UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

REINGENIERÍA DE LA RED DEL LABORATORIO DE GEOMÁTICA Y ESPECIALIDADES DE CIVILES

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

PRESENTA:

RIVERA CRESPO ANTONIO

DIRECTOR DE TESIS:

ING. ALDO JIMÉNEZ ARTEAGA

CIUDAD UNIVERSITARIA, 2015

AGRADECIMIENTOS

A mi madre Camelia Crespo Molina, gracias por apoyarme en todo momento y por ser un ejemplo de profesionalismo y dedicación. Éste, uno de mis más grandes logros, te lo dedico con todo mi amor.

A mi padre Antonio Rivera Perea, gracias por estar siempre conmigo, por ser una de mis más grandes inspiraciones en la vida y por ser un ejemplo de dedicación, responsabilidad y honradez. Porque sin tus enseñanzas y apoyo no estaría en donde estoy, este logro te lo dedico con todo mi amor y admiración.

A mi hermana Viri, gracias por ser siempre mi ejemplo a seguir, por apoyarme incondicionalmente, por todo el cariño que siempre me has brindado y por regalarme una de mis más grandes fuentes de inspiración en la vida, mi sobrino Leonardo.

A Paola, gracias por todo el apoyo que me has brindando, por acompañarme y ayudarme a vencer mis miedos y debilidades, por tu amor incondicional y por tus enseñanzas.

A mi director de tesis, el Ingeniero Aldo Jiménez Arteaga, agradezco todo su apoyo y tiempo dedicado para la realización de esta tesis. A todos los miembros del jurado, gracias por toda la ayuda, por dar seguimiento a la realización de este trabajo y por todas las enseñanzas brindadas.

Al Ingeniero Francisco López Mendieta, gracias por todo el apoyo en la realización de esta tesis y por confiar en mis conocimientos y trabajo.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Entre todos los elementos que son esenciales para la existencia humana, la necesidad de interactuar se encuentra únicamente por debajo de la necesidad de sustentar la vida. Así como el aire, el agua, los alimentos y un lugar para vivir, la comunicación es un aspecto cotidiano de suma importancia para nosotros.

Durante mucho tiempo la red humana estuvo limitada únicamente a conversaciones cara a cara, pero el avance de los medios ha ampliado el alcance de nuestras comunicaciones. Desde la prensa escrita hasta la televisión, cada nuevo desarrollo ha mejorado la comunicación.

En sus inicios, las redes de datos estaban limitadas a intercambiar información basada en caracteres entre sistemas informáticos interconectados. Actualmente las redes han evolucionado y se han ido adaptando a nuevas necesidades de aplicación, agregando voz, video, texto y gráficos a los diferentes tipos de dispositivos que procesan estas formas de representar información. Así las formas de comunicación anteriormente individuales y diferentes se unieron en una plataforma común. Esta plataforma proporciona acceso a una amplia variedad de métodos de comunicación alternativos y nuevos, que permiten a las personas interactuar directamente con otras en forma casi instantánea.

La compartición de recursos es uno de los principales aplicativos de la redes de datos, además se busca que los programas, servicios, datos y dispositivos estén disponibles siempre que se requiera por parte de alguno de los usuarios de la red; este requerimiento es sin duda uno de los objetivos que toda red busca cumplir.

Las redes no solo están integradas por dispositivos finales como computadoras, también otros dispositivos electrónicos como routers, switches, módems, repetidores, etc., juegan un papel fundamental en el funcionamiento de las redes. En conjunto todos estos componentes ayudan a brindar una mayor eficiencia en la transmisión de la información, pero también la integración de más y más componentes origina que la complejidad del funcionamiento y configuraciones aumente, provocando mayor posibilidad de tener errores en el envío de datos. Por eso es indispensable hacer uso de protocolos que digan a los equipos que conforman la red cómo preparar la información para ser enviada, por dónde enviarla y cómo recibirla.

En la actualidad las redes pueden ser tan complejas como las necesidades de funcionamiento lo demanden, lo cual puede traer consigo problemas para efectuar la transmisión de la información, por ejemplo problemas de enrutamiento, saturación de ancho de banda, seguridad, crecimiento del número de usuarios, etc.

Este proyecto está basado en una red de área local que por sus características permite realizar un análisis de funcionamiento, identificación de componentes y configuraciones implementadas, aplicar un plan de mantenimiento preventivo y correctivo y generar una

propuesta de un nuevo diseño de la estructura base de la red. Todo esto debido a que el estado actual de la red no cumple con las características requeridas para su correcto funcionamiento. No cuenta con una administración de red adecuada, no existen planes de mantenimiento preventivo, no hay documentación que describa el estado y configuración de la red y presenta fallas importantes de funcionamiento que afectan a los usuarios finales.

En el capítulo 1 se presentan conceptos y definiciones de redes de datos y administración de redes. Toda la información contenida en este capítulo es muy importante para la comprensión de los siguientes capítulos de esta tesis.

En el capítulo 2 se presenta el estado actual de la red del laboratorio. Se describe la metodología implementada, la cual se basa en el estudio de la red monitoreando el funcionamiento de los equipos y realizando una inspección física para identificar cuáles son las fallas que originan que la disponibilidad de la red se vea afectada.

A partir de los resultados obtenidos en la primera fase de estudio de la red se desarrolla un plan de mantenimiento correctivo y preventivo a bajo costo con el que pueda resolverse la mayor cantidad de fallas detectadas en la red. En el capítulo 3 se describe dicho plan de mantenimiento aplicable en la red del laboratorio.

En el capítulo 4 se describe la implementación del plan de mantenimiento a bajo costo aplicable en la red del laboratorio y los resultados obtenidos una vez realizado un nuevo análisis del estado de la red. Es en este capítulo donde se muestra el impacto que tuvo la implementación de todas las acciones correctivas que pudieron realizarse.

En el capítulo 5 se presenta la propuesta de implementaciones en la red del laboratorio. A partir de los resultados obtenidos y de todos aquellos factores no favorables identificados en la red que no pudieron corregirse o implementarse debido a la necesidad de inversión monetaria, se diseña la propuesta de nuevas implementaciones y correcciones que puedan aplicarse en la red del laboratorio y se realiza el análisis correspondiente que describa los beneficios de invertir en dicha propuesta.

Finalmente se presentan las conclusiones en las cuales se describen los resultados obtenidos con el desarrollo de esta tesis. Se presentan además los beneficios que la red del laboratorio obtuvo una vez implementado el plan de mantenimiento a bajo costo y los beneficios que la propuesta de nuevas implementaciones en la red brindaría en caso de ser desarrollada.

Con este proyecto se busca rediseñar la red del Laboratorio de Geomática y Especialidades de Civiles de la Facultad de Ingeniería de la UNAM, una red plana que desde su implementación hace más de 13 años no ha recibido la administración correcta ni el mantenimiento periódico que toda red debe recibir para que su funcionamiento no

se vea afectado. Además se propone diseñar un plan administrativo básico para que los prestadores de servicio social, quienes son los encargados de atender los asuntos técnicos dentro del laboratorio, puedan atender las necesidades básicas que la red debe recibir.

OBJETIVOS

Objetivo general

Proponer el diseño de la reingeniería de la red del Laboratorio de Geomática y Especialidades de Civiles que permita garantizar mayor disponibilidad, mayor seguridad, mayor calidad en los servicios brindados y adaptabilidad a nuevas tecnologías y al crecimiento del número de usuarios.

Objetivos específicos

- Identificar qué normas y estándares internacionales de redes de datos no cumple la red del laboratorio, cuáles son las fallas físicas y configuraciones que afectan la disponibilidad de la red.

- Generar la documentación descriptiva para el laboratorio que incluya la estructura de la red, su configuración, planos y descripción de sus componentes.

- Diseñar e implementar un plan de mantenimiento correctivo que no requiera de una inversión monetaria significativa para dar solución a la mayor cantidad de problemas actuales que afectan el funcionamiento de la red del laboratorio.

CAPÍTULO I

Conceptos básicos de redes de datos y administración de redes

1.1 Redes de Datos

Una red de datos es un conjunto de dispositivos como computadoras, teléfonos VoIP (Voice over IP), impresoras, routers y switches que pueden comunicarse entre sí a través de un medio de transmisión, siguiendo un conjunto de reglas y protocolos que les permiten realizar el envío y recepción de información de forma ordenada.

Las redes de datos tienen como principal objetivo permitir el intercambio de información entre los dispositivos conectados en la red, así como la compartición de recursos computacionales y el rápido acceso a servicios que pueden incluso estar a grandes distancias.

1.2 Topología de las redes de datos

La topología de una red es la configuración o la relación de los dispositivos de red y las interconexiones entre dichos dispositivos. La topología de una red se puede ver desde dos enfoques distintos que se determinan por el nivel físico y el nivel lógico de la red.

La topología física es la configuración de nodos y las conexiones físicas entre dichos nodos. Representa cómo son utilizados los medios para poder interconectar los dispositivos de la red.

La topología lógica de una red especifica la forma en que es administrado el acceso a la red por parte de los dispositivos conectados a ella. Los métodos de acceso deben proporcionar los procedimientos para administrar el acceso a la red y así garantizar que todas las estaciones puedan hacer uso del medio.

Generalmente las topologías físicas y lógicas utilizadas en las redes son topología punto a punto, topología multiacceso y topología anillo.

1.2.1 Topología punto a punto

En la topología punto a punto se conectan dos nodos directamente entre sí. El protocolo de acceso al medio puede llegar a ser muy simple en este tipo de topología ya que todas las tramas que se envían por los medios únicamente pueden viajar hacia los dos nodos o desde los dos nodos involucrados en la comunicación.

En redes con topología punto a punto se puede operar como un enlace half-duplex, es decir, los datos pueden viajar en una sola dirección; o como un enlace full-duplex, es decir, los datos viajan en ambas direcciones al mismo tiempo.

En este tipo redes proveer de procesos más sofisticados para el control de acceso a los medios agregaría un gasto innecesario.

Figura 1. 1 Topología punto a punto

Los nodos de los extremos que se comunican en una red punto a punto pueden estar conectados físicamente a través de uno o varios dispositivos intermediarios, sin que esto afecte la topología lógica.

En algunos casos, la conexión lógica entre nodos forma un circuito virtual que es una conexión lógica creada dentro de una red entre dos dispositivos de red. Así, los dos nodos transmiten tramas entré sí incluso si dichas tramas están dirigidas a través de dispositivos intermediarios.

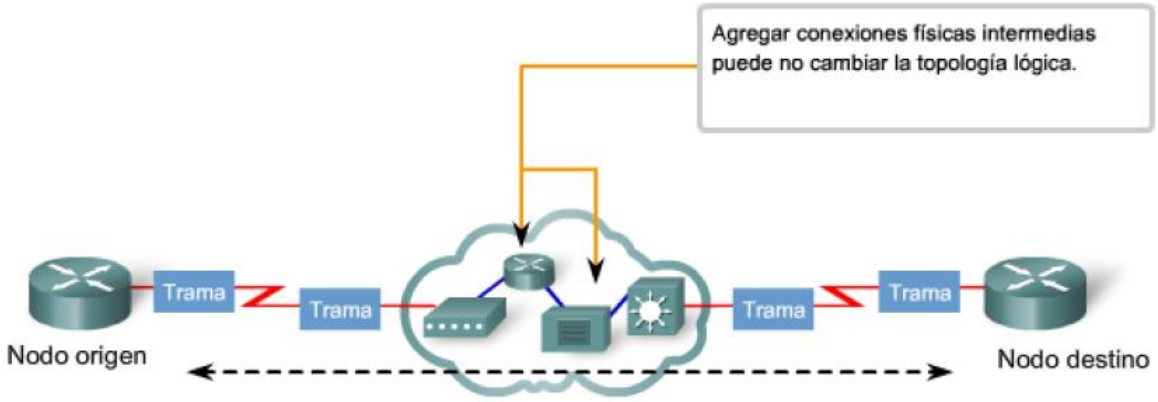


Figura 1. 2 Topología punto a punto con circuito virtual

1.2.2 Topología multiacceso

En una red con topología multiacceso se le permite a una cantidad de nodos comunicarse utilizando los mismos medios compartidos. Un nodo puede colocar en el medio los datos que deseé transmitir en cualquier momento. Así todos los nodos conectados en la red podrán ver las tramas que viajan a través del medio, pero únicamente el nodo al cual las tramas van dirigidas procesará el contenido de dichas tramas.

