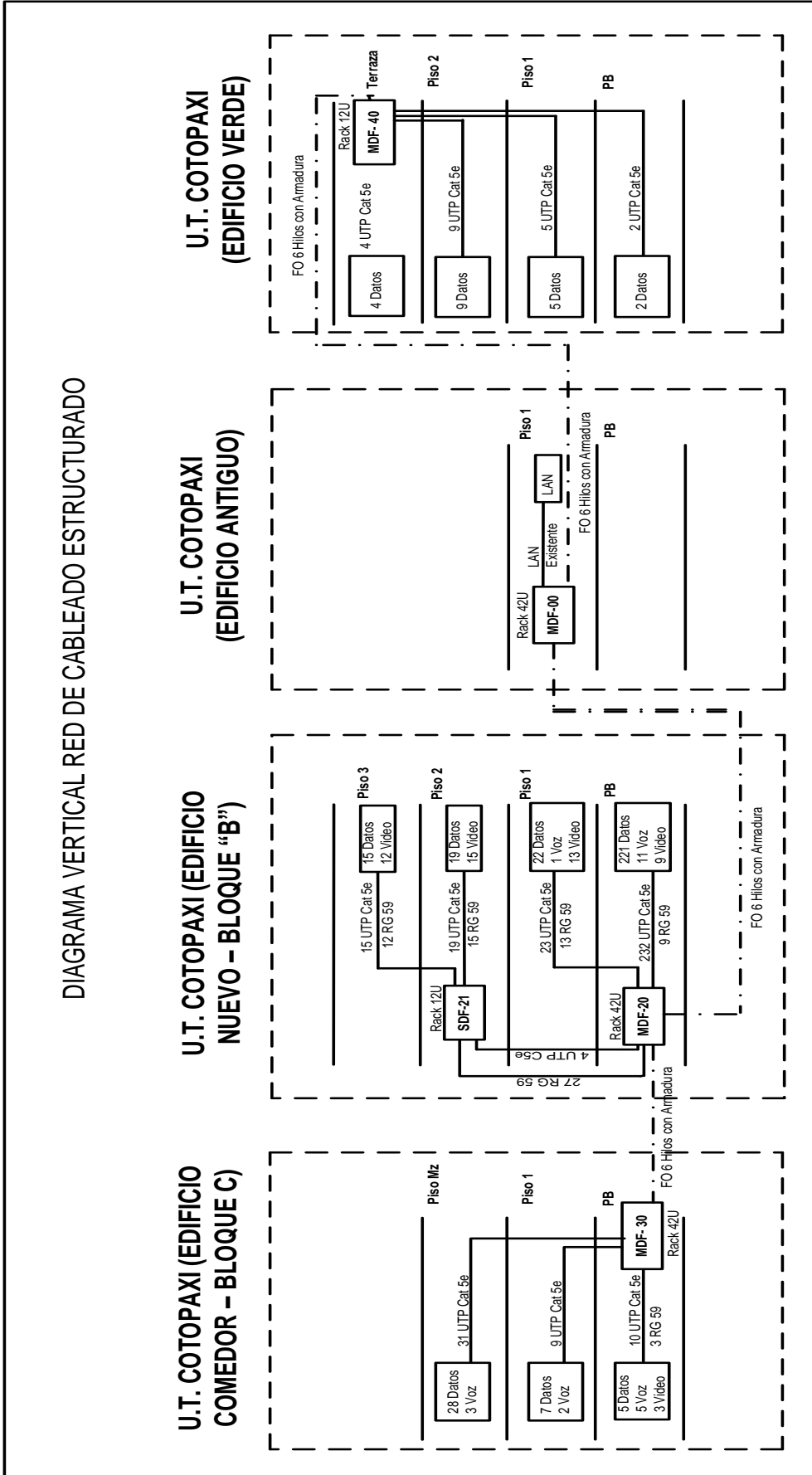
En la figura siguiente podemos encontrar de manera detallada como se encuentran las VLAN en la Universidad hoy en día.

En la página siguiente tenemos:

Figura 3 .7: Diagrama Vertical del cableado Estructurado y VLAN de la UTC

Fuente: Grupo Investigador

DIAGRAMA VERTICAL RED DE CABLEADO ESTRUCTURADO



3.4.2.- SECTORES CRÍTICOS

Los sectores críticos dentro de las VLANS son sectores a los cuales la Calidad de Servicio (QoS) debe darse mayor énfasis. Se deben definir dos tipos de sectores críticos los permanentes y los temporales. Los permanentes son los sectores en los cuales el tráfico siempre esta en aumento. Los temporales son sectores que en la mayor parte del año no tienen mucho trafico pero en épocas especiales (matriculas) el trafico se incrementa.

Los Sectores Permanentes son:

- Secretarías de carrera.
- Dirección de servicios Informáticos.
- Departamento Financiero.
 - Finanzas
 - Contabilidad
 - Colecturía.
- Biblioteca.
- Laboratorios.

Los Sectores Temporales son:

- Laboratorios en época de matriculas.
- Ex oficina de biblioteca de igual manera en época de matriculas

3.4.3.- EDIFICIO

Para la asignación de las VLANs se ha considerado dividir a la universidad por edificios los cuales son los siguientes:

3.4.3.1.- EDIFICIO VERDE

En la actualidad el edificio Verde se encuentra interconectado con el campus antiguo de la universidad con fibra óptica de 6 hilos con armadura la misma que garantiza un alto ancho de banda en las comunicaciones.

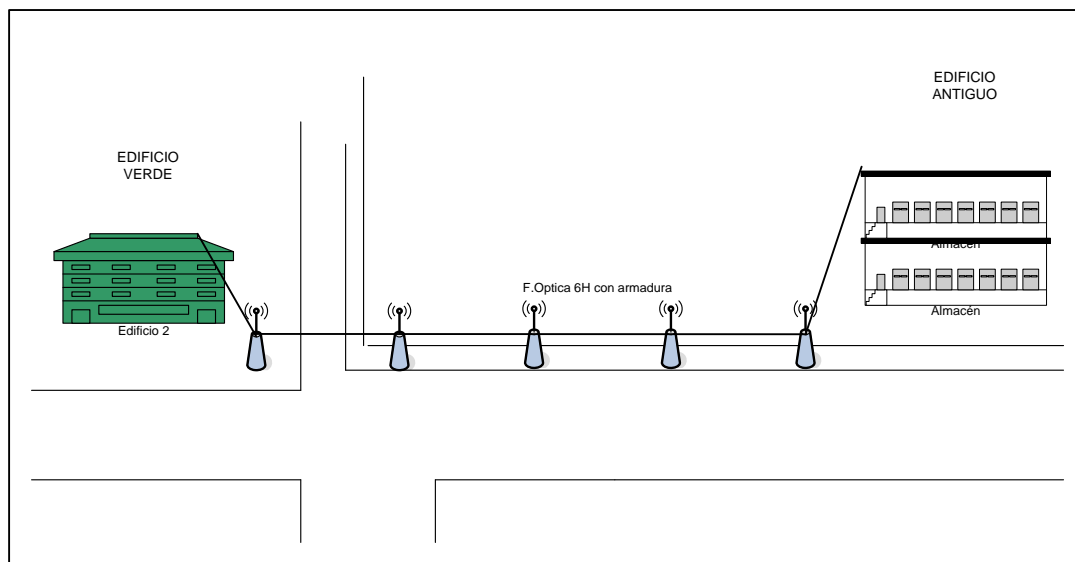


Figura 3.8.- Plano de Comunicación mediante fibra Edificio Antiguo –Edificio Verde

Elaborado por: Grupo Investigador

En la actualidad el edificio verde para una mejor estructuración de sus dependencias en el edificio verde se le ha dividido en 4 plantas la misma que se encuentra dividido en plantas, las dependencias que aquí laboran son:

- Centro Medico
- Dirección de Vinculación Social
- Taller
- Consultorio Medico
- Orientación Vocacional
- Odontología
- Planificación Física
- Secretaria General

- Planificación, Mantenimiento y Construcción.
- Procuraduría
- Bodega
- Cocina
- Practica Docente
- Relaciones Públicas.

