UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE UNA RED MULTISERVICIOS DE ALTA DISPONIBILIDAD EN UN ENTORNO CORPORATIVO

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

JAIME OSCAR BARRIAL CASTILLO

PROMOCIÓN
2001 - I

LIMA – PERÚ
2008

Dedicatoria

A mis padres, por su ánimo permanente en la mejora de nuestra vida personal y profesional.

DISEÑO DE UNA RED MULTISERVICIOS DE ALTA DISPONIBILIDAD EN UN ENTORNO CORPORATIVO

SUMARIO

El presente informe brinda información relacionada al diseño de una red multiservicios, que abarca servicios como la Telefonía IP, Videoconferencia, Transmisión de Datos, etc. El diseño se enfocará en un ambiente corporativo y tendrá una alta disponibilidad.

Para que los conceptos y terminología empleada en este informe se entiendan más claramente con amplitud, se citarán en varios pasajes la implementación de redes ya puestas en producción que nos servirán de base para el presente diseño.

En los tiempos actuales, donde la tecnología evoluciona notablemente día a día, es necesario también adaptarnos ante dichos avances, es por ello, que modernizar nuestras redes se convierte no en una necesidad sino en una obligación efectiva.

ÍNDICE

PRÓLOGO

El presente trabajo trata de proporcionar los lineamientos para poder diseñar una red multiservicios de una manera efectiva, dentro de un entorno corporativo. Hoy en día, las redes de comunicaciones se han convertido en una pieza fundamental en la operatividad de toda empresa, debido a la necesaria tarea de compartir recursos en un ambiente local.

Se iniciará brindando un enfoque global de las tecnologías actuales en la implementación de una red de datos, para luego proporcionar los conceptos para nuestro diseño de la red multiservicios de alta disponibilidad. Se citarán algunos ejemplos de implementación relacionados al diseño y que se encuentran actualmente en producción.

Lo que se desea brindar, es la base para la obtención de una red de datos eficiente y escalable que contribuya al desempeño óptimo y responsable de los recursos de aplicaciones y servicios en un ambiente corporativo. Que en cierta manera, contribuirá a fortalecer la realización de los objetivos a trazar en una compañía.

Deseo dar gracias a las empresas donde he ejercido mi Profesión, de haber recopilado la experiencia racional y práctica que me permite poder elaborar una información útil y necesaria para la elaboración del presente informe, ya que constituye en un gran porcentaje, el sustento para nuestro diseño a sustentar.

CAPITULO I

INTRODUCCION A LAS REDES LAN

LAN (Local Area Network) es la interconexión de varios ordenadores y periféricos para compartir recursos e intercambiar datos y aplicaciones. Su extensión está limitada fisicamente a un edificio o a un entorno de hasta 100 metros. El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información. Hoy en día no es factible pensar en compañías que desarrollen sus actividades de toda índole sin el uso de la Internet, Correo Corporativo, Voz por Internet, Videoconferencia, etc. Nos encontramos sumergidos en la llamada Sociedad de la Información donde la interconexión de servicios es el fin supremo donde la implementación de una red y las tecnologías a implementar es vital para hacer frente a los nuevos retos de la comunicación.

En épocas anteriores a los ordenadores personales, una empresa podía tener solamente un ordenador central, accediendo los usuarios a éste mediante terminales de ordenador con un cable simple de baja velocidad. Las redes como SNA de IBM (Arquitectura de Red de Sistemas) fueron diseñadas para unir terminales u ordenadores centrales a sitios remotos con líneas alquiladas. Las primeras LAN fueron creadas a finales de los años 1970 y se solían crear líneas de alta velocidad para conectar grandes ordenadores centrales a un solo lugar.

Muchos de los sistemas fiables creados en esta época, como Ethernet y ARCNET, fueron los más populares. Todos estas tecnologías fueron creadas para el objetivo primordial que es la interconexión de usuarios en una red que permita el intercambio mutuo de información para el desarrollo de aplicaciones afines. El crecimiento CP/M y DOS basados en el ordenador personal significaron que en un lugar fisico existieran docenas o incluso cientos de ordenadores. La intención inicial de conectar

estos ordenadores fue, generalmente, compartir espacio de disco e impresoras láser, pues eran muy caros en este tiempo. Había muchas expectativas en este tema desde 1983 y la industria informática declaró que el siguiente año sería "El año de las Lan".

En realidad esta idea fracasó debido a la proliferación de incompatibilidades de la capa física y la implantación del protocolo de red, y la confusión sobre la mejor forma de compartir los recursos. Lo normal es que cada vendedor tuviera tarjeta de red, cableado, protocolo y sistema de operación de red. Con la aparición de Netware surgió una nueva solución, la cual ofrecía: soporte imparcial para los más de cuarenta tipos existentes de tarjetas, cables y sistemas operativos mucho más sofisticados que los que ofrecían la mayoría de los competidores. Netware dominaba el campo de las Lan de los ordenadores personales desde antes de su introducción en 1983 hasta mediados de los años 1990, cuando Microsoft introdujo Windows NT Advance Server y Windows for Workgroups.

En una empresa suelen existir muchos ordenadores, los cuales necesitan de su propia impresora para imprimir informes (redundancia de hardware), los datos almacenados en uno de los equipos es muy probable que sean necesarios en otro de los equipos de la empresa, por lo que será necesario copiarlos en este, pudiéndose producir desfases entre los datos de dos usuarios, la ocupación de los recursos de almacenamiento en disco se multiplican (redundancia de datos), los ordenadores que trabajen con los mismos datos tendrán que tener los mismos programas para manejar dichos datos (redundancia de software), etc.

La solución a estos problemas se llama red de área local, esta permite compartir bases de datos (se elimina la redundancia de datos), programas (se elimina la redundancia de software) y periféricos como puede ser un módem, una tarjeta RDSI, una impresora, etc. (se elimina la redundancia de hardware); poniendo a nuestra disposición otros medios de comunicación como pueden ser el correo electrónico y el Chat. Nos permite realizar un proceso distribuido, es decir; las tareas se pueden repartir en distintos nodos y nos permite la integración de los procesos y datos de cada uno de los usuarios en un sistema de trabajo corporativo.

Tener la posibilidad de centralizar información o procedimientos facilita la administración y la gestión de los equipos. Además una red de área local conlleva un importante ahorro, tanto de tiempo, ya que se logra gestión de la información y del trabajo, como de dinero, ya que no es preciso comprar muchos periféricos, se consume menos papel, y en una conexión a Internet se puede utilizar una única conexión telefónica o de banda ancha compartida por varios ordenadores conectados en red.

1.1.- Topologías de Red

La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios. La otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos. Las topologías más comúnmente usadas son las siguientes:

a). Topologías físicas

- Una **topología de bus** usa un solo cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este backbone, sin usar un punto central de administración. En la siguiente figura se muestra la topología en mención :

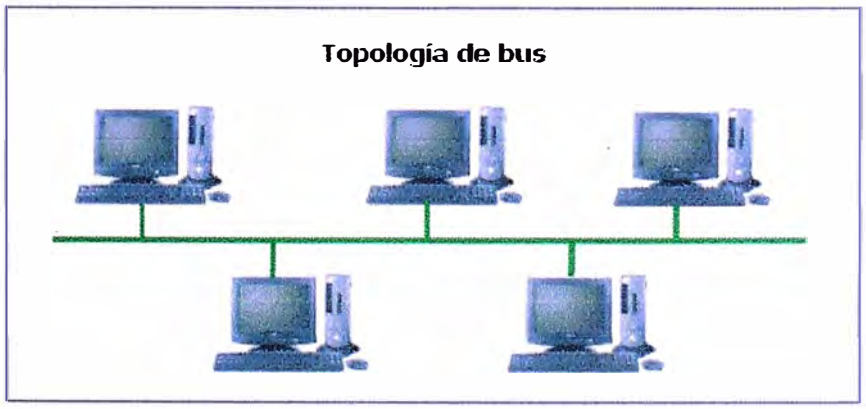

Figura 1.1. Topología Bus

- La **topología de anillo** conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable, el cual se muestra en la siguiente figura de esta topología:

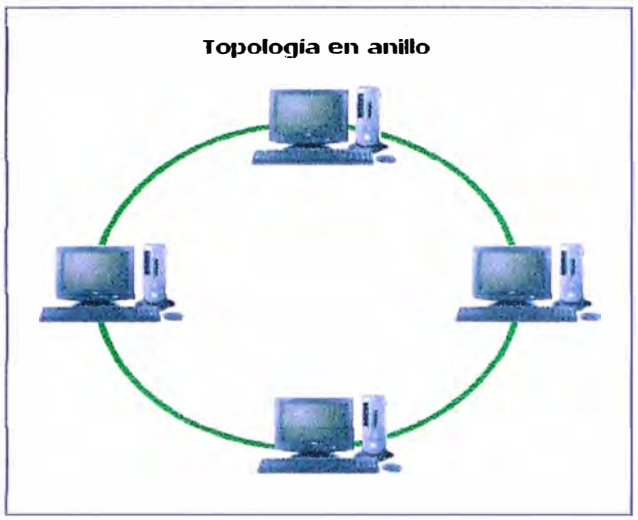

Figura 1.2. Topología en Anillo

- La **topología en estrella** conecta todos los cables con un punto central de concentración. A continuación se muestra el diagrama donde se aprecia la distribución de los dispositivos de red:

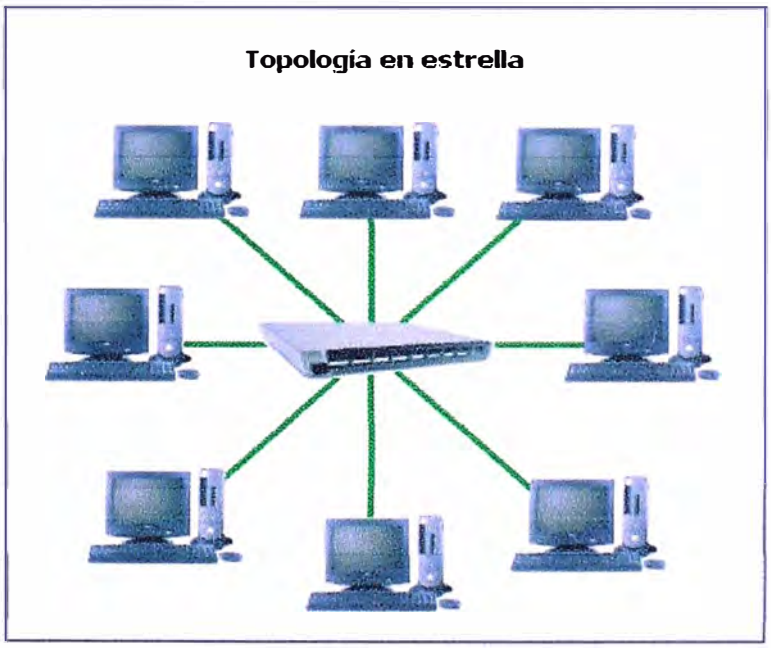

Figura 1.3. Topología en Estrella

- Una **topología en estrella extendida** conecta varias estrellas individuales entre sí mediante la conexión de HUBs o switches. Esta topología específica puede extender el alcance y la cobertura de la red logrando así una optima disponibilidad. A continuación se muestra el diagrama donde se aprecia la distribución de los equipos en esta topología en particular:

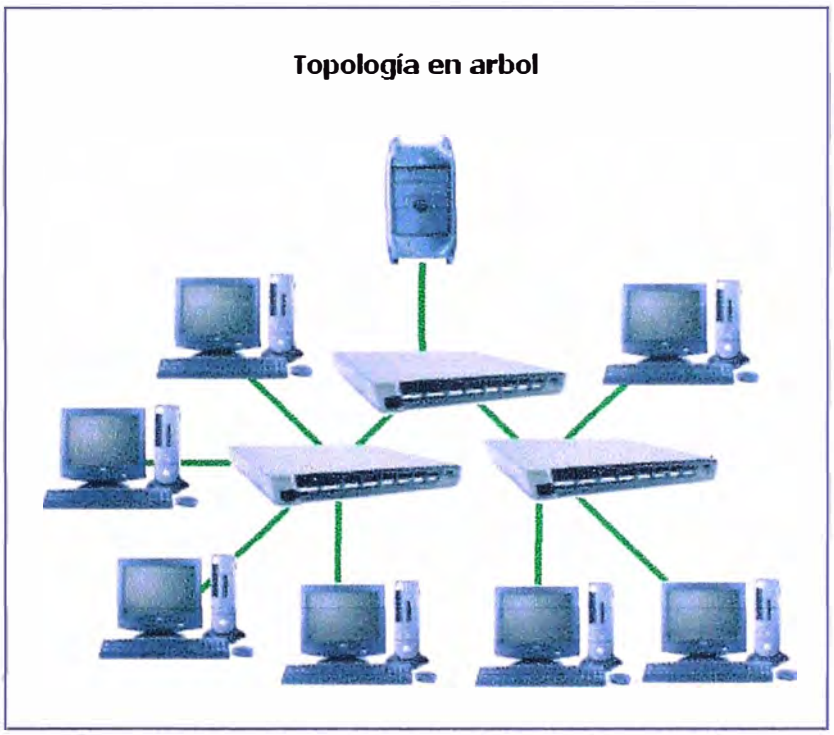

Figura 1.4. Topología en Árbol

- Una **topología jerárquica** es similar a una estrella extendida. Pero en lugar de conectar los HUBs o switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.

- La **topología de malla** se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio. El uso de una topología de malla en los sistemas de control en red de una planta nuclear sería un ejemplo excelente. Internet no adopta este tipo de topología.

b). Topologías lógicas

La topología lógica de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast y transmisión de tokens.

- La **topología broadcast** simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. No existe una orden que las estaciones deban seguir para utilizar la red. Es por orden de llegada, es como funciona Ethernet.

- La **topología transmisión de tokens** controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial. Cuando un host recibe el token, ese host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token al siguiente host y el proceso se vuelve a repetir. Dos ejemplos de redes que utilizan la transmisión de tokens son Token Ring y la Interfaz de datos distribuida por fibra (FDDI). Arcnet es una variación de Token Ring y FDDI. Arcnet es la transmisión de tokens en una topología de bus.

1.2.- Componentes de una LAN

- **Servidor:** El servidor es aquel o aquellos ordenadores que van a compartir sus recursos hardware y software con los demás equipos de la red. Sus características son potencia de cálculo, importancia de la información que almacena y conexión con recursos que se desean compartir.
- **Estación de trabajo**:Los ordenadores que toman el papel de estaciones de trabajo aprovechan o tienen a su disposición los recursos que ofrece la red así como los servicios que proporcionan los Servidores a los cuales pueden acceder.
- **Gateways o pasarelas**: Es un hardware y software que permite las comunicaciones entre la red local y grandes ordenadores (mainframes). El gateway adapta los protocolos de comunicación del mainframe (X25, SNA, etc.) a los de la red, y viceversa.

- **Bridges o puentes**: Es un hardware y software que permite que se conecten dos redes locales entre sí. Un puente interno es el que se instala en un servidor de la red, y un puente externo es el que se hace sobre una estación de trabajo de la misma red. Los puentes también pueden ser locales o remotos. Los puentes locales son los que conectan a redes de un mismo edificio, usando tanto conexiones internas como externas. Los puentes remotos conectan redes distintas entre sí, llevando a cabo la conexión a través de redes públicas, como la red telefónica, RDSI o red de conmutación de paquetes.
- **Tarjeta de red**: También se denominan NIC (Network Interface Card). Básicamente realiza la función de intermediario entre el ordenador y la red de comunicación. En ella se encuentran grabados los protocolos de comunicación de la red. La comunicación con el ordenador se realiza normalmente a través de las ranuras de expansión que éste dispone, ya sea ISA, PCI o PCMCIA. Aunque algunos equipos disponen de este adaptador integrado directamente en la placa base.
- **El medio**: Constituido por el cableado y los conectores que enlazan los componentes de la red. Los medios fisicos más utilizados son el cable de par trenzado, par de cable, cable coaxial y la fibra óptica (cada vez en más uso esta última).
- **Concentradores de cableado**: Una LAN en bus usa solamente tarjetas de red en las estaciones y cableado coaxial para interconectarlas, además de los conectores, sin embargo este método complica el mantenimiento de la red ya que si falla alguna conexión toda la red deja de funcionar. Para impedir estos problemas las redes de área local usan concentradores de cableado para realizar las conexiones de las estaciones, en vez de distribuir las conexiones el concentrador las centraliza en un único dispositivo manteniendo indicadores luminosos de su estado e impidiendo que una de ellas pueda hacer fallar toda la red.

1.3.- Redes Ethernet

1.3.1.- Historia de las Redes Ethernet

En 1972 comenzó el desarrollo de una tecnología de redes conocida como Ethernet

Experimental- El sistema Ethernet desarrollado, conocido en ese entonces como red ALTO ALOHA, fue la primera red de área local (LAN) para computadoras personales (PCs). Esta red funcionó por primera vez en mayo de 1973 a una velocidad de 2.94Mb/s.

Las especificaciones formales de Ethernet de 10 Mb/s fueron desarrolladas en conjunto por las corporaciones Xerox, Digital (DEC) e Intel, y se publicó en el año 1980. Estas especificaciones son conocidas como el estándar DEC-Intel-Xerox (DIX), el libro azul de Ethernet. Este documento hizo de Ethernet experimental operando a 10 Mb/s un estándar abierto.

La tecnología Ethernet fue adoptada para su estandarización por el comité de redes locales (LAN) de la IEEE como IEEE 802.3. El estándar IEEE 802.3 fue publicado por primera vez en 1985.

El estándar IEEE 802.3 provee un sistema tipo Ethernet basado, pero no idéntico, al estándar DIX original. El nombre correcto para esta tecnología es IEEE 802.3 CSMA/CD, pero casi siempre es referido como Ethernet.

IEEE 802.3 Ethernet fue adoptado por la organización internacional de estandarización (ISO), haciendo de el un estándar de redes internacional. Ethernet continuó evolucionando en respuesta a los cambios en tecnología y necesidades de los usuarios. Desde 1985, el estándar IEEE 802.3 se actualizó para incluir nuevas tecnologías. Por ejemplo, el estándar 10BASE-T fue aprobado en

1990, el estándar 100BASE-T fue aprobado en 1995 y Gigabit Ethernet sobre fibra fue aprobado en 1998.

Ethernet es una tecnología de redes ampliamente aceptada con conexiones disponibles para PC, estaciones de trabajo científicas y de alto desempeño, mini computadoras y sistemas mainframe. La arquitectura Ethernet provee detección de errores pero no corrección de los mismos. Tampoco posee una unidad de control central, todos los mensajes son transmitidos a través de la red a cada dispositivo conectado.

Cada dispositivo es responsable de reconocer su propia dirección y aceptar los mensajes dirigidos a ella. El acceso al canal de comunicación es controlado individualmente por cada dispositivo utilizando un método de acceso probabilístico conocido como disputa (contention).

1.3.2- Diferencia entre Ethernet y 802.3

Si bien IEEE 802.3 y Ethernet son similares, no son idénticos. Las diferencias entre ellos son lo suficientemente significantes como para hacerlos incompatibles entres si. Todas las versiones de Ethernet son similares en que comparten la misma arquitectura de acceso al medio múltiple con detección de errores, CSMA/CD (carrier sense múltiple access with collision detection). Sin embargo, el estándar IEEE 802.3 ha evolucionado en el tiempo de forma que ahora soporta múltiples medios en la capa fisica, incluyendo cable coaxil de 50 Ω y 75 Ω, cable par trenzado sin blindaje (Unshielded Twisted Pair o UTP), cable par trenzado con blindaje (Shielded Twisted Pair o STP) y fibra óptica. Otras diferencias entre los dos incluyen la velocidad de transmisión, el método de señalamiento y la longitud máxima del cableado.

1.3.3.- Formato de la Trama

La diferencia más significativa entre la tecnología Ethernet original y el estándar IEEE 802.3 es la diferencia entre los formatos de sus tramas. Esta diferencia es lo suficientemente significativa como para hacer a las dos versiones incompatibles. Una de las diferencias entre el formato de las dos tramas está en el preámbulo. El propósito del preámbulo es anunciar la trama y permitir a todos los receptores en la red sincronizarse a si mismos a la trama entrante. El preámbulo en Ethernet tiene una longitud de 8 bytes pero en IEEE 802.3 la longitud del mismo es de 7 bytes, en este último el octavo byte se convierte en el comienzo del delimitador de la trama.

Fuente:
http://nsrc.org/workshops/2004/CEDIA/presentaciones/cv/switching/Switching-Ethernet.pdf

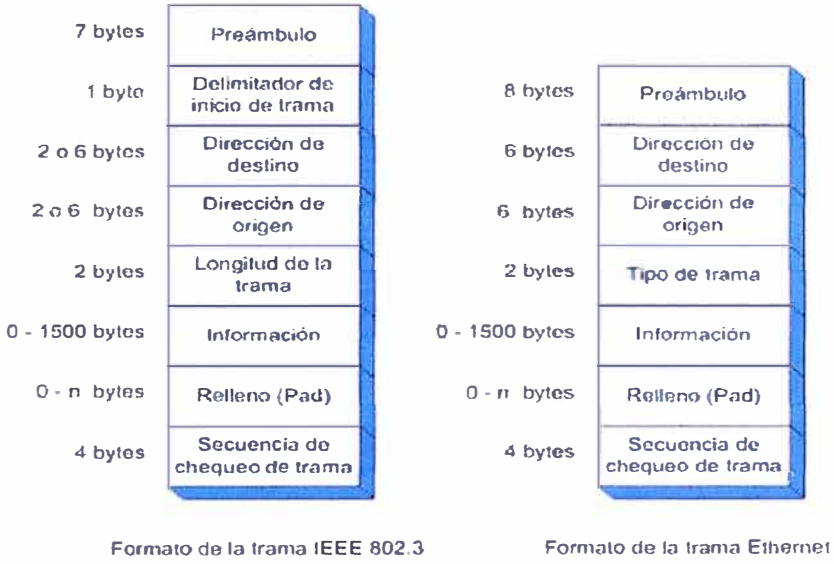

Fig. 1.5. Formatos de Trama

La segunda diferencia entre el formato de las tramas es en el campo tipo de trama que se encuentra en la trama Ethernet. Un campo tipo es usado para especificar al protocolo que es transportado en la trama. Esto posibilita que muchos protocolos puedan ser transportados en la trama. El campo tipo fue reemplazado en el estándar IEEE 802.3 por un campo longitud de trama, el cual es utilizado para indicar el numero de bytes que se encuentran en el campo da datos.

La tercera diferencia entre los formatos de ambas tramas se encuentra en los campos de dirección, tanto de destino como de origen. Mientras que el formato de IEEE 802.3 permite el uso tanto de direcciones de 2 como de 6 bytes, el estándar Ethernet permite solo direcciones de 6 Bytes. El formato de trama que predomina actualmente en los ambientes Ethernet es el de IEEE 802.3, pero la tecnología de red continua siendo referenciada como Ethernet. Existen una gran variedad de implementaciones de IEEE 802.3. Para distinguir entre ellas, se ha desarrollado una notación. Esta notación especifica tres características de la implementación.