Para poder lograr que varios nodos puedan compartir el acceso al mismo medio es necesario que se implementen métodos de control de acceso al medo de enlace de datos, los cuales deben regular la transmisión de datos y así reducir las colisiones entre las diferentes señales.

Los métodos de control de acceso al medio utilizados por las topologías multiacceso son generalmente CSMA/CD (Carrier Sense Multiple Access with Collision Detection) o CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Pero existen otros como el método de paso de token que también puede ser utilizado.

Para las topologías multiacceso, el protocolo de capa de enlace de datos especifica el método de control de acceso al medio que proporcionará el balance apropiado entre el control de la trama, la protección de trama y la sobrecarga de red.

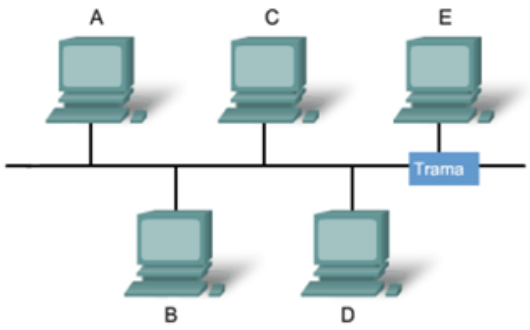


Figura 1. 3 Topología Multiacceso

1.2.3 Topología en anillo

En una red con topología lógica de anillo, cada nodo recibe una trama por turno. En caso de que la trama recibida no vaya dirigida al nodo, éste la pasa al nodo siguiente. Así, la topología implementada utiliza una técnica de control de acceso al medio llamada paso de tokens. Todos los nodos alrededor del anillo entre el nodo origen y el destino deberán examinar la trama.

Existen varias técnicas de control de acceso al medio que pueden ser implementadas en redes con topología lógica en anillo. La técnica seleccionada dependerá del nivel de control requerido.

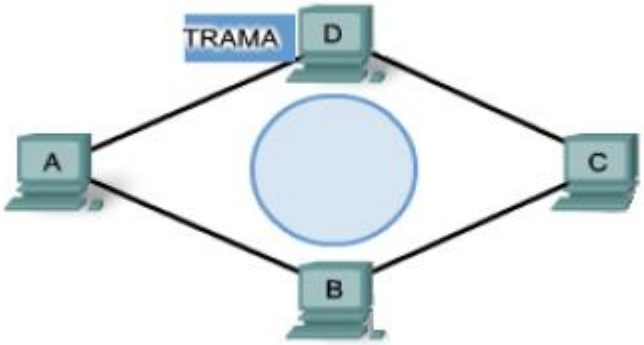


Figura 1. 4 Topología en Anillo

1.3 Componentes de red

Una red está conformada esencialmente por cuatro elementos que son las reglas, los medios, los mensajes y los dispositivos.

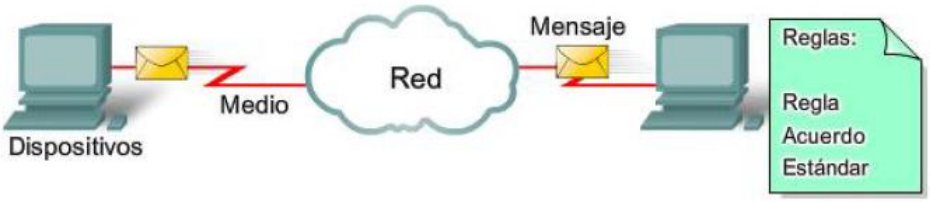


Figura 1. 5 Elementos de una red

Las reglas dentro de las redes juegan un papel fundamental para permitir la comunicación entre los dispositivos. Las reglas son las normas o protocolos que especifican la manera en que se envían los mensajes, cómo se direccionan a través de la red y cómo se interpretan en los dispositivos de destino.

Los medios son el soporte físico que utilizan los dispositivos de red para enviar la información. La mayoría de las redes existentes en la actualidad utilizan como medio de transmisión el cable de par trenzado UTP (Unshielded Twisted Pair), el cable coaxial y cable de fibra óptica, aunque también se utilizan medios inalámbricos.

El mensaje es la información que un dispositivo desea enviar a otro dispositivo de la red, dichos mensajes deben ser convertidos en un formato que pueda ser transmitido a través del medio. Todos los tipos de mensajes deben ser convertidos a bits, señales digitales codificadas en binario, antes de ser enviados a sus destinos. Esto es así sin importar el formato del mensaje original que puede ser texto, video, voz o datos informáticos.

Finalmente los dispositivos de red son aquellos componentes finales o intermediarios que participan activamente en la transmisión de información en la red. Como dispositivos finales se refieren a aquellos nodos de origen o destino como lo son las computadoras, impresoras, teléfonos VoIP, celulares, etc. Como dispositivos intermediarios se refieren a aquellos dispositivos que se encuentran entre los nodos finales y que permiten el reenvío de paquetes o tramas a través de la red como lo son hubs, switches y routers.

Los procesos que se ejecutan en los dispositivos de red intermediarios realizan las siguientes funciones:

- Regenerar y retransmitir señales de datos.
- Mantener información sobre qué rutas existen a través de la red.
- Notificar a otros dispositivos los errores y las fallas de comunicación.
- Direccionar datos por rutas alternas cuando existen fallas en un enlace.
- Clasificar y direccionar mensajes según las prioridades de calidad de servicio.
- Permitir o denegar el flujo de datos con base en las configuraciones de seguridad.

1.4 Arquitectura de Red

Debido al surgimiento de nuevas tecnologías y medios de comunicación, las redes en la actualidad deben de admitir una gran variedad de aplicaciones y servicios, también deben tener la capacidad de funcionar con diferentes tipos de infraestructura física.

Arquitectura de red se refiere a las tecnologías que admiten la infraestructura y a los servicios y protocolos programados que pueden trasladar los mensajes en toda esa infraestructura.

Se destacan cuatro características básicas que la arquitectura de red necesita para cumplir con las expectativas de los usuarios: tolerancia a fallas, escalabilidad, calidad de servicio y seguridad.

1.4.1 Tolerancia a fallas

Una red que cumple con esta característica será capaz de limitar el impacto de una falla de software o de hardware y podrá recuperarse rápidamente cuando se produzca dicha falla. Estas redes dependen de enlaces o rutas redundantes entre el origen y el destino del mensaje. Si un enlace o ruta falla, los procesos garantizan que los mensajes pueden redirigirse en forma instantánea en un enlace diferente, siendo este proceso totalmente trasparente para los usuarios finales.

Esta característica de arquitectura de red busca garantizar la disponibilidad de la red, permitiendo a los usuarios acceder a los recursos de red en todo momento.

1.4.2 Escalabilidad

Esta característica de arquitectura de red permite que la red pueda expandirse rápidamente con la finalidad de admitir nuevos usuarios y aplicaciones sin que estas adiciones afecten el rendimiento del servicio con que cuentan los usuarios antes de dicha expansión.

La capacidad de la red de admitir estas nuevas interconexiones depende de un diseño jerárquico en las capas para la infraestructura física y la arquitectura lógica.

El funcionamiento de cada capa permite a los usuarios y proveedores de servicios integrarse sin afectar el funcionamiento de la red.

Las nuevas tecnologías y nuevas implementaciones informáticas en las empresas demandan que las redes sean capaces de adaptarse a incrementos de usuarios y nuevos servicios dentro de la red, sin tener que suspender o modificar a gran escala la infraestructura de actual.

1.4.3 Calidad de Servicio

Es un conjunto de requisitos de servicio que la red debe cumplir para asegurar un nivel de servicio adecuado en la transmisión de los datos. Por ejemplo las transmisiones de voz y video requieren un nivel de calidad consistente y un envío ininterrumpido. Por lo tanto se puede decir que la calidad de estos servicios se mide con la calidad de experimentar la misma presentación de audio y video en persona.

Las redes convergentes al integrar voz, video y datos requieren de una correcta configuración y control de las prioridades y recursos que se asignan a las diversas aplicaciones o servicios para garantizar que éstos sean distribuidos de la forma esperada.

1.4.4 Seguridad

La infraestructura de red, los servicios y los datos contenidos en las computadoras conectadas a la red son activos comerciales y personales muy importantes. Comprometer la integridad de estos activos puede ocasionar serias repercusiones financieras y comerciales.

No garantizar seguridad en una red genera falta de confianza pública en la privacidad de la información, así los niveles de integridad de los negocios pueden derivar en la pérdida de ventas y finalmente en la quiebra de la empresa.

Asegurar la infraestructura de red incluye la protección física de los dispositivos que proporcionan conectividad de red y evitar el acceso no autorizado al software de administración que en ellos reside. Este aspecto de seguridad está enfocado en proteger aquellos componentes físicos que por su función o contenido son importantes para la red.

La seguridad de contenido se refiere a la protección de la información contenida en los paquetes que son transmitidos en la red y la información almacenada en los dispositivos conectados a la misma.

Diversas herramientas deben ser implementadas para proporcionar seguridad al contenido de los mensajes individuales sobre los protocolos que rigen la forma en que los paquetes se formatean, direccionan y envían. Atendiendo la seguridad en la red se busca garantizar la confidencialidad, mantener la integridad de la comunicación y garantizar la disponibilidad.

1.5 Modelo TCP/IP

El primer modelo de protocolo en capas para comunicaciones de internetwork fue creado en los años setentas, se le conoce con el nombre de modelo de internet. Este modelo define cuatro categorías de funciones que deben de tener lugar para que las comunicaciones sean exitosas. La arquitectura de la suite de protocolos TCP/IP (Transmission Control Protocol/Internet Protocol) sigue la estructura de este modelo.

Ninguna compañía controla la definición de este modelo ya que TCP/IP es un modelo estándar abierto. Las definiciones del estándar y los protocolos TCP/IP se explican en un foro que es público y se definen también en un conjunto de documentos disponibles al público. Estos documentos se denominan Solicitudes de Comentarios (RFCS). Contienen las especificaciones formales de los protocolos de comunicación de datos y los recursos que describen el uso de los protocolos.

Las RFCS también contienen documentos técnicos y organizacionales sobre internet, incluyendo las especificaciones técnicas y los documentos de las políticas producidos por el Grupo de Trabajo de Ingeniería de Internet (IETF).