Dentro del edificio verde podemos encontrar subdividida en plantas las mismas que se encuentran configuradas de la siguiente manera, el cableado estructurado.

Planta Baja:

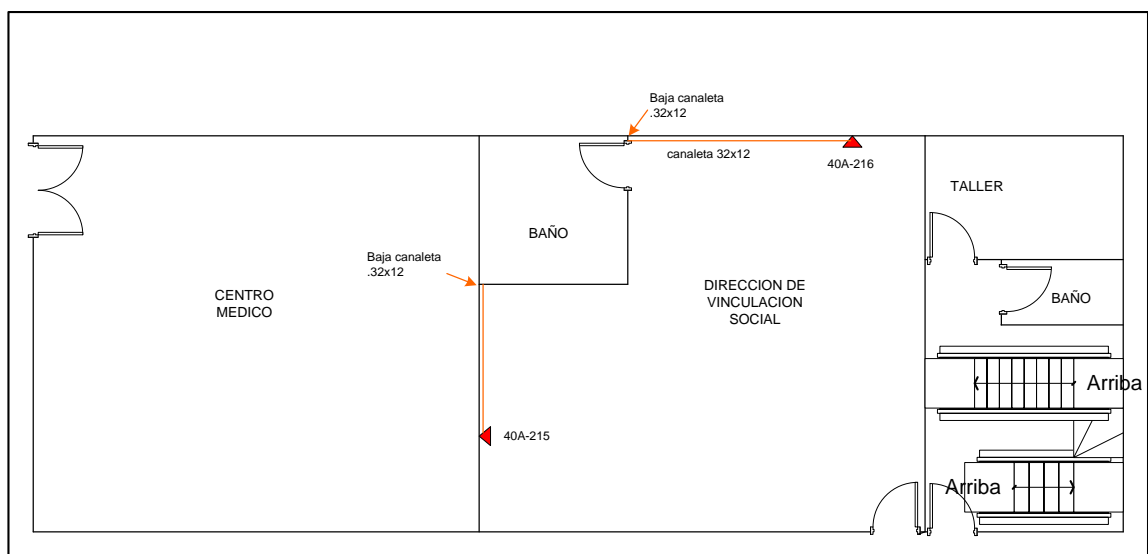


Figura 3.9.- Plano de Comunicación Primera Planta –Edificio Verde

Elaborado por: Grupo Investigador

Primera Planta:

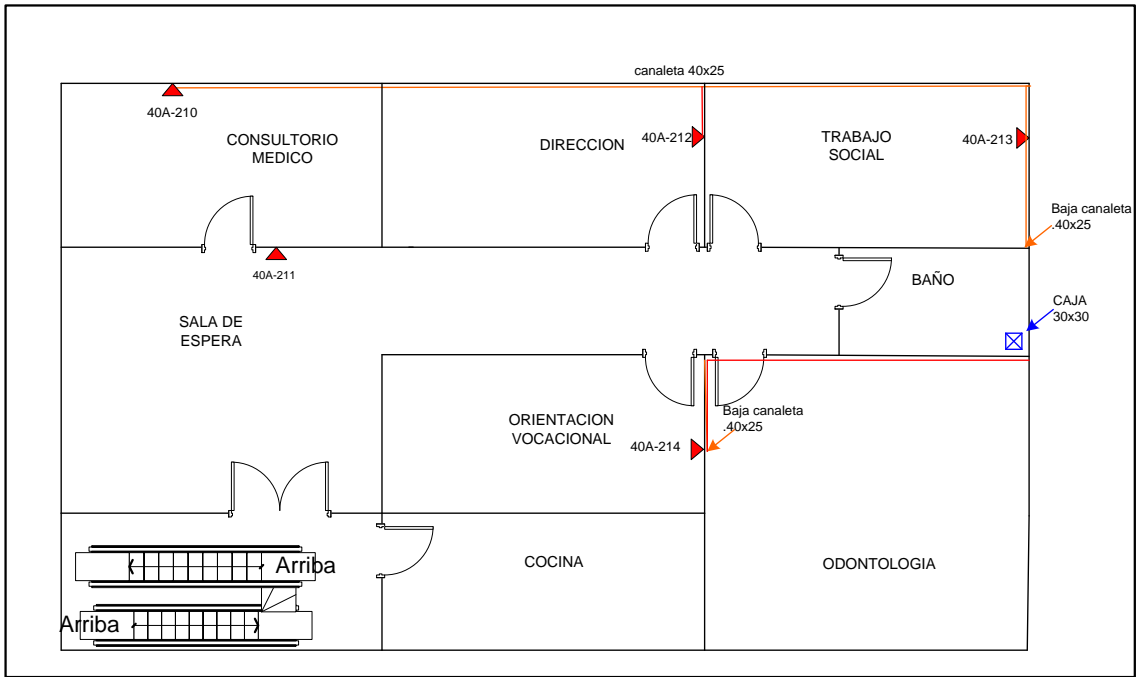


Figura 3.10.- Plano de Comunicación Segunda Planta –Edificio Verde

Elaborado por: Grupo Investigador

Segunda Planta:

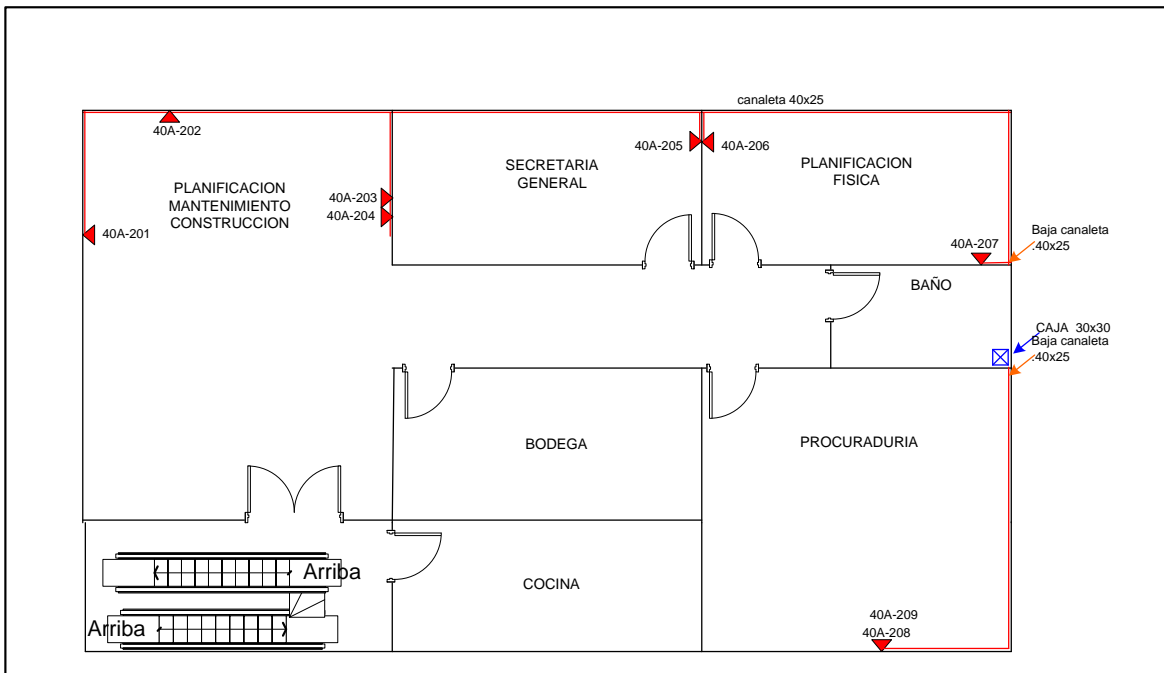


Figura 3.11.- Plano de Comunicación Tercera Planta –Edificio Verde

Elaborado por: Grupo Investigador

Terraza:

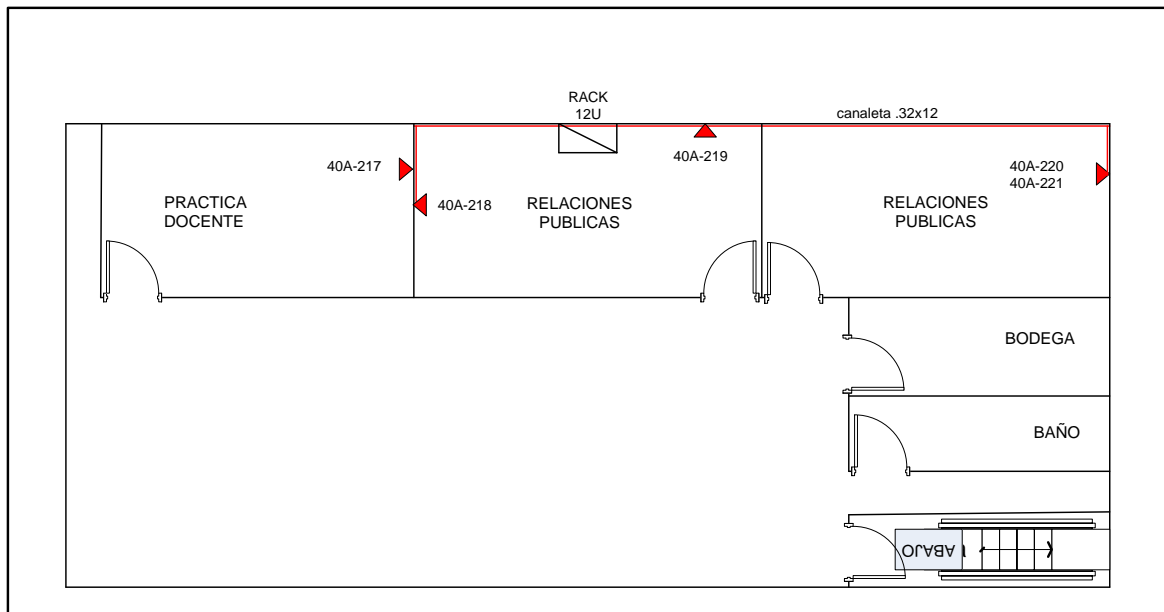
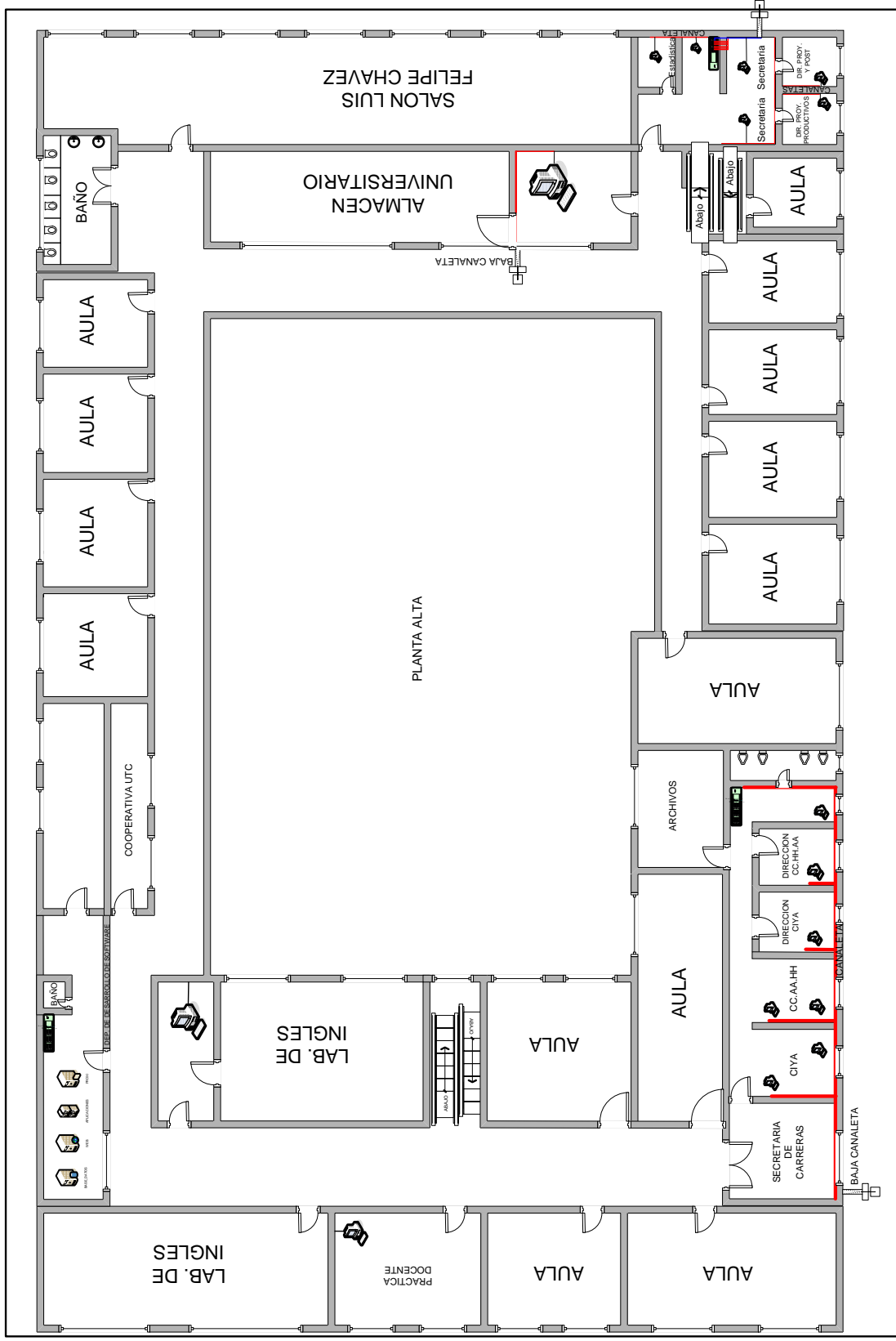


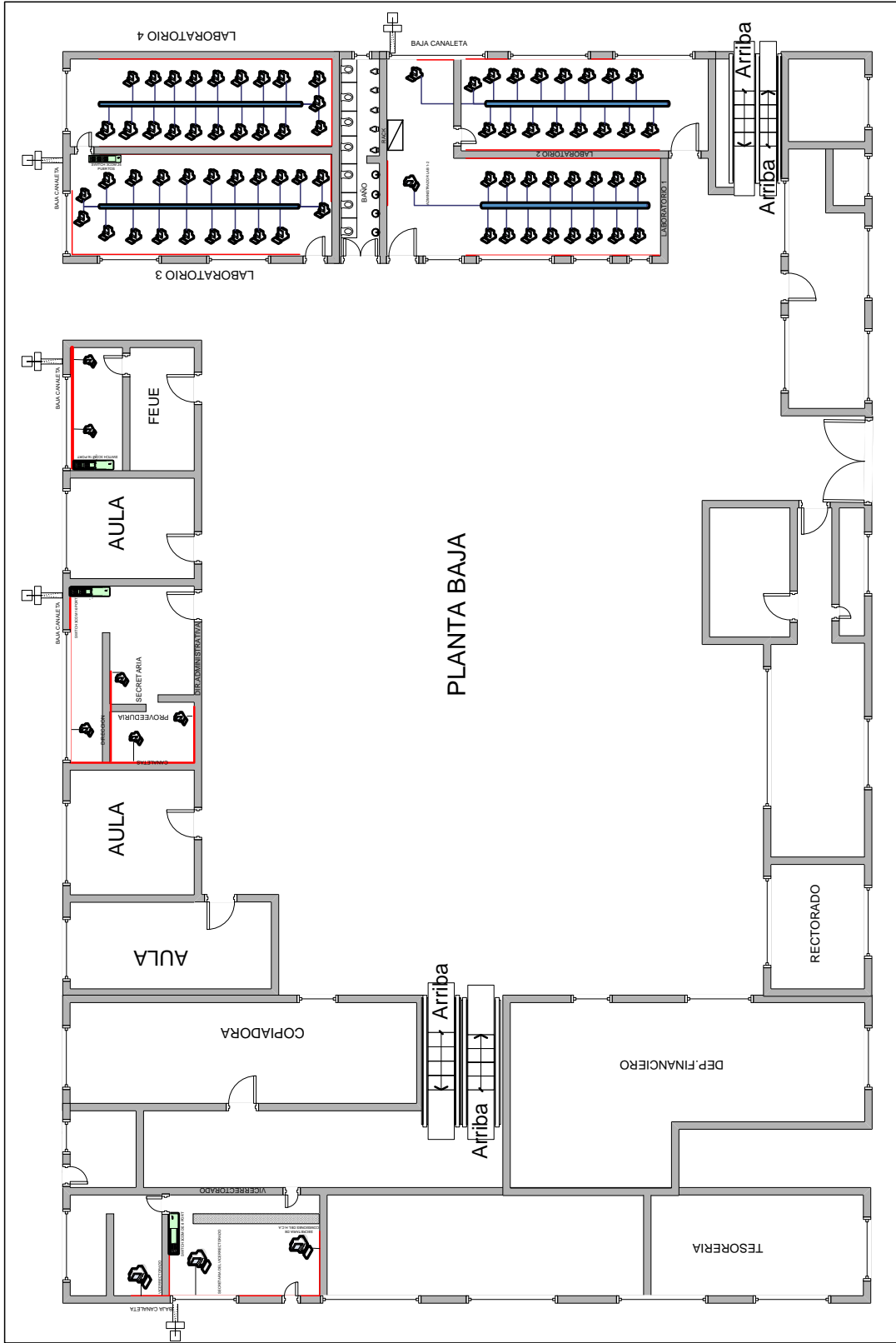
Figura 3.12.- Plano de Comunicación Terraza –Edificio Verde