- La tasa de transferencia de datos en Mb/s
- El método de señalamiento utilizado
- La máxima longitud de segmento de cable en cientos de metros del tipo de medio.

Fuente:
http://nsrc.org/workshops/2004/CEDIA/presentaciones/cv/switching/Switching-Ethernet.pdf

Trama Ethernet

Trama del DIX Ethernet

Preámbulo	**Destino**	**Origen**	**Longitud**	**Datos**	**Relleno**	**FCS**
8 bytes	6 bytes	6bytes	2 bytes	0 a 1500 bytes	0 a 46 bytes	2 ó 4 bytes

Preámbulo	**SOF**	**Destino**	**Origen**	**Tipo**	**Datos**	**Relleno**	**FCS**
7 bytes	1 byte	6 bytes	6bytes	2 bytes	0 a 1500 bytes	0 a 46 bytes	4 bytes

Figura 1.6. Formato Trama Ethernet

Preámbulo

Un campo de 7 bytes (56 bits) con una secuencia de bits usada para sincronizar y estabilizar el medio físico antes de iniciar la transmisión de datos. El patrón del preámbulo es:

10101010 10101010 10101010 10101010 10101010 10101010 10101010

Estos bits se transmiten en orden, de izquierda a derecha y en la codificación Manchester representan una forma de onda periódica.

SOF (Start Of Frame) Inicio de Trama

Campo de 1 byte (8 bits) con un patrón de 1s y 0s alternados y que termina con dos 1s consecutivos. El patrón del SOF es: 10101011. Indica que el siguiente bit será el bit más significativo del campo de dirección MAC de destino.
Aunque se detecte una colisión durante la emisión del preámbulo o del SOF, el emisor debe continuar enviando todos los bits de ambos hasta el fin del SOF.

Dirección de destino
Campo de 6 bytes (48 bits) que especifica la dirección MAC de tipo EUI-48 hacia la que se envía la trama. Esta dirección de destino puede ser de una estación, de un grupo *multicast* o la dirección de *broadcast* de la red. Cada estación examina este campo para determinar si debe aceptar el paquete.

Dirección de origen
Campo de 6 bytes (48 bits) que especifica la dirección MAC de tipo EUI-48 desde la que se envía la trama. La estación que deba aceptar el paquete conoce por este campo la dirección de la estación origen con la cual intercambiará datos.

Tipo
Campo de 2 bytes (16 bits) que identifica el protocolo de red de alto nivel asociado con el paquete o, en su defecto, la longitud del campo de datos. La capa de enlace de datos interpreta este campo. La siguiente comparación es necesario destacar, la relación siguiente
(En la IEEE 802.3 es el campo longitud y debe ser menor de 1536 bytes.)

Datos
Campo de 0 a 1500 Bytes de longitud. Cada Byte contiene una secuencia arbitraria de valores. El campo de datos es la información recibida del nivel de red (la carga útil). Este campo, también incluye los H3 y H4 (cabeceras de los niveles 3 y 4), provenientes de niveles superiores.

Relleno

Campo de 0 a 46 bytes que se utiliza cuando la trama Ethernet no alcanza los 64 bytes mínimos para que no se presenten problemas de detección de colisiones cuando la trama es muy corta.

FCS (Frame Check Sequence - Secuencia de Verificación de Trama)

Campo de 32 bits (4 bytes) que contiene un valor de verificación CRC (Control de redundancia cíclica). El emisor calcula el CRC de toda la trama, desde el campo destino al campo CRC suponiendo que vale 0. El receptor lo recalcula, si el valor calculado es 0 la trama es valida.

1.3.4.- Tipos de Ethernet

Algunos tipos de estas implementaciones de IEEE 802.3 y sus características se detallan a continuación:

Ethernet 1BASE-5

El estándar IEEE para Ethernet en banda base a 1Mb/s sobre cable par trenzado a una distancia máxima de 250m.

10BASE-5

Es el estándar IEEE para Ethernet en banda base a 10Mb/s sobre cable coaxial de 50 Ω troncal y AUI (attachment unit interface) de cable par trenzado a una distancia máxima de 500m.

10BASE-2

El estándar IEEE para Ethernet en banda base a 10MB/s sobre cable coaxial del tipo delgado de 50 Ω con una distancia máxima de 185m.

10BROAD-36

El estándar IEEE para Ethernet en banda ancha a 10Mb/s sobre cable coaxial de banda ancha de 75 Ω con una distancia máxima de 3600m.

10BASE-T

El estándar IEEE para Ethernet en banda base a 10 Mb/s sobre cable par trenzado sin blindaje (Unshielded Twisted Pair o UTP) siguiendo una topología de cableado horizontal en forma de estrella, con una distancia máxima de 100m desde una estación a un switch.

10BASE-F

El estándar IEEE para Ethernet en banda base a 10Mb/s sobre fibra óptica con una distancia máxima de 2.000 metros (2Km).

1.3.4.1. Fast Ethernet

- **100BASE-TX**

El estándar IEEE para Ethernet en banda base a 100Mb/s sobre dos pares (cada uno de los pares de categoría 5 o superior) de cable UTP o dos pares de cable STP.

- **100BASE-T4**

El estándar IEEE para Ethernet en banda base a 100Mb/s sobre 4 pares de cable UTP de categoría 3 (o superior).

- **100BASE-FX**

Es el estándar IEEE para Ethernet en banda base a 100Mb/s sobre un sistema de cableado de dos fibras ópticas de 62.5/125 μm.

- **100BASE-T2**

El estándar IEEE para Ethernet en banda base a 100Mb/s sobre 2 pares de categoría 3 (o superior) de cable UTP.

1.3.4.2. Gigabit Ethernet

- **1000BASE-SX**

  El estándar IEEE para Ethernet en banda base a 1000Mb/s (1Gb/s) sobre 2 fibras multimodo (50/125 μm o 62.5/125 μm) de cableado de fibra óptica.

- **1000BASE-LX**

  El estándar IEEE para Ethernet en banda base a 1000Mb/s (1Gb/s) sobre 2 fibras monomodo o multimodo (50/125 μm or 62.5/125 μm) de cableado de fibra óptica.

- **1000BASE-CX**

  El estándar IEEE para Ethernet en banda base a 1000Mb/s (1Gb/s) sobre cableado de cobre blindado balanceado de 150 Ω. Este es un cable especial con una longitud máxima de 25m.

- **1000BASE-T**

  El estándar IEEE para Ethernet en banda base a 1000Mb/s (1Gb/s) sobre 4 pares de categoría 5 o superior de cable UTP, con una distancia máxima de cableado de 100m.

CAPITULO II

SERVICIOS CONVERGENTES EN UNA RED LOCAL

Hoy en día, los servicios que se ejecutan en una red de datos local son muy diversos comprendiendo a la comunicación de datos, telefonía IP, videoconferencia, servicios multimedia, etc. Todos estos servicios deben ser contenidos en una red que permita que las soporten con un resultado óptimo el cual no de lugar a resultados inesperados como saturación inesperada en el ancho de banda, microcortes en la actividad de servidores y/o equipos de comunicaciones, caídas inesperadas de la red, etc. Todos estos eventos nombrados no son aleatorios y tienen su explicación en como se ha implementado una red en particular y las políticas que la rigieron. Debemos ser conscientes en que la tecnología a implementar en una red de comunicaciones es vital para minimizar a gran escala los eventos anormales en nuestra red. A continuación mostraremos los servicios que pueden ser implementados en una red y también las prácticas habituales que se deben implementar en los equipos de comunicaciones que brinden un adecuado performance de la red de comunicaciones, obteniendo una óptima administración en nuestra red resultando de esta manera mejorar la productividad de nuestra compañía.

Pasaremos a explicar los diversos servicios mencionados con amplitud:

2.1.- Comunicación de datos

Sigue siendo el principal servicio a usar en las redes locales actualmente, debido a que es importante la transferencia de la información de una empresa hacia todos los componentes de la misma ya sea el caso de que estén ubicados en una misma área física o separados geográficamente. Corresponde a la transferencia de datos tanto a nivel local como a nivel externo, es decir; la transferencia de datos a sedes que se ubican remotamente con respecto a la sede principal de una organización.

Mostraremos una topología típica de una red donde es primordial la transferencia de la información.

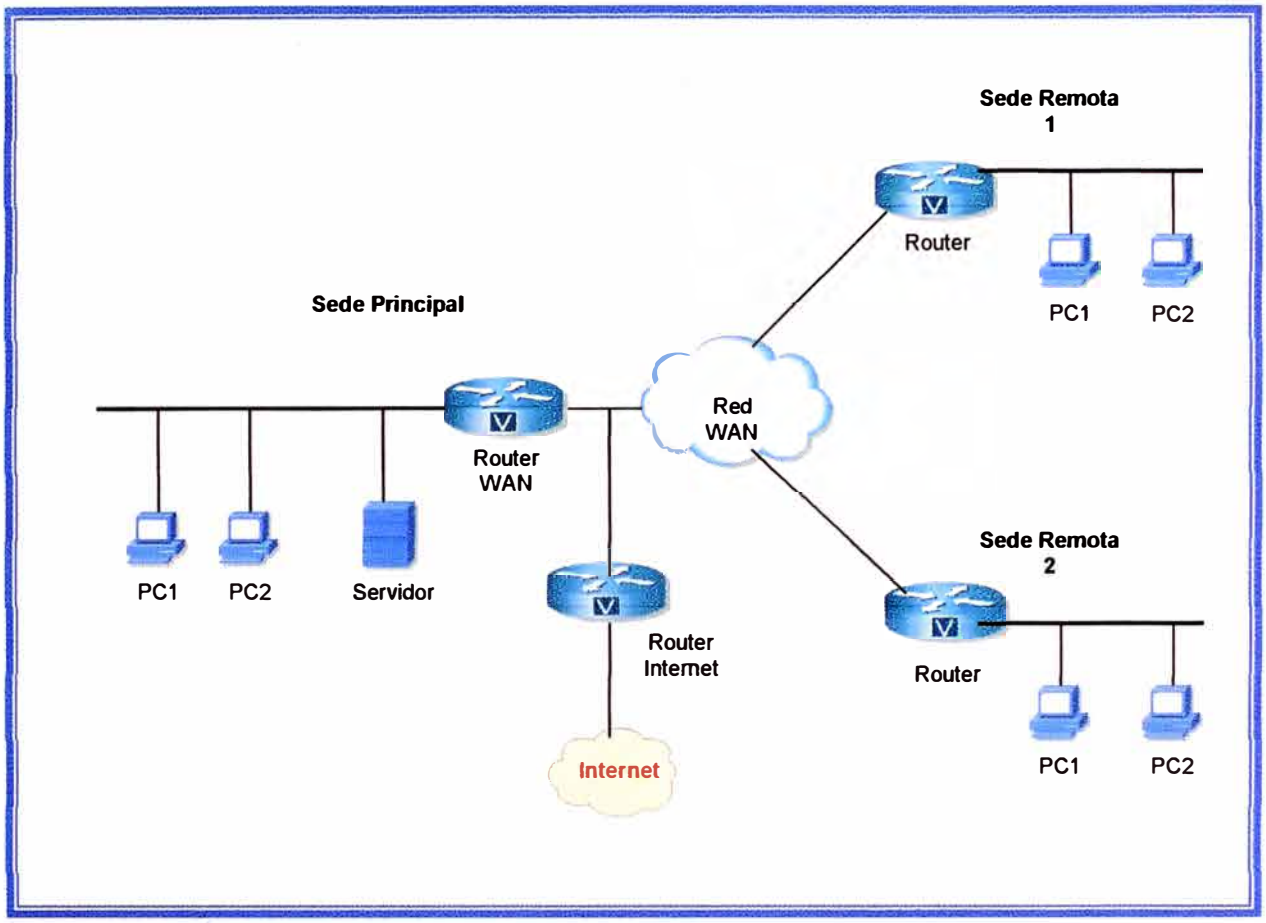

Figura 2.1. Topología de Red

Se observa en la topología descrita a una sede principal y dos sedes remotas donde la transferencia de la información es básica y fundamental. El servidor de datos se encuentra ubicado en la sede principal y las sedes remotas tienen que acceder a dicho servidor para procesar la información de sus aplicaciones.

La ubicación de estas sedes remotas se ha sugerido que se encuentran geográficamente separadas por ello es fundamental que la conectividad WAN este establecida correctamente para la conectividad entre todas las redes de la compañía.

De igual forma, el servicio de Internet solo existe en la sede principal y por medio de la red WAN se logra "llevar" dicho servicio hacia las sedes remotas, evitando de esta

manera costos innecesarios en la instalación del servicio de Internet en las demás sedes de la compañía.

2.1.1- VLANs (VIRTUAL LOCAL AREA NETWORK)

La característica principal de una red de área local es que los dispositivos que la conforman comparten los recursos del medio físico, es decir, el ancho de banda proporcionado por el mismo.

Cuando utilizamos un concentrador o hub dentro de una red, ésta se puede ver como una red de distribución hidráulica, donde las estaciones de trabajo conectadas a la misma toman cierta cantidad de agua, y mientras más máquinas existan en esa LAN, menor será la cantidad de líquido que podrán utilizar. A este segmento de "tubería" se le puede llamar también "dominio de colisiones". El empleo de un switch mejora el rendimiento de la red debido a que este dispositivo segmenta o divide los "dominios de colisiones", es decir, el comportamiento que se tiene en una LAN al utilizar concentradores o hubs es el de compartir el medio o ancho de banda, por ello puede ocurrir que en algún momento el medio esté ocupado por la transmisión de información por parte de alguna de las computadoras, y si otro quiere enviar información en esa precisa hora, no lo podrá hacer hasta que el medio se encuentre disponible.

Por otro lado, si dos computadoras "escuchan" que el medio está vacío enviarán su información, pero debido a que éste es compartido puede suceder que los datos se encontrarán y "chocarán", por lo que se hablará de una colisión y el material se destruirá; al perderse tendrá que volverse a enviar, lo que llevará a muchas retransmisiones de información. En una red LAN, cada uno de los puertos es una "tubería" dedicada a cada una de las casas (computadoras) dentro de la red, donde cada computadora dispone de toda la anchura de banda que la red proporciona, en este caso 10 o 100 Mbps, con objeto de evitar las colisiones que pudieran existir en un medio compartido, por ello cada computadora tiene un tubo individual enlazado con el punto central de distribución que es el switch. Algo que no puede mejorar ni el switch, ni el hub o concentrador, es el envío de mensajes de broadcast dentro de una red LAN, los que se asemejan a aquellos que escuchamos en una tienda

que las personas (computadoras) que estamos dentro de la tienda nos encontramos exentos de hacerlo.

En una LAN estos mensajes de broadcast son enviados a través de todos los puertos de un hub o de un switch. Si una computadora quiere comunicarse con otra y no sabe en dónde se encuentra, entonces la "vocea" dentro de la LAN, creando tráfico dentro de ésta, además

todas las computadoras escucharán el mensaje pero sólo podrá contestarlo la que se está buscando, no importando si se encuentra o no conectada dentro del switch o concentrador.

Estos mensajes de broadcast son, en muchas ocasiones, tráfico innecesario como cuando estamos tratando de encontrar una computadora en específico, pero afectamos a todas las que estén dentro del "dominio de broadcast" o LAN.

Para solventar dicha situación se crea el concepto de Redes de Área Local Virtuales (VLANs), configuradas dentro de los switches, que dividen en diferentes "dominios de broadcast" a un switch, con la finalidad de no afectar a todos los puertos del switch dentro de un solo dominio de broadcast, sino crear dominios más pequeños y aislar los efectos que pudieran tener los mensajes de broadcast a solamente algunos puertos, y afectar a la menor cantidad de máquinas posibles.

Una Red de Área Local Virtual (VLAN) puede definirse como una serie de dispositivos conectados en red que a pesar de estar conectados en diferentes equipos de interconexión (hubs o switches), zonas geográficas distantes, diferentes pisos de un edificio e, incluso, distintos edificios, pertenecen a una misma Red de Área Local.

Con los switchs , el rendimiento de la red mejora en los siguientes aspectos:

- Aísla los "dominios de colisión" por cada uno de los puertos.
- Dedica el ancho de banda a cada uno de los puertos y, por lo tanto, a cada computadora.
- Aísla los "dominios de broadcast", en lugar de uno solo, se puede configurar el switch para que existan más dominios.

- Controla más la administración de las direcciones IP. Por cada VLAN se recomienda asignar un bloque de IPs, independiente uno de otro, así ya no se podrá configurar por parte del usuario cualquier dirección IP en su máquina y se evitará la repetición de direcciones IP en la LAN.
- No importa en donde nos encontremos conectados dentro del edificio de oficinas, si estamos configurados en una VLAN, nuestros compañeros de área, dirección, sistemas, administrativos, etc., estarán conectados dentro de la misma VLAN, y quienes se encuentren en otro edificio, podrán "vernos" como una Red de Área Local independiente a las demás.

  El funcionamiento e implementación de las VLANs está definido por un organismo internacional llamado IEEE Computer Society y el documento en donde se detalla es el IEEE 802.1Q.

Hasta aquí ya hemos hablado de que se aísla el trafico de colisiones y de broadcast, y que cada VLAN es independiente una de otra, pero todavía falta mencionar cómo es que se comunican entre sí, ya que muchas veces habrá que comunicarse entre computadoras pertenecientes a diferentes VLANs. Por ejemplo, los de sistemas con los de redes, o los de redes con finanzas, etc.

En el estándar 802.1Q se define que para llevar a cabo esta comunicación se requerirá de un dispositivo dentro de la LAN, capaz de entender los formatos de los paquetes con que están formadas las VLANs. Este dispositivo es un equipo de capa 3, mejor conocido como enrutador o router, que tendrá que ser capaz de entender los formatos de las VLANs para recibir y dirigir el tráfico hacia la VLAN correspondiente.

2.1.2.- Clases de VLANs

Como respuesta a los problemas generados en redes lan (colisiones, trafico de broadcast, movilidad, etc) se creo una red con agrupamientos lógicos independientes del nivel físico, con lo cual si un usuario se encontraba en el piso uno y debía moverse al piso dos ya no tenía que reconfigurar la máquina ni darle una nueva dirección IP (Internet Protocol) del piso dos, sino que ahora es una acción automática sin necesidad de ahora realizar modificaciones.

Las VLAN (Virtual Local Area Networks; Redes virtuales de área local) forman grupos lógicos para definir los dominios de broadcast. De esta forma existe el dominio de los rojos, donde el broadcast que genera el rojo solo le afectara a este color y el broadcast que genera el amarillo solamente afectara a esta parte de la red. Aunque fisicamente estén conectadas las maquinas al mismo equipo, lógicamente pertenecerán a una VLAN distinta dependiendo de sus aplicaciones con lo que se logra un esquema mas enfocado al negocio. Anteriormente existía la red plana, donde el broadcast se repetía en los puertos y esto provocaba una situación critica. Ahora con las VLAN existe una segmentación lógica o virtual.

Existen dos clases de VLAN: implícitas y explícitas. Las implícitas no necesitan cambios en el frame, pues de la misma forma que reciben información la procesan, ejemplo de ello son las VLAN basadas en puertos.

En esta clase de VLAN el usuario no modifica ni manipula frame, ya que solo posee una marca y por lo tanto el sistema se vuelve propietario. Las VLAN explícitas si requieren modificaciones, adiciones y cambios (MAC) al frame, por lo que sacaron los estándares 802.1p y 802.1q, en donde se colocan ciertas etiquetas o banderas en el frame para manipularlo. Las VLAN deben ser rápidas, basadas en switchs para que sean interoperables totalmente – porque los routers no dan la velocidad requerida- , su información deberá viajar a través del backbone y deberán ser movibles, es decir, que el usuario no tenga que reconfigurar la maquina cada vez que se cambie de lugar.

2.1.3- Generaciones de VLANs

1. Basadas en puertos y direcciones MAC

2. Internet Working; se apoya en protocolo y dirección capa tres.

3. De aplicación y servicios: aquí se encuentran los grupos multicast y las VLAN definidas por el usuario.

4. Servicios avanzados: ya se cumple con los tres criterios antes de realizar alguna asignación a la VLAN; se puede efectuar por medio de DHCP (Dynamic Host

Configuration Protocol ; Protocolo de configuración dinámica) o por AVLAN (Authenticate Virtual Local Area Networks; Redes virtuales autenticadas de área local).

2.1.3.1. VLAN por Puerto

Este tipo es el más sencillo ya que un grupo de puertos forma una VLAN -un puerto solo puede pertenecer a una VLAN - , el problema se presenta cuando se quieren hacer VLAN por MAC ya que la tarea es compleja. Aquí el puerto del switch pertenece a una VLAN , por tanto, si alguien posee un servidor conectado a un puerto y este pertenece a la VLAN amarilla , el servidor estará en la VLAN amarilla.

2.1.3.2. VLAN por MAC

Se basa en MAC Address, por lo que se realiza un mapeo para que el usuario pertenezca a una determinada VLAN. Obviamente dependerá de la política de creación.

Este tipo de VLAN ofrece mayores ventajas, pero es complejo porque hay que meterse con las direcciones MAC y si no se cuenta con un software que las administre, será muy laborioso configurar cada una de ellas.

2.1.3.3. VLAN por Protocolo

Lo que pertenezca a IP sé enrutara a la VLAN de IP e IPX se dirigirá a la VLAN de IPX , es decir, se tendrá una VLAN por protocolo. Las ventajas que se obtienen con este tipo de VLAN radican en que dependiendo del protocolo que use cada usuario, este se conectara automáticamente a la VLAN correspondiente. VLAN por subredes de IP o IPX.

Aparte de la división que ejecuta la VLAN por protocolo, existe otra subdivisión que está dentro de este para que el usuario aunque este conectado a la VLAN del protocolo IP sea asignado en otra VLAN subred que pertenecerá al grupo 10 o 20 dentro del protocolo.

2.1.3.4. VLAN definidas por el usuario

En esta política de VLAN se puede generar un patrón de bits, para cuando llegue el frame. Si los primeros cuatro bits son 1010 se irán a la VLAN de ingeniería, sin importar las características del usuario protocolo, dirección MAC y puerto.
Si el usuario manifiesta otro patrón de bits, entonces se trasladara a la VLAN que le corresponda; aquí el usuario define las VLAN.

2.1.3.5. VLAN Binding

Se conjugan tres parámetros o criterios para la asignación de VLAN: si el usuario es del puerto x, entonces se le asignara una VLAN correspondiente.
También puede ser puerto, protocolo y dirección MAC, pero lo importante es cubrir los tres
requisitos previamente establecidos, ya que cuando se cumplen estas tres condiciones se coloca al usuario en la VLAN asignada, pero si alguno de ellos no coincide, entonces se rechaza la entrada o se manda a otra VLAN.

