INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

UNIDAD CULHUACAN

TESINA

SEMINARIO DE TITULACIÓN
INTERCONECTIVIDAD Y SEGMENTACION EN REDES DE ALTA VELOCIDAD
FNS5052005/14/2008

DISEÑO DE VLAN EN EL AREA DE IMAGENOLOGIA DEL HOSPITAL GENERAL DE MÉXICO

Que como prueba escrita de su examen profesional para obtener el titulo de:
Ingeniero en Comunicaciones y Electrónica

Presentan

CARLOS ANASTACIO GARCIA
HUGO PÉREZ LAFRAGUA

México D.F. **Noviembre 2008**

IPN
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

TESINA

QUE PARA OBTENER EL TITULO DE: INGENIERO EN COMUNICACIONES Y ELECTRONICA

POR LA OPCION DE TITULACION: SEMINARIO DE TITULACION
FNS5052005/14/2008

NOMBRE DEL SEMINARIO: INTERCONECTIVIDAD Y SEGMENTACION EN REDES DE ALTA VELOCIDAD

DEBERA DESARROLLAR: CARLOS ANASTACIO GARCIA
HUGO PÉREZ LAFRAGUA

NOMBRE DEL TEMA

"DISEÑO DE VLAN EN EL AREA DE IMAGENOLOGÍA DEL HOSPITAL GENERAL DE MÉXICO"

CAPITULADO

I. INTRODUCCIÓN
II. INTRODUCCIÓN A LAS REDES
III. DISEÑO DE VLAN
IV. ANEXOS Y BIBLIOGRAFIA
V. CONCLUSIONES

Fecha: México D.F. a 29 de Enero de 2009

M en C Raymundo Santana Alquicira
Director del seminario

Dra. Linda Karina Toscano Medina
Asesor

M. en C. Rocío Toscano Medina
Asesor

M. en C. Luís Carlos Castro Madrid
Jefe de carrera de Ingeniería en Computación

INDICE

INTRODUCCION

Las redes en la vida actual son muy importantes, tanto que ya se ha vuelto algo cotidiano para la mayoría de la gente y es todavía más para las nuevas generaciones, ya que nacen y crecen con este tipo de tecnologías.

La tecnología en los hospitales ha evolucionado de forma acelerada en los últimos años esto implica que los equipos que eran puramente análogos han dejado de ser útiles y en pocos años ha empezado una revolución digital. En muchos de estos casos este cambio se realiza de forma desordenada y en muchos hospitales se adquieren equipos de última tecnología sin pensar en la integración de análogo con digital y las ventajas que se pueden llegar a obtener si se les acopla adecuadamente. El caso del Hospital General de México es uno de estos, pues han adquirido en sus diversas áreas de imagenología equipos con protocolos de comunicación muy actuales. Sin embargo existen muchos problemas de comunicación entre ellos, lo que muchas veces hace añorar al usuario los equipos análogos anteriores que no presentaban problema alguno pues estos no dependían del enlace de todos los equipos.

OBJETIVO

Implementar la segmentación de red por medio de VLAN del departamento imagenología del Hospital General de México para controlar el tráfico en la red.

PROBLEMA

La red de imagenología es de alta prioridad ya que los estudios de los pacientes se necesitan procesar y diagnosticar de forma rápida. También es importante que los datos y las imágenes se visualicen en tiempo real y sin perdida de información. Al procesar o mandar imágenes la red se vuelve muy deficiente (lenta); provocando incluso perdida de estudios, perdida de tiempo, radiación innecesaria al paciente, diagnósticos no confiables y perdida de conexión entre los equipos.

JUSTIFICACION

Administrar adecuadamente la transmisión de información del área de imagenología, mejorando la conectividad entre las diferentes áreas que componen el departamento, optimizando los tiempos de envío en la red y evitando tráfico innecesario de otras áreas ajenas al departamento.

ALCANCE

Esta tesina segmentara grupos de trabajo por medio de VLAN en el áreas de imagenología del Hospital General de México dividiendo por segmentos o VLAN las áreas de Tomografía, Resonancia Magnética, Ultrasonido, Mastografía, cuarto azul y estaciones de diagnóstico, para optimizar las áreas antes mencionadas.

INTRODUCCION A LAS REDES

Cada uno de los tres siglos pasados ha estado dominado por una sola tecnología. El siglo XVIII fue la etapa de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la época de la máquina de vapor. Durante el siglo XX, la tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, hemos asistido a la instalación de redes telefónicas en todo el mundo, a la invención de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de los equipos informáticos, así como a la puesta en orbita de los satélites de comunicación.

A medida que avanzamos hacia los últimos años de este siglo, se ha dado una rápida convergencia de estas áreas, y también las diferencias entre la captura, transporte, almacenamiento y procesamiento de información están desapareciendo con rapidez. Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, simplemente oprimiendo una tecla. A medida que crece nuestra habilidad para recolectar procesar y distribuir información, la demanda de mas sofisticados procesamientos de información crece todavía con mayor rapidez.

La industria de la computación ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener una sola computadora para satisfacer todas las necesidades de calculo de una organización se está reemplazando con rapidez por otro que considera un número grande de equipos de computo separados, pero interconectados, que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de redes de computación. Estas nos dan a entender una colección interconectada de computadoras autónomas. Se dice que las computadoras están interconectadas, si son capaces de intercambia información. La conexión necesita hacerse a través de un hilo de cobre, el uso de láser, microondas y satélites de comunicaciones.

Objetivos de las redes

Las redes en general, consisten en "compartir recursos", y uno de sus objetivos es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a 1000 km de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente.

Un segundo objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. Por ejemplo todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias. Además, la presencia de múltiples CPU significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque se tenga un rendimiento global menor.

Otro objetivo es el ahorro económico. Las computadoras pequeñas tienen una mejor relación costo / rendimiento, comparada con la ofrecida por las máquinas grandes. Estas son, a grandes rasgos, diez veces mas rápidas que el mas rápido de los microprocesadores, pero su costo es miles de veces mayor. Este desequilibrio ha ocasionado que muchos diseñadores de sistemas construyan sistemas constituidos por poderosas computadoras personales, uno por usuario, con los datos guardados una o mas máquinas que funcionan como servidor de archivo compartido.

Este objetivo conduce al concepto de redes con varias computadoras en el mismo edificio. A este tipo de red se le denomina LAN (red de área local), en contraste con lo extenso de una WAN (red de área extendida), a la que también se conoce como red de gran alcance.

Un punto muy relacionado es la capacidad para aumentar el rendimiento del sistema en forma gradual a medida que crece la carga, simplemente añadiendo mas procesadores. Con máquinas grandes, cuando el sistema esta lleno, deberá reemplazarse con uno mas grande, operación que por lo normal genera un gran gasto y una perturbación inclusive mayor al trabajo de los usuarios.

Otro objetivo del establecimiento de una red de computadoras, es que puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre si. Con el ejemplo de una red es relativamente fácil para dos o mas personas que viven en lugares separados, escribir informes juntos. Cuando un autor hace un cambio inmediato, en lugar de esperar varios días para recibirlos por carta. Esta rapidez hace que la cooperación entre grupos de individuos que se encuentran alejados, y que anteriormente había sido imposible de establecer, pueda realizarse ahora.

En la siguiente tabla se muestra la clasificación de sistemas multiprocesadores distribuidos de acuerdo con su tamaño físico. En la parte superior se encuentran las máquinas de flujo de datos, que son computadoras con un alto nivel de paralelismo y muchas unidades funcionales trabajando en el mismo programa. Después vienen los multiprocesadores, que son sistemas que se comunican a través de memoria compartida. En seguida de los multiprocesadores se muestran verdaderas redes, que son computadoras que se comunican por medio del intercambio de mensajes. Finalmente, a la conexión de dos o mas redes se le denomina interconexión de redes.

Aplicación de las redes

El reemplazo de una máquina grande por estaciones de trabajo sobre una LAN no ofrece la posibilidad de introducir muchas aplicaciones nuevas, aunque podrían mejorarse la fiabilidad y el rendimiento. Sin embargo, la disponibilidad de una WAN (ya estaba antes) si genera nuevas aplicaciones viables, y algunas de ellas pueden ocasionar importantes efectos en la totalidad de la sociedad. Para dar una idea sobre algunos de los usos importantes de redes de computadoras, veremos ahora brevemente tres ejemplos: el acceso a programas remotos, el acceso a bases de datos remotas y facilidades de comunicación de valor añadido.

Una compañía que ha producido un modelo que simula la economía mundial puede permitir que sus clientes se conecten usando la red y corran el programa para ver como pueden afectar a sus negocios las diferentes proyecciones de inflación, de tasas de interés y de fluctuaciones de tipos de cambio. Con frecuencia se prefiere este planteamiento que vender los derechos del programa, en especial si el modelo se está ajustando constantemente ó necesita de una máquina muy grande para correrlo.

Todas estas aplicaciones operan sobre redes por razones económicas: el llamar a una computadora remota mediante una red resulta más económico que hacerlo directamente. La posibilidad de tener un precio mas bajo se debe a que el enlace de una llamada telefónica normal utiliza un circuito caro y en exclusiva durante todo el tiempo que dura la llamada, en tanto que el acceso a través de una red, hace que solo se ocupen los enlaces de larga distancia cuando se están transmitiendo los datos.

Una tercera forma que muestra el amplio potencial del uso de redes, es su empleo como medio de comunicación (Internet). Como por ejemplo, el tan conocido por todos, correo electrónico (e-mail), que se envía desde una terminal, a cualquier persona situada en cualquier parte del mundo que disfrute de este servicio. Además de texto, se pueden enviar fotografías e imágenes.

Estructura de una red.

En toda red existe una colección de máquinas para correr programas de usuario (aplicaciones). Seguiremos la terminología de una de las primeras redes, denominada ARPANET, y llamaremos host a las máquinas antes mencionadas. También, en algunas ocasiones se utiliza el término sistema terminal o sistema final. Los host están conectados mediante una subred de comunicación, o simplemente subred. El trabajo de la subred consiste en enviar mensajes entre host, de la misma manera como el sistema telefónico envía palabras entre la persona que habla y la que escucha. El diseño completo de la red simplifica notablemente cuando se separan los aspectos puros de comunicación de la red (la subred), de los aspectos de aplicación (los host).

Una subred en la mayor parte de las redes de área extendida consiste de dos componentes diferentes: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión (conocidas como circuitos, canales o troncales), se encargan de mover bits entre máquinas.

Los elementos de conmutación son computadoras especializadas que se utilizan para conectar dos o mas líneas de de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación deberá seleccionar una línea de salida para reexpedirlos

Ejemplo de redes

Un número muy grande de redes se encuentran funcionando, actualmente, en todo el mundo, algunas de ellas son redes públicas operadas por proveedores de servicios portadores comunes o PTT, otras están dedicadas a la investigación, también hay redes en cooperativas operadas por los mismos usuarios y redes de tipo comercial o corporativo.

Las redes, por lo general, difieren en cuanto a su historia, administración, servicios que ofrecen, diseño técnico y usuarios. La historia y la administración pueden variar desde una red cuidadosamente elaborada por una sola organización, con un objetivo muy bien definido, hasta una colección específica de máquinas, cuya conexión se fue realizando con el paso del tiempo, sin ningún plan maestro o administración central que la supervisara. Los servicios ofrecidos van desde una comunicación arbitraria de proceso a proceso, hasta llegar al correo electrónico, la transferencia de archivos, y el acceso y ejecución remota. Los diseños técnicos se diferencian en el medio de transmisión empleado, los algoritmos de encaminamiento y de denominación utilizados, el número y contenido de las capas presentes y los protocolos usados. Por último, las comunidades de usuarios pueden variar desde una sola corporación, hasta aquella que incluye todas las computadoras científicas que se encuentren en el mundo industrializado.

Redes de comunicación

La posibilidad de compartir con carácter universal la información entre grupos de computadoras y sus usuarios; un componente vital de la era de la información. La generalización de la computadora personal (PC) y de la red de área local (LAN) durante la década de los ochenta ha dado lugar a la posibilidad de acceder a información en bases de datos remotas; cargar aplicaciones desde puntos de ultramar; enviar mensajes a otros países y compartir ficheros, todo ello desde una computadora personal.

Las redes que permiten todo esto son equipos avanzados y complejos. Su eficacia se basa en la confluencia de muy diversos componentes. El diseño de implantación de una red mundial de computadoras es uno de los grandes milagros tecnológicos de las últimas décadas.

Todavía en la década de los setenta las computadoras eran máquinas caras y frágiles que estaban al cuidado de especialistas y se guardaban en recintos vigilados. Para utilizarlos se podía conectar un terminal directamente o mediante una línea telefónica y un módem para acceder desde un lugar remoto. Debido a su elevado costo, solían ser recursos centralizados a los que el usuario accedía por cuenta propia. Durante esta época surgieron muchas organizaciones, las empresas de servicios, que ofrecían tiempo de proceso en una mainframe. Las redes de computadoras no estaban disponibles comercialmente. No obstante, se inició en aquellos años uno de los avances más significativos para el mundo de la tecnología: los experimentos del Departamento de Defensa norteamericano con vistas a distribuir los recursos informáticos como protección contra los fallos. Este proyecto se llama ahora internet.

Redes de área local (LAN)

Uno de los sucesos más críticos para la conexión en red lo constituye la aparición y la rápida difusión de la red de área local (LAN) como forma de normalizar las conexiones entre las máquinas que se utilizan como sistemas ofimáticos. Como su propio nombre indica, constituye una forma de interconectar una serie de equipos informáticos. A su nivel más elemental, una LAN no es más que un medio compartido (como un cable coaxial al que se conectan todas las computadoras y las impresoras) junto con una serie de reglas que rigen el acceso a dicho medio. La LAN más difundida, la Ethernet, utiliza un mecanismo denominado Call Sense Multiple Acces-Collision Detect (CSMS-CD). Esto significa que cada equipo conectado sólo puede utilizar el cable cuando ningún otro equipo lo está utilizando. Si hay algún conflicto, el equipo que está intentando establecer la conexión la anula y efectúa un nuevo intento más adelante. La Ethernet transfiere datos a 10 Mbits/seg, lo suficientemente rápido como para hacer inapreciable la distancia entre los diversos equipos y dar la impresión de que están conectados directamente a su destino.

Ethernet y CSMA-CD son dos ejemplos de LAN. Hay topologías muy diversas (bus, estrella, anillo) y diferentes protocolos de acceso. A pesar de esta diversidad, todas las LAN comparten la característica de poseer un alcance limitado (normalmente abarcan un edificio) y de tener una velocidad suficiente para que la red de conexión resulte invisible para los equipos que la utilizan.

Además de proporcionar un acceso compartido, las LAN modernas también proporcionan al usuario multitud de funciones avanzadas. Hay paquetes de software de gestión para controlar la configuración de los equipos en la LAN, la administración de los usuarios, y el control de los recursos de la red. Una estructura muy utilizada consiste en varios servidores a disposición de distintos (con frecuencia, muchos) usuarios. Los primeros, por lo general máquinas más potentes, proporcionan servicios como control de impresión, ficheros compartidos y correo a los últimos, por lo general computadoras personales.

Routers y bridges

Los servicios en la mayoría de las LAN son muy potentes. La mayoría de las organizaciones no desean encontrarse con núcleos aislados de utilidades informáticas. Por lo general prefieren difundir dichos servicios por una zona más amplia, de manera que los grupos puedan trabajar independientemente de su ubicación. Los routers y los bridges son equipos especiales que permiten conectar dos o más LAN. El bridge es el equipo más elemental y sólo permite conectar varias LAN de un mismo tipo. El router es un elemento más inteligente y posibilita la interconexión de diferentes tipos de redes de computadoras.

Las grandes empresas disponen de redes corporativas de datos basadas en una serie de redes LAN y routers. Desde el punto de vista del usuario, este enfoque proporciona una red físicamente heterogénea con aspecto de un recurso homogéneo.

Redes de área extensa (WAN)

Cuando se llega a un cierto punto deja de ser poco práctico seguir ampliando una LAN. A veces esto viene impuesto por limitaciones físicas, aunque suele haber formas más adecuadas o económicas de ampliar una red de computadoras. Dos de los componentes importantes de cualquier red son la red de teléfono y la de datos. Son enlaces para grandes distancias que amplían la LAN hasta convertirla en una red de área extensa (WAN). Casi todos los operadores de redes nacionales (como DBP en Alemania o British Telecom en Inglaterra) ofrecen servicios para interconectar redes de computadoras, que van desde los enlaces de datos sencillos y a baja velocidad que funcionan basándose en la red pública de telefonía hasta los complejos servicios de alta velocidad (como frame relay y SMDS-Synchronous Multimegabit Data Service) adecuados para la interconexión de las LAN. Estos servicios de datos a alta velocidad suelen denominarse conexiones de banda ancha. Se prevé que proporcionen los enlaces necesarios entre LAN para hacer posible lo que han dado en llamarse autopistas de la información.

Proceso distribuido:

Parece lógico suponer que las computadoras podrán trabajar en conjunto cuando dispongan de la conexión de banda ancha. ¿Cómo conseguir, sin embargo, que computadoras de diferentes fabricantes en distintos países funcionen en común a través de todo el mundo? Hasta hace poco, la mayoría de las computadoras disponían de sus propias interfaces y presentaban su estructura particular. Un equipo podía comunicarse con otro de su misma familia, pero tenía grandes dificultades para hacerlo con un extraño. Sólo los más privilegiados disponían del tiempo, conocimientos y equipos necesarios para extraer de diferentes recursos informáticos aquello que necesitaban.