Elaborado por: Grupo Investigador

3.4.3.2.- EDIFICIO ANTIGUO

De igual manera el edificio antiguo se lo ha dividido en dos partrs principales, como son la Planta Baja y la Planta Alta, las mismas que las ilustramos de mejor manera de la siguiente manera:





3.4.3.3.- EDIFICIO NUEVO

En la actualidad la Universidad cuenta con una moderna edificación la misma que se encuentra equipada con equipos de última tecnología, los dos bloques tanto el B que pertenece a la Carrera de Ciencias de la Ingeniería y Aplicadas y el edificio o bloque C donde se encuentra la biblioteca y el comedor Universitario, cuentan ya con cableado estructurado bajo la norma EIA/TIA 568^a, el mismo que es el complemento al que ya existía en la Universidad centralizando de una manera óptima y adecuada sus concentradores o Switch, debemos mencionar que también cuenta con un circuito cerrado de video y televisión los mismos que complementan con las redes de datos, en un proyecto no muy a futuro se implementara la red inalámbrica que sería un complemento ideal al cableado existente ya que de esta manera descongestionaría en gran medida el uso de los laboratorios.

De igual manera por la red de datos está funcionando la Voz sobre IP (VoIP), el cual ha venido a mejorar el servicio de comunicación entre oficinas y aumentando la utilidad de los equipos con los que ahora cuenta la universidad, pero no por esto debemos dejar de mencionar que hay trabajo aun que realizar ya que los equipos no han llegado a su capacidad de rendimiento promedio peor aun máximo.

La estructuración de las edificaciones nuevas al tratarse de un edificio inteligente hemos creído conveniente utilizar hojas de un formato mayor por lo que vienen adjuntas en los anexos, en los cuales encontramos las 4 plantas del edificio denominado bloque B y las dos plantas del denominado Bloque C.

Gráficos de Distribución de los Bloques B y C con sus plantas mire en <anexos>

3.4.4.- ESTÁNDAR PARA EDIFICIOS, PLANTAS, CUARTO Y BLOQUES.

El nombre del edificio, bloque cuarto y bloque o plantas de la Universidad Técnica de Cotopaxi de la siguiente manera:

Se decidió mantener los nombres antes mencionados salvo cuando se trata de las plantas que se abrevia de la siguiente manera:

- Edificio
- Planta
- Bloque
- Planta Baja PB

- Primera Planta P1
- Segunda Planta P2
- Tercera Planta P3

3.4.4.1 CODIFICACIÓN

La codificación como se puede observar en cuadros que anexamos son claros para la distribución de la red que más adelante detallamos de mejor manera para su total comprensión.

00A-106	BLOQUE B, MDF-20
00A-107	EDIFICIO ANTIGUO, MDF- 40
20A-509	ASOCIACION ESTUDIANTES
20A-510	PRESIDENCIA- ASOCIACION
20A-511	EXPOSICION TRABAJO NE
20A-512	EXPOSICION TRABAJO N0
20A-513	PRESIDENCIA - ASOCIACION
20A-514	ASOCIACION PROFESORES

Tabla 3 .1. Cuadro de Codificación de puntos de Red de la UTC

Fuente: Grupo Investigador

Es una muestra de cómo va a estar organizado los cuadros de distribución de las redes de la universidad Técnica de Cotopaxi.

3.4.5.- ESTÁNDAR PARA NOMENCLATURA DE EQUIPOS DE RED

Para este estándar no se basa en un estándar específico ya que la nomenclatura se la realizara de forma que el administrador identifique a los Equipos de Red en forma rápida y clara.

Para este estándar se ha realizado en mutuo acuerdo con los encargados de la Dirección de Servicios Informáticos de la Universidad Técnica de Cotopaxi

A continuación tenemos la división en la cual se encuentran los equipos de administración de la Red de la Universidad.