2.1.3.6. VLAN por DHCP

Aquí ya no es necesario proporcionar una dirección IP, sino que cuando el usuario enciende la computadora automáticamente el DHCP pregunta al servidor para que tome la dirección IP y con base en esta acción asignar al usuario a la VLAN correspondiente. Esta política de VLAN es de las últimas generaciones.

2.2.- Trunking

2.2.1- Protocolo IEEE 802.1Q

El protocolo **IEEE 802.1Q** fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio fisico, sin problemas de interferencia entre ellas (*Trunking*). Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet.

2.2.1.1. Formato de la trama

802.1Q en realidad no encapsula la trama original sino que añade 4 bytes al encabezado Ethernet original. El valor del campo EtherType se cambia a 0x8100 para señalar el cambio en el formato de la trama.

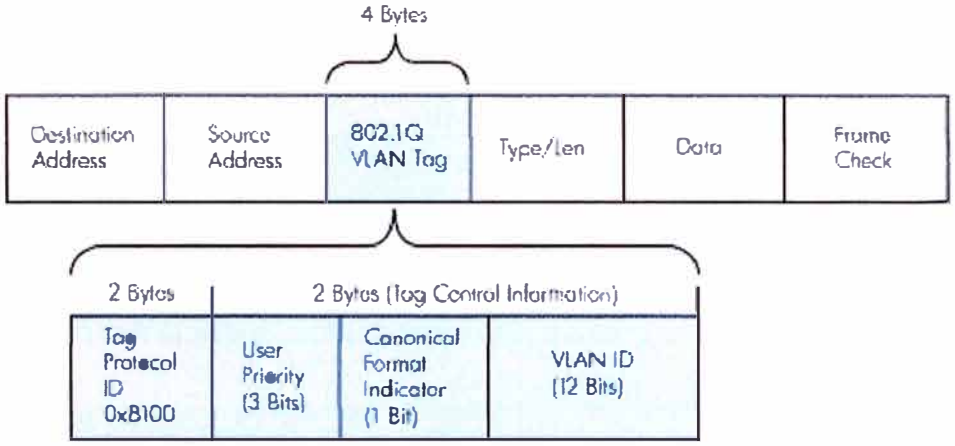

Figura 2.2. Trama 802.1Q

Debido a que con el cambio del encabezado se cambia la trama, 802.1Q fuerza a un recálculo del campo FCS.

2.2.1.2. VLAN nativas

El punto 9 del estándar define el protocolo de encapsulamiento usado para multiplexar varias VLAN a través de un solo enlace, e introduce el concepto de las VLANs nativas. La VLAN nativa es la vlan a la que pertenecía un puerto en un switch antes de ser configurado como trunk. Sólo se puede tener una VLAN nativa por puerto.

Para establecer un trunking 802.1q a ambos lados debemos tener la misma VLAN nativa porque la encapsulación todavía no se ha establecido y los dos switches deben hablar sobre un link sin encapsulación (usan la native VLAN) para ponerse de acuerdo en estos parámetros. En los equipos de Cisco Systems la VLAN nativa por defecto es la VLAN 1. Por la VLAN 1 además de datos datos, se manda información sobre PAgP, CDP, VTP.

Durante el diseño se recomienda:

- La VLAN nativa no debe ser la de gestión.
- Cambiar la VLAN nativa de la 1 a cualquier otra como medida de seguridad.
- Todos los switches en la misma VLAN nativa.
- Usuarios y servidores en sus respectivas VLANs.
- El tráfico entre switches debe ser el único que no se encapsule en enlaces trunk. El resto del tráfico, incluyendo la VLAN de gestión debe ir encapsulado por los trunks. Si no estamos encapsulando cualquiera puede conectar un equipo que no hable 802.1q (switches y hubs) y funcionará sin nuestro control.

2.2.2.-VTP (VLAN Trunking Protocol)

Para conseguir conectividad entre VLAN a través de un enlace troncal entre switches, las VLAN deben estar configuradas en cada switch. El VTP (Vlan Trunking Protocol) proporciona un medio sencillo de mantener una configuración de VLANs coherente a graves de toda la red conmutada. VTP permite soluciones de red

conmutada fácilmente escalable a otras dimensiones, reduciendo la necesidad de configuración manual de la red.

VTP es un protocolo de mensajería de capa 2 que mantiene la coherencia de lá configuración VLAN a través de un dominio de administración común, gestionando las adiciones, supresiones y cambios de nombre de las VLAN a través de las redes. Un dominio VTP son varios switches interconectados que comparten un mismo entorno VTP. Cada switch se configura para residir en un único dominio VTP.

2.3.- STP (Spanning Tree Protocol)

Spanning Tree Protocol *(STP)* es un protocolo de red de la segunda capa OSI, (nivel de enlace de datos). Está basado en un algoritmo diseñado por Radia Perlman mientras trabajaba para DEC. Hay 2 versiones del STP: la original (DEC STP) y la estandarizada por el IEEE (IEEE_802.1D), que no son compatibles entre sí. En la actualidad, se recomienda utilizar la versión estandarizada por el IEEE.

Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice que la topología está libre de lazos. STP es transparente a las estaciones de usuario.

Los bucles infinitos ocurren cuando hay rutas alternativas hacia una misma máquina o segmento de red de destino. Estas rutas alternativas son necesarias para proporcionar redundancia, ofreciendo una mayor fiabilidad. Si existen varios enlaces, en el caso que uno falle, otro enlace puede seguir soportando el tráfico de la red. Los problemas aparecen cuando utilizamos dispositivos de interconexión de nivel de enlace, como un puente de red o un conmutador de paquetes.

Cuando hay lazos en la topología de red, los dispositivos de interconexión de nivel de enlace reenvían indefinidamente las tramas Broadcast y multicast, al no existir ningún campo TTL (Time To Live, *Tiempo de Vida*) en la Capa 2, tal y como ocurre en la Capa 3. Se consume entonces una gran cantidad de ancho de banda, y en muchos caso la red queda inutilizada.

Un router, por el contrario, si podría evitar este tipo de reenvíos indefinidos. La solución consiste en permitir la existencia de enlaces físicos redundantes, pero creando una topología lógica libre de lazos. STP permite solamente una trayectoria activa a la vez entre dos dispositivos de la red (esto previene los bucles) pero mantiene los caminos redundantes como reserva, para activarlos en caso de que el camino inicial falle.

Si la configuración de STP cambia, o si un segmento en la red redundante llega a ser inalcanzable, el algoritmo reconfigura los enlaces y restablece la conectividad, activando uno de los enlaces de reserva. Si el protocolo falla, es posible que ambas conexiones estén activas simultáneamente, lo que podrían dar lugar a un bucle de tráfico infinito en la LAN. Existen varias variantes del *Spanning Tree Protocol*, debido principalmente al tiempo que tarda el algoritmo utilizado en converger. Una de estas variantes es el Rapid Spanning Tree Protocol.

El árbol de expansión (Spanning tree) permanece vigente hasta que ocurre un cambio en la topología, situación que el protocolo es capaz de detectar de forma automática. El máximo tiempo de duración del árbol de expansión es de cinco minutos. Cuando ocurre uno de estos cambios, el puente raíz actual redefine la topología del árbol de expansión o se elige un nuevo puente raíz.

2.3.1. Funcionamiento

Este algoritmo cambia una red fisica con forma de malla, en la que existen bucles, por una red lógica en árbol en la que no existe ningún bucle. Los puentes se comunican mediante mensajes de configuración llamados Bridge Protocol Data Units (B.P.D.U). El protocolo establece *identificadores por puente* y elige el que tiene la prioridad más alta (el número más bajo de prioridad numérica), como el *puente raíz*. Este puente raíz establecerá el camino de menor coste para todas las redes; donde en cada puerto tiene un parámetro configurable: el Span path Cost. Después, entre todos los puentes que conectan un segmento de red, se elige un *puente designado*, el de menor coste (en el caso que haya mismo coste en dos puentes, se elige el que tenga el menor identificador), para transmitir las tramas hacia la raíz. En este puente designado, el puerto que conecta con el segmento, es el *puerto designado* y el que ofrece un camino de menor coste hacia la raíz, el *puerto raíz*. Todos los demás puertos y caminos son bloqueados, esto es en un estado ya estacionario de funcionamiento.

2.3.1.1. Elección del puente raíz

La primera decisión que toman todos los switches de la red es identificar el puente raíz ya que esto afectará al flujo de tráfico. Cuando un switch se enciende, supone que es el switch raíz y envía las BPDU que contienen la dirección MAC de sí mismo tanto en el ID raíz como emisor. Cada switch reemplaza los ID de raíz más alta por ID de raíz más baja en las BPDU que se envían. Todos los switches reciben las BPDU y determinan que el switch que cuyo valor de ID raíz es el más bajo será el puente raíz. El administrador de red puede establecer la prioridad de switch

en un valor más pequeño que el del valor por defecto (32768), lo que hace que el ID sea más pequeño. Esto sólo se debe implementar cuando se tiene un conocimiento profundo del flujo de tráfico en la red.

2.3.1.2. Mantenimiento del Spanning Tree

Cada intervalo de tiempo marcado en el valor "Hello Time" de las BPDU, suele ser 2 segundos, el puente raíz emite un BPDU proponiéndose como raíz. Los puentes designados cambian sus identificadores y recalculan los costes hasta la raíz. Cuando un puente recibe una BPDU en el que el identificador de la raíz es mayor que el suyo propio, intenta convertirse en raíz y envía BPDUs en los que el identificador de la raíz es su propio identificador.

En cambio, si cuando un puente recibe una BPDU en el que el camino a la raíz es mayor que el coste que él mismo puede ofrecer por uno de sus puertos, intenta convertirse en puente designado. Si el coste es el mismo, se compararían identificadores. El algoritmo converge cuando todos los puertos de los puentes están en estado de envío o bloqueo. Se muestra a continuación el diagrama de funcionamiento del STP en que muestra los diversos procesos que se manifiestan:

Fuente: http://www.itesm.mx/viti/servicios/soporte_red/TYR-CCS-P2.pdf

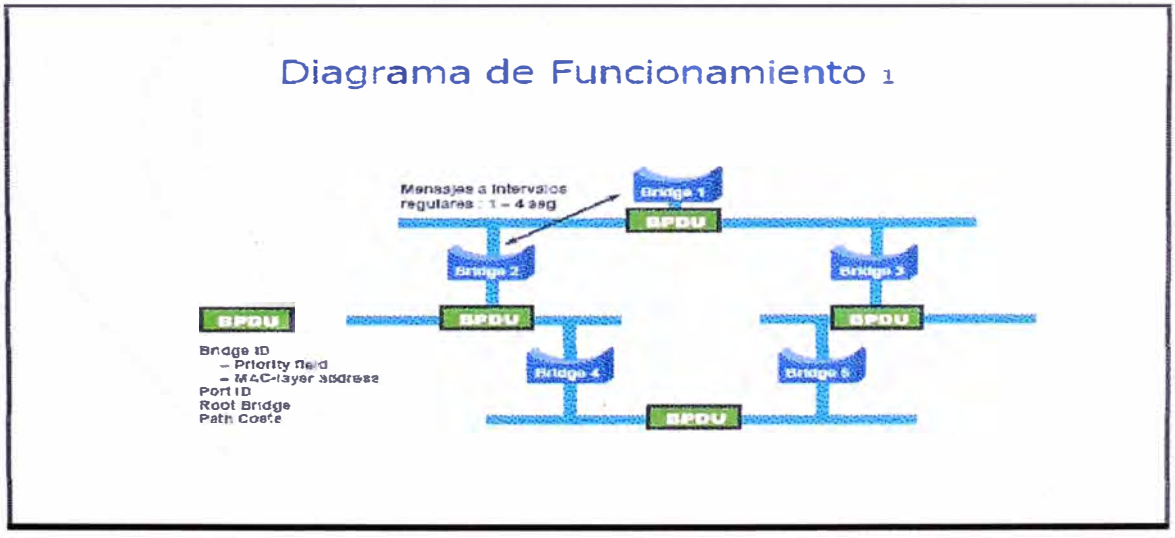

Figura 2.3. Diagrama de Funcionamiento del STP (1)

Fuente: http://www.itesm.mx/viti/servicios/soporte_red/TYR-CCS-P2.pdf

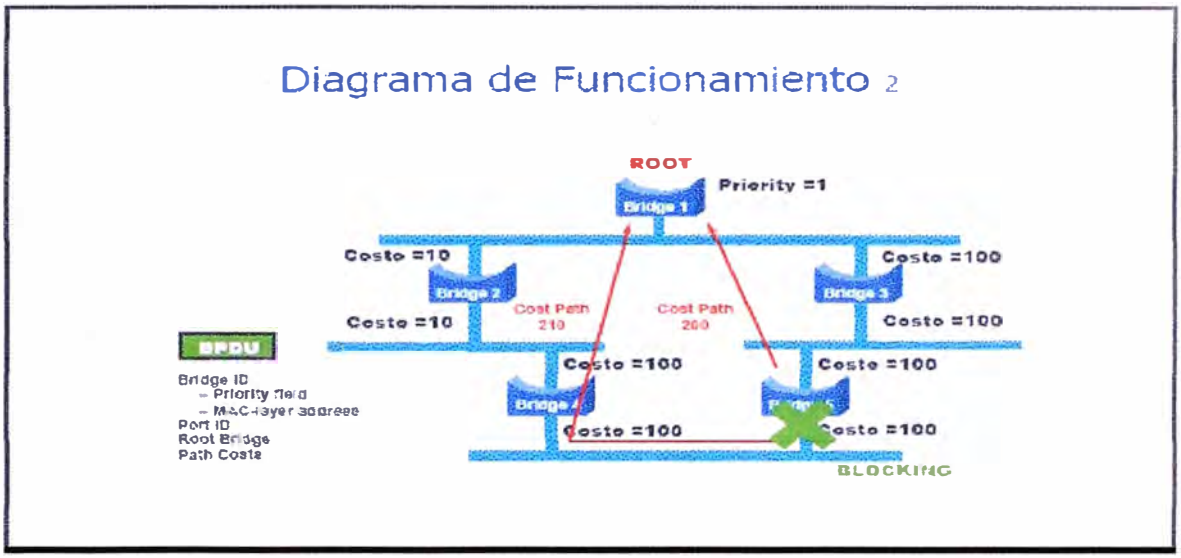

Figura 2.4. Diagrama de Funcionamiento del STP (2)

2.3.1.3. Estado de los puertos

Los estados en los que puede estar un puerto son los siguientes:

- **Bloqueo**: En este estado sólo se pueden recibir BPDU's. Las tramas de datos se descartan y no se actualizan las tablas ARP.
- **Escucha**: A este estado se llega desde Bloqueo. En este estado, los switches determinan si existe alguna otra ruta hacia el puente raíz. En el caso que la nueva ruta tenga un coste mayor, se vuelve al estado de Bloqueo. Las tramas de datos se descartan y no se actualizan las tablas ARP. Se procesan las BPDU.
- **Aprendizaje**: A este estado se llega desde Escucha. Las tramas de datos se descartan pero ya se actualizan las tablas ARP (ya se aprenden las direcciones MAC). Se procesan las BPDU.
- **Envío**: A este estado se llega desde Aprendizaje. Las tramas de datos se envían y se actualizan las tablas ARP. Se procesan las BPDU.
- **Desactivado**: A este estado se llega desde cualquier otro. Se produce cuando un administrador deshabilita el puerto o éste falla. No se procesan las BPDU.

2.4.- Agregación de puertos

2.4.1.-EtherChannel

Hay mucha gente que aun no conoce el concepto de Etherchannel y por culpa de este desconocimiento estamos perdiendo una gran ventaja del switching actual. Un Etherchannel nos permite sumar la velocidad nominal de cada puerto físico y así obtener un único enlace troncal de alta velocidad. Supongamos que tenemos la topología de la siguiente forma como se muestra en la siguiente figura, donde se aprecia que se encuentra instalado una granja de Servidores en la red. Cuando tenemos una serie de servidores que salen por un único enlace trocal, pueda ser que el tráfico generado llegue a colapsar el enlace. Una de las soluciones más prácticas que se suele implementar en estos casos es el uso de Etherchannel. Cuando generamos un EtherChannel lo que estamos haciendo es sumar la velocidad de los puertos que

Fuente:
http://www.cisco.com/en/US/tech/tk389/tk213/technologies_configuration_example09186a0080094470.shtml

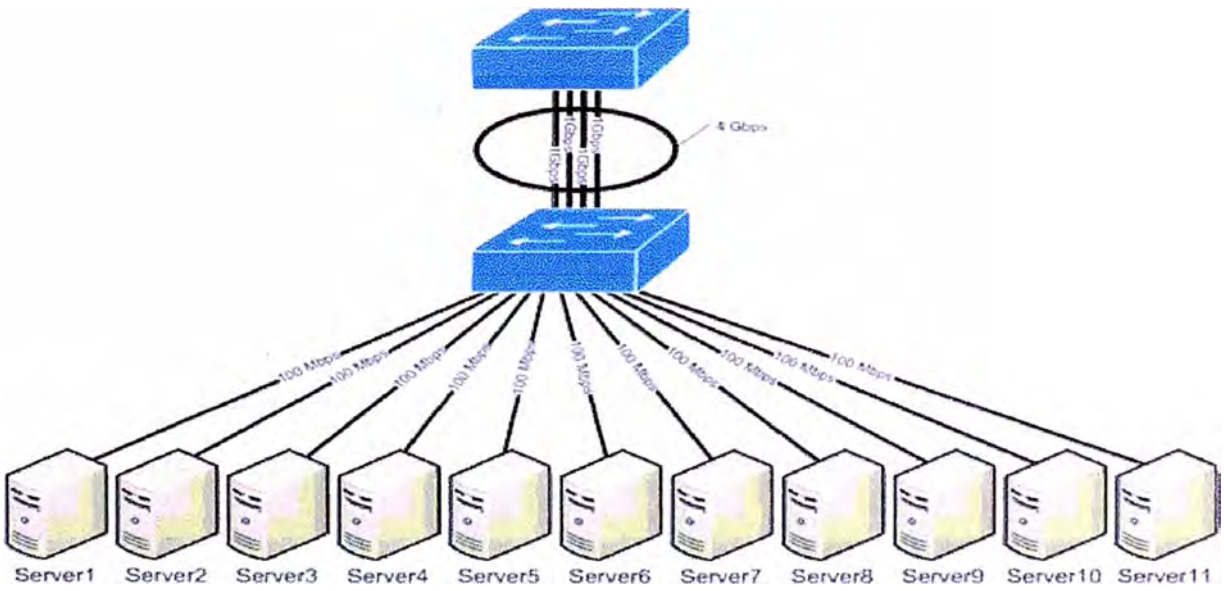

Figura 2.5. Granja de Servidores

agregamos al enlace lógico obteniendo el siguiente resultado, donde se aprecia la siguiente distribución de enlaces:

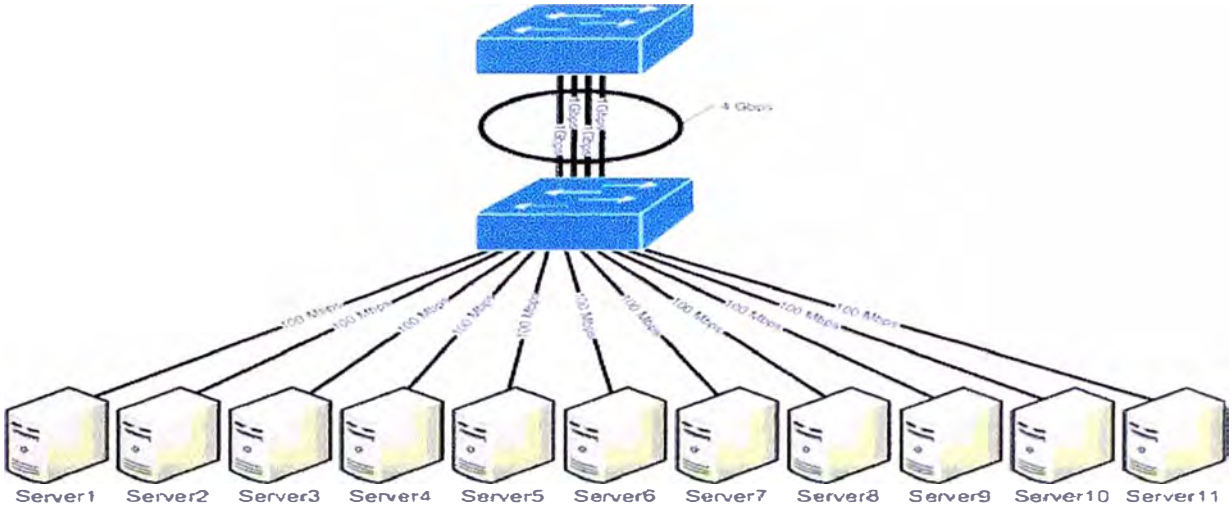

Figura 2.6. Establecimiento del EtherChannel

Esta es una solución muy implementada en servidores Blade, un servidor de estas características es una maquina diseñada para poder ahorrar espacio en los CPD, reducir consumo y simplificar la administración. Un chasis de Blade incorpora las fuentes de alimentación, elementos de ventilación y de conectividad LAN y SAN. Los servidores son delgadas tarjetas que incorporan los componentes propios del servidor como el procesador la memoria y los buses.

Figura 2.7. Chasis Blade

Un chasis de Blade puede tener hasta 16 servidores dependiendo del fabricante y estos chasis en su parte posterior suelen llevar entre uno y cuatro switches. Si queremos sacar todo este tráfico hacia el exterior sin sufrir colapsos en los troncales la solución más recomendable es configurar un Etherchannel. La conexión física quedaría como se puede ver a continuación en el siguiente gráfico, donde se aprecia la agregación de puertos entre el Blade y los servidores donde existe redundancia para poder adicionar el ancho de banda hasta en 04 veces.