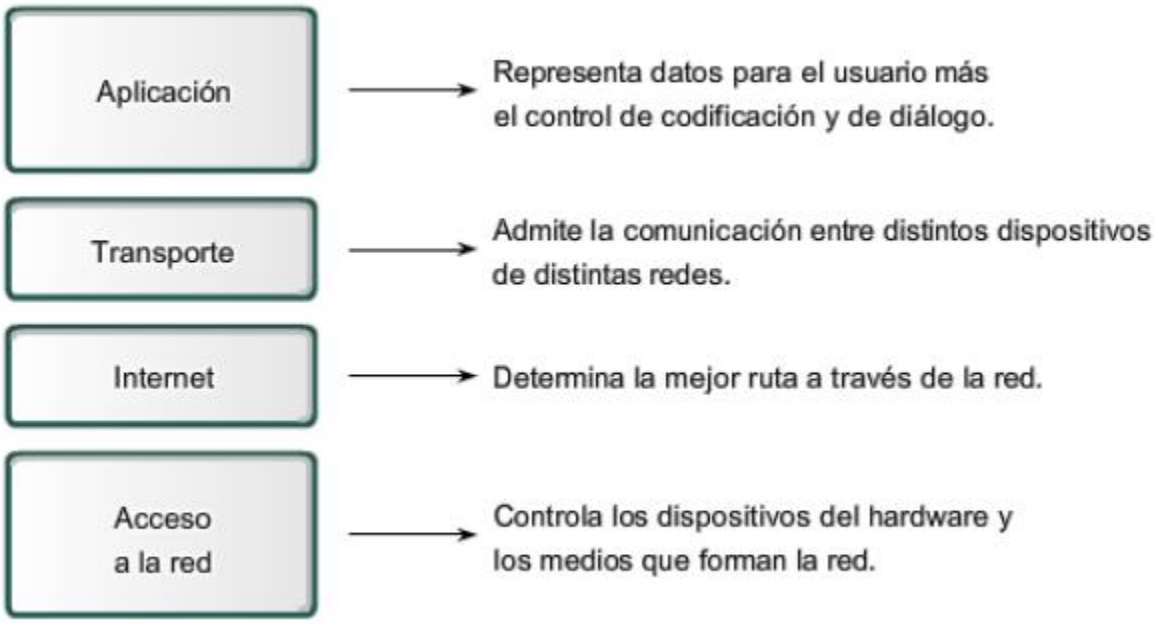


Figura 1. 6 Modelo TCP/IP

El modelo TCP/IP describe la funcionalidad de los protocolos que forman la suite de protocolos TCP/IP. Estos protocolos, que se implementan tanto en el host emisor como en el receptor, interactúan para proporcionar la entrega de aplicaciones de extremo a extremo a través de una red.

Un proceso completo de comunicación incluye los siguientes pasos:

1) Creación de datos a nivel de la capa de aplicación del dispositivo origen.
2) Segmentación y encapsulación de datos cuando pasan por la stack de protocolos en el dispositivo origen.
3) Generación de los datos sobre el medio en la capa de acceso a la red del stack.
4) Transporte de los datos a través de la internetwork, que consiste de los medios y de cualquier dispositivo intermediario.
5) Recepción de los datos en la capa de acceso a la red del dispositivo destino.
6) Desencapsulación y rearmado de los datos cuando pasan por la stack en el dispositivo destino.
7) Traspaso de estos datos a la aplicación en la capa de aplicación del dispositivo destino.

1.6 Modelo de referencia OSI

El modelo OSI (Open System Interconnection) fue diseñado por la Organización Internacional para la Estandarización (ISO), con el fin de proporcionar un marco sobre el cual se pudiera crear una suite de protocolos de sistemas abiertos. Se buscaba que este conjunto de protocolos se utilizara para desarrollar una red internacional que no dependiera de sistemas propietarios.

Sin embargo, la gran velocidad a la que fue adoptada internet basada en TCP/IP y la proporción en la que se expandió ocasionaron que el desarrollo y la aceptación de la suite de protocolos OSI quedaran atrás. Son solamente pocos los protocolos desarrollados mediantes las especificaciones OSI los que se utilizan masivamente en la actualidad, más sin embargo el modelo OSI ha realizado aportaciones muy importantes para el desarrollo de otros protocolos y productos para todos los tipos de nuevas redes.

Como modelos de referencia, el modelo OSI proporciona una amplia lista de funciones y servicios que pueden producirse en cada una de sus siete capas. También describe la interacción de cada capa con las capas directamente por encima o debajo de él.

Figura 1. 7 Modelo OSI

1.7 Red de Área Local LAN

La infraestructura de red puede variar en gran medida en términos del tamaño del área cubierta, la cantidad de usuarios conectados y la cantidad y tipos de servicios disponibles.

Una red individual generalmente cubre una única área geográfica y proporciona servicios y aplicaciones a personas dentro de una estructura organizacional común, como una empresa, un campus o una región. Este tipo de red se denomina red de área local (LAN).

Una red de área local por lo general está administrada por una organización única. El control administrativo que rige las políticas de seguridad y control de acceso está implementado en el nivel de red. La velocidad de operación de una red LAN oscila entre 10 y 100 Mbps.

Algunos ejemplos de este tipo de redes son: Ethernet (IEEE 802.3), Token Bus (IEEE 802.4) y Token Ring (IEEE 802.5).

1.7.1 Ethernet

Diseñada originalmente por Intel, Xerox y Digital por lo que su nombre inicial fue Ethernet DIX. En 1983 fue normalizado como estándar Ethernet 802.3 por IEEE.

Es un protocolo de redes LAN donde su velocidad de transmisión entre computadoras es de 10 Mbps. Inicialmente se utilizaba cable coaxial, posteriormente en los 90's, la extensión de las redes Ethernet permitió el uso de cableado estructurado.

Los cuatro componentes de Ethernet son:

- Medio físico: Son aquellos componentes físicos que son utilizados para transportar la señal entre los equipos de red.
- Componentes de señalización: Son dispositivos electrónicos que envían y reciben señales sobre el canal Ethernet.
- Conjunto de reglas para acceder al medio: Son los protocolos utilizados por la tarjeta de red que controlan el acceso al medio y permiten a los equipos acceder al canal Ethernet.
- Trama Ethernet: Es un conjunto de bits. La trama es la encargada de llevar la información en la red.

1.7.2 Token BUS

Es un protocolo para redes de área local diseñado para la topología tipo bus, pudiendo ésta funcionar lógicamente como una topología tipo anillo.

El paso del token se da punto a punto, pero la forma de transmisión de datos es por difusión. El token es una bandera o estafeta y quien posee el token es el nodo que tiene el derecho de enviar la información. Utiliza cable coaxial o fibra óptica de 75 ohms. En el caso del cable coaxial las velocidades para la transmisión de datos son de 1.5 a 20 Mbps.

1.7.3 Token Ring

La topología más utilizada para las conexiones físicas de token ring es la de estrella. Se utiliza el cable de par trenzado para la comunicación de dispositivos en token ring.

Las redes token ring van desde 4 Mbps hasta 1 Gbps, pero hay que tomar en cuenta que la velocidad de transmisión debe estar configurada de la misma manera en todos los nodos o la comunicación no será posible.

1.8 Direccionamiento

Durante la transmisión de información a través de la red, un flujo de datos se puede dividir en partes y entrelazarse con los mensajes que viajan también a través de la red y que pertenecen a otro proceso de transmisión. Mucha información fragmentada viaja por la red en todo momento, por lo cual es muy importante que cada parte de los datos enviados contenga suficiente información de identificación para poder llegar al destino correcto.

Hay diferentes tipos de direcciones que deben incluirse para que el envío de información se realice satisfactoriamente desde una aplicación de origen hasta su destino. Basado en el modelo de referencia OSI se pueden observar distintas direcciones e identificadores necesarios en cada capa.

Durante todo el proceso de encapsulación se van agregando identificadores de dirección a los datos mientras recorren el stack del protocolo en el host origen. Así como hay múltiples capas de protocolos que preparan los datos para transmitirlos a sus destinos, existen también múltiples capas de direccionamiento para asegurar la correcta entrega.

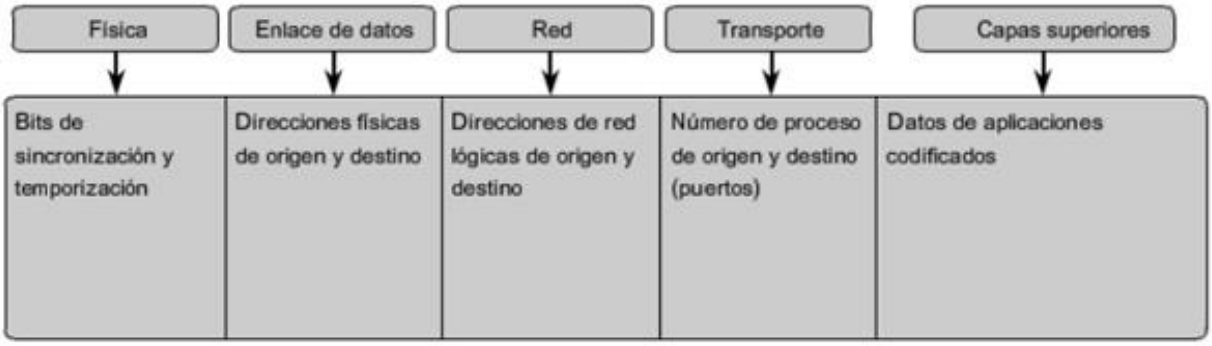


Figura 1. 8 Direcciones e identificadores en cada capa del Modelo OSI

La dirección física del host es el primer identificador, aparecen en el encabezado de la PDU (Protocol Data Unit) de capa 2 y se llama Trama. La capa 2 está relacionada con la entrega de los mensajes en una red local única. La dirección de la capa 2, por lo tanto, es exclusiva en la red local y representa la dirección del dispositivo final en el medio físico. En una LAN que utiliza Ethernet, esta dirección se denomina dirección de Control de Acceso al Medio (MAC).

Los protocolos de capa 3 están diseñados principalmente para mover datos desde una red local a otra red local dentro de una internetwork. Por lo tanto las direcciones de capa 3 deben incluir identificadores que permitan a dispositivos de red intermediarios ubicar hosts en diferentes redes. En la suite de protocolos TCP/IP, cada dirección IP host contiene información sobre la red en la que está ubicado el host.

En la frontera de cada red local, un dispositivo de red intermediario, por lo general un router, desencapsula la trama para leer la dirección host de destino que está contenida en el encabezado del paquete, la PDU de capa 3. Con la porción del identificador de red de esta dirección, los routers determinan qué ruta utilizar para llegar al host de destino.

En la capa 4 la información contenida en el encabezado de la PDU no identifica un host de destino o una red de destino. Lo que si identifica es el proceso o servicio específico que se ejecuta en el dispositivo host de destino que actuará en los datos que se entreguen.

Cada aplicación o servicio es representado por un número de puerto en la capa 4. Un diálogo único ente dispositivos se identifica con un par de número de puerto de origen y de destino de capa 4 que son representativos de las dos aplicaciones de comunicación. Cuando los datos se reciben en el host, se examina el número de puerto para determinar qué aplicación o proceso es el destino correcto de los datos.

1.9 VLAN

Una de las principales características que se presenta en una red de área local es que los dispositivos o nodos que pertenecen a esta red comparten los recursos del medio físico, es decir el ancho de banda proporcionado por el mismo.

El uso de un switch proporciona un mejor rendimiento en la red ya que, a diferencia de un hub, este dispositivo segmenta o divide los dominios de colisiones.

Sin embargo, algo que no pueden mejorar ni el switch ni el hub en una red de área local, es el envío de mensajes de broadcast. En una red LAN estos mensajes de broadcast son enviados a través de todos los puertos del hub o switch. Si un dispositivo quiere comunicarse con otro y no sabe dónde se encuentra, utilizará este recurso generando

tráfico excesivo en el medio ya que todos los dispositivos de la red local recibirán el mensaje, aunque solo lo atenderán si se trata del dispositivo destinado a recibir dicho mensaje.