En los años noventa, el nivel de concordancia entre las diferentes computadoras alcanzó el punto en que podían interconectarse de forma eficaz, lo que le permite a cualquiera sacar provecho de un equipo remoto. Los principales componentes son:

Cliente/Servidor

En vez de construir sistemas informáticos como elementos monolíticos, existe el acuerdo general de construirlos como sistemas cliente/servidor. El cliente (un usuario de PC) solicita un servicio (como imprimir) que un servidor le proporciona (un procesador conectado a la LAN). Este enfoque común de la estructura de los sistemas informáticos se traduce en una separación de las funciones que anteriormente forman un todo. Los detalles de la realización van desde los planteamientos sencillos hasta la posibilidad real de manejar todas las computadoras de modo uniforme.

Tecnología de objetos

Otro de los enfoques para la construcción de los sistemas parte de la hipótesis de que deberían estar compuestos por elementos perfectamente definidos, objetos encerrados, definidos y materializados haciendo de ellos agentes independientes. La

adopción de los objetos como medios para la construcción de sistemas informáticos ha colaborado a la posibilidad de intercambiar los diferentes elementos.

Sistemas abiertos

Esta definición alude a sistemas informáticos cuya arquitectura permite una interconexión y una distribución fáciles. En la práctica, el concepto de sistema abierto se traduce en desvincular todos los componentes de un sistema y utilizar estructuras análogas en todos los demás. Esto conlleva una mezcla de normas (que indican a los fabricantes lo que deberían hacer) y de asociaciones (grupos de entidades afines que les ayudan a realizarlo). El efecto final es que sean capaces de hablar entre sí.

El objetivo último de todo el esfuerzo invertido en los sistemas abiertos consiste en que cualquiera pueda adquirir computadoras de diferentes fabricantes, las coloque donde quiera, utilice conexiones de banda ancha para enlazarlas entre sí y las haga funcionar como una máquina compuesta capaz de sacar provecho de las conexiones de alta velocidad.

La labor de mantenimiento de la operativa de una LAN exige dedicación completa. Conseguir que una red distribuida por todo el mundo funcione sin problemas supone un reto aún mayor. Últimamente se viene dedicando gran atención a los conceptos básicos de la gestión de redes distribuidas y heterogéneas. Hay ya herramientas suficientes para esta importante labor que permiten supervisar de manera eficaz las redes globales.

Las redes de computadoras

Definir el concepto de redes implica diferenciar entre el concepto de redes físicas y redes de comunicación.

Respecto a la estructura física, los modos de conexión física, los flujos de datos, etc. podemos decir que una red la constituyen dos o más computadoras que comparten determinados recursos, sea hardware (impresoras, sistemas de almacenamiento, etc.) sea software (aplicaciones, archivos, datos, etc.).

Desde una perspectiva más comunicativa y que expresa mejor lo que puede hacerse con las redes en la educación, podemos decir que existe una red cuando están involucrados un componente humano que comunica, un componente tecnológico (computadoras, televisión, telecomunicaciones) y un componente administrativo (institución o instituciones que mantienen los servicios). Una red, más que varias computadoras conectados, la constituyen varias personas que solicitan, proporcionan e intercambian experiencias e informaciones a través de sistemas de comunicación.
Atendiendo al ámbito que abarcan, tradicionalmente se habla de:

Redes de Área Local (conocidas como LAN) que conectan varias estaciones dentro de la misma institución,

Redes de Área Metropolitana (MAN),

Área extensa (WAN),

Por su soporte físico:

Redes de fibra óptica,

Red de servicios integrados (RDSI),

Las distintas configuraciones tecnológicas y la diversidad de necesidades planteadas por los usuarios, lleva a las organizaciones a presentar cierta versatilidad en el acceso a la documentación, mediante una combinación de comunicación sincrónica y asincrónica.

La comunicación sincrónica (o comunicación a tiempo real) contribuiría a motivar la comunicación, a simular las situaciones, cara a cara, mientras que la comunicación asincrónica (o retardada) ofrece la posibilidad de participar e intercambiar información desde cualquier sitio y en cualquier momento, permitiendo a cada participante trabajar a su propio ritmo y tomarse el tiempo necesario para leer, reflexionar, escribir y revisar antes de compartir la información. Ambos tipos de comunicación son esenciales en cualquier sistema de formación apoyado en redes.

Se trataría, por lo tanto, de configurar servicios educativos o, mejor, redes de aprendizaje apoyados en:

Videoconferencia que posibilitaría la asistencia remota a sesiones de clase presencial, a actividades específicas para alumnos a distancia, o a desarrollar trabajo colaborativo en el marco de la presencia continuada.

Conferencias electrónicas, que basadas en la computadora posibilitan comunicación escrita sincrónica, complementando y/o extendiendo las posibilidades de la intercomunicación a distancia.

Correo electrónico, listas de discusión que suponen poderosas herramientas para facilitar la comunicación asincrónica mediante computadoras.

Apoyo hipermedia (web) que servirá de banco de recursos de aprendizaje donde el alumno pueda encontrar los materiales además de orientación y apoyo.

Otras aplicaciones de internet tanto de recuperación de ficheros (Gopher, FTP) como de acceso remoto (telnet).

Ello implica, junto a la asistencia virtual a sesiones en la institución sean específicas o no mediante la videoconferencia y la posibilidad de presencia continuada, facilitar la transferencia de archivos (materiales básicos de aprendizaje, materiales

complementarios, la consulta a materiales de referencia) entre la sede (o sedes, reales o virtuales) y los usuarios.

Aunque el sistema de transferencia es variado dependiendo de múltiples factores (tipo de documento, disponibilidad tecnológica del usuario), está experimentando una utilización creciente la transferencia directamente a pantalla de materiales multimedia interactivos a distancia como un sistema de enseñanza a distancia a través de redes. Pero, también, utilizando otros sistemas de transferencia puede accederse a una variada gama de materiales de aprendizaje. Se trata, en todo caso, de un proceso en dos fases: primero recuperación y después presentación.

ETHERNET

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 PCs, estaciones de trabajo científicas y de alta 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).

Objetivos de Ethernet

Los objetivos principales de Ethernet son consistentes con los que se han convertido en los requerimientos básicos para el desarrollo y uso de redes LAN.

Los objetivos originales de Ethernet son:

Simplicidad

Las características que puedan complicar el diseño de la red sin hacer una contribución substancial para alcanzar otros objetivos se han excluido.

Bajo Costo

Las mejoras tecnológicas van a continuar reduciendo el costo global de los dispositivos de conexión.

Compatibilidad

Todas las implementaciones de Ethernet deberán ser capaces de intercambiar datos a nivel de capa de enlace de datos. Para eliminar la posibilidad de variaciones incompatibles de Ethernet, la especificación evita características opcionales.

Direccionamiento flexible

El mecanismo de direccionamiento debe proveer la capacidad de dirigir datos a un único dispositivo, a un grupo de dispositivos, o alternativamente, difundir (broadcast) el mensaje a todos los dispositivos conectados a la red.

Equidad

Todos los dispositivos conectados deben tener el mismo acceso a la red.
Progreso

Ningún dispositivo conectado a la red, operando de acuerdo al protocolo Ethernet, debe ser capaz de prevenir la operación de otros dispositivos.

Alta velocidad

La red debe operar eficientemente a una tasa de datos de 10 Mb/s.

Bajo retardo

En cualquier nivel de tráfico de la red, debe presentarse el mínimo tiempo de retardo posible en la transferencia de datos.

Estabilidad

La red debe ser estable bajo todas las condiciones de carga. Los mensajes entregados deben mantener un porcentaje constante de la totalidad del tráfico de la red.
Mantenimiento

El diseño de Ethernet debe simplificar el mantenimiento de la red, operaciones y planeamiento.

Arquitectura en capas

El diseño Ethernet debe ser especificado en término de capas de forma de separar las operaciones lógicas de los protocolos de capa de enlace de las especificaciones de comunicaciones físicas del canal de comunicación.

Diferencias entre Ethernet y IEEE 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 multiple 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 física, incluyendo cable coaxial 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.

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.

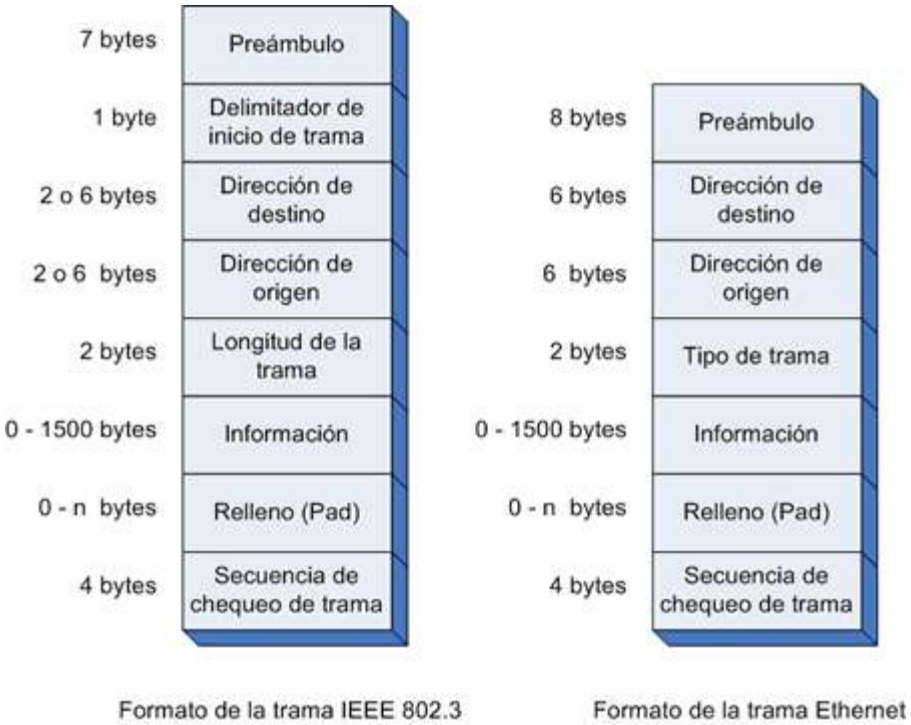


Imagen 1 formato de la trama IEEE 802.3 y Ethernet

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.

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.

Características de Ethernet

Las siguientes son algunas de las características que definen a Ethernet:

Las especificaciones Ethernet (IEEE 802.3) también han sido adoptadas por ISO y se encuentran en el estándar internacional 8802-3.

Ethernet esta basado en la lógica de la topología bus. Originalmente, el bus era una única longitud de cable a la cual los dispositivos de red estaban conectados. En las implementaciones actuales, el bus se ha miniaturizado y puesto en un hub (concentrador) al cuál las estaciones, servidores y otros dispositivos son conectados.

Ethernet usa un método de acceso al medio por disputa (contention). Las transmisiones son difundidas en el canal compartido para ser escuchadas por todos los dispositivos conectados, solo el dispositivo de destino previsto va a aceptar la transmisión. Este tipo de acceso es conocido como CSMA/CD.

Ethernet ha evolucionado para operar sobre una variedad de medios, cable coaxial, par trenzado y fibra óptica, a múltiples tasas de transferencia. Todas las implementaciones son interoperables, lo que simplifica el proceso de migración a nuevas versiones de Ethernet.

Múltiples segmentos de Ethernet pueden ser conectados para formar una gran red LAN Ethernet utilizando repetidores. La correcta operación de una LAN Ethernet depende en que los segmentos del medio sean construidos de acuerdo a las reglas para ese tipo de medio. Redes LAN complejas construidas con múltiples tipos de medio deben ser diseñadas de acuerdo a las pautas de configuración para multisegmentos provistas en el estándar Ethernet. Las reglas incluyen límites en el número total de segmentos y repetidores que pueden ser utilizados en la construcción de una LAN.

Ethernet fue diseñado para ser expandido fácilmente. El uso de dispositivos de interconexión tales como bridges (puente), routers (ruteadores), y switches (conmutadores) permiten que redes LAN individuales se conecten entre si. Cada LAN continúa operando en forma independiente pero es capaz de comunicarse fácilmente con las otras LAN conectadas.

Control de acceso al medio IEEE 802.3 CSMA/CD

Definición de CSMA/CD

El estándar IEEE 802.3 especifica el método de control del medio (MAC) denominado CSMA/CD por las siglas en ingles de acceso múltiple con detección de portadora y detección de colisiones (carrier sense multiple access with collision detection). CSMA/CD opera de la siguiente manera:

Una estación que tiene un mensaje para enviar escucha al medio para ver si otra estación está transmitiendo un mensaje.

Si el medio esta tranquilo (ninguna otra estación esta transmitiendo), se envía la transmisión.

Cuando dos o más estaciones tienen mensajes para enviar, es posible que transmitan casi en el mismo instante, resultando en una colisión en la red.

Cuando se produce una colisión, todas las estaciones receptoras ignoran la transmisión confusa.

Si un dispositivo de transmisión detecta una colisión, envía una señal de expansión para notificar a todos los dispositivos conectados que ha ocurrido una colisión. Las estaciones transmisoras detienen sus transmisiones tan pronto como detectan la colisión.

Cada una de las estaciones transmisoras espera un periodo de tiempo aleatorio e intenta transmitir otra vez.

Detección de portadora

La detección de portadora es utilizada para escuchar al medio (la portadora) para ver si se encuentra libre. Si la portadora se encuentra libre, los datos son pasados a la capa física para su transmisión. Si la portadora está ocupada, se monitorea hasta que se libere.

Detección de colisiones

Luego de comenzar la transmisión, continúa el monitoreo del medio de transmisión. Cuando dos señales colisionan, sus mensajes se mezclan y se vuelven ilegibles. Si esto ocurre, las estaciones afectadas detienen su transmisión y envían una señal de expansión. La señal de expansión de colisión asegura que todas las demás estaciones de la red se enteren de que ha ocurrido una colisión.

Funciones de CSMA/CD

El estándar CSMA/CD de la IEEE define un modelo hecho de hasta seis funciones. Tres de estas funciones están relacionadas con el envió de datos y las otras tres de la recepción de datos. Las funciones de recepción funcionan en paralelo con las de envió.

Encapsulado/Desencapsulado de datos

La función de encapsulación y desencapsulación de datos es llevada a cabo por la subcapa MAC. Este proceso es responsable de las funciones de direccionamiento y del chequeo de errores.

Encapsulado

El encapsulado es realizado por la estación emisora. El encapsulado es el acto de agregar información, direcciones y bytes para el control de errores, al comienzo y al final

de la unidad de datos transmitidos. Esto es realizado luego que los datos son recibidos por la subcapa de control de enlace lógico (LLC). La información añadida es necesaria para realizar las siguientes tareas:

- Sincronizar la estación receptora con la señal.
- Indicar el comienzo y el fin de la trama.
- Identificar las direcciones tanto de la estación emisora como la receptora.
- Detectar errores en la transmisión.
- Desencapsulado

El desencapsulado es realizado por la estación receptora. Cuando es recibida una trama, la estación receptora es responsable de realizar las siguientes tareas:

Reconocer la dirección de destino y determinar si coincide con su propia dirección.

Realizar la verificación de errores.

Remover la información de control que fue añadida por la función de encapsulado de datos en la estación emisora.

Administración de acceso al medio

La función de administración de acceso al medio es realizada por la subcapa MAC.

En la estación emisora, la función de administración de acceso al medio es responsable de determinar si el canal de comunicación se encuentra disponible. Si el canal se encuentra disponible puede iniciarse la transmisión de datos.

Adicionalmente, la función de administración es responsable de determinar que acción deberá tomarse en caso de detectarse una colisión y cuando intentará retransmitir.
En la estación receptora la función de administración de acceso al medio es responsable de realizar las comprobaciones de validación en la trama antes de pasarla a la función de desencapsulado.

Codificación/decodificación de datos

La función de codificación/decodificación es realizada en la capa física. Esta función es responsable de obtener la forma eléctrica u óptica de los datos que se van a transmitir en el medio.

La codificación de datos es realizada por la estación emisora. Esta es responsable de traducir los bits a sus correspondientes señales eléctricas u ópticas para ser trasladadas a través del medio. Adicionalmente, esta función es responsable de escuchar el medio y

notificar al la función de administración de acceso al medio si el medio se encuentra libre, ocupado o se ha detectado una colisión.

La decodificación de datos es realizada en la estación receptora. Esta es responsable de la traducción de las señales eléctricas u ópticas nuevamente en un flujo de bits.

Trama de transmisión CSMA/CD

Se defina a una trama de transmisión como el grupo de bits en un formato particular con un indicador de señal de comienzo de la trama.

El formato de la trama permite a los equipos de red reconocer el significado y propósito de algunos bits específicos en la trama. Una trama es generalmente una unidad lógica de transmisión conteniendo información de control para el chequeo de errores y para el direccionamiento.

El formato de la trama CSMA/CD (IEEE 8023.3) se encuentra a continuación en la figura 2:

Figura 2 Formato de la trama CSMA/CD

Los componentes de la trama CSMA/CD son responsables de las siguientes tareas:

El preámbulo es responsable de proveer sincronización entre los dispositivos emisor y receptor.

El delimitador de inicio de trama indica el comienzo de una trama de datos.
El delimitador de inicio de trama esta formado de la siguiente secuencia de 8 bits, 10101011

Cada campo de dirección, dirección de origen y dirección de destino, puede tener una longitud tanto de 2 bytes como de 6 bytes. Ambas direcciones, origen y destino, deben tener la misma longitud en todos los dispositivos de una red dada. El campo dirección de destino específica la estación o estaciones a las cuales están dirigidos los datos. Una dirección que referencia a un grupo de estaciones es conocida como dirección de grupo de multicast, o dirección de grupo de multidifusión. Una dirección que referencia a todas las estaciones de una red es conocida como dirección de difusión.

La dirección de origen identifica a la estación que está haciendo la transmisión. El campo longitud indica la longitud del campo de datos que se encuentra a continuación. Es necesaria para determinar la longitud del campo de datos en los casos que se utiliza un campo pad (campo de relleno).

El campo información contiene realmente los datos transmitidos. Es de longitud variable, por lo que puede tener cualquier longitud entre 0 y 1500 bytes.