Fuente:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.1E/native/configuration/guide/channel.html

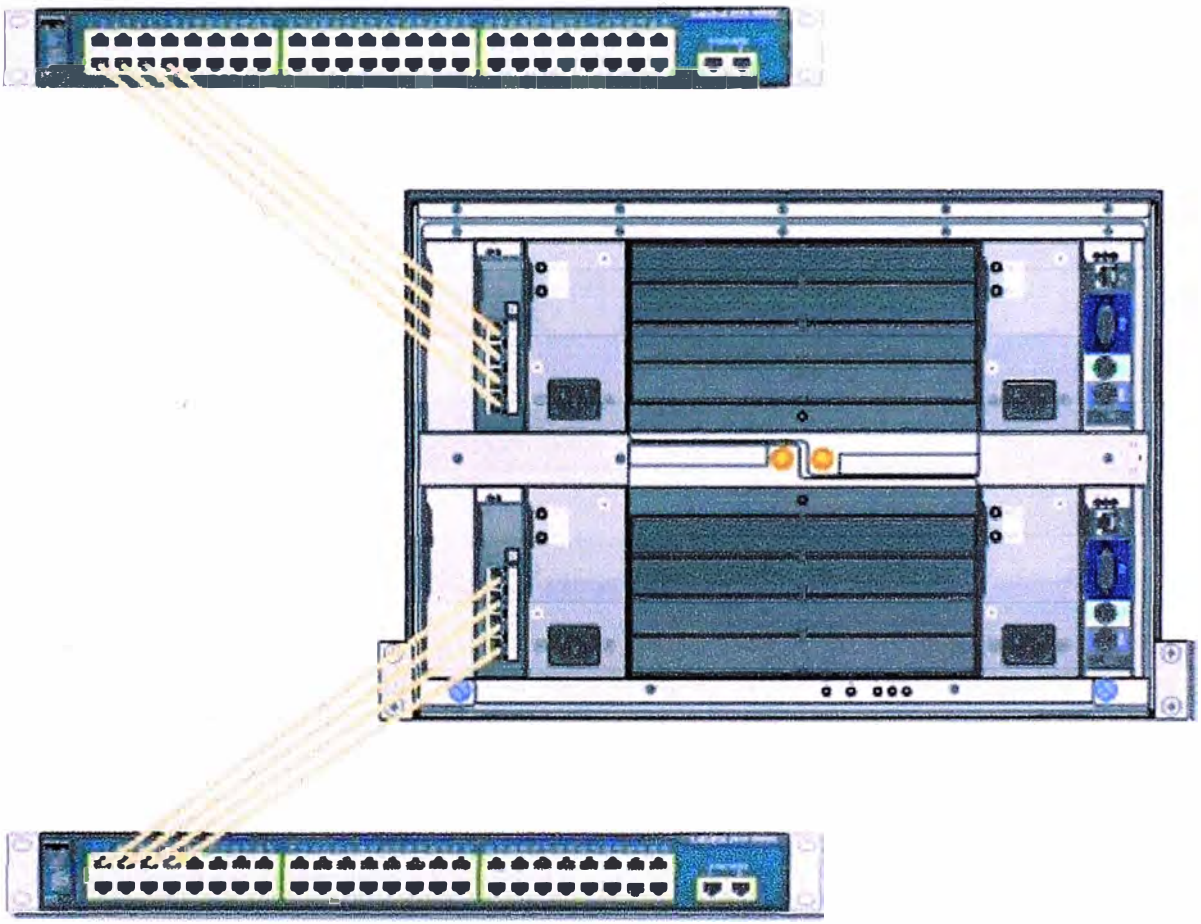

Figura 2.8. Etherchannel

Existen varias formas de configurar un Etherchannel, el objetivo de este post no es

explicar en profundidad como funciona cada uno de los protocolos, pero intentaré dejar lo suficientemente claro cuando usar cada uno de ellos. Podemos configurar un Etherchannel de tres formas diferentes, Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP) o en modo ON, además ambos extremos se han de configurar en el mismo modo. Cuando se configura PAgP o LACP el switch negocia con el otro extremo que puertos deben ponerse activos, aquellos puertos que no sean compatibles se dejan desactivados en versiones anteriores a la 12.2(35) SE, a partir de esta versión el puerto queda activo pero no se agrega al Etherchannel, este puerto seguirá trabajando de forma independiente. Cuando configuramos en modo ON no se realiza ningún tipo de negociación, el switch obliga a todos los puertos compatibles a ponerse activos.

PAgP es un protocolo propietario de Cisco, PAgP se encarga de agrupar puertos de características similares de forma automática. PAgP es capaz de agrupar puertos de la misma velocidad, modo dúplex, troncales o de asignación a una misma VLAN.
PAgP se puede configurar de dos modos:

- Auto, establece el puerto en una negociación pasiva, el puerto solo responderá a paquetes PAgP cuando los reciba, pero nunca iniciará la negociación.
- Desirable, establece el puerto en modo de negociación activa, este puerto negociará el estado cuando reciba paquetes PAgP y también podrá iniciar una negociación contra otros puertos.

Hay que tener en cuenta que un puerto en modo desirable puede formar grupo con otro puerto en el mismo modo, también podrá formar grupo con un puerto en modo auto. Dos puertos en modo auto nunca podrán formar grupo ya que ninguno de ellos puede iniciar una negociación.

LACP es un protocolo definido en el estándar 802.1ad y que puede ser implementado en switches cisco. LACP y PAgP funcionan de forma muy similar ya que LACP también puede agrupar puertos por su velocidad, modo dúplex, troncales, VLAN nativas, etc.

LACP también tiene dos modos de configuración:

- Activo, un puerto en este estado es capaz de iniciar negociaciones con otros puertos

para establecer el grupo en particular según sea el caso específico.
• Pasivo, un puerto en este estado es un puerto que no iniciará ningún tipo de negociación pero si responderá a las negociaciones generadas por otros puertos. Al igual que LAgP, dos puertos pasivos nunca podrán formar grupo. El modo ON es un modo de configuración en el cual se establece toda la configuración del puerto de forma manual, no existe ningún tipo de negociación entre los puertos para establecer un grupo. En este tipo de configuración es totalmente necesario que ambos lados estén en modo ON.

Podríamos profundizar aún más pero creo que con esto es suficiente, se puede aplicar diferentes configuraciones a un Etherchannel según las necesidades, establecer prioridades y otras opciones pero nos extenderíamos demasiado, por eso voy a pasar a explicar una configuración sencilla en la cual generamos un Etherchannel de cuatro puertos en modo ON. Como ya he comentado es imprescindible configurar los puertos en modo ON en ambos lados y no requiere mucho esfuerzo.

Cuando se crea un Etherchannel todos los puertos que pertenecen a este adquieren todos los parámetros del primer puerto agregado al grupo, por eso una recomendación es configurar este primer puerto con todas las opciones que le queramos establecer (STP, VLANs, etc...).

También sería importante seguir estas recomendaciones:
- No se debe configurar un puerto en dos grupos diferentes.
- No se debe configurar un puerto en dos modos diferentes, LACP y PAgP.
- No configurar Switched Port Analyzer (SPAN) como parte de un Etherchannel.
- No configurar securización de puertos.
- Asignar todos los puertos del Etherchannel a la misma VLAN o configurar todos como troncales.

- Verificar que todos los puertos del grupo están en un mismo modo de encapsulación, ISL o 802.1Q.

2.5.- VoIP

La VoIP: Voz sobre IP (Voz transmitida sobre Protocolo Internet) permite a los

usuarios establecer llamadas de voz y fax sobre conexiones IP (redes de datos corporativos, Intranets, Extranet, Internet, etc.), y a la vez reducir considerablemente el presupuesto correspondiente al servicio telefónico , llegando a eliminarlos para comunicaciones internas entre sucursales de una empresa o de un grupo de empresas.
En su origen, el Protocolo Internet se utilizó para el envío de datos, pero en la actualidad, y debido al importante desarrollo tecnológico que está experimentando el campo, disponemos de una tecnología que permite digitalizar la voz y comprimirla en paquetes de datos, que son enviados a través de cualquier moderno sistema de transmisión de datos (Líneas dedicadas, líneas telefónicas, conexiones inalámbricas, etc) para ser reconvertidos de nuevo en voz en el punto de destino.
La conversión de la voz a datos requiere una sofisticada formulación matemática, que comprime la voz humana digitalizada en un conjunto de datos mucho más pequeño y manejable. Una fórmula similar expande los datos comprimidos para devolver la voz a su estado original una vez que llega a su destino, minimizando el ancho de banda consumido, por lo que se optimizan los recursos disponibles. Por ejemplo, una conversación de telefonía IP ocupa aproximadamente la octava parte que una tradicional. Uno de los principales logros de la telefonía IP consiste en realizar todo ese complicado proceso de compresión y descompresión de la voz en una pequeña fracción de segundo.

Debido a que las formulaciones matemáticas y los procesadores de señal para la compresión y descompresión de la voz en datos son cada vez más eficientes, y los anchos de banda disponibles para el traslado de la voz sobre IP cada vez son mayores, la calidad de las comunicaciones de voz sobre IP ha superado la de la telefonía celular, y prácticamente ha igualado a la de las llamadas telefónicas sobre sistemas de telefonía estándar.

Es muy importante diferenciar entre Voz sobre IP (VoIP) y Telefonía sobre IP (ToIP).

- VoIP es el conjunto de normas, dispositivos, protocolos, en definitiva *la tecnología* que permite la transmisión de la voz sobre el protocolo IP.
- ToIP es el conjunto de *nuevas funcionalidades* de la telefonía, es decir en lo que se

convierte la telefonía tradicional debido los servicios que finalmente se pueden llegar a ofrecer gracias a poder portar la voz sobre el protocolo IP en redes de datos.

El crecimiento y fuerte implantación de las redes IP, tanto en local como en remoto, el desarrollo de técnicas avanzadas de digitalización de voz, los mecanismos de control y la priorización de tráfico, protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que permitan la calidad de servicio en redes IP, han creado un entorno donde es posible transmitir telefonía sobre IP lo que no significará en modo alguno la desaparición de las redes telefónicas modo circuito, sino que habrá, al menos temporalmente, una fase de coexistencia entre ambas, y por supuesto la necesaria interconexión mediante pasarelas (gateways), denominadas genéricamente pasarelas VoIP. Este aspecto ha sido abordado tanto por ITU como por el IETF.

Si a todo lo anterior, se le suma el fenómeno Internet, junto con el potencial ahorro económico que este tipo de tecnologías puede llevar acarreado, la conclusión es clara: El VoIP (Protocolo de Voz Sobre Internet - Voice Over Internet Protocol) es un tema "caliente" y estratégico para las empresas.

Hoy, desregulación mediante, la telefonía sobre IP empieza a ver su hora más gloriosa y es el fruto más legítimo de la convergencia tecnológica. El concepto original es relativamente simple: se trata de transformar la voz en "paquetes de información" manejables por una red IP (con protocolo Internet, materia que también incluye a las intranets y extranets). Gracias a otros protocolos de comunicación, como el RSVP, es posible reservar cierto ancho de banda dentro de la red que garantice la calidad de la comunicación. La voz puede ser obtenida desde un teléfono común: existen gateways (dispositivos de interconexión) que permiten intercomunicar las redes de telefonía tradicional con las redes de datos. De hecho, el sistema telefónico podría desviar sus llamadas a Internet para que, una vez alcanzado el servidor más próximo al destino, esa llamada vuelva a ser traducida como información analógica y sea transmitida hacia un teléfono común por la red telefónica tradicional. Vale decir, se pueden mantener conversaciones teléfono a teléfono.

2.5.1.- Estándares para la VoIP

Es innegable la implantación definitiva del protocolo IP desde los ámbitos empresariales a los domésticos y la aparición de un estándar, el VoIP, no podía hacerse esperar. La aparición del VoIP junto con el abaratamiento de los DSP's (Procesador Digital de Señal), los cuales son claves en la compresión y descompresión de la voz, son los elementos que han hecho posible el despegue de estas tecnologías. Para este auge existen otros factores, tales como la aparición de nuevas aplicaciones o la apuesta definitiva por VoIP de fabricantes como Cisco Systems o Nortel-Bay Networks. Por otro lado los operadores de telefonía están ofreciendo o piensan ofrecer en un futuro cercano, servicios IP de calidad a las empresas.

Por lo dicho hasta ahora, vemos que nos podemos encontrar con tres tipos de redes IP:

a). Internet. El estado actual de la red no permite un uso profesional para el tráfico de voz.

b). Red IP pública. Los operadores ofrecen a las empresas la conectividad necesaria para interconectar sus redes de área local en lo que al tráfico IP se refiere. Se puede considerar como algo similar a Internet, pero con una mayor calidad de servicio y con importantes mejoras en seguridad. Hay operadores que incluso ofrecen garantías de bajo retardo y/o ancho de banda, lo que las hace muy interesante para el tráfico de voz.

c). Intranet. La red IP implementada por la propia empresa. Suele constar de varias redes LAN (Ethernet conmutada, ATM, etc..) que se interconectan mediante redes WAN tipo Frame-Relay/ATM, líneas punto a punto, RDSI para el acceso remoto, etc. En este caso la compañía tiene bajo su control prácticamente todos los parámetros de la red, por lo que resulta ideal para su uso en el transporte de la voz.

2.5.2.- Protocolos

Es el lenguaje que utilizarán los distintos dispositivos VoIP para su conexión. Esta

parte es importante ya que de ella dependerá la eficacia y la complejidad de la comunicación.

Por orden de antigüedad (de más antiguo a más nuevo):

H.323 - Protocolo definido por la ITU-T
SIP - Protocolo definido por la IETF
Megaco (También conocido como H.248) y MGCP - Protocolos de control
Skinny Client Control Protocol - Protocolo propiedad de CISCO
MiNet - Protocolo propiedad de MITEL
CorNet-IP - Protocolo propiedad de SIEMENS
IAX - Protocolo original para la comunicación entre PBXs ASTERISK(obsoleto)
Skype - Protocolo propietario peer to peer utilizado en la aplicación SKYPE
IAX2 - Protocolo para la comunicación entre PBXs ASTERISK en reemplazo de IAX
Jingle - Protocolo abierto utilizado en tecnología JABBER

Debido a la ya existencia del estándar H.323 del ITU-T, que cubría la mayor parte de las necesidades para la integración de la voz, se decidió que el H.323 fuera la base del VoIP. De este modo, el VoIP debe considerarse como una clarificación del H.323, de tal forma que en caso de conflicto, y a fin de evitar divergencias entre los estándares, se decidió que H.323 tendría prioridad sobre el VoIP. El VoIP tiene como principal objetivo asegurar la interoperabilidad entre equipos de diferentes fabricantes, fijando aspectos tales como la supresión de silencios, codificación de la voz y direccionamiento, y estableciendo nuevos elementos para permitir la conectividad con la infraestructura telefónica tradicional. Estos elementos se refieren básicamente a los servicios de directorio y a la transmisión de señalización por tonos multifrecuencia (DTMF).

El VoIP/H.323 comprende a su vez una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación:

- Direccionamiento:
- RAS (Registration, Admision and Status). Protocolo de comunicaciones que puede

permitir a una estación H.323 localizar otra estación H.323 a través del Gatekeeper.

- DNS (Domain Name Service). Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS
- Señalización:
- Q.931 Señalización inicial de llamada
- H.225 Control de llamada: señalización, registro y admisión, y paquetización / sincronización del stream (flujo) de voz
- H.245 Protocolo de control para especificar mensajes de apertura y cierre de canales para streams de voz
- Compresión de Voz:
- Requeridos: G.711 y G.723
- Opcionales: G.728, G.729 y G.722
- Transmisión de Voz:
- UDP. La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.
- RTP (Real Time Protocol). Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.
- Control de la Transmisión

Figura 2.9. Control de la Transmisión

2.5.3.- Arquitectura de red

El propio Estándar define tres elementos fundamentales en su estructura:

- **Terminales**: Son los sustitutos de los actuales teléfonos. Se pueden implementar tanto en software como en hardware.

- **Gatekeepers:** Son el centro de toda la organización VoIP, y serían el sustituto para las actuales centrales. Normalmente implementadas en software, en caso de existir, todas las comunicaciones pasarían por él.

- **Gateways:** Se trata del enlace con la red telefónica tradicional, actuando de forma transparente para el usuario.

  Con estos tres elementos, la estructura de la red VoIP podría ser la conexión de dos delegaciones de una misma empresa. La ventaja es inmediata: todas las comunicaciones entre las delegaciones son completamente gratuitas. Este mismo esquema se podría aplicar para proveedores, con el consiguiente ahorro que esto conlleva.

- **Protocolos de VoIP**: Es el lenguaje que utilizarán los distintos dispositivos VoIP para su conexión. Esta parte es importante ya que de ella dependerá la eficacia y la complejidad de la comunicación.
  - H.323 - Protocolo definido por la ITU-T
  - SIP - Protocolo definido por la IETF
  - Megaco (También conocido como H.248) y MGCP - Protocolos de control
  - Skinny Client Control Protocol - Protocolo propiedad de Cisco
  - MiNet - Protocolo propiedad de Mitel
  - CorNet-IP - Protocolo propiedad de Siemens
  - IAX - Protocolo original para la comunicación entre PBXs Asterisk (obsoleto)
  - Skype - Protocolo propietario peer-to-peer utilizado en la aplicación Skype
  - IAX2 - Protocolo para la comunicación entre PBXs Asterisk en reemplazo de IAX
  - Jingle - Protocolo abierto utilizado en tecnología Jabber
  - MGCP- Protocolo propietario de **Cisco**

  Este último es propiedad de Cisco y lo emplea en sus equipos.

2.5.4.- Parámetros de la VoIP

Este es el principal problema que presenta hoy en día la penetración tanto de VoIP como de todas las aplicaciones de IP. Garantizar la calidad de servicio sobre una red **IP**, por medio de retardos y ancho de banda, actualmente no es posible; por eso, se presentan diversos problemas en cuanto a garantizar la calidad del servicio.

a).- Códecs

La voz ha de codificarse para poder ser transmitida por la red IP. Para ello se hace uso de Códecs que garanticen la codificación y compresión del audio o del video para su posterior decodificación y descompresión antes de poder generar un sonido o imagen utilizable. Según el Códec utilizado en la transmisión, se utilizará más o menos ancho de banda. La cantidad de ancho de banda suele ser directamente proporcional a la calidad de los datos transmitidos.Entre los codecs utilizados en VoIP encontramos los G.711 (64Kbps), G.723.1 (6.3Kbps) y el G.729 (8Kbps) (especificados por la **ITU-T**).

b).- Retardo o latencia

Una vez establecidos los retardos de tránsito y el retardo de procesado la conversación se considera aceptable por debajo de los 150 ms.

c).- Calidad del servicio

La calidad de este servicio se está logrando bajo los siguientes criterios:

- La supresión de silencios, otorga más eficiencia a la hora de realizar una transmisión de voz, ya que se aprovecha mejor el ancho de banda al transmitir menos información.
- De esta manera la comunicación de brindará con una mejor calidad y audibilidad en las dos partes que participan en la comunicación inherente.
- Compresión de cabeceras aplicando los estándares RTP/RTCP.
- Priorización de los paquetes que requieran menor latencia. Las tendencias actuales son:

- CQ (Custom Queuing) : Asigna un porcentaje del ancho de banda disponible.
- PQ (Priority Queuing) : Establece prioridad en las colas.
- WFQ (Weight Fair Queuing) : Se asigna la prioridad al tráfico de menos carga.
- DiffServ: Evita tablas de encaminados intermedios y establece decisiones de rutas por paquete.

- La implantación de IPv6 que proporciona mayor espacio de direccionamiento y la posibilidad de tunneling.

2.5.5.- RTP/RTCP

RTP es la abreviación de *Real-time Transport Protocol*, por su denominación en Inglés. Es un estándar creado por la IETF para la transmisión confiable de voz y video a través de Internet. La primera versión fue publicada en 1996 en el documento RFC 1889 y fue reemplazado por el estándar RFC 3550 en 2003.En aplicaciones de Voz sobre IP, RTP es el protocolo responsable de la transmisión de los datos. La digitalización y compresión de la voz y el video es realizada por el CODEC. Para el manejo de señalización o establecimiento de llamada existe el protocolo SIP. Dentro del estándar RFC 3550 se define un protocolo adicional para el envío de datos de control y datos de mediciones realizadas durante la transmisión. Se conoce como RTCP *RTP Control Protocol*. los paquetes RTCP se envían periódicamente dentro de la secuencia de paquetes RTP.

2.5.5.1. Características generales

Aunque RTP tiene algunas características de protocolo de nivel de transporte (Según el modelo OSI), es transportado usando UDP. UDP no maneja sesiones ni mecanismos que garanticen la recepción de los paquetes, pero es usado por RTP en lugar de TCP debido a que reduce el tiempo de envío de los paquetes a través de la red. En aplicaciones de voz y video es más importante una transmisión rápida que la pérdida de algunos paquetes durante el recorrido.

RTP implementa dos mecanismos principales para garantizar una transmisión de voz: El uso de Número de secuencia y un Registro de tiempo. En redes IP es común que

los paquetes tomen caminos diferentes para llegar al destino. En aplicaciones de datos esto no es demasiado importante pero para voz y video puede representar una falla detectable por el oído del usuario final. Por esto RTP usa el número de secuencia para reorganizar los paquetes en caso de que lleguen en desorden y el Registro de tiempo es usado para ajustar los intervalos de muestreo de acuerdo a la secuencia original.

2.5.5.2. Formato y valores de encabezado

El paquete RTP se ubica en el espacio de datos de UDP. RTP no tiene asignado un puerto UDP específico, debido a que es posible que varias aplicaciones de un mismo usuario utilicen RTP. Existen sistemas que no soportan el uso de un mismo puerto por aplicativos diferentes. De acuerdo a las especificaciones se utiliza un número par elegido al azar, y RTCP utiliza el número impar consecutivo.

Los campos más importantes en el encabezado RTP son los siguientes:

Número de secuencia: de 2 bytes, es un número que se incrementa por cada paquete enviado. Es usado para determinar pérdida de paquetes y recuperar correctamente la secuencia de voz.

Registro de tiempo: Mejor conocido como Timestamp, es un campo de 32 bits asignado en el

momento del envío con base en un reloj del sistema. El valor inicial es seleccionado aleatoriamente para evitar confusión con otras secuencias RTP presentes. Existe la posibilidad de sincronizar los relojes de envío y recepción usando el protocolo NTP.

RTP son las siglas de **R**eal-time **T**ransport **P**rotocol (Protocolo de Transporte de Tiempo real). Es un protocolo de nivel de transporte utilizado para la transmisión de información en tiempo real, como por ejemplo audio y vídeo en una video-conferencia. Está desarrollado por el grupo de trabajo de transporte de Audio y Video del IETF, publicado por primera vez como estándar en 1996 como la RFC 1889, y actualizado posteriormente en 2003 en la RFC 3550, que constituye el estándar de Internet STD 64.

Inicialmente se publicó como protocolo multicast, aunque se ha usado en varias aplicaciones unicast. Se usa frecuentemente en sistemas de streaming, junto a RTSP, videoconferencia y sistemas push to talk (en conjunción con H.323 o SIP).

Representa también la base de la industria de VoIP.

La RFC 1890, obsoleta por la RFC 3551 (STD 65), define un perfil para conferencias de audio y vídeo con control mínimo. La RFC 3711, por otro lado, define SRTP (Secure Real-time Transport Protocol), una extensión del perfil de RTP para conferencias de audio y vídeo que puede usarse opcionalmente para proporcionar confidencialidad, autenticación de mensajes y protección de reenvío para flujos de audio y vídeo. Va de la mano de RTCP (RTP Control Protocol) y se sitúa sobre UDP en el modelo OSI.