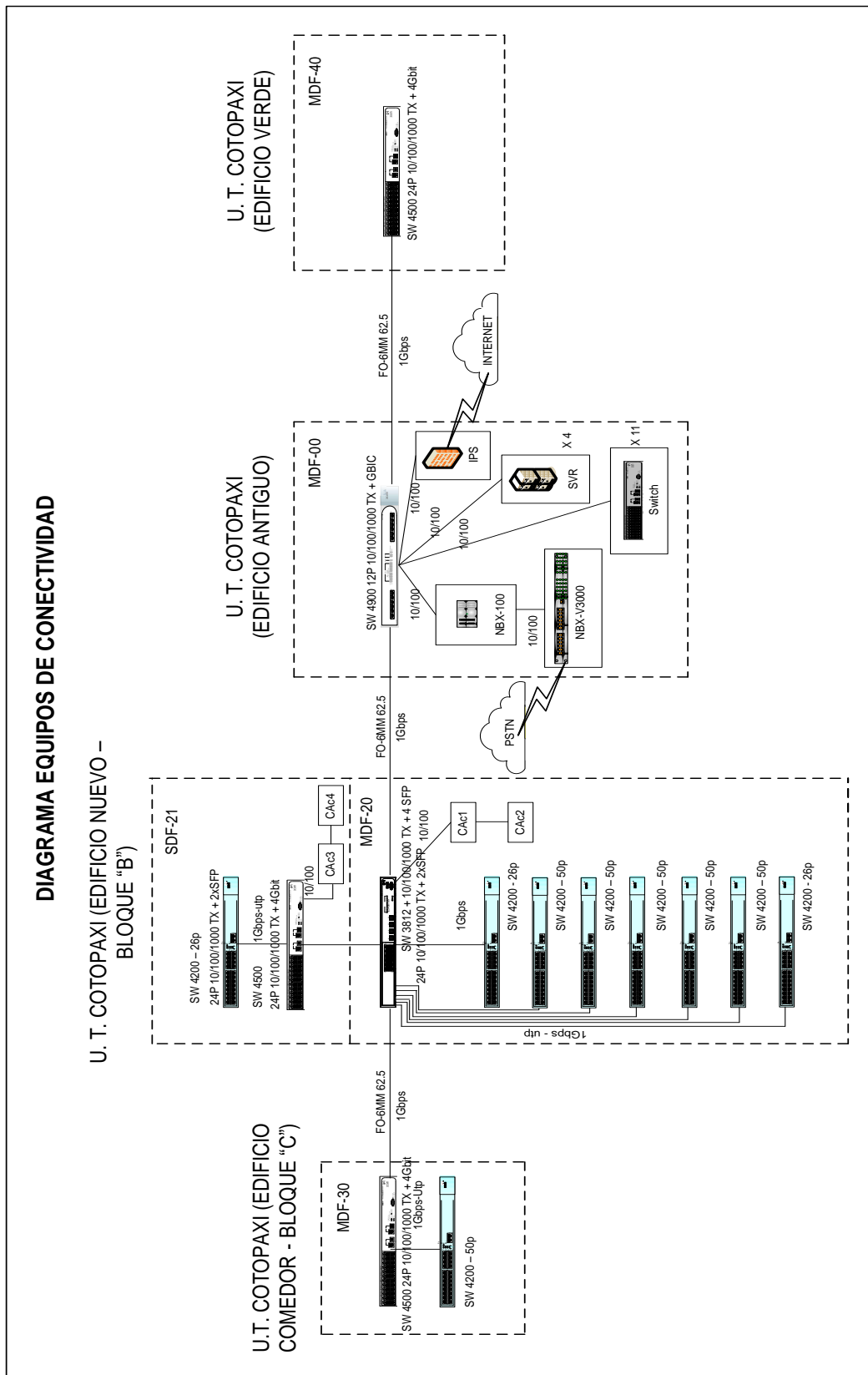


Figura 3.15 : Diagrama de Equipos de Conectividad y Administración

Fuente: Grupo Investigador

3.4.6.- DISTRIBUCIÓN DE PUNTOS DE RED ACTUALES Y POR EXPANSIÓN

3.4.6.1. Enfoque General de la Red

En la actualidad la Universidad Técnica de Cotopaxi tiene conectado su red con todos sus equipos de computación, telefónicos y video.

Considera la instalación de una red de cableado estructurado Categoría 5 enlanced de 213 salidas de computación (datos) y 7 salidas de voz (telefónicas), 2 enlaces de Fibra Óptica multimodo para ducto de 6 hilos con un distribuidor principal centralizado en el Centro de Cómputo en el Edificio Antiguo, 2 distribuidores secundarios en el Bloque B del nuevo Edificio y un distribuidor secundario en el Edificio Anexo, 2 enlaces de cable telefónico para ducto múltipar de 40 pares hacia el Bloque B y un enlace de 20 pares desde el Bloque B hacia el Edificio Anexo y 50 salidas de video en el Bloque B y 3 salidas de video en Edificio Anexo según esquema, el detalle se muestra en las cotizaciones.

El sistema de red de cableado que se propone para ser instalado tiene una topología en estrella con conexión punto a punto entre las áreas de trabajo y los cuartos de equipo. Esta Red de Cableado Estructurado se compone de los siguientes módulos o subsistemas: Subsistema de Cuartos de Distribución, Subsistema de Red Horizontal, Subsistema de Área de Trabajo.

La Red de Cableado Estructurado utilizará componentes UTP Categoría 5 enlazados probados para funcionar con un ancho de banda mínimo de 350 MHz.

Todos los componentes de red y su instalación cumplen con los estándares internacionales 568A de EIA/TIA, para cableados de telecomunicaciones en edificios. El uso de componentes categoría 5 enlazados con ancho de banda de 350 MHz garantiza la conexión y el funcionamiento de equipos de red con tecnología Fast Ethernet, Giga Ethernet y ATM que podrán ser conectados en un futuro próximo; ya que superan los problemas ocasionados por los fenómenos de PowerSum y Resonancia de Enlace Corto que ocurren en las redes de alta velocidad con cableados tradicionales.

3.4.6.2. Subsistema Cuartos de Distribución

El subsistema Cuartos de Distribución comprende los Cuartos de Distribución Secundarios y el Cuarto de Distribución Principal. A estos Cuartos se conectarán los cables de red horizontal, enlaces y también los equipos de conectividad de datos.

CUARTO DE DISTRIBUCION PRINCIPAL

Se instalará un distribuidor principal (MDF) en el lugar destinado como Centro de Cómputo en el segundo piso del edificio Antiguo donde se centralizará toda la red. En este distribuidor se conectará 1 enlace de fibra de 6 hilos para ducto y 1 enlace telefónico multipar de 40 pares para las conexiones hacia el Bloque B. Se instalará una bandeja de fibra tipo modular de 2U con tapa frontal y anillos internos para separación y manejo de fibras, con el propósito de proteger las conexiones de fibra y entradas laterales, patch cord de fibra para conectar el panel a los equipos activos (switches). Para las conexiones telefónicas se usarán paneles de conexión tipo KATT.

El rack de distribución principal será abierto de piso de 42U de alto con kit puntal para sujeción hacia la pared y tendrá también los equipos activos necesarios para las conexiones de fibra y UTP del Bloque B.

CUARTOS DE DISTRIBUCION SECUNDARIA (Bloque B)

Se prevé instalar 2 cuartos de distribución secundarios en el Bloque B, uno localizado en la Planta Baja del Edificio y otro en el Piso 2.

En los Cuartos de Distribución Secundaria se instalarán racks de 42U de alto con kit puntal para sujeción hacia la pared y soportes de pared de 12U de alto respectivamente donde llegarán los enlaces de fibra y cobre y se instalarán salidas de datos y voz con paneles de 24 puertos RJ45 Categoría 5e – 350 MHz, secuencia 568B.

Estos paneles tendrán en su parte frontal etiquetas para la identificación de cada uno de los puertos.

Los cordones de conexión (patch cords) a ser utilizados son Categoría 5e - 350 MHz, de 3 pies de longitud, con conectores RJ45, secuencia 568B y boot de protección en cada extremo. El tipo del cable del cordón es UTP multifilar de 4 pares. Todos estos cordones de conexión son preconectorizados en fábrica (no ensamblados localmente) para cumplir con el estándar EIA/TIA 568A. Tendrá también los equipos activos necesarios para las conexiones de fibra y UTP.

CUARTOS DE DISTRIBUCION SECUNDARIA (Edificio Anexo)

En este distribuidor se conectará 1 enlace de fibra de 6 hilos para ducto y 1 enlace telefónico multipar de 20 pares para las conexiones hacia el Bloque B. Se instalará una bandeja de fibra tipo modular de 2U con tapa frontal y anillos internos para separación y manejo de fibras, con el propósito de proteger las conexiones de fibra y entradas laterales, patch cord de fibra para conectar el panel a los equipos activos (switches). Para las conexiones telefónicas se usarán paneles de conexión tipo KATT.

En este Cuarto de Distribución Secundaria se instalará un soporte de pared de 12U de alto respectivamente donde llegarán los enlaces de cobre y fibra y se instalarán salidas de datos y voz con paneles de 24 puertos RJ45 Categoría 5e – 350 MHz, secuencia 568B.

Estos paneles tendrán en su parte frontal etiquetas para la identificación de cada uno de los puertos.

Los cordones de conexión (patch cords) a ser utilizados son Categoría 5e - 350 MHz, de 3 pies de longitud, con conectores RJ45, secuencia 568B y boot de protección en cada extremo. El tipo del cable del cordón es UTP multifilar de 4 pares. Todos estos cordones de conexión son preconectorizados en fábrica (no ensamblados localmente) para cumplir con el estándar EIA/TIA 568A. Tendrá también los equipos activos necesarios para las conexiones de fibra y UTP.

Para las conexiones de video se utilizarán paneles de conexión configurables con salida tipo BNC armados.

3.4.6.3.Subsistema de Red Horizontal

El subsistema de Cableado Horizontal comprende las placas de uno y dos puertos RJ45 de salida de voz y datos en cada estación de trabajo y las corridas de cable desde las placas hasta los distribuidores secundarios. El cableado horizontal de red tiene una topología en estrella desde cada puerto de salida en el área de trabajo hasta la conexión al panel en el distribuidor. El cable se instala de punto a punto en forma continua y sin empalmes, cuidando no rebasar los límites de curvatura permitidos y con corridas inferiores a 90 metros para cumplir el estándar EIA/TIA 568A.