Un campo pad o campo de relleno es usado para asegurar que la trama alcance la longitud mínima requerida. Una trama debe contener mínimo un número de bytes para que las estaciones puedan detectar las colisiones con precisión.

Una secuencia de chequeo de trama es utilizada como mecanismo de control de errores.

Cuando el dispositivo emisor ensambla la trama, realiza un cálculo en los bits de la trama. El algoritmo usado para realizar este cálculo siempre genera como salida un valor de 4 bytes. El dispositivo emisor almacena este valor en el campo de chequeo de secuencia de la trama.

Cuando el receptor recibe la trama, realiza el mismo cálculo y compara el resultado con el del campo de chequeo de secuencia de la trama. Si los dos valores coinciden, la transmisión se asume como correcta. Si los dos valores son diferentes, el dispositivo de destino solicita una retransmisión de la trama.

Tipos de 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.

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 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 hub.

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).

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.

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

Principios de operación de Ethernet

Cada dispositivo equipado con Ethernet opera en forma independiente del resto de los dispositivos de la red, las redes Ethernet no hacen uso de un dispositivo central de control. Todos los dispositivos son conectados a un canal de comunicaciones de señales compartidas.

Las señales Ethernet son transmitidas en serie, se transmite un bit a la vez. Las transmisiones se realizan a través del canal de señales compartidas donde todos los dispositivos conectados pueden escuchar la transmisión.

Antes de comenzar una transmisión, un dispositivo escucha el canal de transmisión para ver si se encuentra libre de transmisiones. Si el canal se encuentra libre, el dispositivo puede transmitir sus datos en la forma de una trama Ethernet.

Después de que es transmitida una trama, todos los dispositivos de la red compiten por la siguiente oportunidad de transmitir una trama. La disputa por la oportunidad de transmitir entre los dispositivos es pareja, para asegurar que el acceso al canal de comunicaciones sea justo, ningún dispositivo puede bloquear a otros dispositivos.

El acceso al canal de comunicaciones compartido es determinado por la subcapa MAC. Este control de acceso al medio es conocido como CSMA/CS.

Direccionamiento

Los campos de direcciones en una trama Ethernet llevan direcciones de 48 bits, tanto para la dirección de destino como la de origen. El estándar IEEE administra parte del campo de las direcciones mediante el control de la asignación un identificador de 24 bits conocido como OUI (Organizationally Unique Identifier, identificador único de organización).

A cada organización que desee construir interfaces de red (NIC) Ethernet, se le asigna un OUI de 24 bits único, el cual es utilizado como los primeros 24 bits de la dirección de 48 bits del NIC. La dirección de 48 bits es referida como dirección física, dirección de hardware, o dirección MAC.

El uso de direcciones únicas pre asignadas, simplifica el montaje y crecimiento de una red Ethernet.

La topología lógica de una red determina como las señales son transferidas en la red. La topología lógica de una red Ethernet provee un único canal de comunicaciones que transporta señales de todos los dispositivos conectados. Esta topología lógica puede ser diferente de la topología física o de la disposición real del medio. Por ejemplo, si los segmentos del medio de una red Ethernet se encuentran conectados físicamente siguiendo una topología estrella, la topología lógica continua siendo la de un único canal de comunicaciones que transporta señales de todos los dispositivos conectados.

Múltiples segmentos Ethernet pueden ser interconectados utilizando repetidores para formar una red LAN más grande. Cada segmento de medio es parte del sistema de señales completo. Este sistema de segmentos interconectados nunca es conectado en forma de bucle, es decir, cada segmento debe tener dos extremos.

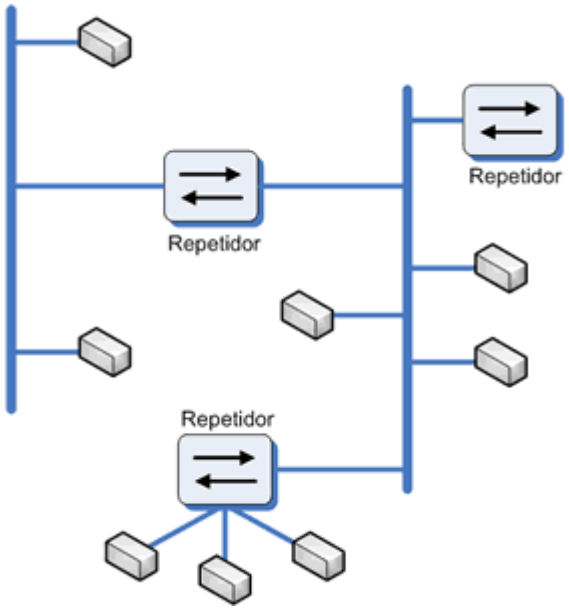


Figura 3 Segmentos de red interconectados

La señal generada por un dispositivo es puesta en el segmento de medio al cual esta conectado. La señal es repetida en todos los otros segmentos conectado de forma que sea escuchada por todos las demás estaciones. Sin importar cual sea la topología física, solo existe un canal de señales para entregar tramas a través de todos los segmentos a todos los dispositivos conectados.

Tiempo de señales

Para que el método de control de acceso al medio funcione correctamente, todas las interfaces de red Ethernet deben poder responder a las señales dentro de una cantidad de tiempo especificada. El tiempo de la señal está basado en la cantidad de tiempo que le toma a una señal ir de un extremo de la red al otro y regresar (Round Trip Time).

El límite del Round Trip Time debe alcanzar, a pesar de que la combinación de segmentos de medio se utilicen en la construcción de la red. Las pautas de configuración proveen las reglas para la combinación de segmentos con repetidores de forma que el tiempo de las señales se mantenga. Si estas reglas no son seguidas, las estaciones podrían no llegar a escuchar las transmisiones a tiempo y las señales de estas estaciones pondrían interferirse entre si, causando colisiones tardías y congestionamiento en la red.

Los segmentos del medio deben ser construidos de acuerdo a las pautas de configuración para el tipo de medio elegido y la velocidad de transmisión de la red (las redes de mayor velocidad exigen un tamaño de red de menor). Las redes locales Ethernet construidas por múltiples tipos de medios deben ser diseñadas siguiendo las pautas para configuraciones multisegmento del estándar Ethernet.

Componentes de Ethernet

Componentes de Ethernet a 10 Mb/s

La especificación original IEEE 802.3 era para Ethernet a 10Mb/s sobre cable coaxial grueso. Hoy en día hay cuatro tipos de Ethernet operando a 10Mb/s, cada uno operando sobre un medio distinto. Estos se resumen a continuación en la figura 4:

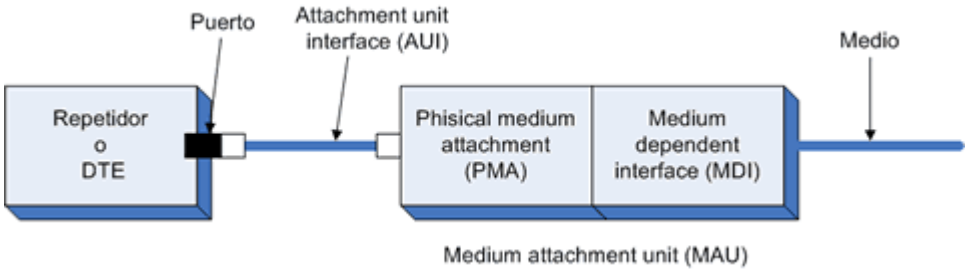


Figura 4a Tipos de Ethernet operando a 10Mbps

Nombre	Medio
10BASE-5	Cable coaxial grueso
10BASE-2	Cable coaxial delgado
10BASE-T	Cable par trenzado
10BASE-F	Cable de fibra óptica

Figura 4b Tipos de Ethernet operando a 10Mbps

Los AUI, PMA, y MDI pueden ser internos o externos al dispositivo de red.

Equipo terminal de datos (Data Terminal Equipment, DTE)

En el estándar IEEE, los dispositivos de red son referidos como equipos terminales de datos (DTE). Cada DTE conectado a la red Ethernet debe estar equipado con una interfaz de red (NIC) Ethernet. La NIC provee una conexión con el canal de comunicación. Esta contiene los componentes electrónicos y el software necesario para realizar las funciones necesarias para enviar una trama ethernet a través de la red.

Interfaz de unidad de conexión (Attachment Unit Interface, AUI)

La AUI provee un camino tanto para señales como para la energía entre las interfaces de red (NIC) Ethernet y el PMA. En el estándar DIX original, este componente era llamado cable transceptor.

Conexión al medio físico (Physical Medium Attachment, PMA)

El PMA es la parte de la capa física que se encarga de el control de la transmisión, detección de las colisione, la recuperación de reloj y la alineación del Retardo de Propagación (Skew).

Interfaz dependiente del medio (Medium Dependent Interface, MDI)

La MDI provee a la PMA de una conexión física y eléctrica al medio de transmisión. Por ejemplo, en el caso de Ethernet 10BASE-T, la MDI es un conector remodular de 8 posiciones, que encaja con un enchufe modular de 8 posiciones acoplado a 4 pares de cable UTP.

Medio

El medio transporta las señales entre los dispositivos conectados. Pueden utilizarse cable coaxial delgado o grueso, cable par trenzado, o cable de fibra óptica.

Componentes de Ethernet a 100 Mb/s

El incremento en diez veces la velocidad resulta en un factor de reducción de diez veces el tiempo que se necesita para transmitir un bit en la red. El formato de la trama, la cantidad de datos transportados, y el método de control de acceso al medio se mantienen sin cambios. Hay cuatro tipos de Ethernet operando a 100Mb/s. Estos se resumen a continuación:

Nombre	Medio
100BASE-T2	2-pares de UTP (Categoría 3 o superior)
100BASE-T4	4-pares de UTP (Categoría 3 o superior)
100BASE-TX	2-pares de cable par trenzado para datos (UTP o STP categoría 5 o superior)
100BASE-FX	Cable de fibra óptica

Figura 5 Tipos de ethernet operando a 100Mbps

Los estándares 100BASE-TX y 100BASE-FX son referidos conjuntamente como 100BASE-X. Estos estándares adoptan los estándares de medios físicos desarrollados por la ANSI para FDDI y TP-PMD. Los estándares 100BASE-T2 y 100BASE-T4 fueron desarrollados para hacer posible el uso de cableado UTP de menor calidad.

Las funciones realizadas por la DTE y MDI son las mismas que para Ethernet a 10Mb/s. Sin embargo, las especificaciones de Fast Ethernet incluyen un mecanismo de auto-negociación. Esto hace posible proveer interfaces de red (NICs) de doble velocidad que pueden operar tanto en 10 como 100Mb/s en forma automática.

Interfaz independiente del medio (Media Independent Interface, MII)

La MII es un conjunto de componentes electrónicos opcionales diseñados para hacer las diferencias en el señalamiento requeridas para diferentes medios transparente

para los chips Ethernet que se encuentran en los NIC de los dispositivos de red. Los componentes electrónicos de MII y el conector de 40 pines y cable asociados hacen posible conectar un dispositivo de red a cualquiera de varios tipos de medio para una mayor flexibilidad.

Dispositivo de capa física (Physical Layer Device, PHY)

El rol de este dispositivo es similar al del transceptor en Ethernet a 10Mb/s. Esta unidad puede ser interna o externa al dispositivo de red. Generalmente, es parte de la interfaz de red y el hub que contiene los circuitos necesarios para transmitir y recibir datos sobre el cable.

Medio

Ethernet a 100 Mb/s puede utilizar cable UTP, STP, o fibra óptica (el cable coaxial no es soportado).

Componentes de Ethernet a 1000 Mb/s

Gigabit Ethernet aumenta aún más la velocidad de transferencia hasta llegar a los 1000 Mb/s (1 Gb/s). Utiliza el mismo formato de trama, opera en full duplex y usa los mismos métodos de control de flujo que las otras versiones de Ethernet. En modo half duplex, Gigabit Ethernet utiliza el mismo meto de acceso al medio CSMA/CD para resolver las disputas por el medio compartido.

Hay cuatro tipos de Ethernet operando a 1Gb/s. Estos se resumen a continuación.

Nombre	Medio
1000BASE-SX	Cable de fibra óptica multimodo (50/125 μm o 62.5/125 μm)
1000BASE-LX	Cable de fibra óptica monomodo o multimodo (50/125 μm o 62.5/125 μm)
1000BASE-CX	Cable de cobre blindado especial
1000BASE-T	4-pares Categoría 5 (o superior) de cable UTP

Figura 6 Tipos de Ethernet operando a 1Gbps

Los estándares SX, LX, y CX son referidos en conjunto como 1000BASE X (IEEE 802.3z). Estos estándares adoptan los estándares para medios físicos desarrollados pro ANSI para fibra óptica. El estándar T (IEEE 802.3ab) fue desarrollado para hacer posible el uso de cableado UTP.

Los componentes utilizados en las redes Ethernet de 1 Gb/s realizan las mismas funciones que en Fast Ethernet. Sin embargo, la interfaz independiente del medio (Media

Independent Interface, MII) ahora es referida como interfaz gigabit independiente del medio (Gigabit Media Independent Interface, GMII).

Topologías Ethernet

Introducción

Las redes ethernet a menudo están formadas por múltiples segmentos individuales interconectados por repetidores. Los segmentos están interconectados entre si siguiendo lo que se denomina un patrón de árbol sin raíz. Cada segmento Ethernet es una rama individual de la red completa.

Se considera sin raíz ya que los segmentos interconectados pueden crecen en cualquier dirección.

Los segmentos Ethernet individuales pueden utilizar diferentes medios. Históricamente cada tipo de medio requiere de una disposición de física de cable diferente. Actualmente la topología física recomendada para las instalaciones es la topología estrella como se especifica en ANSI/TIA/EIA-568-A. La utilización de una topología estrella ha hecho permitido limitar las interrupciones en la red causadas por problemas de cableado.

Topología Bus

Cuando se utiliza cable coaxial delgado, la topología física de la red puede ser únicamente una topología bus. En este diseño, todos los dispositivos son conectados a un único tramo de cable. Este cable provee un camino para las señales eléctricas que es común para todos los dispositivos conectados y transporta todas las transmisiones entre los dispositivos.

Un problema asociado con el diseño bus de cableado es que una falla en cualquier parte del cable coaxial delgado va a interrumpir el camino eléctrico. Como resultado, la operación de todos los dispositivos conectados será interrumpida.

Los dispositivos conectados a un segmento de cable coaxial delgado siguen una topología conocida como cadena tipo margarita. En esta topología, un cable coaxial delgado conectado a un conector T BNC en un dispositivo es conectado a otro conector T en el siguiente dispositivo y así sucesivamente. Los conectores T que se encuentran en los extremos opuestos del segmento son terminales.

En una topología cadena tipo margarita, si cualquier cable coaxial delgado es removido incorrectamente del conector T, todo el segmento queda no funcional para todos los dispositivos conectados. Si el conector T es removido de la interfaz de red Ethernet, el segmento continúa funcionando, ya que la continuidad del cable coaxial no ha sido interrumpida.

También es posible tener segmentos punto a punto en un ambiente de cable coaxial delgado. Utilizando un repetidor multipuerto se puede conectar un segmento en forma directa a un dispositivo. Esto limita el número de dispositivos que pueden ser afectados por el daño a un cable específico.

Topología Estrella

Los segmentos de par trenzado y de fibra óptica son dispuestos en una topología física estrella. En esta topología, los dispositivos individuales son conectados a un concentrador o hub central, formando un segmento. Las señales de cada dispositivo conectado son enviadas al hub y luego difundidas a todos los otros dispositivos conectados. Este diseño permite a Ethernet operar lógicamente como un bus, pero físicamente el bus solo existe en el hub.

Una topología estrella simplifica la administración de la red y la resolución de problemas ya que cada tramo de cable conecta solo dos dispositivos, una a cada extremo del cable. Si un dispositivo no puede comunicarse exitosamente con en la red, puede ser movido físicamente a otra ubicación para establecer si la falla reside en el cableado o en el dispositivo. Este tipo de aislamiento es mucho más difícil en las topologías bus o cadena tipo margarita.

Fast Ethernet

Fast Ethernet, también conocido como 10BASE-T, fue desarrollado en respuesta a la necesidad de una red LAN compatible con Ethernet con mayor tasa de transferencia que pudiera operar sobre el cableado UTP. 100BASE-T fue desarrollado por la IEEE802.3 y es totalmente compatible con 10BASE-T. Las especificaciones de 100BASE-T se encuentran en el estándar IEEE802.3u.

En 100BASE-T, los parámetros de tiempo se incrementan por un factor de diez para alcanzar un incremento de 10 veces de la tasa de transferencia. Sin embargo, el resto del mecanismo de CSMA/CD no se modifica. La diferencia en el nivel de rendimiento es atribuido a cuan frecuentemente son transmitidas las tramas. El formato de la trama, la longitud, el control de errores, y la administración de información son prácticamente idénticas a las que se encuentran en 10BASE-T. Esto permite una mejora en el rendimiento utilizando tecnología familiar.

No obstante, hay algunos cambios en 100BASE-T entre los que se incluyen:

Funciones de control de errores adicionales

No hay soporte para ningún tipo de medio de cable coaxial.

Soporte para auto negociación. Esta es la técnica que permite que dispositivos 10BASE-T y 100BASE-T se reconozcan entre si y que automáticamente cambien a una tasa de transferencia aceptada por ambos.

Fast Ethernet especifica cuatro tipos de transceptores, 100BASE-T2, 100BASE-T4, 100BASE-TX, y 100BASE-FX. Los cuatro son similares con respecto a los requerimientos de componentes, modo de operación y topología. Todos operan dentro de las limitaciones de distancias de cableado especificadas por los estándares ANSI/TIA/EIA-568-A y ISO/IEC 11801 para cableado.