2.5.5.3. Estructura del encabezado

Byte 0				Byte 1		Byte 2	Byte 3
V	P	X	CC	M	PT	Sequence Number	
Time Stamp							
Synchronization Source (SSRC)							
Content Source (CSRC)							
Extension header (EH - opcional)							
Datos							

Figura 2.10. Encabezado

- Número de versión de RTP (V - versión number): 2 bits. La versión definida por la especificación actual es 2.
- Relleno (P - Padding): 1 bit. Si el bit del relleno está colocado, hay uno o más bytes al final del paquete que no es parte de la carga util. El último byte del paquete indica

  el número de bytes de relleno. El relleno es usado por algunos algoritmos de cifrado.
- La extensión (X - Extensión): 1 bit. Si el bit de extensión está colocado, entonces el encabezado fijo es seguido por una extensión del encabezado. Este mecanismo de la extensión posibilita implementaciones para añadir información al encabezado RTP.
- Conteo CSRC (CC): 4 bits. El número de identificadores CSRC que sigue el encabezado fijo. Si la cuenta CSRC es cero, entonces la fuente de sincronización es la fuente de la carga útil.

- El marcador (M - Marker): 1 bit. Un bit de marcador definido por el perfil particular de media.
- La carga útil Type (PT): 7 bits. Un índice en una tabla del perfiles de media que describe el formato de carga útil. Los mapeos de carga útil para audio y vídeo están especificados en el RFC 1890.
- El número de Secuencia: 16 bits. Un único número de paquete que identifica la posición de este en la secuencia de paquetes. El número del paquete es incrementado en uno para cada paquete enviado.
- Sellado de tiempo: 32 bits. Refleja el instante de muestreo del primer byte en la carga útil. Varios paquetes consecutivos pueden tener el mismo sellado si son lógicamente generados en el mismo tiempo - por ejemplo, si son todo parte del mismo *frame* de vídeo.
- SSRC: 32 bits. Identifica la fuente de sincronización. Si la cuenta CSRC es cero, entonces la fuente de carga útil es la fuente de sincronización. Si la cuenta CSRC es distinta a cero, entonces el SSRC identifica el mixer(mezclador).
- CSRC: 32 bits cada uno. Identifica las fuentes contribuyentes para la carga útil. El número de fuentes contribuyentes está indicado por el campo de la cuenta CSRC; Allí puede haber más de 16 fuentes contribuyentes. Si hay fuentes contribuyentes múltiples, entonces la carga útil son los datos mezclados de esas fuentes.
- EH: El tamaño de este dato debe ser CC×32 en bits
- Datos: El tamaño de los datos debe ser de X×((EHL+1)×32) donde EHL es la longitud de la extensión del la cabezera en unidades de 32 bits.

2.5.5.4. Protocolo RTCP (Real-Time Control Protocol). Este protocolo permite completar a RTP facilitando la comunicación entre los extremos para poder realizar el intercambio de datos y monitorear de esta forma la calidad de servicio y obtener información acerca de los participantes en la sesión. RTCP se fundamenta en la transmisión periódica de paquetes de control a todos los participantes en la sesión usando el mismo mecanismo de RTP de distribución de paquetes de datos. El protocolo UDP dispone de distintas puertas (*UDP Port*) como mecanismo de

-**Send report** para emisión y recepción de estadísticas (en tiempo random) desde emisores activos.

-**Receiver Report** para recepción estadísticas desde emisores no activos.

-**Source Description** para un identificador de nivel de transporte denominado CNAME (*Canonical Name*).

-**Bye** para indicar el final de la participación en la conexión.

-**Application** para aplicaciones específicas.

El mensaje Send Report, uno de los más interesantes, disponen de 3 secciones bien diferenciadas:

-Los primeros 8 Bytes se refieren a un encabezado común.

-La segunda parte de 20 Bytes permite la evaluación de diferentes parámetros (retardo, jitter, eficiencia de datos, etc).

-La tercera parte de 24 Bytes lleva reportes que han sido obtenidos desde el último reporte informado. Incluye los siguientes reportes: cantidad total de paquetes RTP perdidos y a la proporción de los mismos; la cantidad de paquetes recibidos y el jitter entre paquetes; el horario del penúltimo paquete recibido y el retardo de la transmisión del mismo.

2.6.- QoS (Calidad de Servicio)

La calidad de servicio consiste en la capacidad de la red para reservar algunos de los recursos disponibles para un tráfico concreto con la intención de proporcionar un determinado servicio. Debemos tener en cuenta que en la red se pueden utilizar diferentes tecnologías de transporte (como pueden ser Frame Relay, X.25, SDH, ATM, etc) de manera que la gestión de QoS implica la interacción con estas tecnologías y con los equipos de conmutación, que son los que finalmente determinarán el nivel de QoS alcanzado en esta oportunidad.

En este momento existen principalmente dos tipos de tecnologías que proporcionan calidad de servicio. La primera se basa en la **reserva**, y asigna recursos basándose en flujos de tráfico. Alternativamente, un segundo tipo de calidad de servicio se caracteriza por la **priorización** de determinado tipo de tráfico. Veremos más adelante que los flujos de datos individuales se van agrupando en grandes agregados de tráfico de acuerdo a la "clase de servicio" a la que pertenezcan, y dependiendo de esa clase de servicio recibirán un distinto trato en los diferentes elementos de la red.

En comunicaciones IP se traduce en dos modelos de trabajo:

o **Modelo Intserv:** basado en la utilización de algún protocolo de reserva (RSVP, ReSerVation Protocol) que permite la reserva de recursos a lo largo de los routers implicados en la comunicación. El principal problema de este modelo es la necesidad de mantener información sobre cada flujo en todos los routers de la red, lo cual lleva a problemas de escalabilidad.

o **Modelo Diffserv**: se basa en la división del tráfico en diferentes clases [6],[7] y en la asignación de prioridades a estos agregados. Utiliza diferente información de la cabecera de los paquetes (por ejemplo, DSCP – Diffserv Code Point) para distinguir clasificar los paquetes y conocer el tratamiento que debe recibir el tráfico en los nodos de la red Diffserv.

2.6.1. Calidad de servicio: Diffserv

Los servicios diferenciados (Diffserv) proporcionan mecanismos de calidad de servicio para reducir la carga en dispositivos de la red a través de un mapeo entre flujos de tráfico y niveles de servicio. Los paquetes que pertenecen a una determinada clase se marcan con un código específico (DSCP – Diffserv CodePoint). Este código es todo lo que necesitamos para identificar una clase de tráfico. La diferenciación de servicios se logra mediante la definición de comportamientos específicos para cada clase de tráfico entre dispositivos de interconexión, hecho conocido como PHB (Per Hop Behavior). De esta manera a través de Diffserv planteamos asignar prioridades a los diferentes paquetes que son enviados a la red.

Los nodos intermedios (routers) tendrán que analizar estos paquetes y tratarlos según sus necesidades. Esta es la razón principal por la que Diffserv ofrece mejores características de escalabilidad que Intserv. Dentro del grupo de trabajo de Diffserv de la IETF [5], se define en [2] el campo DS (Differentiated Services) donde se especificarán las prioridades de los paquetes. En el subcampo DSCP (Differentiated Setvice CodePoint) se especifica la prioridad de cada paquete. Estos campos son validos tanto para IPv4 como IPv6.

Fuente: http://www.it.uc3m.es/cgarcia/articulos/cita2002_diffserv.pdf

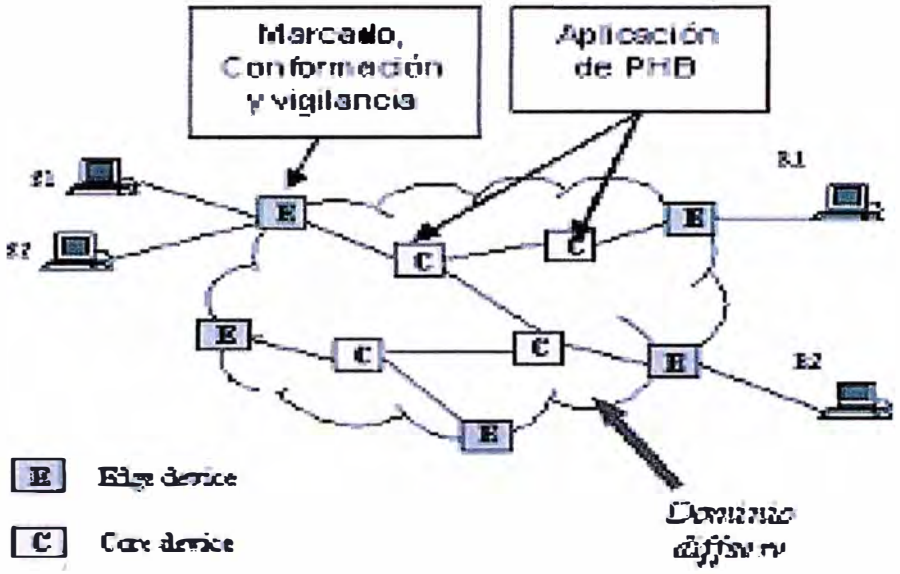

Figura 2.11. Arquitectura Diffserv

Debemos tener en cuenta que un dominio Diffserv puede estar formado por más de una red, de manera que el administrador será responsable de repartir adecuadamente los recursos de acuerdo con el contrato de servicio (SLA – Service Level Agreement) entre el cliente y el proveedor del servicio. Veamos a continuación las diferentes funciones que deben realizar los nodos DS:

o Nodos extremos DS: será necesario realizar diferentes funciones como el acondicionamiento de tráfico entre los dominios Diffserv interconectados. De esta manera debe clasificar y establecer las condiciones de ingreso de los flujos de tráfico en función de: dirección IP y puerto (origen y destino), protocolo de transporte y DSCP, este clasificador se conoce como MF (Multi-Field Classifier).

Una vez que los paquetes han sido marcados adecuadamente, los nodos internos deberán seleccionar el PHB definido para cada flujo de datos. Los nodos DS de entrada serán responsables de asegurar que el tráfico de entrada cumple los requisitos de algún TCA (Traffic Conditioning Agreement), que es un derivado del SLA, entre los dominios interconectados.Por otro lado los nodos DS de salida deberán realizar funciones de acondicionamiento de tráfico o TC (Traffic Conformation) sobre el tráfico transferido al otro dominio DS conectado.

o Nodos internos DS: podrá realizar limitadas funciones de TC, tales como remarcado de DSCP. Los nodos DS internos solo se conectan a nodos internos o a nodos externos de su propio dominio. A diferencia de los nodos externos para la selección del PHB solo ser tendrá en cuenta el campo DSCP, conocido como clasificador BA (Behavior Aggregate Classifier).

2.6.1.1. Protocolo de Gestión de Políticas: COPS

Dentro de este escenario que define Diffserv necesitamos algún modo de comunicación para distribuir las políticas de calidad de servicio entre los elementos de red que las necesiten. Existe un protocolo creado para tal efecto que nos permitirá resolver este problema de comunicación.

El protocolo COPS (Common Open Policy Service) especificado en [3], define un

modelo sencillo de cliente/servidor que proporciona control de políticas para protocolos con señalización de calidad de servicio. El modelo descrito no hace ninguna suposición acerca de los procedimientos utilizados en el servidor de políticas, sino que se basa en un servidor que devuelve decisiones a las peticiones realizadas por los clientes. La definición del protocolo es bastante abierta para que sea extensible y poder soportar los distintos tipos de clientes que pudieran aparecer en el futuro.

El protocolo COPS se basa en sencillos mensajes de petición y respuesta utilizados para intercambiar información acerca de políticas de tráfico entre un servidor de políticas (**PDP**, Policy Decision Point) y distintos tipos de clientes (**PEPs**, Policy

Enforcement Points).

Uno de los objetivos principales del protocolo es proporcionar un modelo sencillo pero fácilmente extensible. Las características principales del protocolo COPS son las siguientes:

o El protocolo emplea un modelo cliente/servidor en el que el PEP envía peticiones y actualizaciones al PDP, y el PDP responde con las decisiones tomadas.

o El protocolo utiliza TCP como protocolo de transporte para asegurar así fiabilidad en el intercambio de mensajes entre los clientes y el servidor.

o El protocolo es extensible en el sentido de que está diseñado para permitir el uso de objetos autoidentificativos y soporta distintos tipos de información específica de clientes, sin tener que realizar ningún tipo de modificación sobre el protocolo. COPS se creó para la administración general, configuración y aplicación de políticas en una red.

o COPS proporciona seguridad a nivel de mensaje mediante autenticación, protección frente al reenvío (replay) e integridad de mensaje. COPS permite además reutilizar otros protocolos de seguridad existentes para proporcionar autenticación y proteger el canal entre el PEP y el PDP.

Fuente: http://www.it.uc3m.es/cgarcia/articulos/cita2002_diffserv.pdf

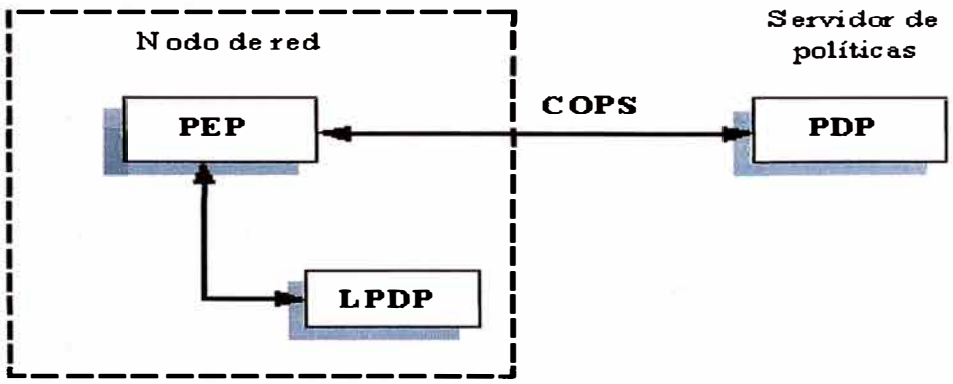

Figura 2.12. El modelo COPS

La figura anterior muestra la disposición de diferentes componentes en un ejemplo COPS típico. En este modelo, el protocolo COPS se utiliza para comunicar la información sobre las políticas de la red entre los puntos de aplicación de políticas (PEPs) y un servidor de políticas remoto (PDP).

Dentro del nodo de red puede existir un PDP local que puede ser utilizado para tomar decisiones locales en ausencia de un PDP. El PEP puede tener también la capacidad de tomar decisiones de política localmente, a través de su LPDP (Local Policy Decision Point), aunque el PDP sigue manteniendo la autoridad en cuanto a las decisiones. Esto quiere decir que cualquier decisión local relevante debe enviarse al PDP. Asimismo, el PDP debe tener acceso a toda la información para poder tomar una decisión final. Para ello, el PEP debe enviar las decisiones locales al PDP a través de un objeto LPDP Decision, y posteriormente atenerse a la decisión que tome el PDP.

2.6.2. La arquitectura de los Servicios Diferenciados (DiffServ)

En esta arquitectura, los paquetes son clasificados y marcados para recibir un trato particular en cuanto al envío en cada salto. Sofisticada clasificación, marcado, política y operaciones de acondicionamiento necesitan sólo ser implementadas en los bordes de la red o en los hosts.
Esta arquitectura logra escalabilidad al implementar un complejas funciones de clasificación y condicionamiento sólo en los nodos del borde de la red, y aplicando conductas por salto a los agregados del tráfico que han sido apropiadamente marcados usando el campo DS en las cabeceras de IPv4 o IPv6.
Es mantenida una distinción entre:

- el servicio provisto a un agregado de tráfico,
- las funciones de condicionamiento y los comportamientos por salto, usados para realizar los servicios,
- el valor del campo DS, usado para marcar paquetes para seleccionar el comportamiento en cada salto, y

los mecanismos de implementación particulares del nodo que realizan un comportamiento por salto.

Esta arquitectura sólo provee servicio diferenciado en una dirección del flujo de tráfico y es por ende asimétrica.

Antes de proseguir y entrar en detalle con el funcionamiento de DiffServ y el análisis de sus componentes, vamos a introducir una breve terminología para así se puede entender con más claridad lo expuesto más adelante.

2.6.2.1. Terminología

Behavior Aggregate (BA, también llamado a veces "agregado de tráfico", TA) : es una colección de paquetes con el mismo DSCP (DiffServ Code Point) atravesando un enlace en una dirección.

BA classifier: es un clasificador que selecciona paquetes basado solo en el contenido del campo de DS.

Enlace de frontera: es un enlace que conecta los nodos de borde de dos dominios.

DS behavior agregate: una colección de paquetes con el mismo código DS, cruzando un enlace en una dirección particular.

código DS: un valor específico de la porción DSCP del campo DS, usado para seleccionar un PHB.

DS-compliant: capaz de soportar funciones y comportamientos de servicios diferenciados.

dominio DS: un dominio capaz de tener DS; un conjunto contiguo de nodos que operan con un conjunto común de políticas de provisionamiento de servicios y definiciones PHB.

nodo de egreso DS: un nodo DS límite en su rol de manejar tráfico a medida que éste deja el dominio DS.

nodo de ingreso DS: un nodo DS límite es su rol de manejar tráfico a medida que éste entra al domino DS.

nodo interior DS: un nodo DS que no es un nodo DS límite.

campo DS: es el octeto TOS de la cabecera de IPv4 o el octeto de la Clase de Tráfico de IPv6. Los bits del campo DSCP contienen el DS codepoint, mientras que los restantes bits no están en uso (se ampliará este tema más adelante).

Dropping: es el proceso de descartar paquetes basándose en reglas específicas; políticas.

Marking (marcado): es el proceso de seteo del DS codepoint en un paquete, basándose en reglas definidas; pre-marcado y re-marcado.

Metering (mediciones): es el proceso de medir las propiedades temporales de una corriente de tráfico seleccionada por un clasificador (classifier).

Microflow (microflujo): es un conjunto de datos, enviados unidireccionalmente entre dos aplicaciones, únicamente identificado por una quíntupla: protocolo de transporte, IP origen, IP destino, puerto origen y puerto destino.

Per-Domain-Behavior (PDB): se define como el trato esperado que un agregado de tráfico va a recibir de borde a borde de un dominio DiffServ.

Per-Hop-Behavior (PHB): define el tratamiento en cada nodo. Es una descripción del comportamiento de reenvío observado exteriormente; puede ser implementado por distintos mecanismos.

Policing: el proceso de descarte de paquetes dentro de un arroyo de tráfico en concordancia con el estado de un correspondiente medidor (meter) cumpliendo un determinado perfil.

Acuerdo del Nivel de Servicio (SLA): un contrato de servicio entre un cliente y un proveedor de servicio que especifica el servicio de envío que un cliente debe recibir.

Shaping (conformador): el proceso de retardar paquetes dentro de un flujo de tráfico, haciendo que conforme cierto perfil de tráfico ya definido.

Traffic Conditioner (acondicionador de tráfico): una entidad que realiza las funciones de condicionamiento del tráfico y que puede contener medidores, marcadores, droppers y conformadores. Están típicamente dispuestos en nodos de borde solamente.

Traffic Conditioning Agreement (TCA): un acuerdo especificando reglas de clasificación y perfiles de tráfico correspondientes, y mediciones, marcado, descarte y/o reglas de conformación que son aplicables a los arroyos de tráfico seleccionados por el clasificador.

2.6.2.2. Requerimientos

La historia de Internet ha sido de un completo crecimiento en cuanto al número de hosts, la gran variedad de aplicaciones y la capacidad de la infraestructura de la red. Por

lo tanto, una arquitectura escalable para servicios diferenciados debe permitir acomodar

este continuo crecimiento.

Los siguientes requerimientos fueron identificados y ubicados en esta arquitectura:

- debe acomodar una amplia variedad de servicios y proveer políticas,
- extendiendo una red punta a punta o una red particular
- debe permitir el desacoplamiento del servicio de la aplicación particular en uso
- debe trabajar con aplicaciones existentes sin la necesidad de cambios en

  interfaces de aplicaciones programables
- debe desacoplar las funciones de condicionamiento de tráfico y
- provisionamiento de servicios de comportamientos de envío implementados en los nodos del núcleo de la red
- no debe depender de la aplicación de señalización salto a salto
- debe requerir solo una pequeña cantidad de comportamientos de envío, cuya complejidad de implementación no domine el costo de un dispositivo de red
- debe utilizar solo estado de clasificación de agregados dentro del núcleo de la red
- debe permitir interoperabilidad razonable con nodos de red no DS capaces
- debe permitir implementaciones de clasificación de paquetes simples en nodos del núcleo de la red
- debe evitar estados por microflujos o por clientes dentro de los nodos del núcleo
- debe acomodar despliegue incremental.

2.6.2.3. Modelo arquitectónico de los Servicios Diferenciados

Las redes IP están compuestas de *nubes*, regiones de relativa homogeneidad en términos del control administrativo, tecnología, ancho de banda. Determinando

dónde terminan las nubes y las fronteras, nosotros determinamos dónde administrar los recursos y dónde el control es aplicado, para asegurarse que la política se lleva a cabo. Dentro de una nube, es posible sacar ventaja de la uniformidad dentro de su frontera, al agregar flujos de tráfico individuales en un número limitado de agregados de tráfico, donde cada uno tendrá un distinto trato de envío. Por lo tanto, el tráfico entrante a la red es clasificado y posiblemente condicionado en los bordes de la red, y asignado a diferentes "behavior aggregates" (BA). Dentro de una nube, todo lo que es importante sobre un paquete para determinar el trato de envío es saber a qué agregado pertenece, siendo posible confiar en una marca puesta en el paquete para indicar su agregado. La forma en que una decisión de política específica sobre QoS es implementada, es por medio de la clasificación, monitoreo, política y otros modos de acondiconamiento del tráfico del paquete en las fronteras de las nubes, luego de los cuales los paquetes reciben un trato uniforme dentro de las nubes. Casi todo el trabajo es confinado al borde de las nubes. Las reglas para alojar recursos deben no ser visibles fuera de la nube, siéndolo, solamente los agregados de comportamiento.

DiffServ utiliza el tráfico agregado como su unidad fundamental de tráfico, mas que como una corriente. Un campo de 6 bits en cada paquete identifica su agregado de tráfico (BA) en el centro de la red y por ende, el trato de envío que cada paquete en el agregado va a recibir, sin importar a que microflujo éste pertenezca.). Cada BA es identificado por una único código DS. Dentro del núcleo de la red, los paquetes son enviados de acuerdo al comportamiento por salto asociado al código DS.
En el borde de la red, más estado de paquetes debe ser guardado al marcar más campos de paquetes; por lo tanto, los agregados del interior podrían estar hechos de paquetes de varios clientes, y ser condicionados y politizados diferente en el borde, pero con la misma expectativa de trato de envío una vez pasado el borde.
Los routers dentro del dominio van a ser configurados para tratar a cada agregado de tráfico en forma diferente: en un dominio que reconoce a N agregados, los routers serán cada uno capaz de tener N comportamientos de envío diferente, uno apropiado para cada agregado.