En muchas ocasiones estos mensajes son tráfico innecesario que consume recursos del medio y que pueden llegar a afectar los servicios proporcionados por la red, tales como disponibilidad o calidad de servicio.

Para atender este problema se crearon la Redes de Área Local Virtuales comúnmente conocidas por sus siglas VLAN. Las VLANs cuales se configuran en los switches permitiendo dividir en diferentes dominios de broadcast a un switch, con la finalidad de no incluir a todos los puertos del switch dentro de un solo dominio de broadcast.

Una VLAN puede definirse como una serie de dispositivos conectados en red, que a pesar de que pueden estar conectados en diferentes equipos de interconexión o zonas geográficas distintas pertenecen a la misma red de área local.

La implementación de VLANs en conjunto con el uso de switches en lugar de hubs brinda una serie de beneficios entre los que destacan:

- Aislamiento de los dominios de colisión por cada uno de los puertos.
- Ancho de banda dedicado a cada uno de los puertos, por lo tanto, a cada dispositivo conectado a ellos.
- Mayor seguridad ya que cada puerto es designado a una VLAN específica y/o dispositivo único.
- Mejor control en la administración de direcciones IP. Cada VLAN preferentemente cuenta con un bloque de direcciones IP.
- Diferentes áreas de la empresa u organización pueden ser asignadas a VLANs independientes, permitiendo así que cada área tenga su red local y ciertos servicios.

Cada VLAN es independiente de otra en función de las necesidades de la red y el por qué fueron configuradas. En ocasiones es necesaria la comunicación entre dispositivos pertenecientes a VLANs distintas. Para ello se requiere de un dispositivo dentro de la LAN que sea capaz de entender los formatos de los paquetes con que están formadas las VLANs. Este dispositivo es un equipo de capa 3, tal como un router o inclusive un switch que cuente con los recursos necesarios para pertenecer a la clasificación de capa 3.

La implementación y funcionamiento de las VLANs está definido por el organismo internacional IEEE Computer Society en el documento descriptivo IEEE 802.1Q.

1.9.1 Clasificación de las VLANs

Anteriormente existía la red plana, donde el broadcast se repetía en todos los puertos del switch y esto provocaba una situación crítica debido al alto consumo de recursos de la red. Actualmente con la implementación de VLANs existe una segmentación lógica o virtual que resuelve este problema.

Aunque las más comunes son las VLANs basadas en puertos (nivel 1), éstas pueden clasificarse en cuatro tipos diferentes según el nivel de la jerarquía del modelo OSI en el que operen:

- ***VLAN por puerto (Nivel 1):*** Conocida como *Port Switching*. Se especifica qué puertos del switch pertenecen a la VLAN, los dispositivos o miembros de dicha VLAN son los que se conectan a esos puertos. No permite la movilidad de los usuarios.

- ***VLAN por MAC (Nivel 2):*** Se asignan hosts a una VLAN en función de su dirección MAC (Media Access Control). Tiene la ventaja de que no hay que reconfigurar el dispositivo de conmutación si el usuario cambia su localización, es decir, si se conecta a otro puerto de ese u otro dispositivo. El principal inconveniente es la asignación de usuarios cuando hay una gran cantidad de ellos.

- ***VLAN por dirección de subred – subred virtual (Nivel 3):*** La cabecera de nivel 3 se utiliza para mapear la VLAN a la que pertenece. En este tipo de VLAN son los paquetes y no las estaciones quienes pertenecen a la VLAN.

- ***VLAN de niveles superiores:*** Se crea una VLAN por cada aplicación: FTP (File Transfer Protocol), flujos multimedia, correo electrónico, etc. La pertenencia a una VLAN puede basarse en una combinación de factores como puertos, direcciones MAC o subredes.

1.9.2 Protocolos de las VLANs

Durante todo el proceso de configuración y funcionamiento de una VLAN es necesaria la participación de una serie de protocolos entre los que destacan el IEEE 802.1Q, STP (Spanning Tree Protocol) y GVRP (Generic VLAN Registration Protocol).

El protocolo IEEE 802.1Q se encarga del etiquetado de las tramas que se asociada inmediatamente con la información de la VLAN.

El cometido principal de Spanning Tree Protocol es evitar la aparición de bucles lógicos para que haya un sólo camino entre dos nodos.

Definido en la 802.1Q, el protocolo GVRP, permite que los conmutadores descubran de forma automática información de las VLANs y sus miembros, proceso que anteriormente requería de configuraciones manuales en todos los conmutadores de la red. Esto permite conocer qué VLANs se encuentran registradas en cada uno de los puertos de un conmutador.

No sólo permite el mantenimiento dinámico de los puertos asociados a una VLAN en un conmutador, sino que además facilita su propagación a otros conmutadores, lo que les permite conocer qué VLANs se encuentran alcanzables por un determinado puerto. De esta manera tan sólo sería necesario configurar la información de las VLANs en un conmutador, propagándose al resto de forma automática.

1.10 Cableado Estructurado

1.10.1 Introducción

Hasta 1985 no había estándares para realizar el cableado en los sistemas de comunicación e información. Cada sistema tenía sus propios requerimientos acerca de las características del cableado que cada uno de ellos necesitaba. La telefonía y la transferencia de datos estaban separadas y los equipos informáticos requerían de cableados con características especiales que dependían de la marca de dichos equipos.

Cuando nuevas tecnologías surgieron y los sistemas informáticos evolucionaron, las empresas y organizaciones comenzaron a requerir de estas nuevas tecnologías, las cuales aún condicionaban al uso de cierto tipo de cables, conectores e instalaciones. Esto provocó inconformidad por parte de los clientes ya que no existía compatibilidad entre las diferentes tecnologías que ellos adquirían.

En 1985 la CCIA (Computer Communications Industry Association) Solicitó a la EIA (Electronic Industries Alliance) realizar un estándar referente a los sistemas de cableado. Se logró así comprender que era necesario realizar un estándar que contemplara todos los requerimientos de cableado de los sistemas de comunicaciones, como voz y datos.

La EIA asignó la tarea de desarrollar estos estándares de cableado al comité denominado TR-41. Este comité se enfocó en desarrollar estándares que fueran independientes de las tecnologías de los sistemas de comunicaciones y de los fabricantes.

Este proyecto que hasta hoy sigue aplicando, ha derivado en un conjunto de recomendaciones (denominados estándares) acerca de las infraestructuras de cableado para edificios comerciales y residenciales.

Aunque no existe una definición oficial para cableado estructurado, no hay mucha diferencia entre las diversas publicaciones. Una definición concisa es: *Cableado estructurado es el sistema de cableado de telecomunicaciones para edificios que soporta aplicaciones de voz, datos y videos*.

Aplicaciones de voz se refiere a la telefonía y audio de alta calidad. Datos es aquella información intercambiada en redes LAN, WAN, Internet; Finalmente video contempla el servicio de videoconferencia, TV por cable, etc.

1.10.2 Objetivos del Cableado Estructurado

Entre los objetivos del cableado estructurado se encuentran:

- Poder realizar una instalación compatible con las tecnologías actuales y las que se visualizan a futuro.
- Proveer de flexibilidad para realizar movimientos internos de equipos dentro de las instalaciones.
- Proporcionar un diseño que permita una fácil administración, supervisión y mantenimiento de la red.

1.10.3 Subsistemas de Cableado Estructurado

Todo el sistema de cableado estructurado se compone a su vez de varios subsistemas que a continuación se describen:

1. ***Entrada de edificio: (Acometida):***

   La entrada de edificio o acometida se refiere a los cables, hardware de conexión, elementos de protección y equipos requeridos para conectar las instalaciones de planta externa de los proveedores de servicio con el sistema de cableado estructurado propiedad del cliente.

2. ***Conexión cruzada principal o intermedia (Cuarto de equipo):***

   La conexión cruzada principal o intermedia puede estar localizada en la misma área que el cuarto de equipo, su principal función es la de proveer servicios de telecomunicaciones en cualquier punto del edificio; lo que se logra a través de

conexiones con cordones de parcheo o cable jumper en consistencia con las conexiones cruzadas horizontales.

3. ***Cableado Vertebral o Backbone:***

   El cableado vertebral o backbone provee la interconexión entre los diferentes armarios de telecomunicaciones, el cuarto de equipo y la entrada al edificio. Los principales componentes del backbone incluyen los cables, las conexiones cruzadas intermedias y la principal, las terminaciones mecánicas y los cordones de parcheo para realizar las conexiones backbone a backbone.

4. ***Armario de Telecomunicaciones (Conexión cruzada horizontal):***

   La función principal del armario de telecomunicaciones es la de concentrar las terminaciones de todo tipo de cable horizontal reconocido por el estándar. Los cables backbone también son terminados aquí con el fin de extender servicios de telecomunicaciones hacia las áreas de trabajo, por medo de cordones de parche o cable jumper.

5. ***Cableado Horizontal (Distribución):***

   El cableado horizontal o de distribución es la parte del sistema que va desde el área de trabajo hasta la conexión cruzada horizontal en el armario de telecomunicaciones. El cableado horizontal incluye los cables de distribución, las salidas de telecomunicaciones en el área de trabajo, las terminaciones mecánicas del cable y cordones de parcheo en el armario de telecomunicaciones.

6. ***Área de Trabajo:***

   Los componentes del área de trabajo son los contenidos desde la salida de telecomunicaciones hasta el equipo del usuario y están fuera del alcance del estándar. Se asumen cordones de parcheo con una distancia máxima de 3 metros.

1.10.4 Normas del Cableado Estructurado

Electronics Industries Asociation (EIA) y Telecommunicatios Industries Asociation (TIA), quienes agrupan a las industrias de electrónica y de telecomunicaciones de los Estados Unidos son quienes dieron a conocer en forma conjunta la norma TIA/EIA 568, la cual establece las pautas a seguir para el diseño e implementación del cableado estructurado.

Las normas TIA/EIA fueron creadas como norma de industria pero han sido empleadas como normas internacionales ya que fueron las primeras en publicarse.

En complemento con la norma TIA/EIA 568-A, ANSI/TIA/EIA emite una serie de normas que a continuación se describen:

1- ***ANSI/TIA/EIA 568-A:*** Especifica un sistema de cableado de telecomunicaciones común para edificios comerciales que soportan un ambiente multiproducto y multifabricante.

   También proporciona métodos requeridos en el diseño de productos de telecomunicaciones para empresas comerciales.

   Su propósito es permitir la planeación e instalación de cableado de edificios comerciales con muy poco comienzo de los productos de telecomunicaciones que serán instalados con posterioridad. Con esto se busca que la instalación de sistemas de cableado durante la construcción o renovación de edificios sea menos costosa.

2- ***ANSI/TIA/EIA 568-B:*** Es un conjunto de estándares que se refieren al cableado e edificios comerciales para productos y servicios de telecomunicaciones. En general da referencia de cómo instalar el cableado.

   Los estándares ANSI/TIA/EIA 568-B fueron publicados en el año 2001 por primera vez y sustituyeron al conjunto de estándares TIA/EIA 568-A que en la actualidad han quedado obsoletos.

   Entre las diversas secciones de este conjunto de estándares están:

   - ***TIA/EIA-568-B1:*** Detalla los requerimientos generales.
   - ***TIA/EIA-568-B2***: Describe los componentes del cableado estructurado mediante par trenzado balanceado. El tipo de cable y calidad del medio de transmisión a implementar.
   - ***TIA/EIA-568-B3:*** Describe los componentes de cableado de fibra óptica.