Tres de los tipos de transceptores, types—100BASE-T4, 100BASE-TX, y 100BASE-FX están definidos en el suplemento IEEE 802.3u publicado en 1995. 100BASE-T2 está definido en el suplemento IEEE 802.3y publicado en 1997.

100BASE-T4, 100BASE-TX, y 100BASE-FX son las versiones más ampliamente adoptadas de Fast Ethernet.

100BASE-T4

Los segmentos de tipo T4 operan sobre UTP categoría 3 o superior. Para permitir que se utilice UTP categoría 3, el esquema de señalamiento utiliza cuatro pares de cables. Los cuatro pares son utilizados en paralelo, lo que reduce el ancho de banda de señales requerido para cada par. Esto se traduce en requerimientos de circuitos para recuperación de datos más simples y un sistema más robusto.

100BASE-T2

En 1995, se formó el grupo de trabajo de la IEEE 802.3y para estudiar la posibilidad de transmitir 100Mb/s sobre dos pares de UTP categoría 3. En 1997 se finalizó el estándar 100BASE-T2.

El nuevo transceptor funciona sobre todos los tipos de medio UTP actualmente utilizados para 100BASE-T4 y 100BASE-TX. Si bien es posible alcanzar una tasa de datos de 100Mb/s sobre dos cables UTP categoría 3, esto es al costo de sofisticadas técnicas de señalamiento digital. Los transceptores de 100BASE-T2 requieren de la cancelación del nearend crosstalk (NEXT) y de ecualización digital adaptativa para realizar su función.

100BASE-X

El estándar 100BASE-FX engloba a 100BASE-TX y 100BASE-FX. Ambos utilizan los estándares para medios físicos desarrollados por ANSI para FDDI. El estándar X combina los estándares Ethernet y FDDI. Utiliza el método de control de acceso al medio CSMA/CD de Ethernet y el tipo de transceptor de FDDI.
100BASE-X contiene dos tipos de transceptores, par trenzado de cobre y fibra óptica multimodo. El Tipo de segmento TX opera sobre dos pares de par trenzado de grado para datos, es decir UTP categoría 5 o superior o STP-A 150 W. El tipo de segmento FX opera sobre dos fibras ópticas multimodo 62.5/125 μm.

100BASE-X no provee un mecanismo para de puente entre Ethernet y las redes FDDI.

La técnica de señalamiento en 100BASE-X transmite datos sobre dos vías de señales, una en cada dirección. Cada vía de señales provee una tasa transferencia de datos completa de 100Mb/s.

La arquitectura 100BASE-X preserva la naturaleza full duplex del canal de comunicación subyacente. Cualquier transceptor 100BASE-X puede ser usado para transmisiones full duplex.

CONMUTACION DE REDES

Redes conmutadas

La transmisión de datos entre dos sistemas de comunicación separados por largas distancias se realiza a través de una red de nodos intermedios. Este concepto que se utiliza en redes WAN también puede aplicarse a redes de menor dimensión dando redes LAN y MAN conmutadas.

A los nodos de conmutación no les concierne el contenido de los datos que se están transmitiendo, sino que tienen la función de prestar servicio de conmutación para trasladar los datos de un nodo al otro hasta alcanzar el destino final. Este tipo de redes se denomina redes de comunicación conmutadas. Los datos provenientes de una de las estaciones (computadoras, terminales, servidores o cualquier dispositivo de comunicación) entran a la red conmutada y se encaminan hasta la estación de destino conmutándolos de nodo en nodo.

Según los tipos de conexión que posean, se pueden distinguir dos tipos de nodos dentro de una red conmutada:

Nodos que solo se conectan con otros nodos. Su tarea es únicamente la conmutación interna de los datos. En el ejemplo los nodos de este tipos son el 2 el 4 y el 6.

Nodos que se conectan con otros nodos y con una o más estaciones. Estos nodos además de proveer conmutación interna de los datos dentro de la red de conmutación, se encargan de distribuir los datos desde y hacia las estaciones a las cuales están conectados. En el ejemplo los nodos de este tipos son el 1 el 3 y el 5 en la figura 7.

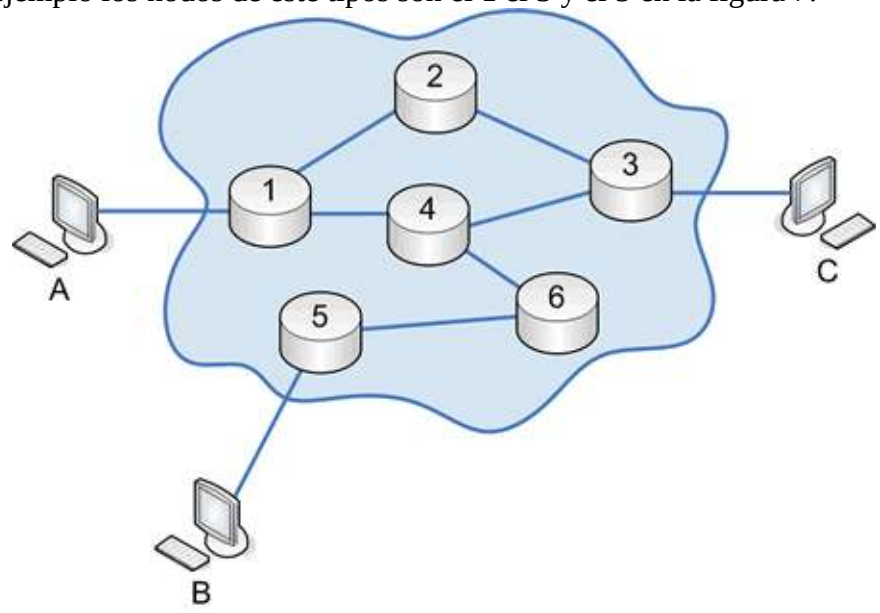


Figura 7 Nodos que se conectan con otros nodos y con una o más estaciones

La conmutación permite que todos los nodos que deseen establecer una comunicación no tengan que estar conectados por un enlace en forma directa. Por lo tanto normalmente la red no está totalmente conectada, es decir no todo par de nodos está conectado mediante un enlace directo. No obstante muchas veces es deseable poseer más de un camino posible a través de la red para entre cada par de estaciones ya que esto mejora la seguridad de la red.

En el ejemplo se puede observar que para comunicarse las estaciones A y C pueden establecerse varios caminos diferentes. Si se quiere enviar datos desde la estación A hasta la C se envían a través del nodo 1 luego hay dos posibilidades, una es a través del nodo 2 y luego pasando al nodo 3 y la otra posibilidad es atravesando por el nodo 4 y luego por el nodo 3 finalmente se llega a destino desde el nodo 3 a la estación C.

En las redes WAN se utilizan casi exclusivamente dos tecnologías de conmutación que se diferencian en la forma en que los nodos realizan la conmutación de la información entre los enlaces que forman el camino desde el origen hasta el destino. Estas son la conmutación de paquetes y conmutación de circuitos.

Conmutación de circuitos

Circuitos físicos

Los circuitos físicos son canales de comunicaciones a través de los cuales los usuarios finales que operan terminales y computadoras se comunican entre sí. A estos también se los llama canales, enlaces, líneas y troncales.

Circuitos virtuales

El termino circuito virtual se utiliza para describir el caso en el que un circuito es compartido por más de un usuario pero estos no tienen conocimiento del uso compartido del mismo. El hecho de compartir el circuito implica el uso de alguna técnica de multiplexación, generalmente multiplexación por frecuencia o por tiempo.

Redes de conmutación de circuitos

La comunicación entre dos estaciones utilizando conmutación de circuitos implica la existencia de un camino dedicado entre ambas estaciones. Dicho camino esta constituido por una serie de enlaces entre algunos de los nodos que conforman la red. En cada enlace físico entre nodos, se utiliza un canal lógico para cada conexión. Esto se denomina circuitos virtuales y en un escenario ideal los usuarios del circuito no perciben ninguna diferencia con respecto a un circuito físico y no tienen conocimiento del uso compartido de circuitos físicos.

Una comunicación mediante circuitos conmutados posee tres etapas bien definidas

Establecimiento del circuito

Cuando un usuario quiere obtener servicios de red para establecer una comunicación se deberá establecer un circuito entre la estación de origen y la de destino. En esta etapa dependiendo de la tecnología utilizada se pueden establecer la capacidad del canal y el tipo de servicio.

Transferencia de datos

Una vez que se ha establecido un circuito puede comenzar la transmisión de información. Dependiendo del tipo de redes y del tipo de servicio la transmisión será digital o analógica y el sentido de la misma será unidireccional o full duplex.

Cierre del circuito

Una vez que se ha transmitido todos los datos, una de las estaciones comienza la terminación de la sesión y la desconexión del circuito. Una vez liberado los recursos utilizados por el circuito pueden ser usados por otra comunicación.

En una conmutación por circuitos, la capacidad del canal se reserva al establecer el circuito y se mantiene durante el tiempo que dure la conexión, incluso si no se transmiten datos.

Un caso típico de utilización de conmutación de circuitos es el sistema telefónico original. En donde al realizar una llamada se establecía un circuito, el cual se mantenía hasta la finalización de la comunicación.

VLAN

Concepto

Una red de área local (LAN) esta definida como una red de computadoras dentro de un área geográficamente acotada como puede ser una empresa o una corporación. Uno de los problemas que nos encontramos es el de no poder tener una confidencialidad entre usuarios de la LAN como pueden ser los directivos de la misma, también estando todas las estaciones de trabajo en un mismo dominio de colisión el ancho de banda de la misma no era aprovechado correctamente. La solución a este problema era la división de la LAN en segmentos físicos los cuales fueran independientes entre si, dando como desventaja la imposibilidad de comunicación entre las LANs para algunos de los usuarios de la misma.
La necesidad de confidencialidad como así el mejor aprovechamiento del ancho de banda disponible dentro de la corporación ha llevado a la creación y crecimiento de las VLAN.
Una VLAN se encuentra conformada por un conjunto de dispositivos de red interconectados (hubs, bridges, switches o estaciones de trabajo) la definimos como una subred definida por software y es considerada como un dominio de broadcast que pueden estar en el mismo medio físico o bien puede estar sus integrantes ubicados en distintos sectores de la corporación (Figura 8).

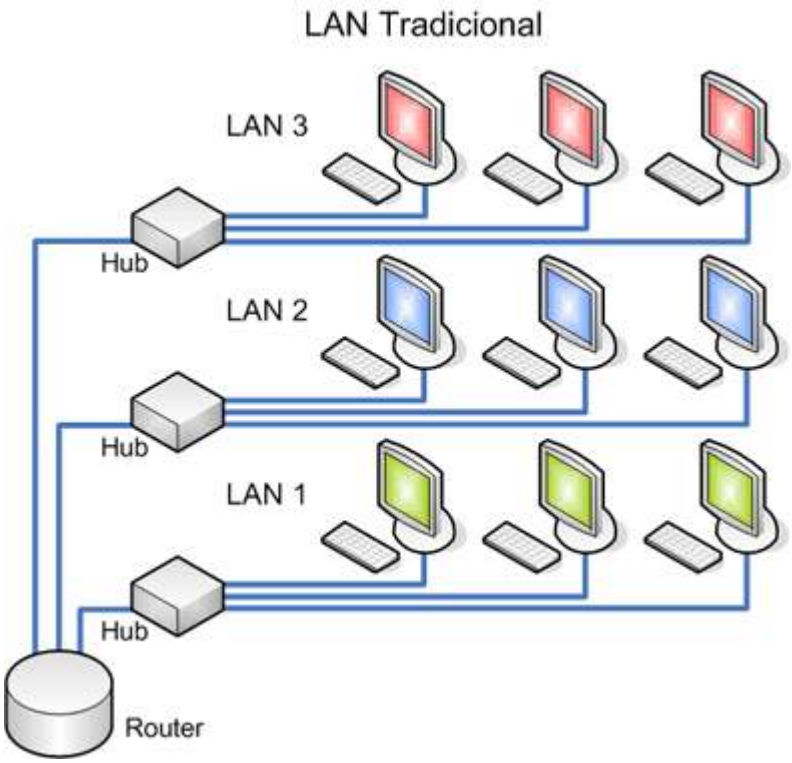


Figura 8 LAN tradicional

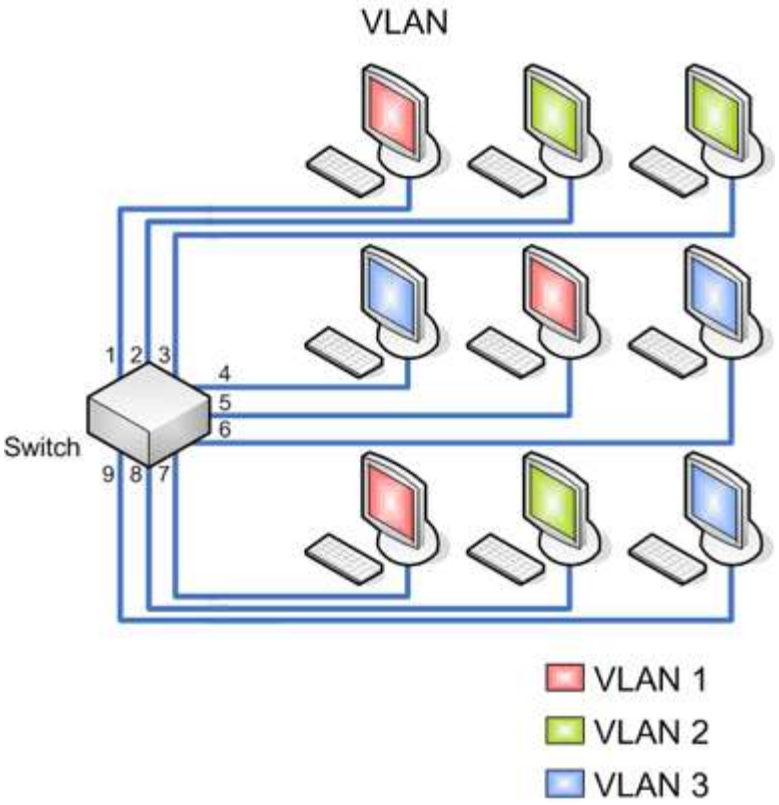


Figura 8 Ejemplo de VLAN

La tecnología de las VLAN se basa en el empleo de switches, en lugar de hubs, de tal manera que esto permite un control mas inteligente del tráfico de la red, ya que este dispositivo trabaja a nivel de la capa 2 del modelo OSI y es capaz de aislar el tráfico, para que de esta manera la eficiencia de la red entera se incremente. Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, se logra el incremento del ancho de banda en dicho grupo de usuarios.

Segmentación

Con los switches se crean pequeños dominios, llamados segmentos, conectando un pequeño hub de grupo de trabajo a un puerto de switch o bien se aplica micro segmentación la cual se realiza conectando cada estación de trabajo y cada servidor directamente a puertos de switch teniendo una conexión dedicada dentro de la red, con lo que se consigue aumentar considerablemente el ancho de banda a disposición de cada usuario.

Una de las ventajas que se pueden notar en las VLAN es la reducción en el trafico de la red ya que solo se transmiten los paquetes a los dispositivos que estén incluidos dentro del dominio de cada VLAN, una mejor utilización del ancho de banda y confidencialidad respecto a personas ajenas a la VLAN, alta performance, reducción de latencia, facilidad para armar grupos de trabajo.

La comunicación que se hace entre switches para interconectar VLAN utiliza un proceso llamado Trunking. El protocolo VLAN Trunk Protocol (VTP) es el que se utiliza para esta conexión, el VTP puede ser utilizado en todas las líneas de conexión incluyendo ISL, IEEE 810.10. IEEE 810.1Q y ATM LANE.

Tipos de VLAN

VLAN de puerto central

Es en la que todos los nodos de una VLAN se conectan al mismo puerto del switch.

VLAN Estáticas

Los puertos del switch están ya preasignados a las estaciones de trabajo.

Por puerto

Se configura por una cantidad "n" de puertos en el cual podemos indicar que puertos pertenecen a cada VLAN. Para la Figura 9 tendríamos en el Switch 9 puertos de los cuales el 1,5 y 7 pertenecen a la VLAN 1; el 2, 3 y 8 a la VLAN 2 y los puertos 4, 6 y 9 a la VLAN 3 como la tabla lo indica (Figura 9).

Puerto	VLAN
1	1
2	2
3	2
4	3
5	1
6	3
7	1
8	2
9	3

Figura 9 Asignación de puertos a VLAN

Ventajas:

Facilidad de movimientos y cambios.

Micro segmentación y reducción del dominio de broadcast.

Multiprotocolo: La definición de la VLAN es independiente del o los protocolos utilizados, no existen limitaciones en cuanto a los protocolos utilizados, incluso permitiendo el uso de protocolos dinámicos.

Desventajas:

Administración: Un movimiento en las estaciones de trabajo hace necesaria la reconfiguración del puerto del switch al que esta conectado el usuario. Esto se puede facilitar combinando con mecanismos de LAN Dinámicas.

Por dirección MAC

Los miembros de la VLAN están especificados en una tabla por su dirección MAC (Figura 10).

MAC	VLAN
12.15.89.bb.1d.aa	1
12.15.89.bb.1d.aa	2
aa.15.89.b2.15.aa	2
1d.15.89.6b.6d.ca	2
12.aa.cc.bb.1d.aa	1

Figura 10 VLAN asignadas por MAC

Ventajas:

Facilidad de movimientos: No es necesario en caso de que una terminal de trabajo cambie de lugar la reconfiguración del switch.

Multiprotocolo.

Se pueden tener miembros en múltiples VLAN.

Desventajas:

Problemas de rendimiento y control de Broadcast: el tráfico de paquetes de tipo Multicast y Broadcast se propagan por todas las VLAN.

Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo. También se puede emplear soluciones de DVLAN.

Por protocolo

Asigna a un protocolo una VLAN. El switch se encarga de dependiendo el protocolo por el cual venga la trama derivarlo a la VLAN correspondiente (Figura 11).