2.6.2.4. Separación del control y envío

En el envío IP, la conectividad es lograda por la interacción de dos componentes: la parte del envío del paquete y la parte del ruteo. El envío usa la cabecera del paquete para encontrar una tabla de ruteo que determine la interfase de salida del paquete. El ruteo setea las entradas en esa tabla y puede necesitar reflejar un rango de tránsito y otras políticas así como también el mantener registro de las fallas de ruta.
Un servicio es una descripción de todo el trato que el tráfico de un cliente recibe a través de un dominio administrativo particular, a través de un conjunto de dominios interconectados o de punta a punta.

2.6.2.5. Definiendo las primitivas del camino de envío

a). Requerimientos básicos.

La clasificación saca corriente de paquetes. La política se encarga de asegurar que el comportamiento cumpla con las reglas que gobiernan la corriente de paquetes. El marcado propaga información sobre el agregado corriente abajo. PHB's de envío son generalmente implementados por colas de paquetes. Y el encolamiento aísla una corriente de tráfico de otra.

b). Marcado de DiffServ.

Cada paquete IP lleva un byte llamado octeto de Tipo de Servicio **(TOS octet).** Es una característica poco utilizada de IP. En la nueva versión 6 de IP de 128 bits, hay un byteequivalente llamado octeto de Clase de Servicio.

Fuente: http://www.it.uc3m.es/cgarcia/articulos/cita2002_diffserv.pdf

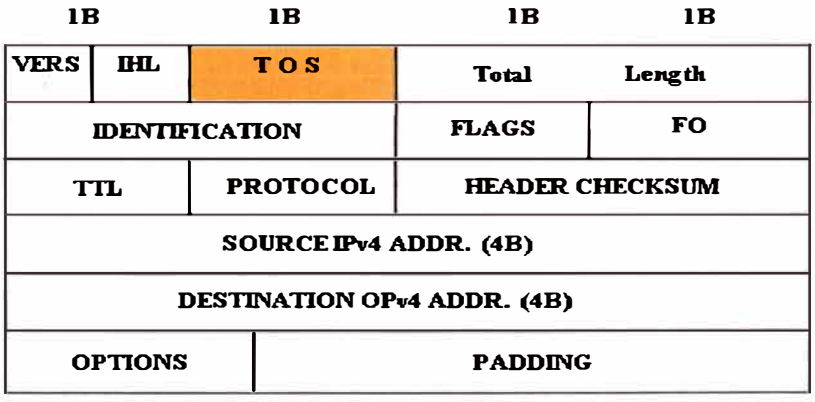

Figura 2.13. Paquete IP

Fuente: http://www.it.uc3m.es/cgarcia/articulos/cita2002_diffserv.pdf

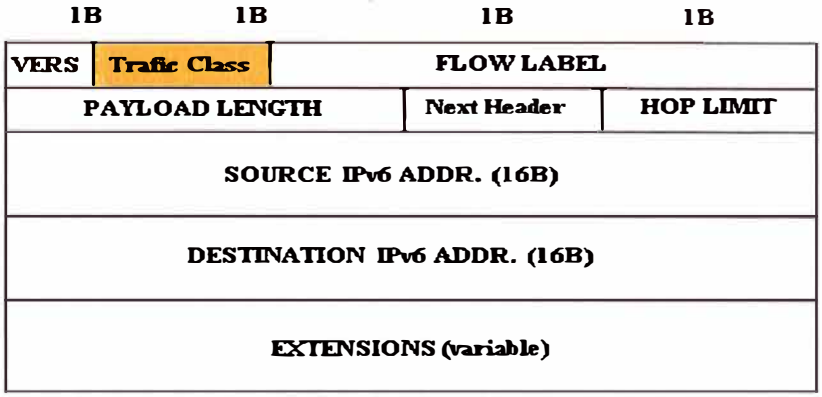

Fig. 2.14: (a) Campo DS - campo TOS de IPv4 ; (b) Campo DS – Campo de Clase de Tráfico de IPv6.

La primera tarea del grupo de DiffServ fue re-especificar este byte. Este campo de 6 bits es conocido como el campo de los Servicios Diferenciados y es marcado con un patrón específico de bits llamado código DS, usado para indicar cómo cada router debe tratar al paquete. Para enfatizar el hecho de que ninguna información de sesión se necesita guardar, este tratamiento es conocido como Per-Hop Behavior (PHB). El octeto luce así:

Fuente: http://www.it.uc3m.es/cgarcia/articulos/cita2002_diffserv.pdf

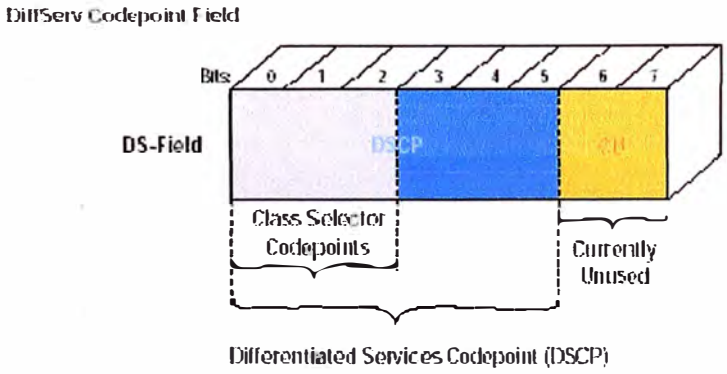

Fig. 2.15: Aspecto del octeto TOS.

El campo de 6 bits contiene hasta 64 diferentes valores binarios. Los códigos extra

restantes dejan espacio para innovación y optimizaciones operacionales locales. El marcado puede ocurrir en dos lugares:

• la fuente original de tráfico, como ser un servidor web, marca el tráfico. Esto tiene la ventaja de que el clasificador pude tener conocimiento explícito de la aplicación en uso y puede por consecuencia marcar paquetes de una manera dependiente de la aplicación.
• un router, como el primer router que el tráfico encuentra, clasifica y marca el tráfico. Esto tiene la ventaja de que no se necesita ningún cambio a servidores, pero requiere de alguna "inteligencia" extra en los routers.

c). Usando la marca.

Cuando un paquete entra en un router, la lógica de ruteo selecciona su puerto de salida y
el valor DSCP es usado para conducir el paquete a una cola específica o tratamiento específico en ése puerto. El PHB particular es configurado por un mecanismo administrador de red, seteando la tabla de comportamiento de QoS dentro del router. Los PHB's estándares son hasta ahora los siguientes:
• **Default behavior**. Acá el valor de DSCP es cero y el servicio esperado es exactamente el servicio por defecto de la Internet de hoy (por ej. la congestión y pérdida son completamente descontroladas).
• **Class selector behavior**. Acá, siete valores DSCP funcionan desde el 001000 al 111000 y son específicos para seleccionar hasta siete comportamientos, cada uno de los cuales tiene una mayor probabilidad de un envío a tiempo que su predecesor.

• **Expedited Forwarding behavior(EF).** El valor recomendado es 101110. La tasa de partida del tráfico EF debe igualar o superar una tasa configurable. EF intenta permitir la creación de servicios en tiempo real con una tasa de throughput configurable. El objetivo es que el flujo agregado vea siempre o casi

siempre, la cola vacía.

• **Assured Forwarding (AF) behavior.-** Consiste en tres sub-comportamientos, AF_1, AF_2, AF_3. Cuando la red está congestionada, los paquetes marcados con el DSCP para AF_1 tienen la menor probabilidad de ser descartados por cualquier router y los paquetes marcados para AF_2 la más alta. En general, hay N clases independientes con M niveles de descarte dentro de cada clase. Lo más común es N= 4 y M= 3. A cada clase se le deben asignar una mínima cantidad de recursos, pudiendo obtener más si es que hay exceso.

2.7.- WLAN (Wireless Local Area Network)

WLAN (en inglés; Wireless Local Area Network) es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Las WLAN van adquiriendo importancia en muchos campos, como almacenes o para manufactura, en los que se transmite la información en tiempo real a una terminal central. También son muy populares en los hogares para compartir el acceso a Internet entre varias computadoras. Hoy en día es importante definir el nivel de seguridad al acceso inalámbrico que nos permita brindar una red segura libre de accesos no deseados.

2.7.1. Características

- **Movilidad:** permite transmitir información en tiempo real en cualquier lugar de la organización o empresa a cualquier usuario. Esto supone mayor productividad y posibilidades de servicio.
- **Facilidad de instalación:** al no usar cables, se evitan obras para tirar cable por muros y techos, mejorando así el aspecto y la habitabilidad de los locales, y reduciendo el tiempo de instalación. También permite el acceso instantáneo a usuarios temporales de la red.

- **Flexibilidad:** puede llegar donde el cable no puede, superando mayor número de obstáculos, llegando a atravesar paredes. Así, es útil en zonas donde el cableado no es posible o es muy costoso: parques naturales, reservas o zonas escarpadas.

2.7.2. Principios de las redes WLAN

Fig. 2.16: Punto de Acceso WiFi

Se utilizan ondas de radio para llevar la información de un punto a otro sin necesidad de un medio físico guiado. Al hablar de ondas de radio nos referimos normalmente a portadoras de radio, sobre las que va la información, ya que realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final.

A este proceso se le llama modulación de la portadora por la información que está siendo transmitida. Si las ondas son transmitidas a distintas frecuencias de radio, varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas. Para extraer los datos el receptor se sitúa en una determinada frecuencia, frecuencia portadora, ignorando el resto. En una configuración típica de LAN sin cable los puntos de acceso (transceiver) conectan la red cableada de un lugar fijo mediante cableado normalizado. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. El punto de acceso (o la antena conectada al

punto de acceso) es normalmente colocado en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada. El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena. La naturaleza de la conexión sin cable es transparente a la capa del cliente.

2.7.3. Configuraciones de red para radiofrecuencia

Pueden ser de muy diversos tipos y tan simples o complejas como sea necesario. La más básica se da entre dos ordenadores equipados con tarjetas adaptadoras para WLAN, de modo que pueden poner en funcionamiento una red independiente siempre que estén dentro del área que cubre cada uno. Esto es llamado red de igual a igual (peer to peer). Cada cliente tendría únicamente acceso a los recursos del otro cliente pero no a un servidor central. Este tipo de redes no requiere administración o preconfiguración.

Instalando un Punto de Acceso se puede doblar la distancia a la cuál los dispositivos pueden comunicarse, ya que estos actúan como repetidores. Desde que el punto de acceso se conecta a la red cableada cualquier cliente tiene acceso a los recursos del servidor y además gestionan el tráfico de la red entre los terminales más próximos. Cada punto de acceso puede servir a varias máquinas, según el tipo y el número de transmisiones que tienen lugar. Existen muchas aplicaciones en el mundo real con un rango de 15 a 50 dispositivos cliente con un solo punto de acceso.

Los puntos de acceso tienen un alcance finito, del orden de 150 m en lugares u zonas abiertas. En zonas grandes como por ejemplo un campus universitario o un edificio es probablemente necesario más de un punto de acceso. La meta es cubrir el área con células que solapen sus áreas de modo que los clientes puedan moverse sin cortes entre un grupo de puntos de acceso. Esto es llamado roaming, el diseñador de la red puede elegir usar un Punto de Extensión (EPs) para aumentar el número de puntos de acceso a la red, de modo que funcionan como tales pero no están enganchados a la red cableada como los puntos de acceso. Los puntos de extensión funcionan como su nombre indica: extienden el alcance de la red retransmitiendo las señales de un cliente a un punto de acceso o a otro punto de extensión. Los puntos de extensión

pueden encadenarse para pasar mensajes entre un punto de acceso y clientes lejanos de modo que se construye un puente entre ambos.

Uno de los últimos componentes a considerar en el equipo de una WLAN es la antena direccional. Por ejemplo: si se quiere una Lan sin cable a otro edificio a 1 km de distancia. Una solución puede ser instalar una antena en cada edificio con línea de visión directa. La antena del primer edificio está conectada a la red cableada mediante un punto de acceso. Igualmente en el segundo edificio se conecta un punto de acceso, lo cual permite una conexión sin cable en esta aplicación.

2.7.4. Asignación de Canales

Los estándares 802.11b y 802.11g utilizan la banda de 2.4 – 2.5 Ghz. En esta banda, se definieron 11 canales utilizables por equipos WIFI, los que pueden configurarse de acuerdo a necesidades particulares. Sin embargo, los 11 canales no son completamente independientes (canales contiguos se superponen y se producen interferencias) y en la práctica sólo se pueden utilizar 3 canales en forma simultánea (1, 6 y 11). Esto es correcto para USA y muchos países de América Latina, pues en Europa, el ETSI ha definido 13 canales. En este caso, por ejemplo en España, se pueden utilizar 4 canales no-adyacentes (1, 5, 9 y 13). Esta asignación de canales usualmente se hace sólo en el Access Point, pues los "clientes" automáticamente detectan el canal, salvo en los casos en que se forma una red "Ad-Hoc" o punto a punto cuando no existe Access Point.

2.7.5. Seguridad

Uno de los problemas de este tipo de redes es precisamente la seguridad ya que cualquier persona con una terminal inalámbrica podría comunicarse con un punto de acceso privado si no se disponen de las medidas de seguridad adecuadas. Dichas medidas van encaminadas en dos sentidos: por una parte está el cifrado de los datos que se transmiten y en otro plano, pero igualmente importante, se considera la autenticación entre los diversos usuarios de la red. En el caso del cifrado se están realizando diversas investigaciones ya que los sistemas considerados inicialmente se han conseguido descifrar. Para la autenticación se ha tomado como base el protocolo

de verificación EAP (Extensible Authentication Protocol), que es bastante flexible y permite el uso de diferentes algoritmos.

2.7.5.1. Autenticación y Asociación WLAN

La autenticación de las WLAN se produce en la Capa 2 del modelo OSI. Es el proceso de autenticar el dispositivo no al usuario. Este es un punto fundamental a tener en cuenta con respecto a la seguridad, detección de fallos y administración general de una WLAN.

El proceso se inicia cuando el cliente envía una trama de petición de autenticación al AP y éste acepta o rechaza la trama. El cliente recibe una respuesta por medio de una trama de respuesta de autenticación. También puede configurarse el AP para derivar la tarea de autenticación a un servidor de autenticación, que realizaría un proceso de credencial más exhaustivo.

La asociación que se realiza después de la autenticación es el estado que permite que un cliente use los servicios del AP para transferir datos.

Tipos de autenticación y asociación:

• No autenticado y no asociado:

El nodo está desconectado de la red y no está asociado a un punto de acceso.

• Autenticado y no asociado:

El nodo ha sido autenticado en la red pero todavía no ha sido asociado al punto de acceso.

• Autenticado y asociado:

El nodo está conectado a la red y puede transmitir y recibir datos a través del punto de acceso.

2.7.5.2. Métodos de Autenticación:

2.7.5.2.1. WEP

WEP (Wired Equivalency Privacy) es un sistema de cifrado incluido en el estándar 802.11 como protocolo para redes Wireless que permite encriptar la información que se transmite. Proporciona encriptación a nivel 2. Está basado en el algoritmo de encriptación RC4, y utiliza claves de 64 bits, de 128 bits o de 256 bits. Es poco seguro debido a su arquitectura, por lo que al aumentar los tamaños de las claves de encriptación sólo aumenta el tiempo necesario para romperlo.

2.7.5.2.2. WPA

WPA (Wi-Fi Protected Access - Acceso Protegido Wi-Fi) es un sistema para asegurar redes inalámbricas, creado para corregir las falencias de seguridad de WEP; los investigadores han encontrado varias debilidades en WEP (tal como un ataque estadístico que permite recuperar la clave WEP). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era preparado.
WPA fue diseñado para utilizar un servidor de autenticación (normalmente un servidor RADIUS), que distribuye claves diferentes a cada usuario; sin embargo, también se puede utilizar en un modo menos seguro de clave pre-compartida (PSK - Pre-Shared Key). La información es cifrada utilizando el algoritmo RC4, con una clave de 128 bits y un vector de inicialización de 48 bits.

Una de las mejoras sobre WEP es dada por el Protocolo de Integridad de Clave Temporal (TKIP - Temporal Key Integrity Protocol), que cambia claves de una forma

dinámica a medida que el sistema es utilizado. Cuando esto se combina con un vector de inicialización (IV) mucho más grande, evita los ataques de recuperación de clave (ataques estadísticos) a los que es susceptible WEP.

Adicionalmente a la autenticación y cifrado, WPA también mejora la integridad de la información cifrada. El comparador de redundancia cíclica (CRC) utilizado en WEP es inseguro, ya que es posible alterar la información y actualizar el CRC del mensaje sin conocer la clave WEP. WPA implementa un chequeo de integridad del mensaje llamado "Michael". Además WPA incluye protección contra ataques de "repetición", ya que incluye un contador de tramas.

Al incrementar el tamaño de las claves, el número de llaves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que la entrada no autorizada a redes inalámbricas sea mucho más difícil. El algoritmo Michael fue el más fuerte que los diseñadores de WPA pudieron crear, bajo la premisa de que debía funcionar en las tarjetas de red inalámbricas más viejas; sin embargo es suceptible a ataques. Para limitar este riesgo, las redes WPA se desconectan durante 30 segundos cada vez que se detecta un intento de ataque.

2.7.5.2.3. WPA-2

WPA-2 está basada en el nuevo estándar IEEE 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no soporta todas las características, mientras que WPA-2 ya implementa el estándar completo. Particularmente WPA no se puede utilizar en redes ad-hoc.

2.8.- VPN (Virtual Private Network)

La Red Privada Virtual (RPV), en inglés Virtual Private Network (VPN), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada , como por ejemplo Internet.

Ejemplos comunes son, la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación:

- Autenticación y autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.
- Integridad: La garantía de que los datos enviados no han sido alterados. Para ello se utiliza funciones de Hash. Los algoritmos de hash más comunes son los Message Digest (MD2 y MD5) y el Secure Hash Algorithm (SHA).
- Confidencialidad: Dado que los datos viajan a través de un medio potencialmente hostil como Internet, los mismos son susceptibles de intercepción, por lo que es fundamental el cifrado de los mismos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES).
- No repudio: es decir, un mensaje tiene que ir firmado, y el que lo firma no puede negar que el mensaje lo envió.

2.8.1. Requerimientos básicos

- Identificación de usuario: Las VPN deben verificar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentren autorizados.
- Codificación de datos: Los datos que se van a transmitir a través de la red pública (Internet), antes deben ser cifrados, para que así no puedan ser leídos. Esta tarea se realiza con algoritmos de cifrado como DES o 3DES que solo pueden ser leidos por el emisor y receptor.
- Administración de claves: Las VPN deben actualizar las claves de cifrado para los usuarios.

2.8.2. Tipos de VPN

Básicamente existen tres arquitecturas de conexión VPN:

2.8.2.1. VPN de acceso remoto

Es quizás el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura «dial-up» (módems y líneas telefónicas).

2.8.2.2. VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales. Es más común el punto anterior, también llamada tecnología de túnel o tunneling.

2.8.3. Tunneling

Internet se construyó desde un principio como un medio inseguro. Muchos de los protocolos utilizados hoy en día para transferir datos de una máquina a otra a través de la red carecen de algún tipo de cifrado o medio de seguridad que evite que nuestras comunicaciones puedan ser interceptadas y espiadas. HTTP, FTP, POP3 y otros muchos protocolos ampliamente usados, utilizan comunicaciones que viajan en claro a través de la red. Esto supone un grave problema, en todas aquellas situaciones en las que queremos transferir entre máquinas información sensible, como pueda ser una cuenta de usuario (nombre de usuario y contraseña), y no tengamos un control absoluto sobre la red, a fin de evitar que alguien pueda interceptar nuestra comunicación por medio de la técnica del hombre en el medio (man in the middle), como es el caso de la Red de redes.

El problema de los protocolos que envían sus datos en claro, es decir, sin cifrarlos, es que cualquier persona que tenga acceso físico a la red en la que se sitúan las

máquinas puede ver dichos datos. De este modo, alguien que conecte su máquina a una red y utilice un sniffer recibirá y podrá analizar por tanto todos los paquetes que circulen por dicha red. Si alguno de esos paquetes pertenece a un protocolo que envía sus comunicaciones en claro, y contiene información sensible, dicha información se verá comprometida. Si por el contrario, se cifran las comunicaciones con un sistema que permita entenderse sólo a las dos máquinas que son partícipes de la comunicación, cualquiera que intercepte desde una tercera máquina los paquetes, no podrá hacer nada con ellos, al no poder descifrar los datos.

Una forma de evitar este problema, sin dejar por ello de utilizar todos aquellos protocolos que carezcan de medios de cifrado, es usar una técnica llamada tunneling. Básicamente, esta técnica consiste en abrir conexiones entre dos máquinas por medio de un protocolo seguro, como puede ser SSH (Secure SHell), a través de las cuales realizaremos las transferencias inseguras, que pasarán de este modo a ser seguras. De esta analogía viene el nombre de la técnica, siendo la conexión segura (en este caso de ssh) el túnel por el cual se envían los datos para que nadie más aparte de los interlocutores que se sitúan a cada extremo del túnel, pueda ver dichos datos. Este tipo de técnica requiere de forma imprescindible tener una cuenta de acceso seguro en la máquina con la que se quiere comunicar.

2.8.4. IP Sec (Internet Protocol Security)

IPsec consta de dos protocolos que han sido desarrollados para proporcionar seguridad a nivel de paquete, tanto para IPv4 como para IPv6:

- Authentication Header (AH) proporciona integridad, autenticación y no repudio si se eligen los algoritmos criptográficos apropiados.
- Encapsulating Security Payload (ESP) proporciona confidencialidad y la opción -altamente recomendable- de autenticación y protección de integridad.

Los algoritmos criptográficos definidos para usar con IPsec incluyen HMAC- SHA1

para protección de integridad, y Triple DES-CBC y AES-CBC para confidencialidad. Más detalles en la RFC 4305.

2.8.4.1. Authentication Header (AH)

AH está dirigido a garantizar integridad sin conexión y autenticación de los datos de origen de los datagramas IP. Para ello, calcula un Hash Message Authentication Code (HMAC) a través de algún algoritmo hash operando sobre una clave secreta, el contenido del paquete IP y las partes inmutables del datagrama. Este proceso restringe la posibilidad de emplear NAT, que puede ser implementada con NAT transversal. AH protege la carga útil IP y todos los campos de la cabecera de un datagrama IP excepto los campos mutantes, es decir, aquellos que pueden ser alterados en el tránsito. En IPv4, los campos de la cabecera IP mutantes (y por lo tanto no autenticados) incluyen TOS, Flags, Offset de fragmentos, TTL y suma de verificación de la cabecera. AH opera directamente por encima de IP, utilizando el protocolo IP número 51. Una cabecera AH mide 32 bits como se muestra:

0 - 7 bit	**8 - 15 bit**	**16 - 23 bit**	**24 - 31 bit**
Next header	Payload length	RESERVED	
Security parameters index (SPI)			
Sequence number			
Hash Message Authentication Code (variable)			

Fig 2.17: Cabecera AH

2.8.4.1.1. Significado de los campos:

Next header

Identifica el protocolo de los datos transferidos.

Payload length

Tamaño del paquete AH.