3- ***ANSI/TIA/EIA-569***: Especifica la infraestructura del cableado de telecomunicaciones, a través de tuberías, registros, pozos, trincheras, canales, entre otros, para su buen funcionamiento y desarrollo a futuro.

4- ***ANSI/TIA/EIA-570:*** Especifica las normas para la instalación de Sistemas de Telecomunicaciones en áreas residenciales y comerciales de baja densidad.

5- ***ANSI/TIA/EIA-606***: Regula y sugiere los métodos para la administración de los sistemas de telecomunicaciones. La administración hace referencia a documentación, etiquetación, planos, reportes y hojas de trabajo.

6- ***ANSI/TIA/EIA-607***: Regula las especificaciones sobre los sistemas de puesta a tierra y sistemas de alimentación bajo los cuales se deberán operar y proteger los elementos del sistema estructurado.

7- ***TIA/EIA TSB-67:*** Regula las especificaciones de equipos para la prueba, medición y certificación de sistemas de cableado estructurado.

8- ***TIA/EIA TSB-72:*** Regula la instalación de sistemas centralizados bajo la tecnología de fibra óptica.

9- ***TIA/EIA TSB-75***: Regula lo relacionado a los espacios de oficinas abiertas u oficinas con mucho movimiento por parte del personal.

1.10.5 Componentes del Cableado Estructurado

En la siguiente sección se detallan los componentes más comunes en las instalaciones de cableado estructurado de alcance medio.

1.10.5.1 Cables de red

Los cables de red para transmisión y/o transferencia de datos que son utilizados comúnmente son:

- ***UTP Unshielded Twisted Pair (par trenzado sin blindaje):*** Cable de pares trenzados de cobre, por lo general no protegidos, simplemente están aislados con un plástico PVC, por lo tanto sujetos a la interferencia electromagnética, con una longitud máxima de 100 metros, más longitud provocaría una pérdida de información y de la señal. Existen 7 categorías:

  Categoría 1: Los cables se componen de dos pares de polos y son implementados únicamente para el uso del teléfono.

  Categoría 2: Con una tasa máxima de transferencia de 4 Mbps, se utilizan principalmente para el uso del teléfono.

Categoría 3: Conocido como Ethernet 10BaseT, tienen una velocidad máxima de 10 Mbps.

Categoría 4: Conocido como Ethernet 10baseT/TokenRing con una velocidad máxima de 20 Mbps.

Categoría 5: Conocido como Ethernet 100BaseT/10BaseT con una velocidad máxima de 100 Mbps. Actualmente se utiliza en la mayoría de redes corporativas y del hogar. Con el tiempo se acabó convirtiendo en un estándar. Actualizado a la categoría 5e.

Categoría 6: Resiste muy bien el ruido de interferencias de señal gracias a su blindaje, alcanza velocidades de hasta 1 Gbps. Y puede transmitir datos hasta distancias de 100 metros.

Categoría 7: Posee blindaje para cada par hilos de cobre y para el cable entero, de esta forma resiste muy bien el ruido de interferencias de señal, permite transmisiones de una velocidad de 10 Gbps a distancias de hasta 100 metros.

- ***FTP Foiled Twisted Pair (par trenzado frustrado o pantalla global):*** Los cables no están apantallados, pero si dispone de un apantallamiento global que mejora la protección en contra de posibles interferencias externas, las propiedades de transmisión son muy similares a las del cable UTP.

- ***STP Shielded Twisted Pair (par trenzado con blindaje):*** Muy similar al UTP, pero protegido con una funda o malla metálica. Resiste mucho más a las perturbaciones externas y radiaciones electromagnéticas, suele ser utilizado para las conexiones entre dispositivos de comunicación de datos (routers y switches).

- ***Optical Fiber (Fibra Óptica):*** Está formado por un par de cables de fibra de vidrio, cada uno consta de un núcleo central de plástico o cristal con un alto índice de refracción, rodeado de una capa de un material similar con un índice de refracción ligeramente menor. Existen dos tipos: Mononodo y Multinodo.

  Mononodo: Solo transmite por un modo de haz de luz axial y se utiliza para grandes distancias, a su vez es mucho más vulnerable en cuanto a su manejo.

  Multinodo: Transmite por miles de modos de haces de luz de rebote y se utiliza para transmisión de conexiones a poca distancia. Es capaz de transportar y/o recibir señales de luz hasta unos 40 kilómetros.

- ***Thinnet coaxial (Cable Coaxial):*** Cable coaxial con un diámetro de aproximadamente 0,6 cm y el cual puede transportar datos hasta una distancia de 180 metros.

- ***Coaxial Thicknet:*** Cable de red muy similar al coaxial Thinnet, pero con un diámetro de aproximadamente 1,3 cm y puede transferir datos hasta una distancia de unos 500 metros.

Figura 1. 9 UTP Par trenzado sin blindaje

Figura 1. 10 FTP Par trenzado de pantalla global

Figura 1. 11 STP Par trenzado con blindaje

Figura 1. 12 Fibra Óptica

Figura 1. 13 Cable Coaxial

Figura 1. 14 Cable Coaxial Thicknet

1.10.5.2 Plug RJ-45

Es un plug de 8 contactos o pines que es similar al plug RJ11 utilizado en telefonía, pero con mayor capacidad. Idealmente posee los contactos bañados en oro.

Figura 1. 15 Plug RJ45

1.10.5.3 Conectores RJ-45 Hembra

Es un dispositivo modular de conexión mono línea, hembra, destinado para conectar el plug RJ-45. Diseñado para permitir su inserción en rosetas y frentes de patch panel.

Figura 1. 16 Conector RJ45 hembra

1.10.5.4 Roseta RJ-45 Hembra

Es una pieza plástica de soporte que se monta en las paredes, la cual permite comúnmente insertar 2 conectores RJ-45 hembra.

Figura 1. 17 Roseta RJ45 hembra

1.10.5.5 Tapa para RJ-45

Es una pieza plástica plana utilizada como soporte y tapa de una caja estándar de electricidad, comúnmente permite insertar dos conectores RJ-45 hembra.

Figura 1. 18 Tapa para RJ45

1.10.5.6 Patch Panel

Es un panel metálico o plastificado que se encarga de recibir todas las conexiones que existan en el cableado estructurado de una red. Una de sus principales características es que permite organizar las conexiones entrantes de la red, además su correcta implementación evita que se trabaje directamente con los equipos intermediarios (router, switch, etc.), previniendo posibles daños al tener que conectar y desconectar constantemente los cables en los puertos de los equipos.

Figura 1. 19 Patch Panel

1.10.5.7 Rack o gabinete

Un rack es un soporte metálico utilizado para montar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están normalizadas para que sean compatibles con equipos de cualquier fabricante.

Figura 1. 20 Rack o gabinete

1.10.5.8 Canaleta

Las canaletas son tubos metálicos o plásticos que proporcionan al cable una mayor protección en contra de interferencias electromagnéticas originadas por los diferentes motores eléctricos. Para que las canaletas protejan a los cables de dichas perturbaciones es indispensable la óptima instalación y la conexión perfecta en sus extremos.

Figura 1. 21 Canaleta

1.10.5.9 Pinzas crimpeadoras (ponchadoras)

Son pinzas especiales para crimpear conectores. Usualmente cuentan con aditamentos como cortador de cable y pela cable.

Figura 1. 22 Pinzas crimpeadoras o ponchadoras

1.10.5.10 Pinzas de impacto

Son pinzas diseñadas para dar distintas presiones de trabajo en función de los conectores que se desean armar. En redes son utilizadas en los conectores RJ-45 hembra al momento de realizar la configuración con los cables.

Figura 1. 23 Pinzas de impacto

1.10.5.11Pinzas desnudadoras o pelacables

Las pinzas desnudadoras son una herramienta diseñada para pelar cables, es decir, quitar el aislante que los recubre.

Figura 1. 24 Pinzas desnudadoras o pelacables

1.10.5.12 Probador de cableado o tester

Permiten detectar fácilmente la correcta configuración y armado de los cables verificando si existen fallas provocadas por algún corto circuito, desgaste en los cables o mal armado.

Figura 1. 25 Probador de cableado o tester

1.10.6 Beneficios del Cableado Estructurado

Son muchos los beneficios que se obtienen al diseñar e implementar una red basándose en los estándares internacionales de cableado estructurado. Entre algunos de estos beneficios se puede mencionar que:

- Reduce considerablemente el tiempo de improductividad al momento de presentarse un problema o falla en la red ya que es un sistema modular y flexible.

- Al implementar un sistema de cableado estructurado se obtiene la facilidad de interconexión temporal para poder trasladar usuarios rápidamente en lugar de requerir cables adicionales.

- Un sistema de cableado estructurado está diseñado para ser independiente de un proveedor y aplicación específicos. Gracias a esto los cambios que se requieran realizar en la red y en el equipamiento pueden llevarse a cabo con las instalaciones existentes.

- Un sistema de cableado estructurado bien normalizado posee una vida útil mayor a los 10 años, por lo cual el sistema de cableado durará en promedio mucho más que cualquier otro componente de la red.

- Es altamente administrable por el usuario.

- Está diseñado para adaptarse fácilmente a nuevas tecnologías.

CAPÍTULO II
Estado actual de la red

El Laboratorio de Geomática y Especialidades de Civiles de la Facultad de Ingeniería de la UNAM ha brindado servicio a profesionales, académicos y alumnos desde hace ya más de 13 años, cumpliendo el objetivo de brindarles las herramientas necesarias para el desarrollo y aplicación de conocimientos a los departamentos de la División de Ingenierías Civil y Geomática, Estructuras, Construcción, Geotecnia, Ingeniería de Sistemas y Planeación, Ingeniería Hidráulica, Ingeniería Sanitaria y Ambiental.

Este laboratorio es coordinado por el Ingeniero Francisco López Mendieta, quien en conjunto con un ayudante de laboratorio y prestadores de servicio social brindan todos los servicios técnicos y administrativos que se llevan a cabo en el laboratorio.

Sin embargo, dentro del laboratorio no existe el personal especializado en atender los requerimientos básicos de análisis, mantenimiento y mejoras constantes en la red del laboratorio; lo cual ha derivado en que después de más de 13 años de servicio continuo, existan fallas en la red que afectan de manera importante los servicios que se brindan a los usuarios.

No existe documentación acerca de la red, planos, manuales de uso o configuración de dispositivos, ni tampoco documentos que describan cómo dar mantenimiento a los componentes de la red.

Los servicios de red, tanto a nivel local como de internet, son la base del funcionamiento del laboratorio. Muchas de las herramientas que son utilizadas requieren de los servicios de internet, además, profesores que complementan sus clases teóricas con sesiones prácticas en el laboratorio demandan servicios de red locales con el fin de compartir material didáctico a sus alumnos de manera ágil.

Es por esto que es necesario realizar un análisis del estado actual de la red, con el fin de poder aplicar un plan de mantenimiento correctivo y preventivo que permita que los servicios que el laboratorio brinda a la comunidad universitaria no se vean interrumpidos por fallas en la red.

En este capítulo se describirá el estado actual de la red. Primero se monitoreará la red para poder registrar todos los eventos o fallas que se presenten; después se realizará el descubrimiento de la red, es decir, de todos los componentes que la conforman, del cableado estructurado y de los dispositivos de interconexión. Se realizará la documentación descriptiva de la red, misma que será entregada al coordinador del laboratorio.