Protocolo	VLAN
IP	1
IPX	2

IPX	2
IPX	2
IP	1

Figura 11 Asignación de VLAN por protocolo

Ventajas:

Segmentación por protocolo.

Asignación dinámica.

Desventajas

Problemas de rendimiento y control de Broadcast: Por las búsquedas en tablas de pertenencia se pierde rendimiento en la VLAN.

No soporta protocolos de nivel 2 ni dinámicos.

Por direcciones IP

Esta basado en el encabezado de la capa 3 del modelo OSI. Las direcciones IP a los servidores de VLAN configurados. No actúa como router sino para hacer un mapeo de que direcciones IP están autorizadas a entrar en la red VLAN. No realiza otros procesos con la dirección IP.

Ventajas:

Facilidad en los cambios de estaciones de trabajo: Cada estación de trabajo al tener asignada una dirección IP en forma estática no es necesario reconfigurar el switch.

Desventajas:

El tamaño de los paquetes enviados es menor que en el caso de utilizar direcciones MAC.

Perdida de tiempo en la lectura de las tablas.

Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo.

Por nombre de usuario

Se basan en la autenticación del usuario y no por las direcciones MAC de los dispositivos.

Ventajas:

Facilidad de movimiento de los integrantes de la VLAN.

Multiprotocolo.

Desventajas:

En corporaciones muy dinámicas la administración de las tablas de usuarios.

VLAN Dinámicas (DVLAN)

Las VLAN dinámicas son puertos del switch que automáticamente determinan a que VLAN pertenece cada puesto de trabajo. El funcionamiento de estas VLAN se basa en las direcciones MAC, direcciones lógicas o protocolos utilizados. Cuando un puesto de trabajo pide autorización para conectarse a la VLAN el switch chequea la dirección MAC ingresada previamente por el administrador en la base de datos de las mismas y automáticamente se configura el puerto al cual corresponde por la configuración de la VLAN. El mayor beneficio de las DVLAN es el menor trabajo de administración dentro del armario de comunicaciones cuando se cambian de lugar las estaciones de trabajo o se agregan y también notificación centralizada cuando un usuario desconocido pretende ingresar en la red.

Capa de Red: ELAN o Redes LAN Emuladas

Si bien el concepto de VLAN se creo para las redes LAN, la necesidad llevo a ampliar los horizontes con el crecimiento de las redes ATM. Para los administradores de las VLAN se crearon una serie de estándares para simular en una red ATM una VLAN. Por un lado una tecnología orientada a no conexión, qué es el caso de las LANS y por el otro una orientada a conexión como en el caso de ATM. En el caso de las LANS se trabaja con direcciones MAC, mientras en ATM se usan direcciones ATM y se establecen circuitos virtuales permanentes, por esta razón se requiere hacer cambios de direcciones MAC a ATM.

Ventajas:

Facilidad de administración.

Facilidad de movimientos y cambios.

Multiprotocolo.

Desventajas:

Aplicable solo a Ethernet y Token Ring.

No explota la calidad de Calidad de servicio (QoS) de ATM.

Tipos de conexión y procesamiento de paquetes

Tipos de conexión

Los dispositivos en una VLAN pueden estar conectados de tres formas diferentes, dependiendo de que las conexiones sean con VLAN controlados o VLAN no controlados. Los switches que transmiten los paquetes de la VLAN se dicen que son VLAN-controlados, pero las estaciones de trabajo o impresoras pueden no serlo. Solo los dispositivos VLAN-controlados saben que son miembros de una VLAN y trabajan bajo el formato de una VLAN.

Enlace troncal

Un enlace troncal conecta a dos dispositivos de LAN que sean VLAN-controlados como por ejemplo dos switches que tengan la función de ruteo (Figura 12). El paquete es transmitido a través del enlace es explícitamente etiquetada con el encabezado de VLAN. El router hará llegar al destino el paquete etiquetado haciendo la consulta a la base de datos.

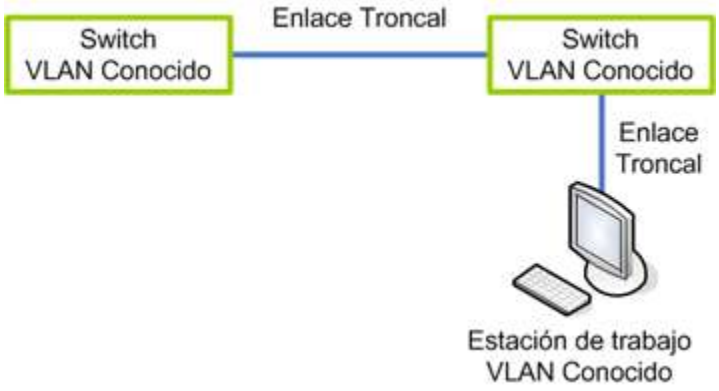


Figura 12 Enlace troncal

Enlace de acceso

Un enlace de acceso comunica un dispositivo VLAN-controlado con uno que no lo sea (Figura 13). Los paquetes son transmitidos por el enlace sin incluir el encabezado de VLAN, pero son implícitamente etiquetados por el dispositivo ruteador de la VLAN.

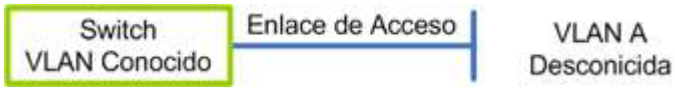


Figura 13 Enlace de acceso

Enlace híbrido

Conecta un dispositivo VLAN-controlado con un dispositivo que no lo sea (Figura 14). Para una VLAN específica los paquetes transmitidos por el enlace que pueden ser para la misma LAN todos etiquetados o para otras VLANs no etiquetados.

Figura 14 VLAN controlado con un dispositivo que no lo sea

Procesamiento de paquetes

Un bridge recibe los paquetes y determina a que VLAN pertenecen en base a los datos que estén explícitos o implícitos en la etiqueta. En el etiquetado explícito los datos de mismo se agregan al paquete. El bridge conserva los datos de los usuarios de la VLAN para determinar que paquetes se deben enviar.

Filtrado por base de datos

La información de los miembros de la VLAN está almacenada como ya se ha mencionado en una base de datos. El filtrado por base de datos consiste en algunos de los siguientes accesos.

Acceso estático

La información es agregada, modificada o eliminada solo por el administrador.

Los accesos no son automáticamente eliminados luego de un tiempo, pero si puede ser eliminado explícitamente por el administrador. Hay dos tipos de accesos estáticos:

Registro de accesos: Se especifica a que puerto los paquetes deben ser enviados, si debe ser enviado a una dirección MAC específica, la dirección de un grupo y en que VLAN específica debe ser reenviado o eliminado, o debe continuar la entrada dinámica.

Registro de grupo: Especifica si los paquetes que deben ser mandados a una VLAN especifica deben ser etiquetados o no etiquetados y que puertos están registrados para cada VLAN.

Accesos dinámicos

Los accesos dinámicos son memorizados por el bridge y no creados o actualizados por el administrador. El proceso de memorización controla los puertos para cada paquete, con la dirección fuente y la identificación de la VLAN, es recibido y actualizado el filtro de la base de datos. El acceso es actualizado solo si todas las condiciones siguientes son satisfechas:

Este puerto permite la memorización

La dirección origen es una estación de trabajo y no un grupo de direcciones
Si el espacio esta disponible en la base de datos

Los accesos son eliminados de la base de datos en base al tiempo que están inactivos, luego de un cierto tiempo especificado por el administrador, los accesos son automáticamente reconfigurados por el filtrado de la base de datos si la topografía de la red cambia. Hay tres tipos de accesos dinámicos.

Registro de acceso: Cuando los paquetes deben ser enviados a una dirección MAC específica y hacia una cierta VLAN debe ser enviada o eliminada.

Registro de grupo: Cuando se indica para cada puerto los paquetes deben ser enviados a un grupo de direcciones MAC y una cierta VLAN en la que deba ser filtrada o descargada. Estas entradas son agregadas y borradas usando Group Multicast Registration Protocol (GRMP). Estos multicast mencionados son enviados dentro de una

VLAN en particular sin afectar las otras VLAN.

Registro de entradas dinámico: Se especifica que puertos están registrados para una VLAN específica. Los accesos a la VLAN son agregados y borrados utilizando el protocolo de Registración de VLAN GARP (GVRP).

El GVRP es utilizado no solo para la actualización de entradas dinámicas, también cumplen la función de transmitir los paquetes hacia otros bridges.

Para que la VLAN envíe la información al destino correcto, todos los bridges en la VLAN deben contener la misma información en sus respectivas bases de datos de filtrado. GVRP permite estaciones de trabajo VLAN conocidas y bridges emite y revoca miembros de la VLAN. Los bridges VLAN conocidos registra y propaga los miembros de la VLAN a todos los puertos la topología de la VLAN. La topología activa de una red es determinada cuando los bridges se conectan o bien cuando un cambio en la topología activa es detectado.

La topología activa de la red es determinada utilizando el algoritmo de Spaning Tree previendo la formación de ciclos en la red por puertos desconectados. Una vez designada la topografía activa de la red, los bridges determinan la topología en particular para cada VLAN. Siempre la topología de una VLAN es un subconjunto de la topografía activa de la red.

Etiquetado

Cuando los paquetes son enviados a través de la red, se necesitará una forma de indicar a la VLAN pertenece, para que el bridge pueda reenviar los paquetes solo hacia los puertos que pertenecen a esa VLAN, en cambio los puertos de salida hacen esto normalmente. La información es agregada al paquete como un encabezado. Además el encabezado:

Permite especificar la información respecto de la prioridad del usuario.

Permite información de control de la ruteo.

Indica el formato de la dirección MAC.

Los paquetes que tienen el encabezado agregado son llamados paquetes etiquetados. Los paquetes etiquetados llevan la información de la VLAN a través de la red.

Los paquetes etiquetados que circulan por el enlace troncal y el híbrido contienen el encabezado.

El encabezado de VLAN consta de los siguientes campos en la figura 15:

TPID	Prioridad Usuario	CFI	Id VLAN
16 bits	3 bits	1 bit	12 bits

Figura 15 Encabezado de VLAN

TPID: Identificador de protocolo.

Prioridad Usuario: Brinda hasta 8 niveles de prioridad de los usuarios.

CFI: Indicador de otros paquetes desconocidos para la VLAN.

Id VLAN: Identificador a de la VLAN a la que pertenece el paquete.

Paquete ethernet

El encabezado de VLAN descrito se inserta en el encabezado correspondiente al protocolo con que se trabaje, por ejemplo en paquetes ethernet con lo cual el tamaño del paquete se incrementa en 4 Bytes.

Trama ethernet estándar:

Preambulo/IDM	DD	DO	Largo/Tipo	Datos/Relleno	CRC
1 Byte	6 Bytes	6 Bytes	2 Bytes	42-1500 Bytes	4 Bytes

Figura 16 Trama Ethernet estándar

Preámbulo/IDM: Patrón de bits para sincronización de los relojes y bit de inicio de paquete.

DD: Dirección destino.

DO: Dirección origen.

VLAN Enc: Encabezado de VLAN.

Largo/Tipo: Indica el largo de los datos.

Datos/Relleno: Datos que transporta el paquete, en caso de no hacer transporte de datos se utiliza un relleno de 42 bytes.

CRC: Control de redundancia cíclica.

Trama con encabezado VLAN

Preambulo/IDM	DD	DO	VLAN Enc.	Largo/Tipo	Datos/Relleno	CRC
1 Byte	6 Bytes	6 Bytes	4 Bytes	2 Bytes	42-1500 Bytes	4 Bytes

Figura 17 Trama con encabezado VLAN

Notamos la incorporación a la trama del encabezado de VLAN el cual consta de los siguientes campos:

Id Protocolo: Identificador del encabezado VLAN (0x8100).

Prioridad usuario: Indica la prioridad de la transmisión de los datos del usuario dentro de la VLAN (0-7).

Id Protocolo	Prioridad Usuario	CFI	Id VLAN
2 Bytes	3 Bits	1 Bit	12 Bytes

Figura 18 Prioridad de usuario

CFI: Indica si la dirección MAC esta en forma canónica.

Id VLAN: Identificador de la VLAN valor comprendido entre 0 y 4095

Paquete Token Ring y FDDI

Preambulo	DD	DO	RIF	VLAN Enc.	Largo/Tipo	Datos	PAD	FCS
1 Byte	6 Bytes	6 Bytes	0-30 Bytes	4 Bytes	2 Bytes	46-1500 Bytes		4 Bytes

Figura 19 Paquete Token Ring y FDDI

Preámbulo: Patrón de bits para sincronización de los relojes y bit de inicio de paquete, los 7 primeros se encargan de la sincronización y el octavo es el delimitador..

DD: Dirección destino.

DO: Dirección origen.

VLAN Enc: Encabezado de VLAN, idéntico al encabezado visto anteriormente.

RIF: Contiene información de ruteo.

Largo/Tipo: Indica el largo de los datos o el tipo de paquete del cual se trata..

Datos/PAD: Datos que transporta el paquete, en caso de no hacer transporte de datos se utiliza un relleno de 42 bytes.

FCS: Chequeo de paquete.

ESTADO ACTUAL

Hay diferentes departamentos que componen imagenología, los cuales están conectados entre sí: Tomografía, Resonancia Magnética, Ultrasonido, Mastografía, Cuarto Azul y Estaciones de diagnóstico que incluyen equipos muy diversos, diferentes marcas, diferentes funciones, diferentes modelos, pero con un mismo protocolo de comunicación llamado DICOM (Digital Imaging and Communications in Medicine). Éste protocolo se basa en TCP/IP para transmitir y recibir imágenes médicas y datos relacionados en una red. En el anexo 1 de la página 64 se muestra la imagen de la red actual del Hospital.

El estado actual de la red en el Hospital General de México en el área de imagenología es una red plana donde todos los equipos están interconectados sin administración alguna en un mismo switch. Esto provoca un bajo rendimiento en la transmisión y recepción de los datos entre los diversos equipos de la red. Para ilustrarlo mejor se realizó una simulación que se encuentra en el anexo 2 en la página 65

En las características actuales de esta red encontramos que las direcciones ip de los host de cada área se encuentran en el mismo dominio 200.15.80.XX. Como se menciono anteriormente esto se debe a que solamente se fueron anexando las ip de los host que se iban sumando a la red existente; lo que ocasionó los problemas ya mencionados. Esto se especifica en la siguiente tabla

Direcciones ip actuales en el switch 1

Tomografía

Estación de diagnóstico Siemens	200.15.80.10/24	Puerto	0/24
Tomógrafo Siemens	200.15.80.11/24	Puerto	0/2
Interfase Kodak Tomógrafo Toshiba	200.15.80.12/24	Puerto	0/3
Impresora laser Kodak	200.15.80.13/24	Puerto	0/4

Resonancia Magnética

Resonancia Magnética GE	200.15.80.20/24	Puerto	0/5
Impresora laser Kodak	200.15.80.21/24	Puerto	0/6
Impresora Térmica Kodak	200.15.80.22/24	Puerto	0/7

Ultrasonido

Ultrasonido Siemens	200.15.80.30/24	Puerto	0/8
Ultrasonido Siemens	200.15.80.31/24	Puerto	0/9
Ultrasonido Siemens	200.15.80.32/24	Puerto	0/10
Ultrasonido Siemens	200.15.80.33/24	Puerto	0/11
Impresora laser Kodak	200.15.80.34/24	Puerto	0/12

Mastografía			
Digitalizador Kodak	200.15.80.40/24	Puerto	0/13
Impresora laser Kodak	200.15.80.41/24	Puerto	0/14
Cuarto Azul			
Digitalizador Kodak	200.15.80.50/24	Puerto	0/15
Digitalizador Kodak	200.15.80.51/24	Puerto	0/16
Impresora laser Kodak	200.15.80.52/24	Puerto	0/17
Impresora laser Kodak	200.15.80.53/24	Puerto	0/18
Enlace de captura Kodak	200.15.80.54/24	Puerto	0/19
Panel Remoto Kodak	200.15.80.55/24	Puerto	0/20
Panel Remoto Kodak	200.15.80.56/24	Puerto	0/21
Panel Remoto Kodak	200.15.80.57/24	Puerto	0/22
Jefatura de imagenología			
Estación de diagnóstico	200.15.80.60/24	Puerto	0/23
Direcciones ip actuales en el switch 2			
Hemodinamia			
Interfase Kodak Hemodinamia GE	200.15.80.70/24	Puerto	0/2
Medicina Nuclear			
Sistema Medicina Nuclear	200.15.80.80/24	Puerto	0/3

ANÁLISIS DEL PROBLEMA

La tecnología en los hospitales ha evolucionando de forma acelerada en los últimos años. Esto implica que los equipos meramente análogos han dejado de ser útiles y en pocos años ha empezado una revolución digital. En muchos de estos casos este cambio se realiza de forma desordenada y en muchos hospitales se adquieren equipos de última tecnología sin pensar en la integración de análogo con digital y las ventajas que se pueden llegar a obtener si se les acopla adecuadamente. El caso del Hospital General de México es uno de estos, pues ha adquirido en sus diversas áreas de imagenología equipos con protocolos de comunicación muy actuales. Sin embargo existen muchos problemas de comunicación entre ellos y muchas veces hace añorar al usuario los equipos análogos anteriores que no presentaban problema, pues estos no dependían del enlace de todos los equipos.

A continuación se presenta una explicación de las áreas de imagenología que presentan este caso y los host que contienen cada uno y que se tienen forzosamente que intercomunicar entre sí.

Tomografía

Cuenta con una estación de trabajo Siemens, un tomógrafo Siemens, un tomógrafo Toshiba conectado a una interfase Kodak. Todos estos equipos tienen comunicación DICOM.

Tanto la estación de trabajo Siemens y el tomógrafo Siemens hacen alrededor de 24 estudios por día, cada estudio consta de 22 imágenes y tiene un tamaño de 11 Mb.