RESERVED

Reservado para uso futuro (hasta entonces todo ceros).

Security parameters index (SPI)

Indica los parámetros de seguridad que, en combinación con la dirección IP, identifican la asociación de seguridad implementada con este paquete.

Sequence number

Un número siempre creciente, utilizado para evitar ataques de repetición.

HMAC

Contiene el valor de verificación de integridad (ICV) necesario para autenticar el paquete; puede contener relleno.

2.8.5. Encapsulating Security Payload (ESP)

El protocolo ESP proporciona autenticidad de origen, integridad y protección de confidencialidad de un paquete. ESP también soporta configuraciones de sólo cifrado y sólo autenticación, pero utilizar cifrado sin autenticación está altamente desaconsejado porque es inseguro[12] Al contrario que con AH, la cabecera del paquete IP no está protegida por ESP (aunque en ESP en modo túnel, la protección es proporcionada a todo el paquete IP interno, incluyendo la cabecera interna; la cabecera externa permanece sin proteger). ESP opera directamente sobre IP, utilizando el protocolo IP número 50.

<table>
<tr><td>0 - 7 bit</td><td>8 - 15 bit</td><td>16 - 23 bit</td><td>24 - 31 bit</td></tr>
<tr><td colspan="4">Security parameters index (SPI)</td></tr>
<tr><td colspan="4">Sequence number</td></tr>
<tr><td colspan="4">Payload data (variable)</td></tr>
<tr><td></td><td colspan="2">Padding (0-255 bytes)</td><td></td></tr>
<tr><td></td><td></td><td>Pad Length</td><td>Next Header</td></tr>
<tr><td colspan="4">Authentication Data (variable)</td></tr>
</table>

Fig 2.18: Paquete ESP

2.8.5.1. Significado de los campos

Security parameters index (SPI)

Identifica los parámetros de seguridad en combinación con la dirección IP.

Sequence number

Un número siempre creciente, utilizado para evitar ataques de repetición.

Payload data

Los datos a transferir.

Padding

Usado por algunos algoritmos criptográficos para rellenar por completo los bloques.

Pad length

Tamaño del relleno en bytes.

Next header

Identifica el protocolo de los datos transferidos.

Authentication data

Contiene los datos utilizados para autenticar el paquete.

CAPITULO III

DISEÑO DE UNA RED MULTISERVICIOS DE ALTA DISPONIBILIDAD EN UN ENTORNO CORPORATIVO

Se trabajará en un ambiente donde se ha creado una red multiservicios donde atiende varios servicios como interconexión de datos, telefonía IP, videoconferencia, servicio wireless y servicios VPN con acceso remoto.

La siguiente es la topología a emplear en el presente diseño donde se aprecia la existencia de diversas aplicaciones como la VoIP, transferencia de datos , VLANs, Agregación de Puertos; Wireless, conexiones VPN donde se dictarán las normativas que nos permitan una fácil administración y monitoreo de todas estas aplicaciones a implementar. También se mostrarán algunas configuraciones típicas de algunos equipos de comunicaciones que permitan el establecimiento adecuado de una eficiente administración de una red de datos, como pueden ser los switches de borde, el Core, configuración de teléfonos IP en una Call Manager, configuración de seguridad en un servidor RADIUS para acceso inalámbrico, configuración de un firewall ASA para accceso VPN remoto desde el Internet. Todas estas muestras son tomadas de ambientes que se encuentran en producción y son prácticas habituales en las redes de hoy en día. Sólo es necesario que los administradores tomen conocimiento de tales prácticas para logra un optimo desempeño de la red que están administrando. En mayor parte se ha proyectado el uso de equipos marca Cisco que actualmente predomina en las redes de las compañías locales y es en base a dicha marca que nos enfocamos en el desarrollo del presente informe y serán mostradas en las siguientes páginas para un mejor conocimiento e ilustración en los conceptos que ya hemos descrito en el capitulo anterior. En el siguiente gráfico se muestra la implementación de una red de comunicaciones, donde están integrados diversos servicios como la transmisión de datos a nivel local y externo, telefonía IP, conexión inalámbrica; todos ellos protegidos por un equipo de seguridad (firewall) ante las solicitudes de conexiones externas como el Internet.

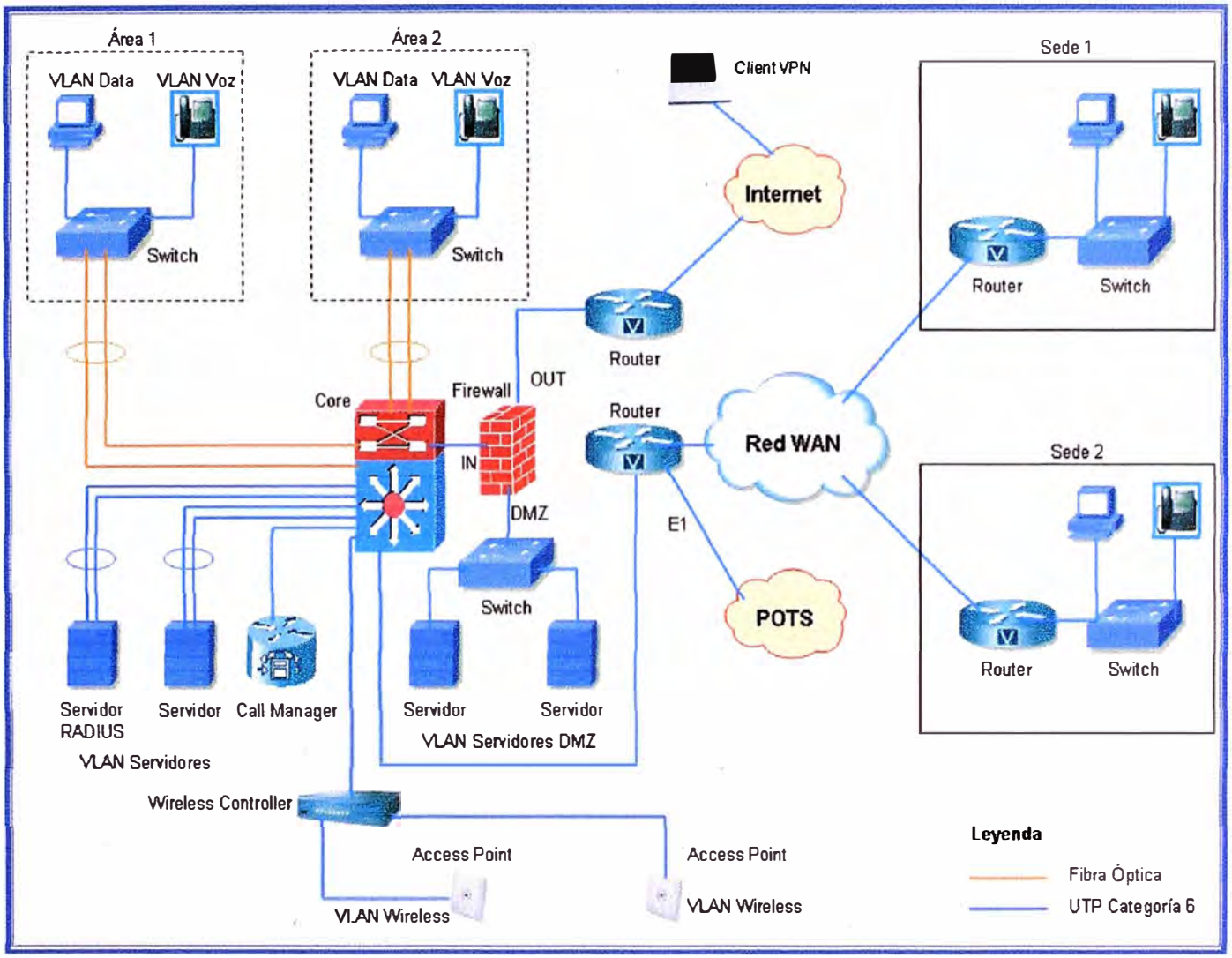

Figura 3.1. Red de Multiservicios

3.1.- Red de Datos

Donde se ha segmentado la red en varias VLANs para reducir el trafico broadcast en la red. La interconexión inter-VLAN lo dirige el Core el cual enruta la comunicación entre los diversos segmentos. Se ha configurado una VLAN por área geográfica para limitar los broadcasts. Los Servidores se encuentran en una VLAN especial para restringir el tráfico hacia dichos equipos de comunicaciones. También se ha

configurado una VLAN para el servicio telefónico IP.

También se observa la existencia del firewall que se encuentra ubicado detrás del router de Internet, teniendo 03 zonas:

Zona OUT (Exterior)
Zona IN (Interior)
Zona DMZ (Servidores)

En la zona IN se encuentran los servidores de archivos, FTP y otros de aplicación interna. En la zona DMZ; se hallan los servidores que necesitan la salida a Internet para que puedan ser accesados desde el exterior. Por ello, tienen que residir en una zona desmilitarizada.

Las VLANs tienen restricción en la interconexión entre ellas por medio de reglas de control que restringirá la comunicación entre segmentos y solo dejara "pasar" el tráfico hacia la VLAN de Servidores.

Además, existe redundancia en la comunicación entre el Core y los Servidores cuyos puertos están configurados con la opción "etherchannel". Esto permitirá incrementar notablemente el ancho de banda en la comunicación hacia los servidores. Los servidores tienen necesariamente conexiones de 1Gbps debido al alto trafico que originan.

Igualmente la conexión entre los switches de borde y el Core presenta redundancia para tener una alta disponibilidad en la comunicación de datos en caso de caídas en algunos enlaces específicos. Por otro lado, estas conexiones también tienen que ser por fibra óptica para obtener un ancho de banda óptimo para el manejo de tráfico.

El STP (Spanning Tree Protocol) está configurado en todos los switches para proteger a la red en caso de "loops" . Cada VLAN existente se encuentra configurado el STP correspondiente.

3.1.1. Muestra de configuración de un Switch Core

spanning-tree mode pvst

```
no spanning-tree optimize bpdu transmission
no spanning-tree vlan 20
spanning-tree vlan 1,10,20,30-31,40,50,60,70,80,90,160,170,180,190 priority 0
spanning-tree vlan 200,210,220,270,280 priority 0
spanning-tree vlan 150,230,240,250,260,801 priority 1
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands

redundancy
 mode sso
 main-cpu
auto-sync running-config
  auto-sync bootvar
  auto-sync standard

vlan internal allocation policy ascending
vlan access-log ratelimit 2000

interface Port-channel1
no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30,40,50,90,150,801
switchport mode trunk
```

```
interface Port-channel2
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface GigabitEthernet2/16
 no ip address
 switchport
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active

interface GigabitEthernet2/17
 no ip address
 switchport
 switchport mode trunk
 channel-protocol lacp
!
 channel-group 1 mode active
 interface GigabitEthernet2/39
 no ip address
 switchport
 switchport access vlan 50
```

```
interface GigabitEthernet2/40
 no ip address
 switchport
 switchport access vlan 50

interface Vlan40
 ip address 172.30.2.2 255.255.255.0

 standby 2 ip 172.30.2.1
 standby 2 priority 120
 standby 2 preempt

interface Vlan50
 ip address 10.3.0.102 255.255.255.0
 standby 3 ip 10.3.0.1
 standby 3 priority 120
 standby 3 preempt
ip classless
ip route 0.0.0.0 0.0.0.0 172.30.1.201
ip route 192.168.0.0 255.255.192.0 192.168.3.1
ip route 192.168.90.0 255.255.255.0 172.30.28.6
ip http server
ip http path bootflash:
```

3.1.2. Muestra de configuración de un Switch de Borde

```
switch 1 provision ws-c3750g-24ts-1u
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id

interface GigabitEthernet1/0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

En este escenario también se muestra la interconexión de la sede principal con una sede remota en nuestra red planteada. Por lo que el Router que se encuentra instalado en una red de datos multiservicios deberá tener en su configuración la presencia de las "sub-interfaces" para cada VLAN existente; por lo que una muestra de la configuración podría ser como se muestra a continuación:

```
Router_A(config)#interface fastethernet 0/0
Router_A(config-if)#no shutdown
Router_A(config-if)#interface fastethernet 0/0.1
Router_A(config-subif)#encapsulation dot1q 1
Router_A(config-subif)#ip address 192.168.1.1 255.255.255.0
Router_A(config-if)#interface fastethernet 0/1.2
Router_A(config-subif)#encapsulation dot1q 10
Router_A(config-subif)#ip address 192.168.5.1 255.255.255.0
Router_A(config-if)#interface fastethernet 0/0.3
Router_A(config-subif)#encapsulation dot1q 20
Router_A(config-subif)#ip address 192.168.7.1 255.255.255.0
```