El cable de red es un cable de cobre de pares trenzados no blindado (UTP) de 4 pares categoría 5e, con un ancho de banda de 350 MHz y chaqueta PVC. Los pares trenzados son de colores con sus secundarios en azul, naranja, verde y café y en pares con el color

principal en blanco. Para las conexiones de video se utilizará cable coaxial tipo RG59 con 95% de malla.

La conducción de los cables desde el distribuidor a las estaciones de trabajo se realizará por medio de ductos (bandeja metálica colocada sobre el techo falso y tubería) que se instalarán en el edificio y que son responsabilidad del constructor de la obra su montaje y guiado.

Las salidas en las estaciones de trabajo son placas sobrepuestas con uno o dos jacks tipo RJ45, secuencia 568B, Categoría 5 - 350 MHz. Incluyen etiquetas para la identificación de cada estación de red. Las salidas en las estaciones de trabajo para las conexiones de video son placas sobrepuestas con una salida BNC. Incluyen etiquetas para la identificación.

3.4.6.4.Subsistema de Área de Trabajo

Este subsistema comprende los elementos de conexión al terminal de datos (computador) en cada estación de trabajo; esto es, el cordón de conexión; y, cualquier adaptador que cambie el tipo de conector en caso de que el equipo terminal así lo necesite.

En cada salida de estación se instalarán cordones de conexión (patch cords) Categoría 5e - 350 MHz, de 7 pies de longitud, con conectores RJ45, secuencia 568B y boot de protección en cada extremo. El tipo del cable del cordón es UTP multifilar de 4 pares. Todos estos cordones de conexión son preconectorizados en fábrica (no ensamblados localmente) para cumplir con el estándar EIA/TIA 568A.

Para las conexiones de video se utilizarán cordones de conexión BNC/BNC de 1 metro armados.

3.4.6.5.Rotulación y Verificación

Cada salida de estación y puerto de los paneles de conexión en los distribuidores se rotulará para identificar su ubicación dentro del piso y el sistema. El número identificador consta de 4 dígitos por cada puerto de estación o de panel de conexión de acuerdo al siguiente formato: RPNN (R: Rack, P: Patch Panel, NN: Número de puerto). Esto permite identificar adecuadamente cada salida para su ubicación dentro del piso y en los cuartos de comunicaciones.

Así mismo, cada canal de comunicación se verificará el cumplimiento de los estándares de Categoría 5 con un Lan Tester nivel III (conforme el estándar TSB-67 de EIA/TIA). El lan tester realizará las pruebas para la certificación de categoría 5 tales como atenuación, diafonía en el extremo cercano (NEXT), longitud de cable, secuencia, resistencia de lazo y retardo de propagación. Estas pruebas se emiten por escrito y son parte del proceso de certificación de red.

Se entregarán diagramas con la descripción de la red instalada y los cuadros de distribución de las conexiones de las redes para el uso de los Administradores de la Red.

3.4.6.6. Equipos Activos

Para la conexión de la red de datos se instalará en el Centro de Cómputo (MDF) core del sistema, 1 switch 3Com 4900 Capa 2, 3 y 4 con 12 puertos 100/1000 y 1 tarjeta de 4 puertos de fibra óptica para conexiones en Gigabit y se conectará el enlace de fibra con el Bloque B mediante un switch 3Com 3812 Capa 2 con 12 puertos 10/100/1000 y 4 puertos dual propósito para conexiones en Gigabit cobre o fibra.

Los servidores se conectarán a los puertos Gigabit del 4900 para ofrecer velocidad de 1Gbps aprovechando el backplane del equipo de 32Gbps con el propósito de mejorar la respuesta de la aplicaciones instaladas en los servidores hacia los usuarios ya que el equipo posee un procesamiento de 23.8 Mpps.

El switch 3812 colocado en el distribuidor de planta baja del Bloque B recibirá la conexión de fibra óptica que viene desde el Centro de Cómputo y del Edificio Anexo mediante 2 módulos SFP SX apropiado para conexiones en longitudes menores a 220m conforme al estándar. También proporcionará la conexión a 1 Gigabit a los switches 4226T y 4250T que se instalarán para recibir las conexiones de los laboratorios y oficinas del Bloque B.

En el distribuidor del Piso 2 instalará 1 Switch 3Com 4226T de 24 puertos 10/100 y 2 100/1000 con características de Capa 2; un backplane de 8.8 Gbps y diseñados para correr aplicaciones en tiempo real como voz y video con un procesamiento de 6.6 Mpps. Todas las estaciones de trabajo conectadas a estos distribuidores estarán corriendo a 100 Mbps.

En el distribuidor del Edificio Anexo se instalará 1 Switch 3Com 3226 de 24 puertos 10/100 y 2 puertos dual Gigabit para recibir conexiones en cobre o fibra con características de Capa 2 y 3; un backplane de 8.8 Gbps y diseñados para correr aplicaciones en tiempo real como voz y video con un procesamiento de 6.6 Mpps. Todas

las estaciones de trabajo conectadas a estos distribuidores estarán corriendo a 100 Mbps. Se pretende tener una red administrable en su totalidad por tal razón todos los equipos propuestos son administrables vía consola, vía web y puede hacerse uso del Network Supervisor de 3 Com para complementar la administración (software gratuito incluido) en equipos.

En virtud de lo anteriormente expuesto hemos considerado realizar unas tablas las mismas que explican como se encuentra distribuidos los puntos de acuerdo a su ubicación o al número de VLAN activa para este segmento de red. La distribución está dada de acuerdo al RACK asignado para el MDF de cada una de las VLAN's físicas de la Universidad, tenemos que estar claros que en las secciones anteriores detallamos la nomenclatura que tenemos y que vamos a tener dentro del presente proyecto investigativo.

CUADRO DISTRIBUCIÓN DE RED

Usuario: UNIVERSIDAD TECNICA DEL COTOPAXI
Dirección (d/c): LATACUNGA
Fecha: 28-mar-07

Distribuidor:		Distribuidor Principal MDF-00 - BLOQUE A		
Ubicación del distribuidor:		Piso - 1, Cuarto de equipos RACK A		
Id de patch panel: 00A-1		Tipo de patch panel: PF-6 - AFR-00112		
Puerto de panel	Id de cable	Id de canal	Ubicación de área de trabajo	Planta
1	FO1	00A-101	BLOQUE B, MDF-20	P1
2	FO1	00A-102	BLOQUE B, MDF-20	P1
3	FO1	00A-103	BLOQUE B, MDF-20	P1
4	FO1	00A-104	BLOQUE B, MDF-20	P1
5	FO1	00A-105	BLOQUE B, MDF-20	P1
6	FO1	00A-106	BLOQUE B, MDF-20	P1
7	FO3	00A-107	EDIFICIO ANTIGUO, MDF- 40	P1
8	FO3	00A-108	EDIFICIO ANTIGUO, MDF- 40	P1
9	FO3	00A-109	EDIFICIO ANTIGUO, MDF- 40	P1
10	FO3	00A-110	EDIFICIO ANTIGUO, MDF- 40	P1
11	FO3	00A-111	EDIFICIO ANTIGUO, MDF- 40	P1
12	FO3	00A-112	EDIFICIO ANTIGUO, MDF- 40	P1

Tabla 3.2: Cuadro de distribución de Red

Fuente: Grupo Investigador

En el tabla 3.2. podemos determinar como se encuentra distribuido el bloque B esto principalmente para la distribución de los nuevos laboratorios y las oficinas del director de Carrera y las secretarías de carrera, podemos también observar que algunas de los segmentos que se encuentran en este RACK están destinados al edificio antiguo.