El tomógrafo Toshiba tiene 10 estudios por día con 22 imágenes cada estudio y el tamaño es de 11 Mb. Ambos equipos trabajan los 7 días a la semana incluyendo tres turnos.

Resonancia Magnética

El área cuenta con un equipo de resonancia magnética, una impresora laser Kodak y una impresora térmica Kodak. La resonancia magnética hace 14 estudios al día con 41 imágenes por estudio y cada estudio en promedio es de 20.5 Mb, trabaja 5 días a la semana.

Ultrasonido

Aquí hay cuatro salas cada una con un equipo de ultrasonido siemens y una impresora laser Kodak. En las cuatro salas se realizan 80 estudios al día con 11 imágenes cada uno y cada estudio tiene en promedio 5.5 Mb los 7 días de la semana.

Mastografía

En el lugar encontramos un digitalizador Kodak y una impresora laser Kodak

El digitalizador hace un promedio de 20 estudios al día con cuatro imágenes por estudio con un tamaño de cada estudio de 200 Mb y trabaja 5 días a la semana.

Cuarto Azul

Los equipos en esta área son: dos digitalizadores Kodak, dos impresoras laser Kodak, tres paneles remotos y un Capture Link.

Aquí realizan 250 estudios al día con dos imágenes por estudio y su tamaño es de 20 Mb, trabaja los 7 días de la semana y 24 horas al día.

El Capture Link es un dispositivo que mediante software hace transparente la información y las imágenes en todos los dispositivos conectados a él como los paneles remotos y los digitalizadores de imagen, cabe mencionar que trabaja 24 horas al día y los 7 días de la semana, de no ser así el flujo de trabajo se interrumpe considerablemente

Estaciones de diagnóstico

Solo hay una estación de diagnóstico en la oficina del jefe de imagenología.

Salas de Rayos X

En las salas de rayos x hay tres equipos más que también tienen comunicación DICOM.

Hemodinamia

Esta hemodinamia se enlaza por medio de una interfase Kodak, genera 10 estudios por día con 22 imágenes cada estudio y el tamaño de éste es de 11 Mb.

Medicina Nuclear

Consta de un sistema de medicina nuclear compatible con DICOM realizando 11 estudios por día con 22 imágenes cada estudio y el tamaño del estudio es de 10 Mb.

Entre los problemas más comunes en estas áreas son la falta de comunicación entre modalidades (equipos de ultrasonido, tomógrafo, resonancia, etc.) e impresora, lo que ocasiona perdidas de estudios o lentitud en el flujo de trabajo al tener que direccionar a otra impresora.

También hay problemas de visualización de estudios entre modalidades, es decir eventualmente, los estudios que debiesen verse simultáneamente en dos o más equipos de visualización de imágenes como CR y Estaciones de trabajo no permiten esta capacidad. Además hay pérdida de comunicación con el servidor (capture link) entre CRs.

Al trabajar con las impresoras, los CRs y las estaciones de trabajo, nos damos cuenta que estos trabajan la mayoría de las veces adecuadamente. Se encuentran, considerablemente, problemas con la red del área pues en muchos casos a pesar de estar todo bien conectado físicamente, no existe comunicación alguna.

Verificando la instalación de la red en general encontramos un cableado estructurado aceptable dentro de los estándares, incluyendo un site con 2 switches pero sin ninguna configuración. Lo que debido al gran ancho de banda requerido por las modalidades resulta obsoleto para la gran cantidad de datos que aquí se manejan.

Al realizar ping entre los host de la simulación 1, la cual representa el estado actual de la red, nos damos cuenta que los dominios de colisión se transmiten en toda la red, esto por estar todos los host en el mismo dominio.

SOLUCIÓN

La solución que se propone es la siguiente:

Al no contar este site con ninguna administración y debido al gran ancho de banda requerido por la transmisión de imágenes médicas se opta por segmentar la red en ocho redes virtuales que corresponden a cada sección de imagenología (tomografía, resonancia magnética, ultrasonido, mastografía, cuarto azul, jefatura de imagenología, hemodinamia y medicina nuclear).

Entre las características por las cuales se opto por la utilización de VLAN son la segmentación, flexibilidad y seguridad que estas proveen, ya que al implementar las redes virtuales se obtiene una mejor administración a un bajo costo y sin necesidad de aditamentos especiales. Además se comportan como bridges separados y se puede expandir a cuantos switches sean necesarios. Al segmentar el dominio del broadcast se realiza una mejora considerable en la transmisión de datos

Ethernet tiene la capacidad para crear redes de área local virtuales o VLAN. Una VLAN es un agrupamiento lógico de estaciones y dispositivos de red. Las VLAN se pueden agrupar por función laboral o departamento, sin importar la ubicación física de los usuarios. El tráfico entre las VLAN está restringido. Los switches y puentes envían tráfico unicast, multicast y broadcast sólo en segmentos de LAN que atienden a la VLAN a la que pertenece el tráfico. Así pues los dispositivos en la VLAN sólo se comunican con los dispositivos que están en la misma VLAN y los routers suministran la conectividad entre diferentes VLAN

Las VLAN mejoran el desempeño general de la red agrupando a los usuarios y los recursos de forma lógica.

Una VLAN es una agrupación lógica de estaciones, servicios y dispositivos de red que no se limita a un segmento de LAN físico.

Las VLAN facilitan la administración de grupos lógicos de estaciones y servidores que se pueden comunicar como si estuviesen en el mismo segmento físico de LAN. También facilitan la administración de mudanzas, adiciones y cambios en los miembros de esos grupos.

Las VLAN segmentan de manera lógica las redes conmutadas según las funciones laborales, departamentos o equipos de proyectos, sin importar la ubicación física de los usuarios o las conexiones físicas a la red. Todas las estaciones de trabajo y servidores utilizados por un grupo de trabajo en particular comparten la misma VLAN, sin importar la conexión física o la ubicación.

Las VLAN se crean para brindar servicios de segmentación proporcionados tradicionalmente por routers físicos en las configuraciones de LAN. Las VLAN se ocupan de la escalabilidad, seguridad y gestión de red. Los routers en las topologías de VLAN proporcionan filtrado de broadcast, seguridad y gestión de flujo de tráfico. Los switches no puentean ningún tráfico entre VLAN, dado que esto viola la integridad del dominio de broadcast de las VLAN. El tráfico sólo debe enrutarse entre VLAN.

La implementación de VLAN en un switch hace que se produzcan ciertas acciones:

El switch mantiene una tabla de puenteo separada para cada VLAN.

Si la trama entra en un puerto en la VLAN 1, el switch busca la tabla de puenteo para la VLAN 1.

Cuando se recibe la trama, el switch agrega la dirección origen a la tabla de puenteo si es desconocida en el momento.

Se verifica el destino para que se pueda tomar una decisión de envío.

Para aprender y enviar se realiza la búsqueda en la tabla de direcciones para esa VLAN solamente.

Una VLAN se compone de una red conmutada que se encuentra lógicamente segmentada. Cada puerto de switch se puede asignar a una VLAN. Los puertos asignados a la misma VLAN comparten broadcasts. Los puertos que no pertenecen a esa VLAN no comparten esos broadcasts. Esto mejora el desempeño de la red porque se reducen los broadcasts innecesarios. Las VLAN de asociación estática se denominan VLAN de asociación de puerto central y basadas en puerto. Cuando un dispositivo entra a la red, da por sentado automáticamente que la VLAN está asociada con el puerto al que se conecta.

En la asociación de VLAN de puerto central basada en puerto, el puerto se asigna a una asociación de VLAN específica independiente del usuario o sistema conectado al puerto. Al utilizar este método de asociación, todos los usuarios del mismo puerto deben estar en la misma VLAN. Un solo usuario, o varios usuarios pueden estar conectados a un puerto y no darse nunca cuenta de que existe una VLAN. Este método es fácil de manejar porque no se requieren tablas de búsqueda complejas para la segmentación de VLAN.

La cantidad de VLAN en un switch varía según diversos factores:

Patrones de tráfico

Tipos de aplicaciones

Necesidades de administración de red

Aspectos comunes del grupo

El esquema de direccionamiento IP es otra consideración importante al definir la cantidad de VLAN en un switch.

A medida que los paquetes son recibidos por el switch desde cualquier dispositivo de estación final conectado, se agrega un identificador único de paquetes dentro de cada encabezado. Esta información de encabezado designa la asociación de VLAN de cada paquete. El paquete se envía entonces a los switches o routers correspondientes sobre la base del identificador de VLAN y la dirección MAC. Al alcanzar el nodo destino, el ID de VLAN es eliminado del paquete por el switch adyacente y es enviado al dispositivo conectado. El etiquetado de paquetes brinda un mecanismo para controlar el flujo de broadcasts y aplicaciones, mientras que no interfiere con la red y las aplicaciones.

Las VLAN estáticas son puertos en un switch que se asignan manualmente a una VLAN. Esto se hace con una aplicación de administración de VLAN o configurándose directamente en el switch mediante la CLI. Estos puertos mantienen su configuración de VLAN asignada hasta que se cambien manualmente. Este tipo de VLAN funciona bien en las redes que tienen requisitos específicos:

Todos los movimientos son controlados y gestionados.

Existe un software sólido de gestión de VLAN para configurar los puertos.

El gasto adicional requerido para mantener direcciones MAC de estación final y tablas de filtrado personalizadas no es aceptable.

La creación de una VLAN en un switch es una tarea muy directa y simple. Si se usa un switch basado en comandos del IOS, se puede usar el comando VLAN database en el modo EXEC privilegiado para entrar al modo de configuración de VLAN. También se puede configurar un nombre de VLAN, de ser necesario:

```
Switch#vlan database
Switch(vlan)#vlan vlan_number
Switch(vlan)#exit
```

Al salir, se aplica la VLAN al switch. El paso siguiente es asignar la VLAN a una o más interfaces:

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#switchport access vlan vlan_number
```

El comando que aparece a continuación se utiliza para eliminar una VLAN de un switch:

Switch#vlan database
Switch(vlan)#no vlan 300

Cuando se elimina una VLAN, todos los puertos asignados a esa VLAN quedan inactivos. Los puertos, sin embargo, quedan asociados a la VLAN eliminada hasta que se los asigna a una nueva VLAN.

Las siguientes reglas son aplicadas a las VLAN:

Una VLAN creada permanece sin usar hasta que se la asigna a puertos de switch.

Todos los puertos Ethernet son asignados a VLAN 1 por defecto.

Para asignar una nueva VLAN a un puerto éstos son los pasos:

Switch#configure terminal
Switch(config)#interface fastethernet 0/9
Switch(config-if)#switchport access vlan *vlan_number*
Switch(config-if)#exit
Switch(config)# exit

Y para poder visualizar la configuración de las VLAN se puede usar show vlan

Switch#show vlan

O también

Switch#show vlan brief

PLANEACIÓN

A continuación se dan los pasos seguidos para la realización de nuestro diseño, incluyendo una explicación. Tomando en cuenta que en el site se trabajará con 2 switches Cisco Catalyst 2950, por lo que se trabajara con el IOS de Cisco. El diseño propuesto de la red se muestra en el anexo 7 en la página 70 y para efectos de simulación utilizaremos el simulador Packet Tracer 4.11. El estado final de las VLAN se muestra diferenciado por colores en el anexo 8 en la página 71.

Generación de VLAN

En la primera etapa se nombran y configuran las nueve VLAN de las áreas de imagenología. Los comandos se muestran a continuación y se ejecutaron en la simulación 2. Este nombramiento será de vital importancia para el administrador de la red ya que esto nos permite ubicar fácilmente la VLAN con el área física respectiva.

Utilizando los comandos del IOS de CISCO, primero se debe entrar en modo privilegiado, utilizando:

Switch>enable

También se debe entrar al modo de configuración con el siguiente comando:

Switch#configure terminal

Enseguida se y por motivos administrativos se da nombre al switch con el comando:

switch(config)#hostname RX1

Para nombrar a las VLAN es necesario, entrar con el siguiente comando que nos sirve entre otras funciones para nombrar a las VLAN.

RX1#vlan database

Finalmente se nombran las VLAN con el comando que a continuación se muestra:

RX1(vlan)#vlan 2 name NOMBRE DE LA VLAN
VLAN 2 added:
Name: NOMBRE DE LA VLAN

La programación completa de la asignación de nombres a las VLAN se encuentra referida en el anexo 3 en la página 66.

Como segundo paso se dan de alta las IP de las 8 VLAN como se muestra a continuación. Esto se realiza solamente en el switch RX1

Vlan 2 200.15.81.254--- Tomografia
Vlan 3 200.15.82.254--- Resonancia Magnetica
Vlan 4 200.15.83.254--- Ultrasonido
Vlan 5 200.15.84.254--- Mastografia
Vlan 6 200.15.85.254--- Cuarto azul
Vlan 7 200.15.86.254--- Jefatura de Imagenologia
Vlan 8 200.15.87.254--- Hemodinamia
Vlan 9 200.15.88.254--- Medicina Nuclear

Para realizar la programación respectiva de esta etapa, se debe entrar en modo de configuración en el switch con el comando:

RX1#configure terminal

Después para poder asignar la IP se entra en el modo de configuración de interface de la VLAN especificando el número de la VLAN respectiva, con el comando:

RX1(config)#interface vlan 2

En este caso la VLAN en uso es la VLAN 2 que corresponde a la VLAN de TOMOGRAFIA.

Finalmente se asigna la IP y la submascara correspondiente a la VLAN con el comando:

RX1(config-if)#ip address 200.15.81.254 255.255.255.0

Es importante tener en cuenta que se debe salir de la fase de configuración de la interface de la VLAN en curso, antes de configurar la siguiente. Esto se realiza con el comando:

RX1(config-if)#exit

La programación detallada de esta etapa se explica en el anexo 4 en la página 66

Asignación de puertos a las VLAN creadas

En la tercera etapa del diseño, se asigna cada uno de los puertos del switch a los host de cada área. La programación de estas se muestra en el anexo 5 en la página 67. Utilizando los comandos del IOS ya mencionados, en total se utilizaran veinticinco puertos de los dos switch por lo que además quedaran puertos libres considerando un crecimiento futuro en el área.

En la cuarta etapa se cambian las IP a los host de cada área siguiendo la siguiente tabla:

Configuración en el switch RX1

Tomografía	Estación de diagnóstico Siemens	200.15.81.1/24	Puerto	0/24
	Tomógrafo Siemens	200.15.81.2/24	Puerto	0/2
	Interface Kodak Tomógrafo Toshiba	200.15.81.3/24	Puerto	0/3
	Impresora laser Kodak	200.15.81.4/24	Puerto	0/4
Resonancia Magnética	Resonancia Magnética GE	200.15.82.1/24	Puerto	0/5

	Impresora laser Kodak	200.15.82.2/24	Puerto	0/6
	Impresora Térmica Kodak	200.15.82.3/24	Puerto	0/7
Ultrasonido	Ultrasonido Siemens	200.15.83.1/24	Puerto	0/8
	Ultrasonido Siemens	200.15.83.2/24	Puerto	0/9
	Ultrasonido Siemens	200.15.83.3/24	Puerto	0/10
	Ultrasonido Siemens	200.15.83.4/24	Puerto	0/11
	Impresora laser Kodak	200.15.83.5/24	Puerto	0/12
Mastografía	Digitalizador Kodak	200.15.84.1/24	Puerto	0/13
	Impresora laser Kodak	200.15.84.2/24	Puerto	0/14
Cuarto Azul	Digitalizador Kodak	200.15.85.1/24	Puerto	0/15
	Digitalizador Kodak	200.15.85.2/24	Puerto	0/16
	Impresora laser Kodak	200.15.85.3/24	Puerto	0/17
	Impresora laser Kodak	200.15.85.4/24	Puerto	0/18
	Enlace de captura Kodak	200.15.85.5/24	Puerto	0/19
	Panel Remoto Kodak	200.15.85.6/24	Puerto	0/20
	Panel Remoto Kodak	200.15.85.7/24	Puerto	0/21
	Panel Remoto Kodak	200.15.85.8/24	Puerto	0/22
Jefatura de imagenología	Estación de diagnóstico	200.15.86.1/24	Puerto	0/23

Configuración en el switch RX2

Hemodinamia	Interface Kodak Hemodinamia GE	200.15.87.1/24	Puerto	0/2
Medicina Nuclear	Sistema Medicina Nuclear	200.15.88.1/24	Puerto	0/3

Realización de enlace troncal

En la quinta etapa se realiza el enlace entre los dos switch ya que estamos considerando un crecimiento de los equipos de cómputo del área de imagenología. Para realizar el enlace entre VLAN de los 2 diferentes switch se utiliza el protocolo 802.1q: conectar un cable cruzado del puerto 1 del switch RX1 al puerto 24 del switch RX2.

Para configurar este enlace se debe entrar al modo privilegiado con el comando

RX1>enable.

Después se entra en modo de configuración de la terminal con el comando:

RX1#configure terminal.

Para configurar el puerto en el que se va a realizar el entronque utilizamos:

RX1(config)#interface fastEthernet 0/1

Y para realizar el entronque se utiliza el comando:

RX1(config-if)#switchport mode trunk

Para realizar el enlace en el otro switch RX2 (cliente)

Igualmente se debe accesar en modo privilegiado, después en modo de configuración de interface pero esta vez en el puerto 24 esto se realiza con el comando:

RX2(config)#interface fastEthernet 0/24

Y también se utiliza el comando:

RX2(config-if)#switchport mode trunk

Para realizar el entronque, este se explica detalladamente en el anexo 6 en la página 69.

PRUEBAS

Se recurre al comando show vlan para poder apreciar la configuración de las VLAN en el switch tales como ip, nombres de las VLAN y puertos asignados a cada VLAN.

En RX1 se entra en modo privilegiado y se introduce el comando ya mencionado:

RX1>enable
RX1#show vlan

Por consiguiente el switch nos muestra una tabla de 4 columnas, que identifican el numero, el nombre, el estado y los puertos asignados a cada VLAN.

Así también esta tabla nos muestra 14 filas incluyendo entre ellas a cada una de las 10 VLAN creadas.

Por lo que podemos verificar que efectivamente y según lo programado:

- La VLAN 2 tiene asignado el nombre de TOMOGRAFIA y tiene asignados los puertos 0/2, 0/3, 0/4 y 0/24.

- La VLAN 3 tiene asignado el nombre de RM y tiene asignados los puertos 0/5, 0/6 y 0/7.

- La VLAN 4 tiene asignado el nombre de US y tiene asignados los puertos 0/8, 0/9, 0/10, 0/11 y 0/12.

- La VLAN 5 tiene asignado el nombre de MASTOGRAFIA y tiene asignados los puertos 0/13 y 0/14.

- La VLAN 6 tiene asignado el nombre de CAZUL y tiene asignados los puertos 0/15, 0/16, 0/17, 0/18, 0/19, 0/20, 0/21 y 0/22.

- La VLAN 7 tiene asignado el nombre de JEFATURA y tiene asignado el puerto 0/23.

- También se ejecuta este comando en RX2 por lo que se comprueba que efectivamente el puerto 0/1 esta asignado a la VLAN 7, y que los puertos 0/2 y 0/3 están asignados respectivamente a las VLAN 8 y VLAN 9.

Estas tablas se muestran en el anexo 9 y 10 en las páginas 72 y 73 respectivamente.

Después de verificar la configuración en el switch, se comprueba la conexión entre los switch RX1 y RX2

Para tal efecto se realiza ping entre los host “VA Kodak” conectado a RX1 y “JEFATURA” conectado a RX2 obteniendo los siguientes resultados:

```
Reply from 200.15.86.2: bytes=32 time=160ms TTL=128
Reply from 200.15.86.2: bytes=32 time=73ms TTL=128
Reply from 200.15.86.2: bytes=32 time=83ms TTL=128
Reply from 200.15.86.2: bytes=32 time=77ms TTL=128

Ping statistics for 200.15.86.2:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 73ms, Maximum = 160ms, Average = 98ms
```

Se comprueba que es satisfactoria la comunicación entre host conectados en diferentes switch y la misma VLAN.

Se realiza ping entre host pertenecientes a distintas VLAN. Obteniendo los siguientes resultados.

PC>ping 200.15.82.1

Pinging 200.15.82.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 200.15.82.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Por lo que se concluye que no hay comunicación.

Finalmente se realiza ping entre host pertenecientes a la misma VLAN obteniendo los siguientes resultados

Pinging 200.15.81.2 with 32 bytes of data:

Reply from 200.15.81.2: bytes=32 time=108ms TTL=128
Reply from 200.15.81.2: bytes=32 time=66ms TTL=128
Reply from 200.15.81.2: bytes=32 time=63ms TTL=128
Reply from 200.15.81.2: bytes=32 time=52ms TTL=128

Ping statistics for 200.15.81.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 52ms, Maximum = 108ms, Average = 72ms

Podemos concluir que hay comunicación satisfactoria.

Sin embargo, tal como ocurre con la conmutación básica de LAN, se pueden producir problemas cuando se implementan las VLAN.
Los siguientes pasos explican cómo se aísla un problema en una red conmutada:

Verificar las indicaciones físicas como el estado de LED.

Comenzar con una sola configuración en un switch y prosiga el proceso hacia afuera.

Verificar el enlace de Capa 1.

Verificar el enlace de Capa 2.

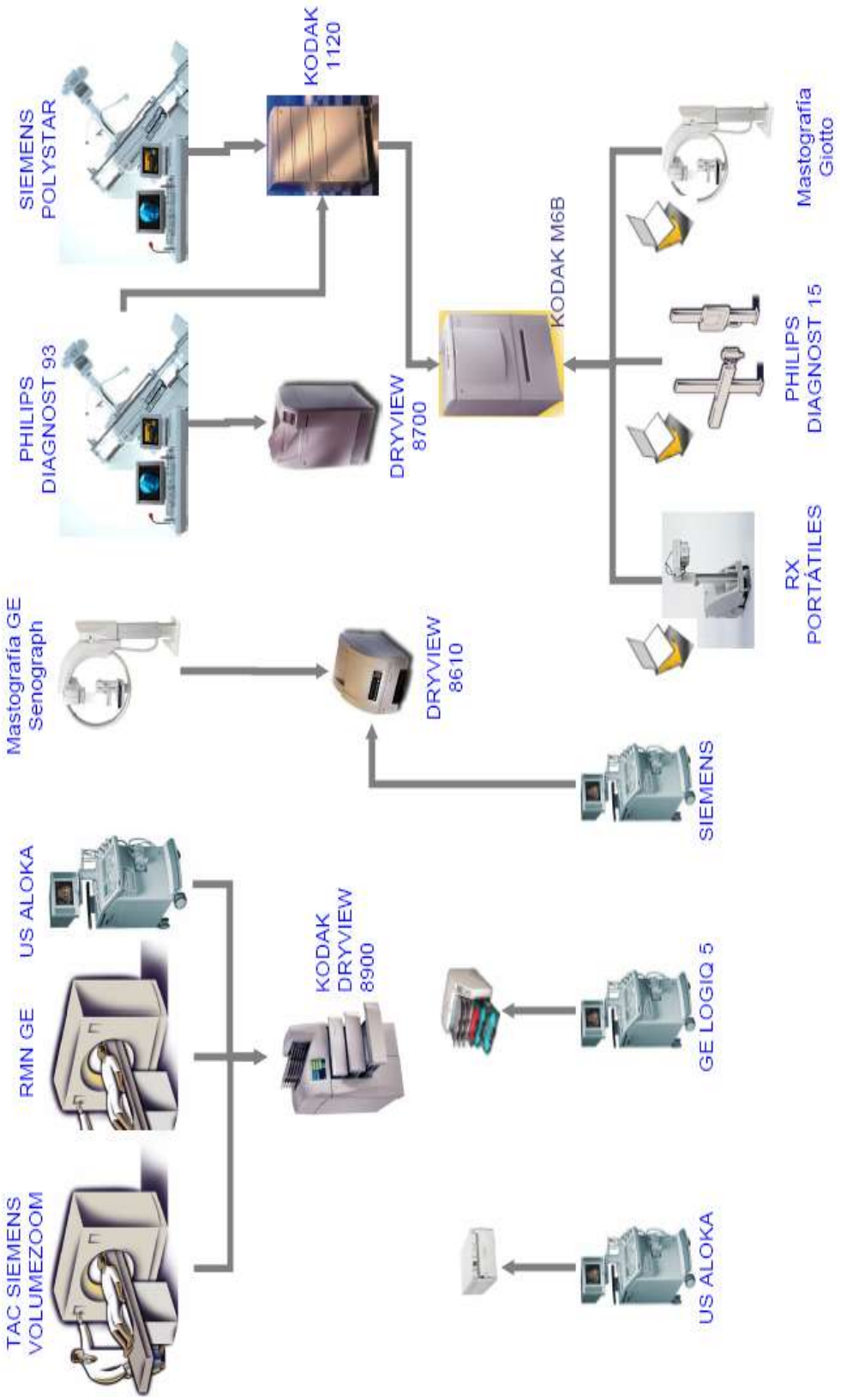
Hacer el diagnóstico de fallas de las VLAN que abarcan varios switches.

Al realizar el diagnóstico de fallas, hay que verificar si el problema es un problema recurrente en lugar de una falla aislada. Algunos problemas recurrentes se deben a un crecimiento de la demanda de servicios por parte de puertos de estación de trabajo que excede los recursos de configuración, enlace troncal o capacidad para acceder a los recursos de servidor. Por ejemplo, el uso de tecnologías de Web y aplicaciones tradicionales, como la transferencia de archivos y correo electrónico, provoca un crecimiento en el tráfico de red.

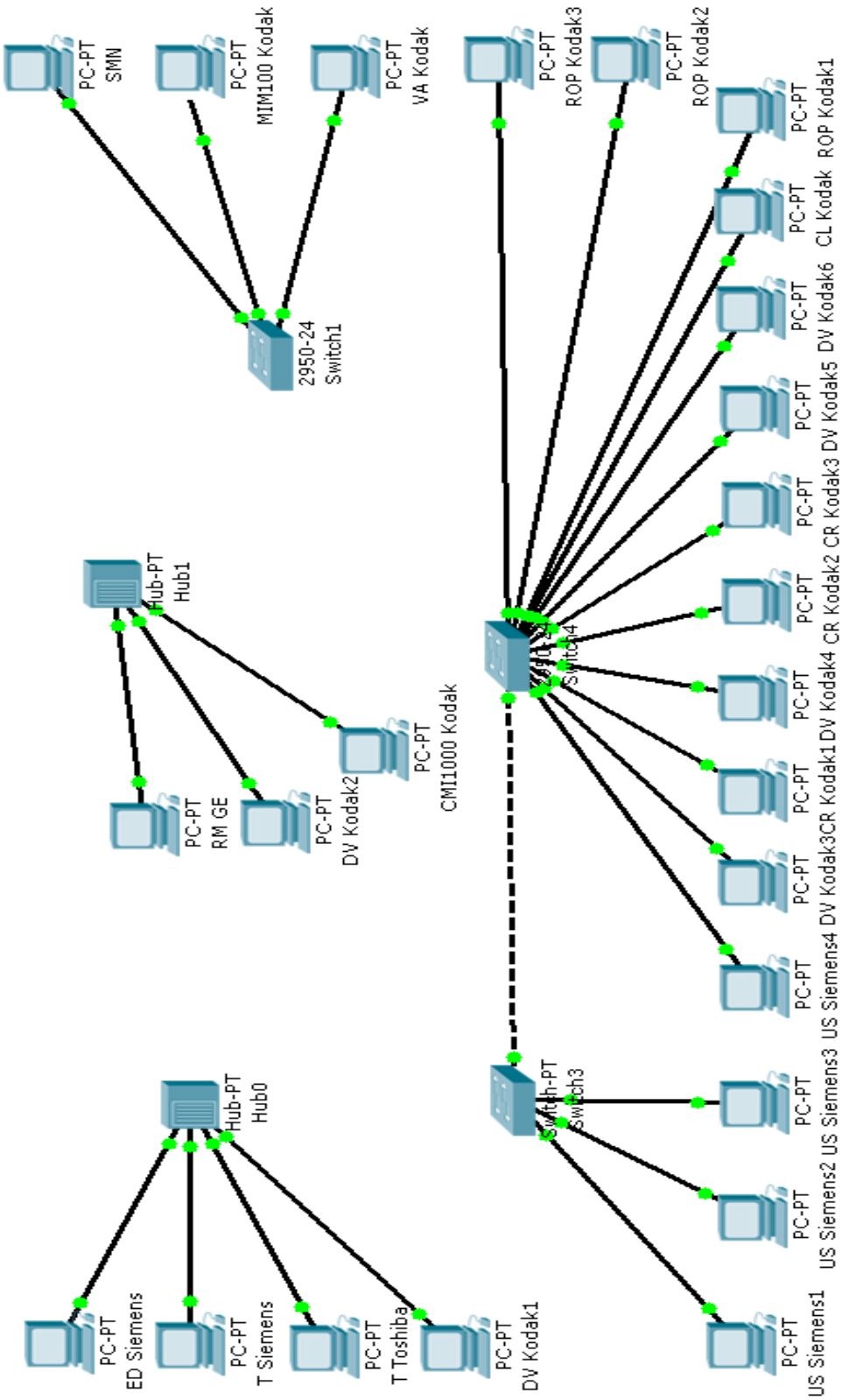
Muchas LAN se enfrentan a patrones de tráfico de red impredecibles resultantes de la combinación de tráfico de intranet y el uso creciente de aplicaciones multicast. La exploración de Web interna ahora permite que los usuarios localicen y accedan a la información desde cualquier lugar en la intranet. Los patrones de tráfico están determinados por la ubicación de los servidores y no por las configuraciones del grupo de trabajo físico con el que se agrupan.

Si una red presenta con frecuencia síntomas de cuello de botella, como desbordes excesivos, tramas descartadas y retransmisiones, es posible que haya demasiados puertos en un solo enlace troncal o demasiados requerimientos de recursos globales y acceso a los servidores de intranet.

Los síntomas de cuello de botella también pueden producirse porque la mayor parte del tráfico se ve obligado a atravesar el backbone. Otra causa puede ser que el acceso de "cualquiera a cualquiera" es común.



ANEXO1 IMAGEN RED ACTUAL



ANEXO2 SIMULACION RED ACTUAL

ANEXO 3 ASIGNACION DE NOMBRES A LAS VLAN

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname RX1
switch(config)#hostname RX1
RX1#vlan database
RX1(vlan)#vlan 2 name TOMOGRAFIA
VLAN 2 added:
   Name: TOMOGRAFIA
RX1(vlan)#vlan 3 name RM
VLAN 3 added:
   Name: RM
RX1(vlan)#vlan 4 name US
VLAN 4 added:
   Name: US
RX1(vlan)#vlan 5 name MASTOGRAFIA
VLAN 5 added:
   Name: MASTOGRAFIA
RX1(vlan)#vlan 6 name CAZUL
VLAN 6 added:
   Name: CAZUL
RX1(vlan)#vlan 7 name JEFATURA
VLAN 7 added:
   Name: JEFATURA
RX1(vlan)#vlan 8 name HEMODINAMIA
VLAN 8 added:
   Name: HEMODINAMIA
RX1(vlan)#vlan 9 name MNUCLEAR
VLAN 9 added:
   Name: MNUCLEAR
RX1(vlan)#end
```

ANEXO 4 ASIGNACION DE IP A VLAN

```
RX1#configure terminal
RX1(config)#interface vlan 2
RX1(config-if)#ip address 200.15.81.254 255.255.255.0
RX1(config-if)#exit
RX1(config)#interface vlan 3
RX1(config-if)#ip address 200.15.82.254 255.255.255.0
RX1(config-if)#exit
RX1(config)#interface vlan 4
RX1(config-if)#ip address 200.15.83.254 255.255.255.0
RX1(config-if)#exit
RX1(config)#interface vlan 5
```

```
RX1(config-if)#ip address 200.15.84.254 255.255.255.0
RX1(config-if)#exit
RX1(config)#interface vlan 6
RX1(config-if)#ip address 200.15.85.254 255.255.255.0
RX1(config-if)#exit
RX1(config)#exit
```

ANEXO 5 ASIGNACION DE PUERTOS A VLAN

```
RX1#configure terminal
RX1(config)#interface fastEthernet 0/24
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 2
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/2
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 2
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/3
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 2
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/4
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 2
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/5
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 3
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/6
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 3
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/7
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 3
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/8
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 4
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/9
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 4
RX1(config-if)#exit
```

```
RX1(config)#interface fastEthernet 0/10
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 4
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/11
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 4
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/12
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 4
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/13
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 5
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/14
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 5
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/15
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 6
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/16
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 6
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/17
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 6
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/18
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 6
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/19
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 6
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/20
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 6
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/21
RX1(config-if)#switchport mode access
```

```
RX1(config-if)#switchport access vlan 6
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/22
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 6
RX1(config-if)#exit
RX1(config)#interface fastEthernet 0/23
RX1(config-if)#switchport mode access
RX1(config-if)#switchport access vlan 7
RX1(config-if)#exit
RX1(config)#end
```

Y en RX2

```
RX2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RX2(config)#interface fastEthernet 0/1
RX2(config-if)#switchport mode access
RX2(config-if)#switchport access vlan 7
RX2(config-if)#exit
RX2(config)#interface fastEthernet 0/2
RX2(config-if)#switchport mode access
RX2(config-if)#switchport access vlan 8
RX2(config-if)#exit
RX2(config)#interface fastEthernet 0/3
RX2(config-if)#switchport mode access
RX2(config-if)#switchport access vlan 9
RX2(config-if)#exit
```