```
Router_A(config-subif)#end
```

3.2.- Telefonía IP

De igual manera en nuestra red existe el servicio de Telefonía IP mediante un equipo central (Call Manager) el cual administra el servicio de telefonía. La siguiente es una muestra de la configuración del Call Manager Cisco para el servicio telefónico IP, donde se han creado varias regiones, device pools:

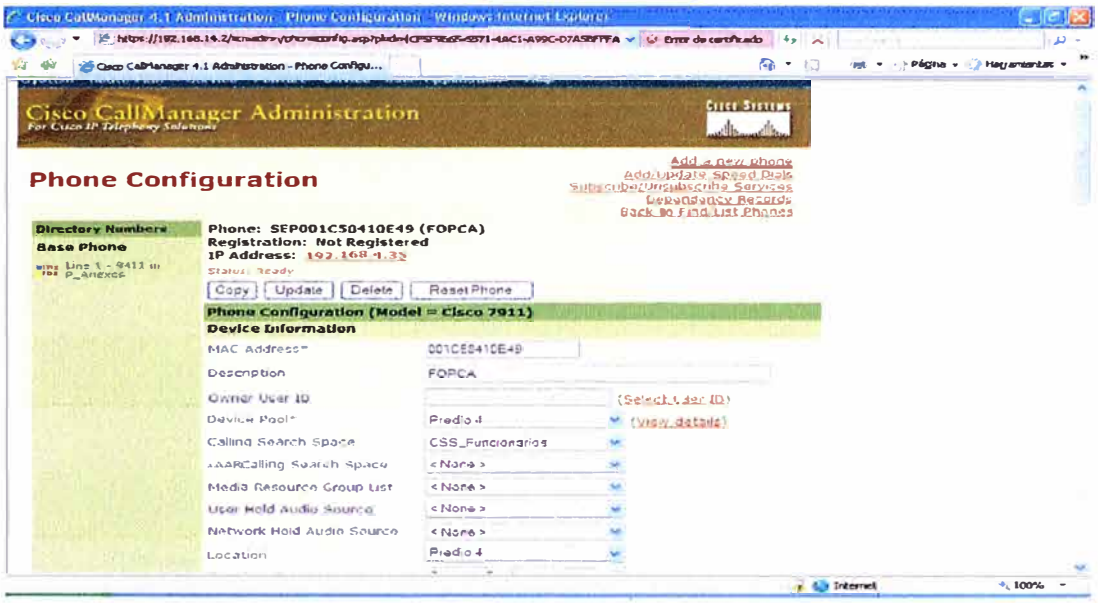

Figura 3.2. Configuración de un Teléfono IP (Parte 1)

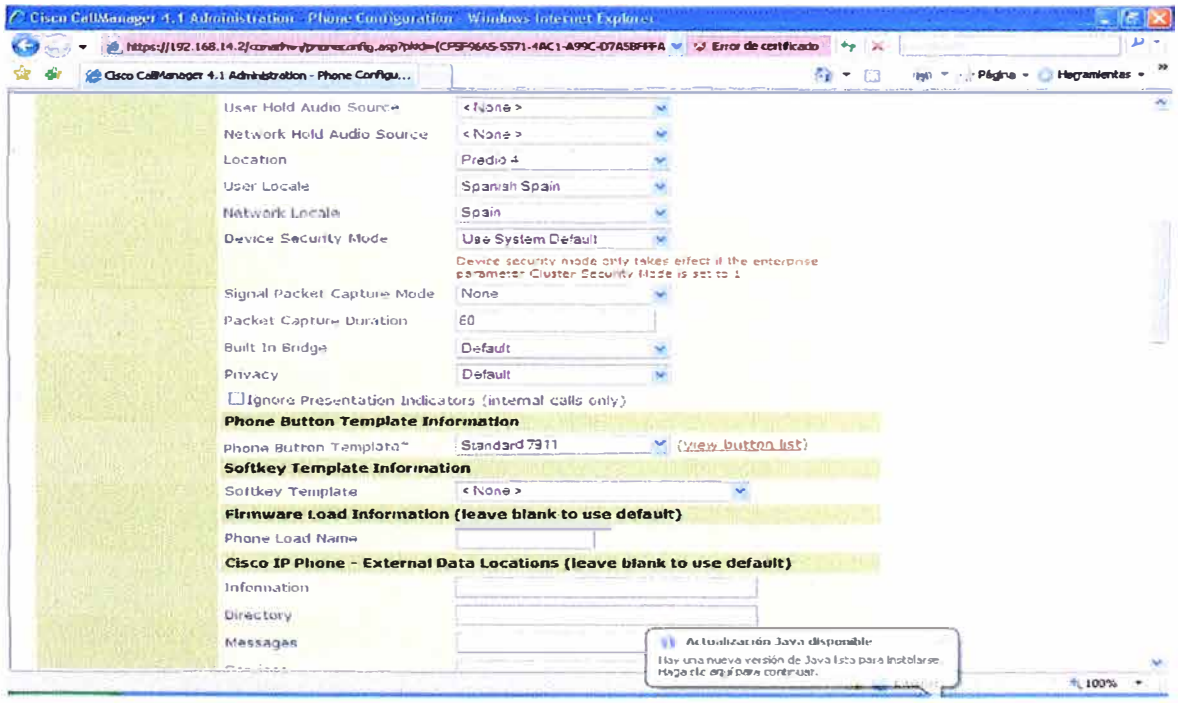

Figura 3.3. Configuración de un Teléfono IP (Parte 2)

Los teléfonos IP radican en la VLAN de Voz de manera que el tráfico de voz sea solo contenido a dicho dominio de broadcast en la red de datos.

Para los teléfonos IP que residen en cada sede, es recomendable separarlos en un "Device Pool" para una mejor administración. Además, los "Calling Search Space" serán diferenciados para que determinen que particiones específicas permitirán terminar una llamada a los teléfonos IPs.

Para ello, las redes de las sedes remotas tendrán que estar inscritas en el router principal para la conectividad necesaria. De igual manera el Call Manager, conocerá dichas subredes respectivas para la asignación correspondiente de las direcciones IPs para los teléfonos ubicados en las sedes remotas.

3.3.- Servicio Wireless

Para el servicio wireless, se empleará como equipos centralizador de los access points a un "Wireless Controller" el cual permitirá la administración centralizada del servicio wireless en los access points. En este servicio inalámbrico, existirán 02 VLANs:

VLAN Wireless
VLAN Internet

En la VLAN Wireless, los usuarios que tengan acceso a este servicio; tendrán los privilegios para poder usar la red interna con las aplicaciones de todos los servidores existentes en la red. Para ello, tendrán que autenticarse mediante un Servidor RADIUS que esta alojado como un "servicio" dentro del Domain Controller de la red interna. En la VLAN Internet, los usuarios que tengan acceso a dicho servicio; solo podrán conectarse al Internet y no podrán ingresar en ningún modo a la red interna de la compañía. La siguiente es la configuración del servidor RADIUS (Remote Authentication Dial-In User Server), en ambiente Windows seria relacionado al IAS (Internet Authentication Service); donde se muestra una configuración parcial de un

servidor RADIUS en producción resaltando las políticas de acceso ye l método de autenticación.

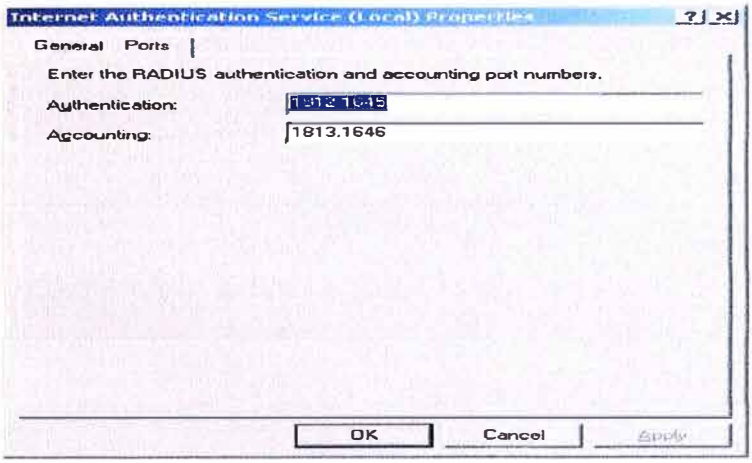

Figura 3.4. Configuración del RADIUS (19

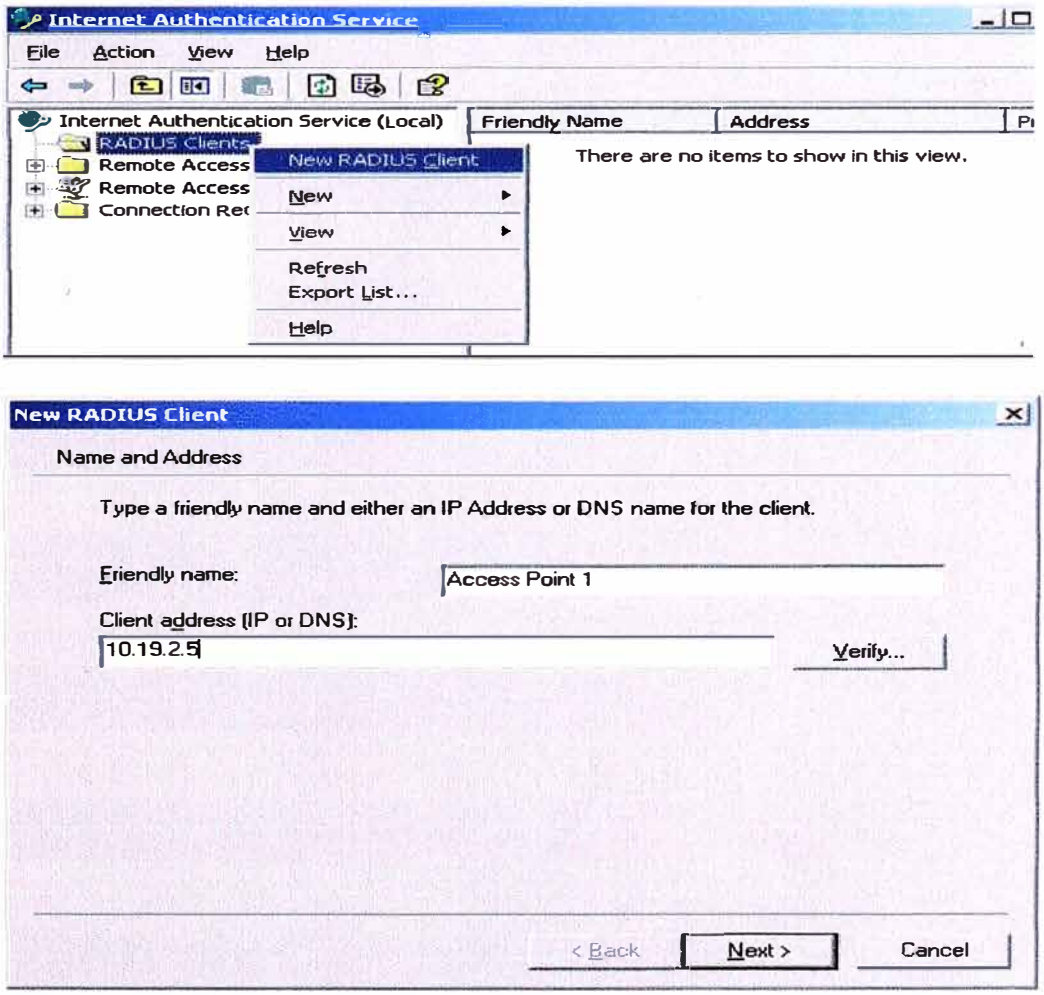

Figura 3.5. Configuración del RADIUS (2)

Donde se aprecia la configuración del cliente en el servidor RADIUS, asignando la correspondiente dirección IP un nombre amigable para poder reconocerlo en el servidor.

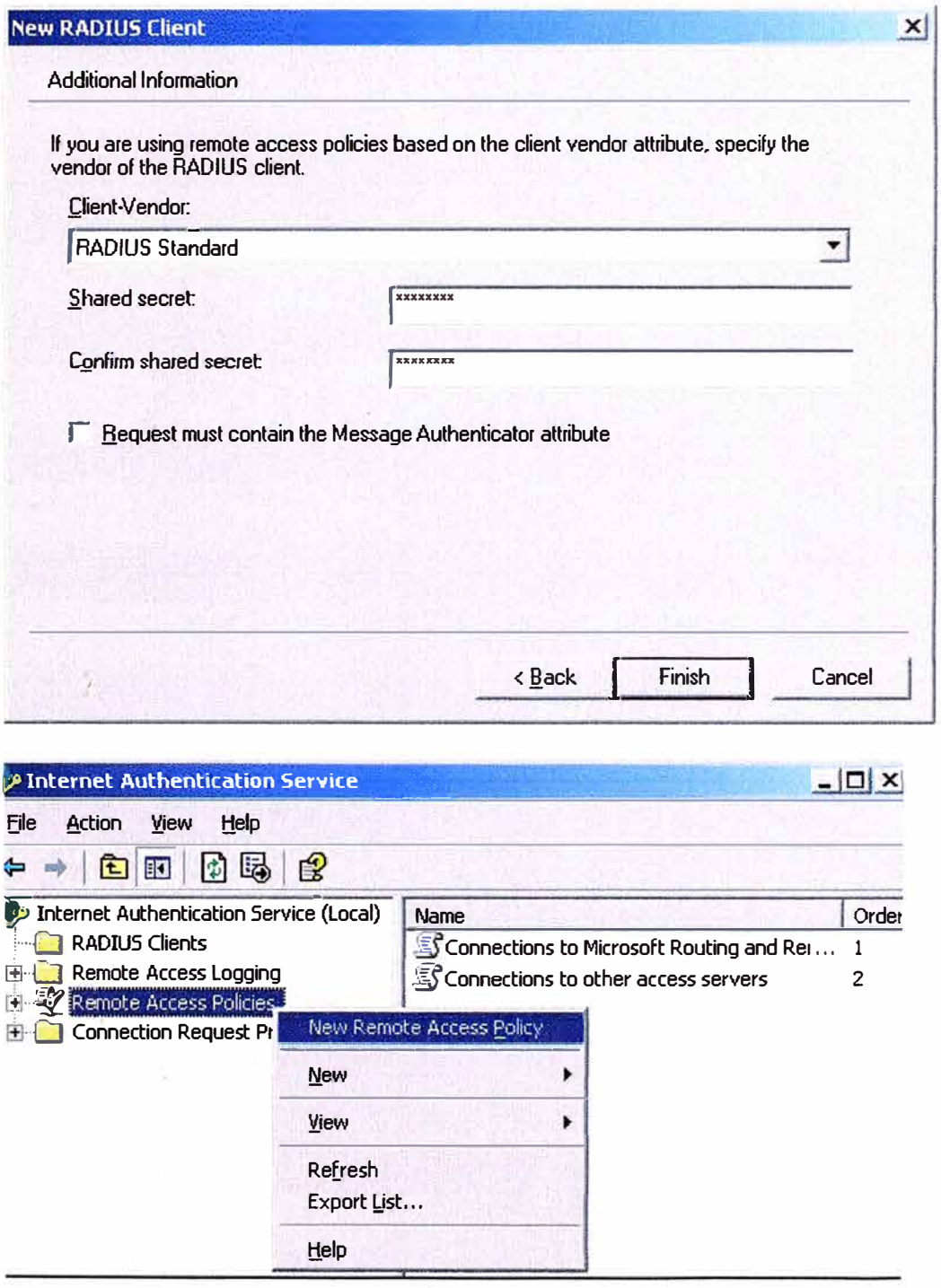

Figura 3.6. Configuración del RADIUS (3)

Donde se aprecia la generación de la clave compartida tanto para el servidor como para el cliente creado. Además de generar una política de acceso remoto que se asociar con el Domain Controller de la organización.

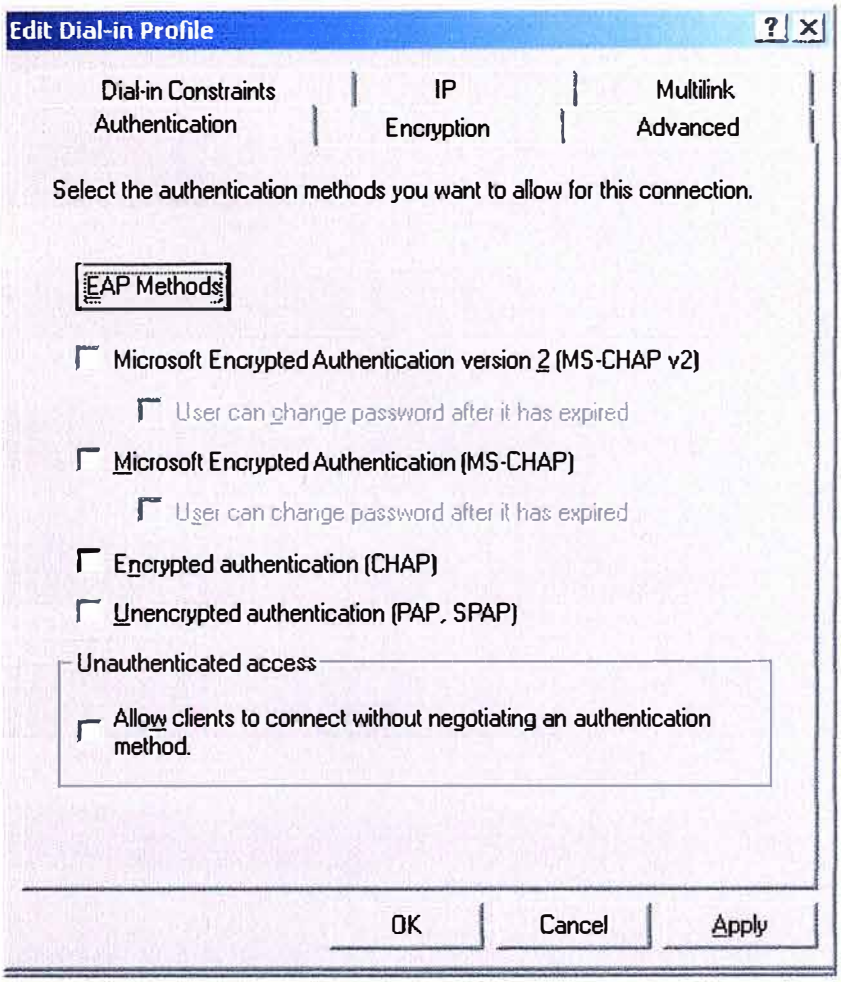

Figura 3.7. Configuración del RADIUS (4)

Los hosts (equipos inalámbricos) que deseen hacer uso del servicio inalámbrico en la VLAN Wireless, tendrán que configurar adecuadamente los perfiles de radio asociados al servicio para que puedan autenticarse correctamente al controlador inalámbrico y puedan hacer uso de las aplicaciones internas de red.

3.4.- Conexiones VPN

A continuación se muestra un ejemplo de configuración del ASA (Adaptive Security Appliance) Cisco para el servicio de VPN de Acceso Remoto, haciendo uso del ASDM (Adaptive Security Device Manager):

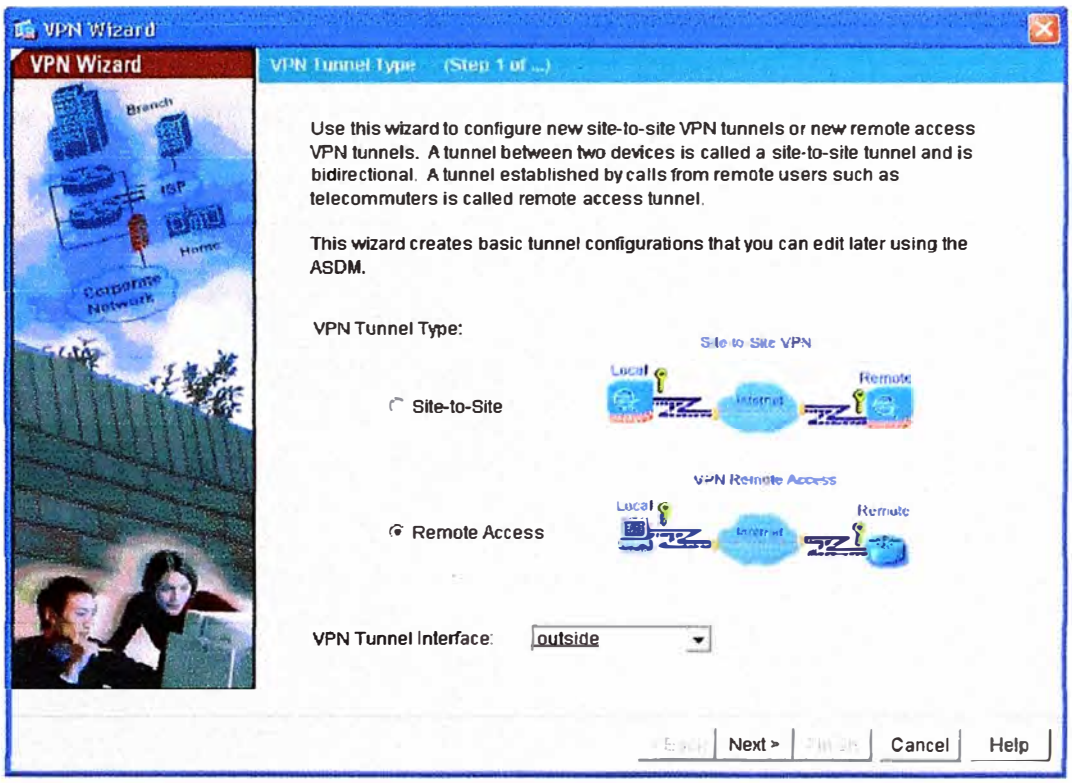

Figura 3.5. Configuración del ASDM (1)

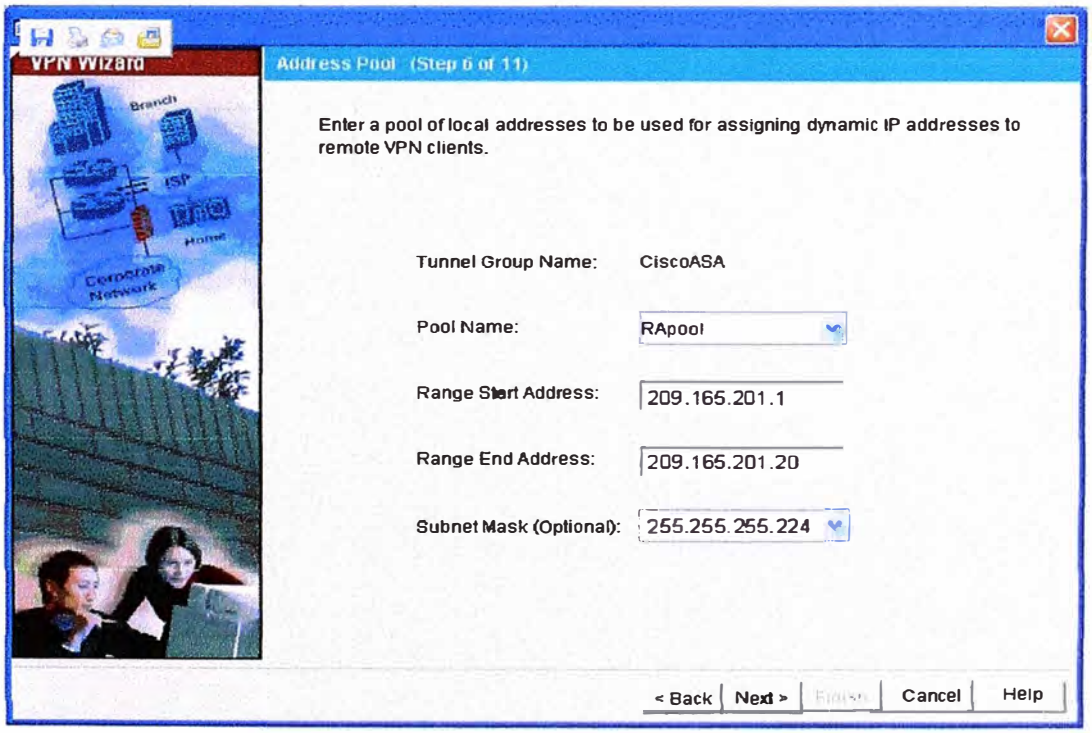

Figura 3.6. Configuración del ASDM (2)

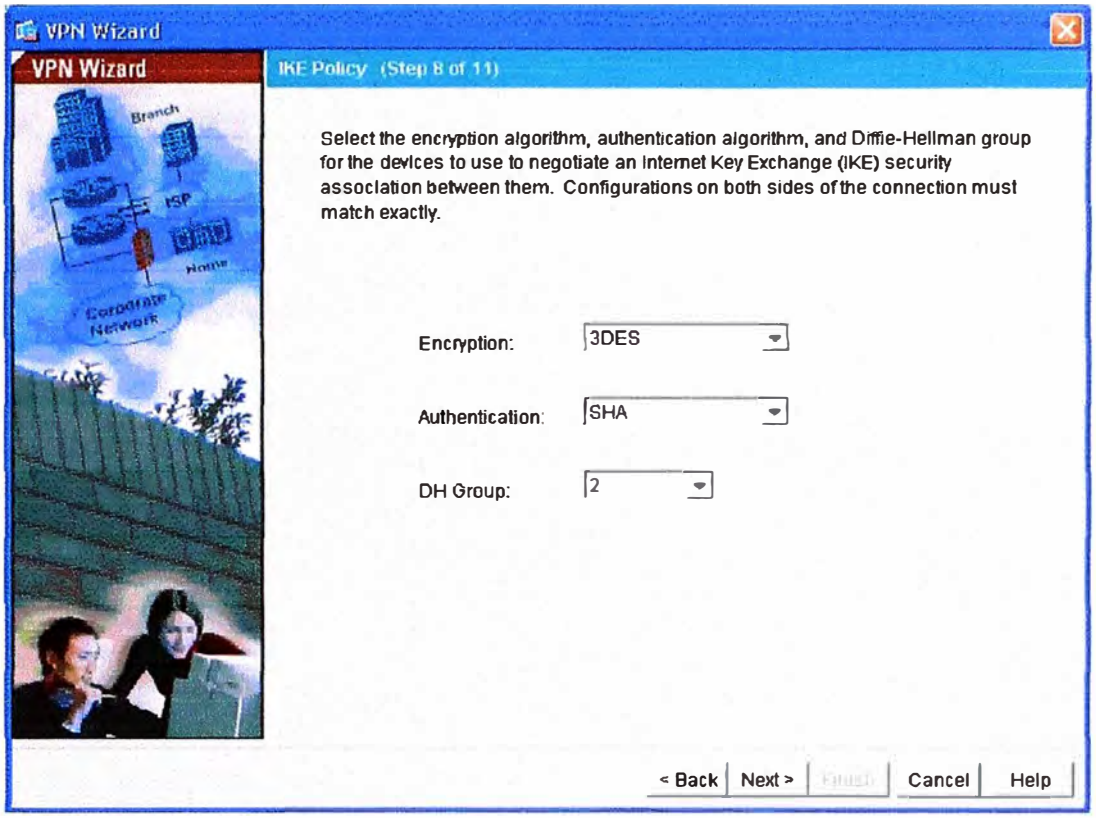

Figura 3.7. Configuración del ASDM (3)

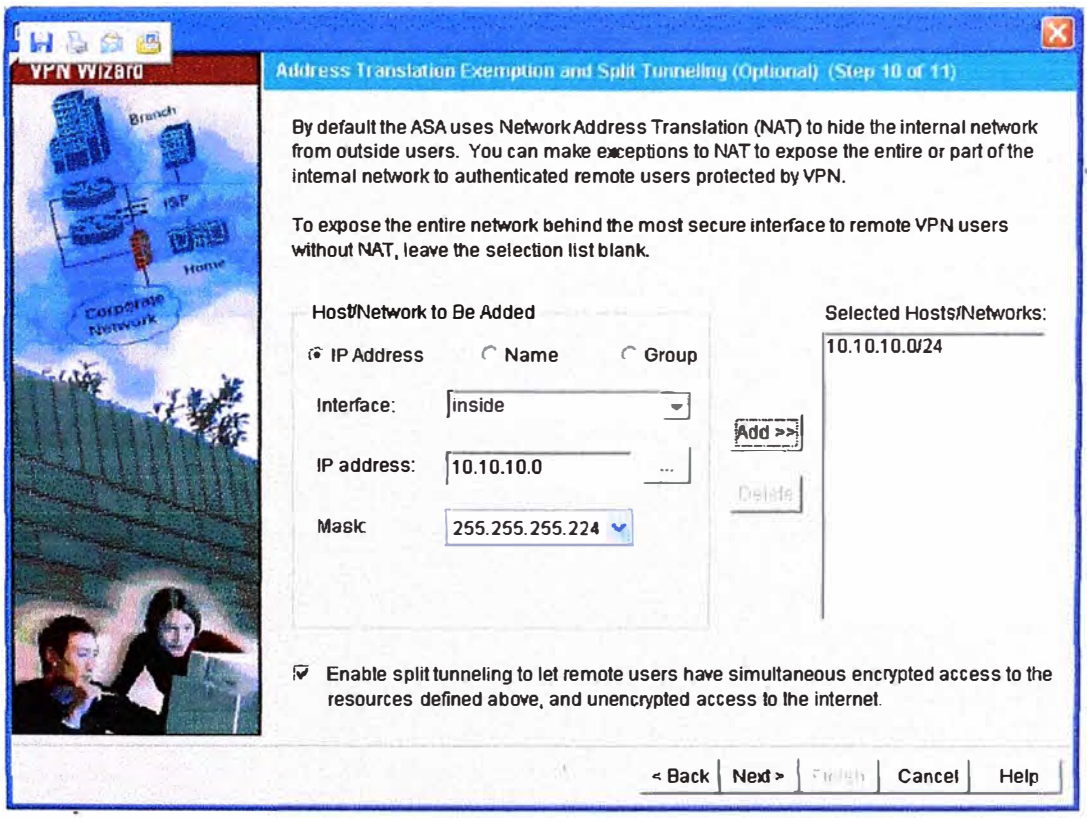

Figura 3.8. Configuración del ASDM (4)

CONCLUSIONES

Se observa que para tener una red de datos con múltiples servicios es necesario emplear todos los parámetros que posibilitan un óptimo desempeño en el performance de la red como el STP (Spanning Tree Protocol), LACP (Link Aggregation Control Protocol), VLAN (Virtual Local Access Network), Seguridad de Datos en Ambientes Wireless y en Conexiones Remotas VPN.

La administración de una red implica el conocimiento de todas las herramientas necesarias para brindar una gestión funcional ante distintas respuestas de índole práctica, supervisora y analítica; que nos permitirán una rápida respuesta ante posibles caídas en los servicios de la red en particular.

Si hasta el momento, en una compañía en particular no se ha aplicado las herramientas que se han detallado en este informe; se debe elaborar un Plan de Trabajo sobre la forma como aplicarlos en un ambiente en producción de tal manera que no afecte los actuales servicios existentes. El impacto en la red que se produciría, debe calcularse en la medida de lo posible para que éste sea lo más mínimo en caso de que se presente.

Es necesario mencionar que si estuviéramos frente a una nueva implementación de una red de comunicaciones, las condiciones serán las mejores y el ambiente sería el ideal debido a que el planeamiento del diseño de la red se daría con todas las funcionalidades a ejecutar.

Se debe evaluar los servicios que se emplearán en una red en particular ya que esta información será determinante en la topología a implementar debido a que esta plataforma tendrá un ancho de banda que soportara con eficiencia la transferencia de datos en la red en mención.

ANEXO A

GLOSARIO

DiffServ	Servicios Diferenciados
DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Services Code Point
IETF	Internet Engineering Task Force
IP	Internet Protocol
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
MAC	Medium Access Control
NAT	Network Address Translation
OSI	Open System Interconnection
PAgP	Port aggregation Protocol
PHB	Per Hop Behaviour
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Server
RFC	Request for Comments
RTP	Real-Time Transport Protocol
RTCP	Real-Time Control Protocol
SLA	Service Level Agreement
SNA	System Network Architecture
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WEP	Wired Equivalent Policy
WLAN	Wireless Local Area Netwok

BIBLIOGRAFIA

1.- A. S. Tanenbaum, "Redes de Ordenadores", 2ª ed., Prentice-Hall, Englewood Cliffs (NJ), 2000.

2.- F. Halsall, "Comunicación de Datos, Redes de Computadores y Sistemas.

3.- Stallings, William: Comunicaciones y Redes de Computadores, 6ª Ed. Prentice Hall, 2000.

4.- Siyan: Microsoft Windows 2000 TCP/IP. Edición Especial. Prentice Hall

5.- https://cisco.hosted.jivesoftware.com/docs/DOC-2663

6.- http://nsrc.org/workshops/2004/CEDIA/presentaciones/cv/switching/Switching-Ethernet.pdf

7.- http://www.windowsnetworking.com/kbase/WindowsTips/Windows2000/AdminTips/Security/SettingupWindows2000Radiustoauthenticatewireless802.1xclients.html

http://www.cisco.com/en/US/tech/tk389/tk213/technologies_configuration_example09186a0080094470.shtml

9.- http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00807f54b2.shtml