CUADRO DISTRIBUCIÓN DE RED

Usuario: UNIVERSIDAD TECNICA DEL COTOPAXI
Dirección (d/c): LATACLUNGA
Fecha: 28-mar-07

Distribuidor:		Distribuidor Principal MDF-20 - BLOQUE B		
Ubicación del distribuidor:		Piso - PB, Cuarto de equipos RACK A		
Id de patch panel: 20A-1		Tipo de patch panel: PF-12 - AFR-00112		
Puerto de panel	Id de cable	Id de canal	Ubicación de área de trabajo	Planta
1	FO1	20A-101	EDF. ANTIGUO C.COMPUTO MDF-00	PB
2	FO1	20A-102	EDF. ANTIGUO C.COMPUTO MDF-00	PB
3	FO1	20A-103	EDF. ANTIGUO C.COMPUTO MDF-00	PB
4	FO1	20A-104	EDF. ANTIGUO C.COMPUTO MDF-00	PB
5	FO1	20A-105	EDF. ANTIGUO C.COMPUTO MDF-00	PB
6	FO1	20A-106	EDF. ANTIGUO C.COMPUTO MDF-00	PB
7	FO2	20A-107	BLOQUE C (EDF. COMEDOR) MDF-30	PB
8	FO2	20A-108	BLOQUE C (EDF. COMEDOR) MDF-30	PB
9	FO2	20A-109	BLOQUE C (EDF. COMEDOR) MDF-30	PB
10	FO2	20A-110	BLOQUE C (EDF. COMEDOR) MDF-30	PB
11	FO2	20A-111	BLOQUE C (EDF. COMEDOR) MDF-30	PB
12	FO2	20A-112	BLOQUE C (EDF. COMEDOR) MDF-30	PB

Tabla 3.3: Cuadro de distribución de Red

Fuente: Grupo Investigador

En el tabla 3.3. Se puede observar la distribución de I segmento de red del edificio antiguo toda el área que comprende el Centro de Computo, así como del área del Bloque C de la nueva construcción al área del comedor en donde se planifica la implementación de las redes inalámbricas.

CUADRO DISTRIBUCIÓN DE RED

Usuario: UNIVERSIDAD TECNICA DEL COTOPAXI
Dirección (d/c): LATACUNGA
Fecha: 28-mar-07

Distribuidor:		Distribuidor Principal MDF-20 - BLOQUE B		
Ubicación del distribuidor:		Piso - PB, Cuarto de equipos RACK A		
Id de patch panel: 20A-2		Tipo de patch panel: PP-24C5e - PID-00174		
Puerto de panel	Id de cable	Id de canal	Ubicación de área de trabajo	Planta
1	1	20A-201	AULA 1	P1
2	2	20A-202	AULA 2	P1
3	3	20A-203	AULA 3	P1
4	4	20A-204	AULA 4	P1
5	5	20A-205	EXPOSICION TRABAJO E	P1
6	6	20A-206	AULA 8	P1
7	7	20A-207	AULA 7	P1
8	8	20A-208	EXPOSICION TRABAJO NE	P1
9	9	20A-209	AULA 6	P1
10	10	20A-210	AULA 5	P1
11	11	20A-211	EXPOSICION TRABAJO NO	P1
12	12	20A-212	CUBICULO PROFESORES	P1
13	13	20A-213	CUBICULO PROFESORES	P1
14	14	20A-214	EXPOSICION TRABAJO SO	P1
15	15	20A-215	EXPOSICION TRABAJO SE	P1
16	16	20A-216	ACCESS POINT - TERRAZA CUBIERTA GRADAS NE	P1
17	17	20A-217	ACCESS POINT - HALL E	P1
18	18	20A-218	ACCESS POINT - SALA DE CONSEJO SE	P1
19	19	20A-219	ACCESS POINT - HALL W	P1
20	20	20A-220	SALA DE CONSEJO - TERRAZA CUBIERTA SE	P1
21	Bd1	20A-221	BACKBONE DATOS PB - P2	PB
22	Bd2	20A-222	BACKBONE DATOS PB - P2	PB
23	Bd3	20A-223	BACKBONE DATOS PB - P2	PB
24	Bd4	20A-224	BACKBONE DATOS PB - P2	PB

Tabla 3.3: Cuadro de distribución de Red

Fuente: Grupo Investigador

En el tabla 3.3. Se puede observar la distribución del segmento de red del edificio nuevo denominado bloque B, que comprende las aulas, el esqueleto de la red, los Access point para la red inalámbrica, además del área de oficina de profesores.

Dentro de estas tablas están las principales de acuerdo al RACK de la posición dada en el PATCH PANEL de aquí en mas el resto de ubicaciones están dadas en base a esta clasificación, el resto de puntos de red están siendo dados en los anexos del presente trabajo Investigativo.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1.- CONCLUSIONES

1. Los esquemas VLAN (Virtual LAN, o red Virtual) proporcionan los medios adecuados para solucionar la problemática por medio de la agrupación realizada de una forma lógica, en lugar de física. Sin embargo, las redes virtuales siguen compartiendo las características de los grupos de trabajo físicos, en el sentido de que todos los usuarios comparten sus dominios de broadcast.
2. Al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos se logra, como consecuencia directa, el incremento del ancho de banda en dicho grupo de usuarios.
3. Las VLAN's en una agrupación de puertos físicos pueden tener lugar sobre un switch o también, en algunos casos, sobre varios switch's. La asignación de los equipos a la VLAN se hace en base a los puertos que están conectados físicamente.
4. La combinación de técnicas de Calidad de Servicio (QoS) en un entorno VLAN permite a los administradores de TI tomar el control del tráfico de datos para asegurar el rendimiento de la red y en consecuencia de la organización de un modo más eficiente.
5. El avance de las tecnologías a influenciado notablemente en la reestructuración de los estándares de la IEEE y dentro de estos se ha implementado Calidad de Servicio (QoS) en las diferentes capas del Modelo OSI; uno de estos estándares el 802.1D esta enfocado en las VLAN, priorización y clasificación del tráfico con lo cual podemos generar Calidad de Servicio en la capa de Enlace del modelo OSI.
6. El estándar IEEE 802.1Q define un mecanismo que permite a múltiples redes compartir transparentemente el mismo medio físico sin problemas de interferencia entre las redes que comparten el medio (Trunking).
7. Los equipos de red existentes en la institución han generado algunos inconvenientes principalmente en la realización del trunking entre equipos Cisco y 3Com los cuales después de haber realizado todas las pruebas y consultas necesarias no se ha podido realizar dicha operación.

8. Por el crecimiento normal de la red los equipos que proporcionan el servicio no satisfacen las necesidades actuales a tal grado que ya no se puede satisfacer el normal crecimiento.
9. La falta de documentación depurada puede confundir a los administradores de la red al momento de existir un inconveniente al cual se necesita dar solución de la manera más óptima.
10. Mediante la implementación de este proyecto de grado se ha podido identificar del tráfico de red con el cuál se dar un mejor servicio a los usuarios.
11. El campus San Felipe de la Universidad Técnica de Cotopaxi y la Dirección de Servicios Informáticos con la aplicación de este presente proyecto de grado podrá garantizar que cada paquete que circule en la red tendrá calidad de servicio, dando un mejor servicio a los usuarios.

4.2.- RECOMENDACIONES

1. Para evitar cuellos de botella, mayor retardo en transmisión, jitter; se debe eliminar la presencia de equipos hub en algunas dependencias que todavía tienen.
2. VLAN's es un método muy efectivos para separa a los usuarios por lo cual se debería mantener este esquema dentro de la institución.
3. Los grupos establecidos en la Universidad son los necesarios en la actualidad pero para un futuro con el crecimiento se debería pensar en incrementar estos grupos pero de una manera controlada y no excediendo las especificaciones técnicas de cada equipo.
4. Los estándares aplicados en este proyecto de tesis están siempre en actualización por lo cual no se debe dejar de revisar dichas actualizaciones y aplicar a la institución para poder dar un mejor servicio a los usuarios y para mantener un mejor control sobre estos.
5. Se recomienda la capacitación en el manejo del software de todo el hardware que últimamente se ha adquirido para una correcta Gestión de la Red para tener un método más eficiente de los usuarios y los puntos de red para poder dar solución a los inconvenientes propios de la red.
6. Para evitar conflictos de incompatibilidad de equipos de red y otros problemas se recomienda se tome como política de la Dirección de Servicios Informáticos la adquisición a futuro de una sola marca de equipos de red (Switch).
7. Se debe pensar ya en la adquisición de nuevos equipos de red para suplir las necesidades existentes en la institución.