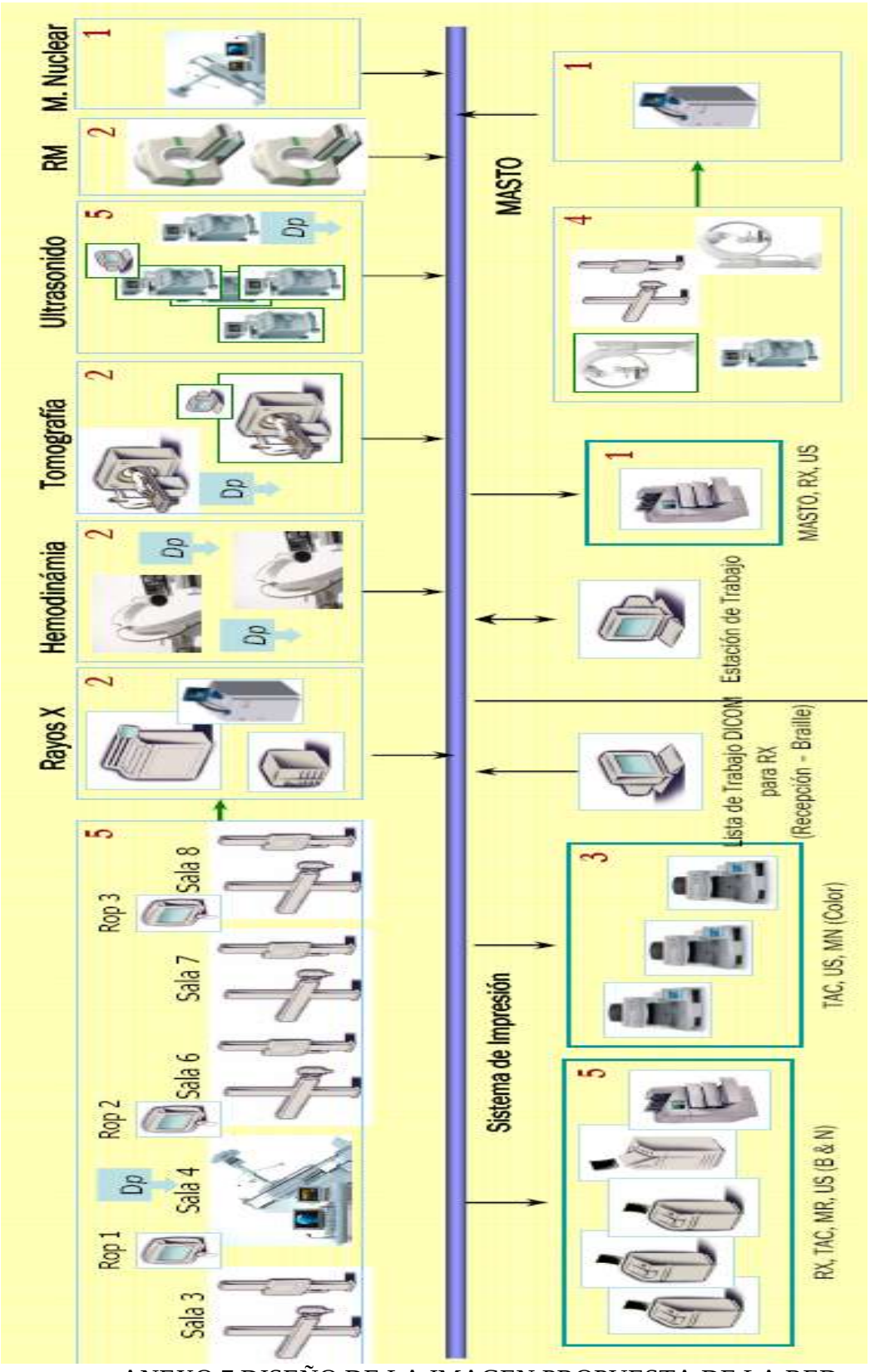
ANEXO 6 CONFIGURACION DEL ENLACE TRONCAL

En el switch RX1(Servidor)

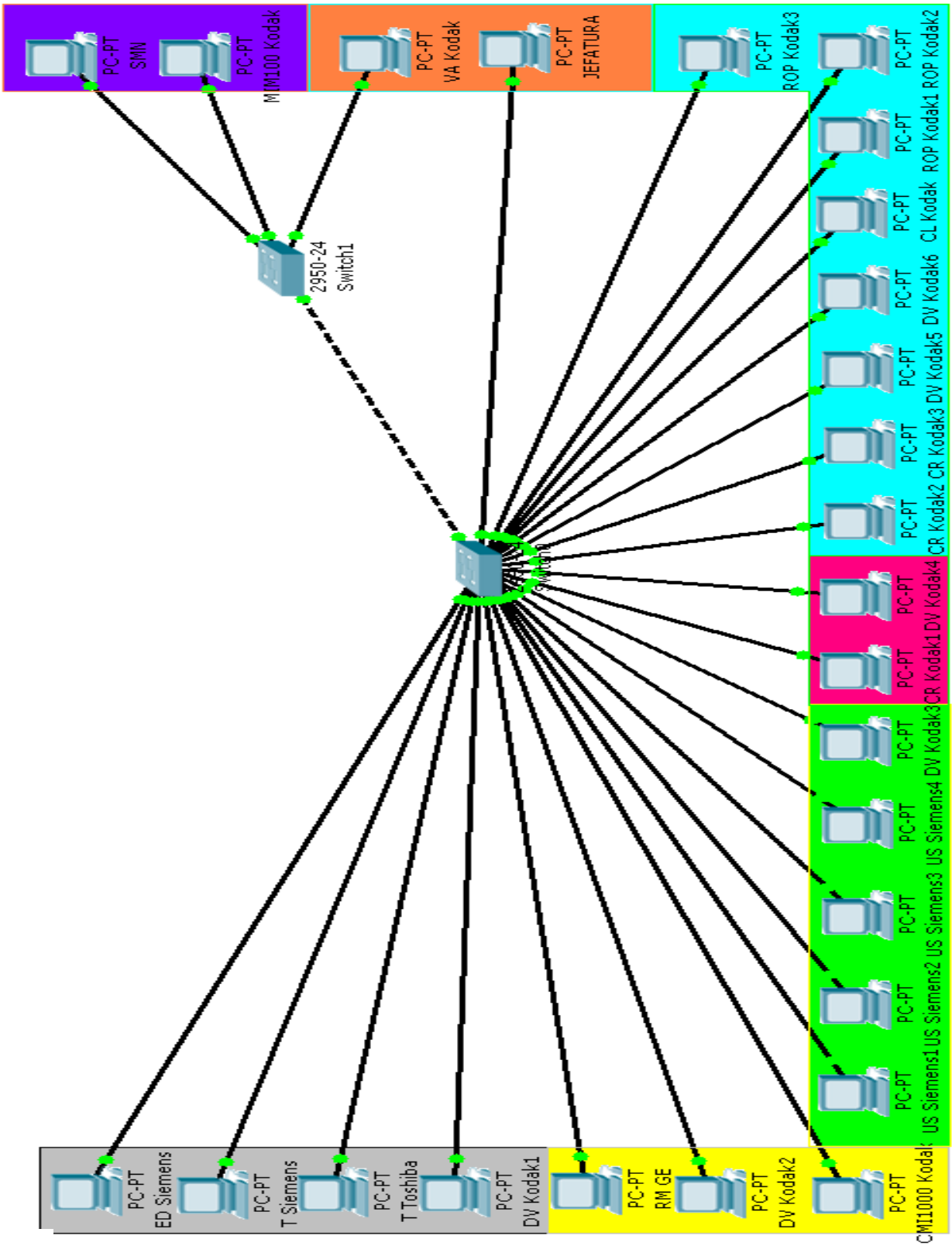
```
RX1>enable
RX1#configure terminal
RX1(config)#interface fastEthernet 0/1
RX1(config-if)#switchport mode trunk
```

Y en el otro switch RX2 (cliente)

```
RX2>enable
RX2#configure terminal
RX2(config)#interface fastEthernet 0/24
RX2(config-if)#switchport mode trunk
```



ANEXO 7 DISEÑO DE LA IMAGEN PROPUESTA DE LA RED



ANEXO 8 SIMULACION DEL DISEÑO DE LA RED

```
RX1>enable
RX1#show vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active
2    TOMOGRAFIA                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/24
3    RM                                  active    Fa0/5, Fa0/6, Fa0/7
4    US                                  active    Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                   Fa0/12
5    MASTOGRAFIA                         active    Fa0/13, Fa0/14
6    CAZUL                               active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                   Fa0/19, Fa0/20, Fa0/21, Fa0/22
7    JEFATURA                            active    Fa0/23
8    HEMODINAMIA                         active
9    MNUCLEAR                            active
10   IMPRESION                           active
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
4    enet  100004     1500  -      -      -        -    -        0      0
5    enet  100005     1500  -      -      -        -    -        0      0
6    enet  100006     1500  -      -      -        -    -        0      0
7    enet  100007     1500  -      -      -        -    -        0      0
8    enet  100008     1500  -      -      -        -    -        0      0
9    enet  100009     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
1002 enet  101002     1500  -      -      -        -    -        0      0
1003 enet  101003     1500  -      -      -        -    -        0      0
1004 enet  101004     1500  -      -      -        -    -        0      0
1005 enet  101005     1500  -      -      -        -    -        0      0

RX1#
```

ANEXO 9 TABLA ESTADO DE VLANS EN RX1

```
RX2#enable
RX2#show vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                   Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                   Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                   Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                   Fa0/22, Fa0/23
2    VLAN0002                            active    Fa0/4, Fa0/5
7    VLAN0007                            active    Fa0/1
8    VLAN0008                            active    Fa0/2
9    VLAN0009                            active    Fa0/3
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
7    enet  100007     1500  -      -      -        -    -        0      0
8    enet  100008     1500  -      -      -        -    -        0      0
9    enet  100009     1500  -      -      -        -    -        0      0
1002 enet  101002     1500  -      -      -        -    -        0      0
1003 enet  101003     1500  -      -      -        -    -        0      0
1004 enet  101004     1500  -      -      -        -    -        0      0
1005 enet  101005     1500  -      -      -        -    -        0      0
```

ANEXO 10 TABLA ESTADO DE VLANS EN RX2

CONCLUSIONES

Una VLAN es una agrupación de servicios de red que no se limita a un segmento o switch de LAN físico. La configuración o reconfiguración de las VLAN se realiza mediante software que hace que resulte innecesario conectar o mover físicamente cables y equipo. Las VLAN se ocupan de la escalabilidad, seguridad y gestión de red. Los switches no puentean ningún tráfico, dado que esto viola la integridad del dominio de broadcast de las VLAN.

El beneficio principal de las VLAN es que permiten que el administrador de red organice la LAN de forma lógica en lugar de física. Esto incluye la capacidad para mover estaciones de trabajo en la LAN, agregar estaciones de trabajo a la LAN, cambiar la configuración de la LAN, controlar el tráfico de red y mejorar la seguridad.

Una VLAN es un dominio de broadcast creado por uno o más switches. Las VLAN se usan para crear dominios de broadcast para mejorar el desempeño general de la red. Al implementar VLAN en un switch, el switch mantiene una tabla de puenteo separada para cada VLAN. Si viene la trama a un puerto en la VLAN 1, el switch busca la tabla de puenteo para la VLAN 1. Cuando se recibe la trama, el switch agrega la dirección origen a la tabla de puenteo si no se la conoce actualmente. El switch entonces verifica el destino para que se pueda tomar una decisión de envío. Para aprender y enviar se realiza la búsqueda en la tabla de direcciones para esa VLAN solamente.

Las VLAN estáticas son puertos en un switch que se asignan manualmente a una VLAN utilizando la aplicación de gestión de VLAN o trabajando directamente dentro del switch. Estos puertos mantienen su configuración de VLAN asignada hasta que se cambien manualmente. Las VLAN dinámicas no se basan en puertos asignados a una VLAN específica. Se usan los comandos show vlan, show vlan brief, o show vlan id *id_number* para verificar las configuraciones de VLAN.

Se aplica un enfoque sistemático para el diagnóstico de fallas en una VLAN. Para aislar un problema, verifique las indicaciones físicas como el estado de LED. Hay que comenzar con una sola configuración en un switch y seguir el proceso hacia afuera. También hay que verificar el enlace de Capa 1 y luego el de Capa 2. Posteriormente hacer el diagnóstico de fallas de las VLAN que abarcan varios switches. Algunos problemas recurrentes se deben a un crecimiento de la demanda de servicios por parte de puertos de estación de trabajo que excede los recursos de configuración, enlace troncal o capacidad para acceder a los recursos de servidor.

Para este diseño en particular se tomaron en cuenta diferentes factores como son las diferentes áreas. Al realizar el diseño de la red por medio de VLAN asociada a cada área de imagenología del Hospital General de México se mejoro considerablemente el flujo de datos en la red verificándolo en el simulador, ya que en lugar de mandar paquetes de datos hacia todos los host de la red conectados al switch RX1, sólo se envían entre los host asociados a la misma VLAN configurados en el mismo switch.

INDICE DE FIGURAS

GLOSARIO

ALOHA Protocolo de conexión de redes por medio de un enlace radioeléctrico, utilizado para la interconexión de las diferentes islas de Hawai de diferentes equipos. Inventado por Norman Abranson de la Universidad de Hawai. Existen dos tipos ALOHA (mas susceptible a colisiones) y ALOHA Ranurado (Menos susceptible a colisiones)

ARP En Ingles *Addres Resolution Protocol.* Hace la relación entre la dirección lógica (IP) y la física (Dirección de la tarjeta). Muestra y modifica entradas en la caché de Protocolo de resolución de direcciones (ARP), que contiene una o varias tablas utilizadas para almacenar direcciones IP y sus direcciones físicas Ethernet o Token Ring resueltas. Existe una tabla independiente para cada adaptador de red Ethernet o Token Ring instalados en el equipo.

Banda Ancha Transmite múltiples señales de portadora de alta frecuencia, emplea FDM. Envía señales de forma simultáneamente. Maneja múltiples canales de diferentes velocidades,

Banda Base Transmisión Digital de una señal, la transmisión se realiza una a la vez. Utiliza TDM, puede enviar voz datos pero siempre y cuando sean digitalizados, es barata.

Bit Símbolo que se propaga en el canal de información en un determinado tiempo (referido al canal de información). unidad mas pequeña de información.

Bridge En español *puente*. Se utiliza para conectar dos redes que sean diferentes en su capa de Enlace de Datos

Broadcast Envió de información a múltiples destinos que son desconocidos para el transmisor. normalmente utilizado por los routers para reconocimientos de host

Colisión Es aquella que sucede cuando 2 o mas tramas que se estén enviando por un medio de transmisión coincidan y choquen entre ellas y esto haga que las tramas se fracturen y por lo tanto el destino no pueda reconocer la información y por lo tanto se pierda

CRC Código de redundancia cíclica. Este es utilizado para la detección y corrección de errores al momento de enviar información, regularmente se encuentra ubicado dentro de la trama de información.

CSMA/CD En ingles Carrier Sense Múltiple Access / Colision Detect. Acceso Múltiple por Detección de Portadora / Detección de Colisiones. Utilizado por Ethernet para la detección de colisiones y esta ubicado en la subcapa MAC del modelo OSI

DICOM Protocolo de comunicación de imágenes medicas. Digital Imaging and Communication in Medicine.

Dúplex En ingles Full Duplex es la forma de comunicación de un sistema. Este puede transmitir información en ambos sentidos y puede transmitir y recibir información al mismo tiempo

Ethernet Ether- Eter, Net- Red Red de Eter. Es el nombre que se le dio a la Red debido a su similitud que tiene con todo en el universo, ya que esta red es un universo de información.

FCS En ingles Frame Check Secuence. Esta se utiliza para la detección de errores al momento de enviar información. Se encuentra dentro del Trailer de la trama. Es parte del CRC

FDDI En ingles Fiber Disitribution Data Interface . Permite integrar otro tipo de redes, utilizando anillos de Fibra Óptica. Emplea Estaciones DAS y SAS. Sus enlaces entere las interfaz es de hasta 2 Km.

Frame Bloque de datos en una transmisión por tarjeta de red, se le conoce como trama (es el formato de un paquete). También se aplica para describir el Formato de una pagina de Internet

FTP En ingles File Transfer Protocol. Protocolo de Transferencia de Archivos. Este es el que nos permite transferir archivos en internet, a demás de copiarlos y poder distinguir entre dos tipos de archivos que pueden ser binarios o ASCII.

Gateway En español Pasarela. Es una dirección que se tiene en el router puede ser interior o exterior.

Host Es una estación de trabajo que se conecta a través de TCP/IP, es el anfitrión.

Hostname Es un comando que se utiliza para mostrar la parte correspondiente al nombre de host del nombre completo del equipo.

Hub Es un dispositivo de interconexión de redes de área local, Esta ubicado en la capa física del modelo OSI. El propósito de un hub es regenerar y re temporizar las señales de red

Interfase En ingles Interface. Que significa entre caras, es un acoplamiento mecánico

IP En ingles Internet Protocol. Protocolo de internet, es el que se encarga del encaminamiento y selección de las rutas. Se encuentra en la capa de red del modelo OSI.

LAN En ingles Local Area Network. Red de Área Local, es un conjunto de computadoras las cuales pueden estar conectadas en diferentes topologías

LLC En ingles Logic Link Control. Control de Enlace Lógico, es el procedimiento de enlace entre dos maquinas de forma lógica para no confundir la transmisión.

MAC En ingles Médium Access Control. Control de Acceso al Medio. Son las reglas que se utilizan para normar la forma de cómo los nodos van a funcionar, es la que va a determinar que maquina va a tener prioridad.

Multicast Envío de información a múltiples destinos conocidos. Esto se utiliza en las direcciones de Clase D de IP.

Paquete	Es un bloque de datos, una trama
Protocolo	Conjunto de reglas necesarias para poder establecer una comunicación entre dos estaciones de trabajo y así intercambiar información.
Red	Interconexión de nodos a través de medios de transmisión alambricos o inalámbricos
Repetidor Multipuerto	Un repetidor es la expresión mínima de un concentrador, o también se puede decir, que un concentrador es un repetidor multipuerto.
Router	Dispositivo de la red utilizado para conectar dos redes de área local con diferentes capas de Red.
Switch	El switch segmenta la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final. El switch funciona una capa mas arriba y es mas inteligente que el hub.
TCP	En ingles Transmisión Control Protocol. Interfaz entre las aplicaciones y la dirección IP. Localizado en la capa de enlace del modelo OSI.
Telnet	Proporciona servicios que permite a un usuario comunicarse con el sistema operativo de una host remota. Ubicado en la capa de aplicación del modelo OSI
Token	Es conocido como Ficha o Testigo. Es una trama pequeña que no tiene datos de usuario, solo tiene Header y Trailer. Este es usado en Token Ring y Token Bus.
TTL	En ingles Time to Life. Tiempo de Vida media que el datagrama puede sobrevivir en la red, antes de ser desechada la trama.
VLAN	Virtual Local Area Network
WAN	En Ingles Wide Area Network. Red de Área Amplia, esta es de un rango mayor a las redes de área local.

BIBLIOGRAFÍA

-http://www.cisco.com/web/learning/netacad/index.html

-Sistemas de autentificación para seguridad en redes, Rolf Oppliger, Alfaomega-Ra-Ma, 1998

-Redes de computadoras, Andrew S. Tanenbaum, Pearson Prentice Hall, 2003

-Instalación y mantenimiento de servicios de redes locales, Francisco J. Molina, Alfaomega-Ra-Ma.

-http://www.criptored.upm.es

-http://ecampus.kodak.com

http://www.textoscientificos.com