En conjunto con los documentos descriptivos de la red y sus componentes, se realizarán los planos del laboratorio, en los cuales se indicará el tendido del cableado, la ubicación de nodos, canaletas y el tendido en el cuarto de telecomunicaciones.

Con todas estas actividades se pretende detectar la mayor cantidad de fallas en la red, tanto físicas como lógicas, estándares o normas que no se cumplan y así poder realizar un análisis del estado de la red que permita desarrollar un plan de mantenimiento para corregir la mayor cantidad de fallas detectadas.

2.1 Monitoreo de la red

Con la finalidad de obtener un registro confiable de eventos o fallas ocurridas en la red del laboratorio, se configurará un monitor Nagios.

Nagios es un sistema de monitoreo de código abierto que permite vigilar el comportamiento del hardware y software de los equipos, según se especifique en su configuración. Es capaz de identificar el estado del uso del procesador, del disco duro, de la memoria y del estado de los dispositivos, entre muchos otros servicios.

Además, es un sistema que permite crear registros de todos los eventos ocurridos y también facilita la consulta de dichos registros en función de ciertos parámetros que sean requeridos, como por ejemplo, mostrar un historial de fallas provocadas por exceso de carga en el procesador.

Su compatibilidad con sistemas Windows y Linux permite que se implemente en el laboratorio sin ningún conflicto. No es un sistema que demande muchos recursos, y su interfaz gráfica y fácil configuración permite que su manejo sea sencillo.

2.1.1 Requerimientos e instalación del servidor Nagios

Los requerimientos mínimos para poder instalar el sistema de Nagios en una computadora se presentan en la *Tabla 1*:

Requerimientos del Sistema del Servidor	

Sistema Operativo	• *Linux: Kernel 2.4+:*
	  ○ *RHEL*
	  ○ *SLES*
	  ○ *Ubuntu*
	  ○ *Fedora*
	  ○ *Debian*
	  ○ *CentOS*

	• *Unix:*
	  ○ *Solaris 9+*
	  ○ *FreeBSD 6.4+*

Hardware	• *1 GHz CPU, 512 RAM (mínimo)* • *2 GHz+ CPU, 1GB+ RAM (recomendado)*
Almacenamiento	• *512 MB de espacio libre (mínimo)* • *2 GB de espacio libre (recomendado)*
Software	• *Firefox 2.0+* • *Internet Explorer 5.5+* • *Safari 2.0+* • *Apache* • *PHP*

Tabla 1 Requerimientos del sistema para la instalación de Nagios

Los requerimientos mínimos garantizan que puedan ser monitoreados hasta 50 equipos y 250 servicios, es decir, 5 servicios por cada equipo que sea monitoreado.

El laboratorio cuenta con equipos asignados para los alumnos, administración y servicio social. Sin embargo, no hay posibilidad de emplear alguno de estos equipos para el monitoreo debido a que son requeridos diariamente y el monitoreo de la red requiere de un equipo dedicado para esta función.

El equipo propuesto para la instalación de Nagios es un equipo portátil pero con buenos recursos que permitirán que el sistema de Nagios trabaje de manera eficiente. A continuación se muestran las características del equipo a utilizar como servidor Nagios en la *Tabla 2*.

Características de equipo propuesto como servidor Nagios	
Sistema Operativo	*Ubuntu 12.04 LTS*
Hardware	*CPU Dual Core a 1.86 GHz, 3GB RAM*
Almacenamiento	*160 GB de espacio libre*
Exploradores	*Firefox Mozilla 28.0*

Tabla 2 Equipo propuesto para la instalación de Nagios

Con estas características, el equipo dedicado a realizar el monitoreo de la red puede, según las especificaciones oficiales de Nagios, monitorear 100 computadoras y hasta 600 servicios sin presentar problemas. Cantidades que cubren perfectamente las requeridas en el laboratorio.

La instalación de Nagios requiere la descarga del software desde el portal oficial *www.nagios.com*, también es recomendada la creación de un usuario dedicado al uso de

Nagios dentro del sistema. El proceso de instalación se omite debido a que es público en el portal oficial de Nagios.

2.1.1.1 Configuración de Nagios

Nagios es altamente configurable, lo que permite que con una correcta configuración no se desperdicien recursos de la computadora monitoreando servicios que no se desean.

La configuración requerida para monitorear el laboratorio es muy sencilla. Se requieren agregar manualmente todos los equipos (hosts) que se van a monitorear, declarar los servicios que se desean atender y, para una mejor organización y reconocimiento de los equipos, se deben crear grupos que especifiquen las diferentes secciones del laboratorio y sus correspondientes equipos.

Para la definición de un host, se debe editar el archivo *windows.cfg*, mismo que se encuentra en el directorio del sistema: */usr/local/nagios/etc/objects,* Por cada host que se quiere monitorear se debe agregar la siguiente sentencia:

```
define host{
        use             windows-server  ;
        host_name       EQUIPO69        ; The name we're giving to this host
        hostgroups      LE02
        alias           Equipo69        ; A longer name associated with the host
        address         192.168.199.69  ; IP address of the host
        }
```

Los campos requeridos para cada sentencia son:

- ***use:*** Especifica qué plantilla se requiere utilizar, en este caso como los dispositivos a monitorear utilizan un sistema operativo Windows, se debe utilizar la plantilla *windows-server.*
- ***host_name:*** Es el nombre que se le quiere dar al host definido. Idealmente se coloca el nombre del equipo para facilitar su identificación.
- ***hostgroups:*** Es el nombre del grupo al que pertenece el host definido. El grupo debe estar definido.
- ***alias:*** Es un nombre que puede ser de mayor longitud que el *host_name,* y que se asocia al host definido.
- ***address:*** Es la dirección IP del host definido.

Para la definición de grupos, también se debe configurar el archivo *windows.cfg*, agregando por cada grupo requerido la siguiente sentencia:

```
}

define hostgroup{
        hostgroup_name  LE01 ; The name of the hostgroup
        alias           LE01 ; Long name of the group
}
```

Únicamente se requieren los campos *hostgroup_name* y *alias, ya que es en la definición de cada host en donde se especifica a que grupo pertenece.*

Para la configuración necesaria en el laboratorio, únicamente se requiere la creación de 2 grupos, el grupo LE01 y el grupo LE02. Cada uno pertenece a una sección del laboratorio que más adelante de este capítulo se describirán.

Finalmente, es necesaria la declaración de los servicios que se requiere que Nagios revise. Estas declaraciones también se llevan a cabo en el archivo *windows.cfg* y se realizan de la siguiente manera:

```
define service{
        use                     generic-service
        hostgroup_name          LE02,LE01
        service_description     NSClient++ Version
        check_command           check_nt!CLIENTVERSION
        }
```

Los campos requeridos son:

- ***use:*** Específica qué plantilla se requiere utilizar para la definición del servicio, en este caso se utilizará la plantilla genérica de Nagios.
- ***hostgroup_name:*** Especifica a qué grupos, previamente definidos, se les asociará con el servicio que se define.
- ***service_description:*** Es el nombre o identificador del servicio, que servirá como referencia.
- ***check_command:*** Es el comando que Nagios ejecutará para la comprobación del funcionamiento del servicio definido.

A continuación se ilustran los 6 servicios que se configuraron en este servidor Nagios.

- Para el servicio que revisa que la aplicación NSClient esté funcionando y se encuentre actualizada.

```
define service{
        use                     generic-service
        hostgroup_name          LE02,LE01
        service_description     NSClient++ Version
        check_command           check_nt!CLIENTVERSION
        }
```

- Para el servicio que monitorea el tiempo de actividad del equipo:

```
define service{
        use                     generic-service
        hostgroup_name          LE02,LE01
        service_description     Uptime
        check_command           check_nt!UPTIME
        }
```

- Para el servicio que monitorea la carga del procesador:

```
define service{
        use                     generic-service
        hostgroup_name          LE02,LE01
        service_description     CPU Load
        check_command           check_nt!CPULOAD!-l 5,80,90
        }
```

- Para el servicio que monitorea el uso de memoria:

```
define service{
        use                     generic-service
        hostgroup_name          LE02,LE01
        service_description     Memory Usage
        check_command           check_nt!MEMUSE!-w 80 -c 90
        }
```

- Para el servicio que monitorea el uso del disco duro:

```
define service{
        use                     generic-service
        hostgroup_name          LE02,LE01
        service_description     C:\ Drive Space
        check_command           check_nt!USEDDISKSPACE!-l c -w 80 -c 90
        }
```

- Para el servicio que monitorea el estado de la aplicación *explorer.exe* de los sistemas windows:

```
define service{
        use                     generic-service
        hostgroup_name          LE02,LE01
        service_description     Explorer
        check_command           check_nt!PROCSTATE!-d SHOWALL -l Explorer.exe
        }
```

Con la definición de estos servicios se busca que el sistema Nagios pueda monitorear no solo aspectos relacionados con fallas que puedan presentarse en la red, también vigilará el estado de los equipos. Con estos servicios se puede realizar el registro de cuantas veces un equipo se desconectó de la red, cuantas veces tuvo sobrecarga del procesador, sobrecarga de memoria o simplemente si el equipo falló a nivel software.

2.1.2 Configuración de los equipos a monitorear

El laboratorio cuenta únicamente con computadoras con sistema operativo Windows. Nagios promueve el uso del agente de monitoreo para Windows NSClient++, el cual permite que la computadora con sistema Windows pueda ser monitoreada por el servidor Nagios.

Es necesario instalar este agente de monitoreo en todas las computadoras que se requiere sean monitoreadas.

Durante la instalación, únicamente es necesario especificar la dirección IP del servidor Nagios y asegurarse que se especifique que el servicio de este agente de monitoreo se inicie al momento del arranque del sistema operativo.

Esta aplicación es un servicio totalmente transparente que no afecta el funcionamiento de las computadoras ni modifica su uso. La descarga de este agente es totalmente gratuita y se realiza desde la página oficial *http://www.nsclient.org/.*

2.1.3 Monitoreo

Una vez configurado el servidor Nagios y los clientes, se lleva a cabo el monitoreo de la red.

El laboratorio está conformado por las secciones LE-01 y LE-02 que corresponden al área de Geomática y al área de Civiles respectivamente. Todos los equipos instalados dentro de estas dos áreas corresponden a los equipos que se asignan a los alumnos y profesores. Estos son todos los equipos que se requieren monitorear para poder registrar todas las fallas que se presenten.

El laboratorio da servicio a grupos de alumnos en horarios asignados semanalmente, pero además se solicitan sesiones extras que pueden ser asignadas en cualquier día de la semana dependiendo de la demanda de uso de las instalaciones. Esto provoca que no exista un escenario constante que pueda ser monitoreado y tampoco se puede tener la certeza de que siempre se tenga la misma demanda de recursos en la red o de equipos. Por esta razón se seleccionaron cuatro diferentes escenarios posibles para llevar a cabo el monitoreo de la red.

- **Escenario 1 (E1):** Todos los equipos de las secciones LE-01 y LE-02 se encuentran encendidos pero no están en uso. Este escenario se presenta una vez a la semana cuando se lleva a cabo el mantenimiento a los equipos y en un periodo de tiempo se encuentran encendidos pero sin ningún usuario ocupándolos.

- **Escenario 2 (E2):** La sección LE-01 tiene todos sus equipos encendidos y usuarios están ocupando equipos de éste laboratorio. La sección LE-02 tiene todos sus equipos apagados.