4.3.- GLOSARIO DE TÉRMINOS Y SIGLAS

Amplitud de banda

La amplitud de banda especifica la cantidad de datos que pueden transmitirse en una cantidad de tiempo fija. En el caso de los dispositivos digitales, la amplitud de banda se define en bits por segundo (bps) o bytes por segundo.

ASIC

Circuito integrado específico de una aplicación. Chip personalizado diseñado para una aplicación específica.

Asignaciones de amplitud de banda

La cantidad de amplitud de banda asignada a una aplicación, usuario o interfaz específicos.

Capa 2

Capa de vínculo de datos o capa MAC. Contiene la dirección física de un cliente o estación de servidor. El proceso de la capa 2 es más rápido que el de la capa 3 porque hay menos información que deba procesarse.

Capa 4

Establece una conexión y garantiza que todos los datos lleguen a su destino. Los paquetes inspeccionados en el nivel de la capa 4 se analizan y las decisiones se reenvían en función de sus aplicaciones.

Capa MAC

Subcapa de la capa de control de vínculo de datos (DTL).

Class of Service (Clase de servicio)

La clase de servicio es el esquema de prioridad 802.1p. La CoS proporciona un método para asignar etiquetas a los paquetes con información sobre la prioridad. Un valor de CoS situado entre 0 y 7 se agrega al encabezado de la capa 2 de los paquetes, donde cero es la prioridad más baja y siete es la más alta.

Transmisión de superposición de dos o más paquetes que colisionan. Los datos transmitidos no pueden utilizarse, y la sesión se reinicia.

Dirección IP

Dirección del protocolo de Internet. Dirección exclusiva asignada a un dispositivo de red con dos o más LAN o WAN interconectadas.

Dirección MAC

Dirección Media Access Control. La dirección MAC es una dirección específica del hardware que identifica cada nodo de red.

DSCP

DiffServe Code Point (DSCP). DSCP proporciona un método de asignación de etiquetas de paquetes IP con información de prioridad QoS.

Router

Dispositivo que conecta redes separadas. Los routers reenvían paquetes entre dos o más redes. Los routers funcionan al nivel de la Capa 3.

Ethernet

Ethernet se estandariza como IEEE 802.3. Ethernet es el estándar de LAN implementado más común. Admite velocidades de transferencia de datos de Mbps, compatibles con velocidades de 10, 100 ó 1000 Mbps.

FIFO

Primeras entradas, primeras salidas. Proceso de colocación en cola en el que el primer paquete de la cola es el primer paquete que sale del paquete.

Fragmento

Paquetes Ethernet de tamaño inferior a los 576 bits.

GARP

Protocolo de registro de atributos general. Registra estaciones cliente en un dominio multidifusión.

Gigabit Ethernet

Gigabit Ethernet transmite a 1000 Mbps y es compatible con los estándares Ethernet 10/100 Mbps existentes.

GVRP

Protocolo de registro VLAN GARP. Registra estaciones cliente en una VLAN.

ICMP

Protocolo de mensajes de control de Internet. Permite a la puerta de enlace o al sistema principal de destino comunicarse con un sistema principal de origen; por ejemplo, para informar sobre un error de proceso.

IEEE

Institute of Electrical and Electronics Engineers. Organización de ingeniería que desarrolla estándares de comunicación y redes.

IEEE 802.1d

Utilizado en el protocolo de árbol extensible, el estándar IEEE 802.1d es compatible con el puente de MAC para evitar bucles de red.

IEEE 802.1p

Prioriza el tráfico de red en la subcapa de vínculo de datos/MAC.

IEEE 802.1Q

Define el funcionamiento de los puentes VLAN que permite definir, hacer funcionar y administrar VLAN dentro de las infraestructuras de LAN con puente.

Mejor esfuerzo

El tráfico se asigna a la cola de prioridad más baja, y no se garantiza la entrega de los paquetes.

Multicast

Transmite copias de un único paquete a varios puertos.

Paquetes

Bloques de información para la transmisión en sistemas de conmutación de paquetes.

QoS

Calidad de servicio. QoS permite a los administradores de red decidir qué tráfico de red se reenvía y cómo se reenvía en función de las prioridades, tipos de aplicación y direcciones de origen y destino.

Switch

Filtra y reenvía paquetes entre segmentos de LAN. Los conmutadores admiten cualquier tipo de protocolo de paquetes.

TFTP

Protocolo trivial de transferencia de archivos. Utiliza el protocolo de datos de usuario (UDP) sin características de seguridad para transferir archivos.

Trama

Los paquetes que contienen el encabezado y la información de cola que requiere el medio físico.

Tramas gigantes

Permiten transportar datos idénticos en menos tramas. Las tramas gigantes reducen el coste, necesitan un tiempo de procesamiento inferior y garantizan menos interrupciones.

Velocidad de puerto

Indica la velocidad del puerto. La velocidad de los puertos incluye:

Ethernet 10 Mbps

Fast Ethernet 100 Mbps

Gigabit Ethernet 1000 Mbps

4.4.- BIBLIOGRAFÍA

- Building Cisco Multilayer Switched Networks; Cisco System, Cisco Press, 2000.
- Cisco CCNA Exam #640-607; Cisco System, Cisco Press, 2002.
- Implementing Cisco Quality of Service v 2.0; Cisco System, Cisco Press, 2003.

4.4.1.- WEB BIBLIOGRAFÍA

- <http://www.monografias.com/vlans.htm>
- http://www.cudi.edu.mx/primavera_2005/presentaciones/felipe_alvarez.pdf
- <http://www.si.uji.es/bin/ponencias/ipp.pdf>
- <http://www.idg.es/comunicaciones/especial-avether160/Pag08.pdf>
- <http://www.iec.uia.mx/proy/titulacion/proy14/vpnprin.htm>
- <http://lauca.usach.cl/~lsanchez/Vlan/>
- http://www.eduangi.com/documentos/3_CCNA2.pdf
- <http://www.avantel.net/~rcruz/Cap3qosrba.pdf>
- <http://www.lavioleta.net/Capitulo1.htm>
- <http://www.commlogik.com.ar/cisco.html>
- <http://informatica.uv.es/doctorado/SST/docto-2-qos.ppt#389,2,Sumario>
- http://www.3com.es/news/reportajes/pdfs/switching_comunicaciones_world.pdf
- <http://dmi.uib.es/~loren/docencia/webxtel/bibliografia/tutorial%20VLAN.pdf>
- <http://net21.ucdavis.edu/newvlan.htm>
- http://www.itlp.edu.mx/publica/revistas/revista_isc/anteriores/jun99/vlan.html
- <http://iie.fing.edu.uy/~rgaglian/Docs/VPLS.pdf>
- http://www.emagister.com/frame.cfm?id_user=8893020050269674850674870704555&id_centro=57953030052957564866666952674548&id_curso=65425040050167555457685550674555&url_frame=http://www.emagister.com/public/pdf/comunidad_emagister/01793120043168694849677065484567-config-ciscos.pdf
- <http://www.it.iitb.ac.in/~it605/resources/Local/Docs/VLAN/VLANIntro.pdf>
- <http://www.isa.uniovi.es/docencia/redes/tema4.pdf>
- <http://www.mythdragon.com/QoS/documents/QoS%20routing%20for%20support%20MM%20apps.pdf>
- http://www.alcatel.ch/com/en/appcontent/apl/A0506-Broadband_QoS-ES_tcm172-287901635.pdf

- Estándar IEEE 802.1Q versión 2003
<http://standards.ieee.org/getieee802/download/802.1Q-2003.pdf>
- Estándar IEEE 802.1D versión 2004
<http://standards.ieee.org/getieee802/download/802.1D-2004.pdf>