- **Escenario 3 (E3):** La sección LE-02 tiene todos sus equipos encendidos y usuarios están ocupando equipos de éste laboratorio. La sección LE-01 tiene todos sus equipos apagados.

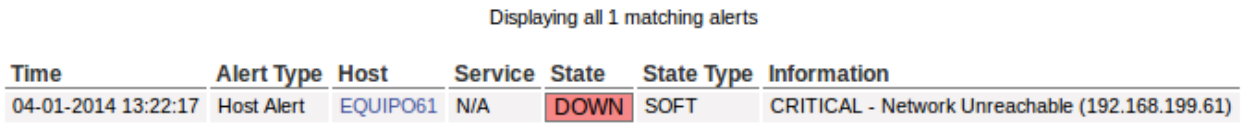
- **Escenario 4 (E4):** Ambas secciones del laboratorio se encuentran en uso. Todos los equipos se encuentran encendidos y algunos, o todos los equipos, están siendo utilizados por los usuarios.

El tiempo de monitoreo establecido se determinó en un periodo de tiempo de 3 semanas. Debido a la gran necesidad que se tenía de dar solución a los problemas que se presentaban en la red y que impedían que se brindaran los servicio adecuados, el tiempo de monitoreo tuvo que ser a corto plazo.

Semanalmente se monitorearon cada uno de estos escenarios 3 veces, en un periodo de tiempo programado de una hora y media cada sesión.

Durante cada sesión, al término del monitoreo se generaba un reporte mediante la interfaz de Nagios que permite mostrar los eventos ocurridos que se deben a ciertas causas, ya sea la baja de un equipo en la red, sobrecarga del procesador, exceso en el uso de memoria, etc.

Por ejemplo, el siguiente reporte muestra la baja o desconexión de un equipo de la red que se detectó durante el monitoreo.



Displaying all 1 matching alerts

Time	Alert Type	Host	Service	State	State Type	Information
04-01-2014 13:22:17	Host Alert	EQUIPO61	N/A	DOWN	SOFT	CRITICAL - Network Unreachable (192.168.199.61)

Figura 2. 1 Reporte de Nagios de eventos registrados

Se muestra la hora en que sucedió el evento, la fecha, el nombre del equipo como identificador y la falla detectada.

A continuación se resume la tabla con todos los eventos detectados durante las 3 semanas de monitoreo en cada escenario.

Escenario 1			
Cantidad de equipos monitoreados	Horas de monitoreo	Evento	Cantidad de Incidencias
36	13 hrs. 48 min.	Falla en red	3
36	13 hrs. 48 min.	Sobrecarga CPU	0
36	13 hrs. 48 min.	Uso de memoria	1
36	13 hrs. 48 min.	Interfaz de Windows	0

Tabla 3 Registro de eventos de monitoreo E1

Escenario 2			
Cantidad de equipos monitoreados	Horas de monitoreo	Evento	Cantidad de Incidencias
17	13 hrs. 36 min.	Falla en red	6
17	13 hrs. 36 min.	Sobrecarga CPU	4
17	13 hrs. 36 min.	Uso de memoria	0
17	13 hrs. 36 min.	Interfaz de Windows	0

Tabla 4 Registro de eventos de monitoreo E2

Escenario 3			
Cantidad de equipos monitoreados	Horas de monitoreo	Evento	Cantidad de Incidencias
19	13 hrs. 41 min.	Falla en red	16
19	13 hrs. 14 min.	Sobrecarga CPU	0
19	13 hrs. 14 min.	Uso de memoria	0
19	13 hrs. 14 min.	Interfaz de Windows	0

Tabla 5 Registro de eventos de monitoreo E3

Escenario 4			
Cantidad de equipos monitoreados	Horas de monitoreo	Evento	Cantidad de Incidencias
36	13 hrs. 52 min.	Falla en red	22
36	13 hrs. 52 min.	Sobrecarga CPU	6
36	13 hrs. 52 min.	Uso de memoria	0
36	13 hrs. 52 min.	Interfaz de Windows	0

Tabla 6 Registro de eventos de monitoreo E4

Los eventos de mayor importancia y de mayor incidencia son por fallas en la red, éstos se deben a que el equipo dejó de responder al servidor Nagios por diversas razones que al final de este capítulo se detallarán, debido a que fueron detectadas mediante la revisión de los equipos, cableado y estado de los componentes de la red.

2.2 Descubrimiento de la red y documentación

Además del monitoreo de la red, con el cual es posible generar un registro de la cantidad de fallas que se presentan, también es indispensable hacer un descubrimiento de la red. Esto es, revisar los componentes físicos, el cableado y las instalaciones, con la finalidad de poder detectar el origen de la mayor cantidad de fallas que se presentan.

También esta revisión física de la red permite detectar si existen normas o estándares que no se estén cumpliendo, ayuda a poder generar la documentación que describa cómo es que está estructurada la red del laboratorio, permite conocer la cantidad de dispositivos que tiene, la cantidad de cableado y sus diversos componentes.

2.2.1 Reconocimiento físico de la red

El Laboratorio de Geomática y Especialidades de Civiles se encuentra seccionado por 4 diferentes áreas de trabajo:

Laboratorio de Geomática (LE-01): Es un laboratorio acondicionado para prestar servicios computacionales a los alumnos y profesores de las carreras de Geomática y afines. Entre los requerimientos esenciales de funcionalidad se encuentran el acceso a internet y compartición de recursos a nivel local.

En la *Tabla 7* se muestran la cantidad de nodos o rosetas que hay libres en este laboratorio y la cantidad de nodos utilizados que hay.

Laboratorio de Geomática LE-01		
Nodos libres	Nodos utilizados	Total de nodos
19	17	36

Tabla 7 Nodos del laboratorio LE-01

Laboratorio de Especialidades de Civiles (LE-02): Es un laboratorio acondicionado para prestar servicios a los alumnos y profesores de las carreras de Civiles y afines. Entre los requerimientos esenciales de funcionalidad se encuentran el acceso a internet y compartición de recursos a nivel local, además de alta disponibilidad de la red debido al uso de software que requiere el manejo de licencias por medio de un servidor local.

En la *Tabla 8* se muestran la cantidad de nodos o rosetas que hay libres en este laboratorio y la cantidad de nodos utilizados que hay.

Laboratorio de Especialidades de Civil LE-02		
Nodos libres	Nodos utilizados	Total de nodos
16	20	36

Tabla 8 Nodos del laboratorio LE-02

Área de Servicio Social: Esta área de trabajo está designada para las actividades realizadas por los prestadores de servicio social, requiere principalmente alta disponibilidad de la red debido a que son los equipos que trabajan en esta área quienes realizan el monitoreo de los equipos que están siendo utilizados en el laboratorio.

En la *Tabla 9* se muestran la cantidad de nodos o rosetas que hay libres en esta sección del laboratorio y la cantidad de nodos utilizados que hay.

Área de Servicio Social		
Nodos libres	Nodos utilizados	Total de nodos
0	4	4

Tabla 9 Nodos del área de Servicio Social

Área Administrativa: Es el área de trabajo designada para la administración de todo el laboratorio, requiere conexión a internet debido a las diversas actividades que aquí se realizan. También es indispensable la comunicación a nivel local para la compartición de recursos y archivos con el área de Servicio Social.

En la *Tabla 10* se muestran la cantidad de nodos o rosetas que hay libres en esta sección del laboratorio y la cantidad de nodos utilizados que hay.

Área Administrativa		
Nodos libres	Nodos utilizados	Total de nodos
2	2	4

Tabla 10 Nodos del área Administrativa

Además de las áreas de trabajo mencionadas, el laboratorio cuenta con un cuarto o área de telecomunicaciones.

Área o cuarto de Telecomunicaciones: En esta sección del laboratorio se encuentran instalados los equipos de comunicaciones. Es el área donde el tendido del cableado horizontal termina y se realiza la conexión con los equipos de comunicación y panel de parcheo. El cuarto de telecomunicaciones cuenta con los siguientes componentes:

I. Equipos de comunicaciones.
    a. 4 switches 3com 3C16980
        i. No administrables
        ii. 24 puertos Fast Ethernet 10/100 Mbps
        iii. Apilables
    b. Servidor Ubuntu 5.10 (Sin acceso a su administración)
        i. Firewall

II. Panel de parcheo
    a. 4 Patch Panel
        i. Cat5 universal
        ii. 24 Puertos

III. Soportes
    a. Rack PANDUIT vertical

Área de Cableado Horizontal: El área de cableado horizontal se extiende a lo largo de las áreas de trabajo del laboratorio. Consta de una distribución o tendido del cableado por medio de canaletas expuestas en los muros. Estas canaletas expuestas tienen como finalidad distribuir a lo largo del laboratorio el cableado y permitir la instalación de las rosetas. Todas las canaletas convergen en una canaleta que se encuentra debajo del piso falso con que cuenta el laboratorio, la cual distribuye todo el cableado al área o cuarto de telecomunicaciones.

2.2.1.1 Fotografiado de las instalaciones

Figura 2. 2 Laboratorio de Geomática LE-01

Figura 2. 3 Laboratorio de Civiles LE-02

Figura 2. 4 Canaleta expuesta de área de trabajo

Figura 2. 5 Entrada al piso falso de canaleta de área de trabajo

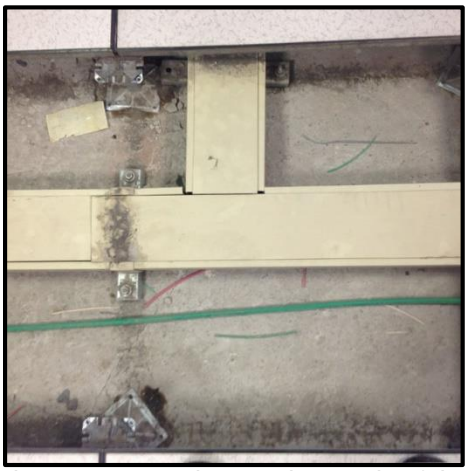


Figura 2. 6 Canaleta oculta en piso falso

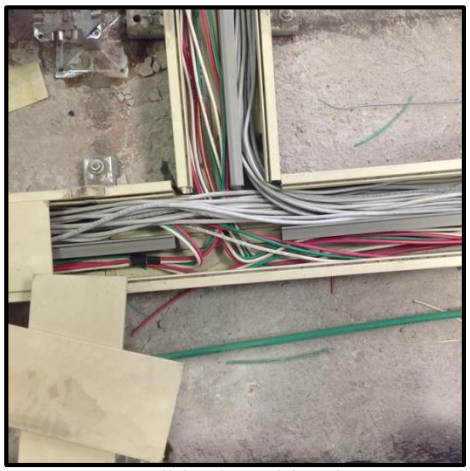


Figura 2. 7 Tendido de cableado en canaleta oculta

Figura 2. 8 Unión de canaletas en piso falso

Figura 2. 9 Tendido terminal de cable a roseta de piso

Figura 2. 10 Roseta en canaleta lateral

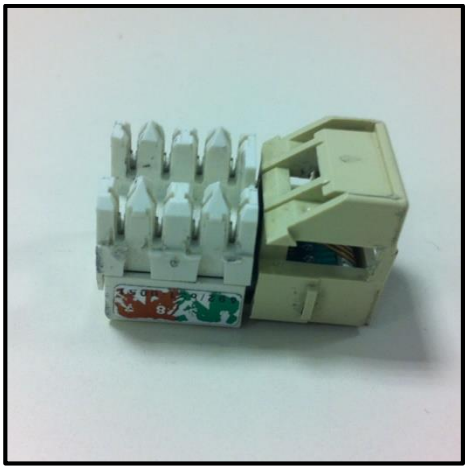


Figura 2. 11 Revisión de conectores de rosetas laterales

Figura 2. 12 Roseta de piso

Figura 2. 13 Revisión de conectores de rosetas de piso

Figura 2. 14 Equipos laterales

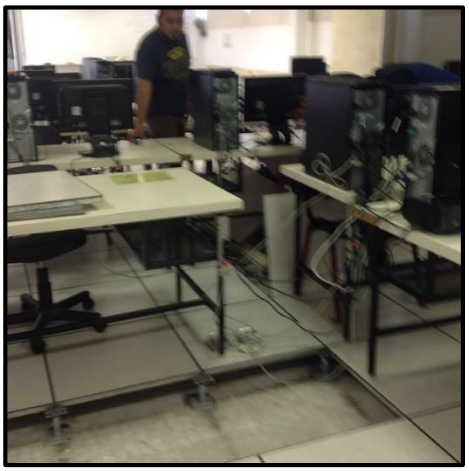


Figura 2. 15 Equipos centrales

Figura 2. 16 Área de telecomunicaciones, acceso

Figura 2. 17 Llegada de cableado al Rack

Figura 2. 18 Rack y cableado de patch panel - switch

Figura 2. 19 Marca y modelo de switch

Figura 2. 20 Switches y cableado de patch panel

Figura 2. 21 Condiciones físicas de los equipos de comunicación

Figura 2. 22 Servidor Firewall

Figura 2. 23 Sistema de ventilación único

2.2.2 Descubrimiento lógico de la red

La red del laboratorio cuenta con un esquema de direccionamiento único, es decir, todos los equipos pertenecen al mismo segmento de red sin tomar en cuenta si pertenecen a grupos o áreas de trabajo distintos.

La dirección de red que utiliza el laboratorio para su entorno local es la *192.168.199.0* con una máscara de red *255.255.255.0*.

La asignación de direcciones IP en los dispositivos finales o hosts del laboratorio no está distribuida de manera adecuada. Aunque los equipos de trabajo pertenecientes a los laboratorios LE-01 y LE-02 tienen configurada una dirección IP estática, los equipos utilizados por prestadores de servicio social no tienen asignado un rango de direcciones IP del segmento. Esto provoca que en muchas ocasiones haya duplicidad de direcciones IP provocando fallas en la red.

Al pertenecer todos los dispositivos finales al mismo segmento de red, independientemente del área de trabajo al que están asignados, todos pueden comunicarse de manera local con los demás equipos de la red.

Todos los equipos utilizados en las áreas de trabajo del laboratorio tienen instalado el sistema operativo Windows. Este sistema operativo permite definir un grupo de trabajo que da permisos y privilegios a los equipos en red para la compartición de recursos; todos los equipos del laboratorio pertenecen al mismo grupo de trabajo.

2.2.3 Documentación

El laboratorio no cuenta con ningún documento descriptivo de la red. No existen planos que muestren el tendido del cableado, ubicación de rosetas, nodos finales ni distribución del cuarto de telecomunicaciones.

No se conocen las características de los equipos de interconexión switches, de las tarjetas de red de los equipos de trabajo, del cableado ni conectores.

Es por todo esto que, con base en el descubrimiento de red tanto físico como lógico, se documentará el estudio realizado para dar informe del estado actual de la red y de las características de todos los dispositivos y componentes de red con que cuenta el laboratorio.

Además se desarrollarán los planos del laboratorio en los cuales se pueda visualizar el tendido del cableado, ubicaciones de las rosetas, conectores, equipos de trabajo y distribución en el cuarto de telecomunicaciones.

A continuación se describen los apartados que contiene el documento descriptivo de la red del laboratorio desarrollado con base en el descubrimiento de red que se realizó.

Esta documentación será entregada al área administrativa del laboratorio con la finalidad de tener físicamente la información del estado y configuración de la red.

Componentes de la red

En este apartado de la documentación se detallan cuáles son las características de todos los componentes, desde los dispositivos finales o computadoras, dispositivos de interconexión y componentes del cableado estructurado de la red.

La finalidad de esta sección es dar a conocer cuál es el estado físico de la red, además que se tenga el conocimiento de toda la infraestructura de red a la que se tiene acceso en el laboratorio y cuales son todos aquellos componentes a los que se les debe dar mantenimiento periódicamente.

Configuración de la red

En esta sección de la documentación se detallan las configuraciones lógicas de la red, cuál es el segmento de red utilizado, el tipo de topología física y lógica implementada y la asignación de parámetros de red a los equipos de trabajo.

Normas y Estándares Internacionales de Cableado Estructurado

Además de dar un marco teórico con base en las normas o estándares internacionales relacionados con el cableado estructurado, se describe la problemática del laboratorio con base en las normas o estándares que no se estén cumpliendo por alguna razón. La finalidad de esta sección es dar a conocer qué tipo de afectación puede tener el seguir incumpliendo estas normativas a largo plazo.

Seguridad de la red

En esta sección se describe el estado de la red en materia de seguridad. Se dan a conocer cuáles son las vulnerabilidades detectadas y cómo podría verse afectada la red si no se corrigen estas fallas. La finalidad de este apartado es, en primera instancia, dar a conocer el estado de la red en cuanto a la seguridad. Además se pretende concientizar al personal del laboratorio de la importancia de mantener protegidos los activos con que se cuenta, en este caso todos los componentes de la red y la información almacenada.

Planos

La elaboración de los planos permite al laboratorio conocer de manera real la distribución del cableado estructurado, además permite identificar de manera clara los componentes de la red y cómo se distribuye el tendido del cableado a lo largo del laboratorio. Es sin duda, parte fundamental de la base de nuevos proyectos que requieran implementarse en el laboratorio.

Los planos que a continuación se ilustran fueron desarrollados con el software AutoCAD. En ellos se plasman a escala las instalaciones de la red del laboratorio, ubicación de nodos o dispositivos finales, ubicación de rosetas, distribución del cableado por medio de las canaletas y el cuarto de telecomunicaciones. Los planos elaborados forman parte de la documentación de este proyecto desarrollada para el laboratorio, por lo mismo éstos serán entregados al área administrativa.

A continuación se presentan vistas de los planos desarrollados, en los cuales se muestra el tendido del cableado de red, la ubicación de los conectores, rosetas, canaletas y equipos en el laboratorio.

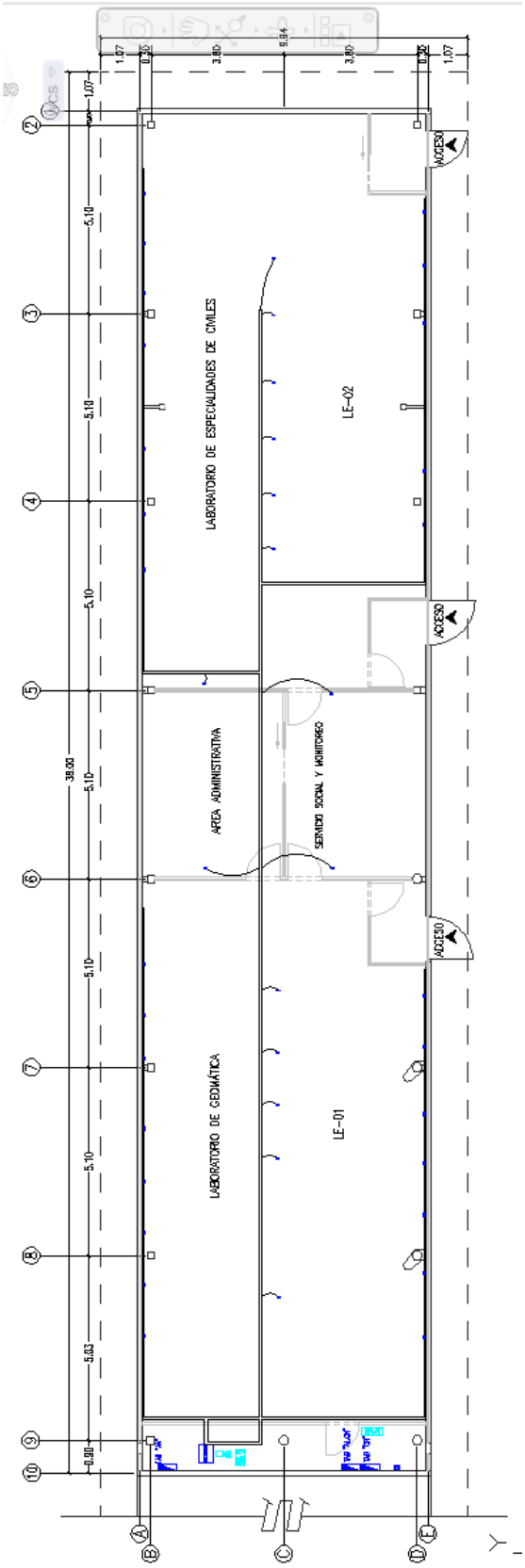


Figura 2. 24 Tendido del cableado y rosetas

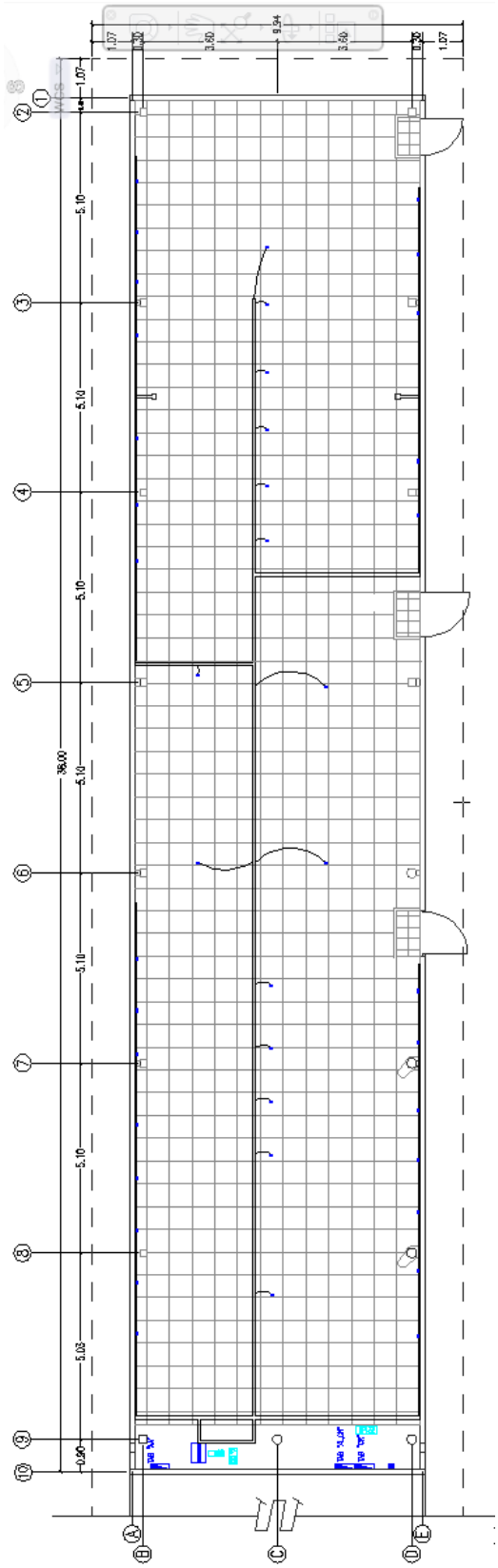


Figura 2. 25 Posicionamiento del cableado y piso falso

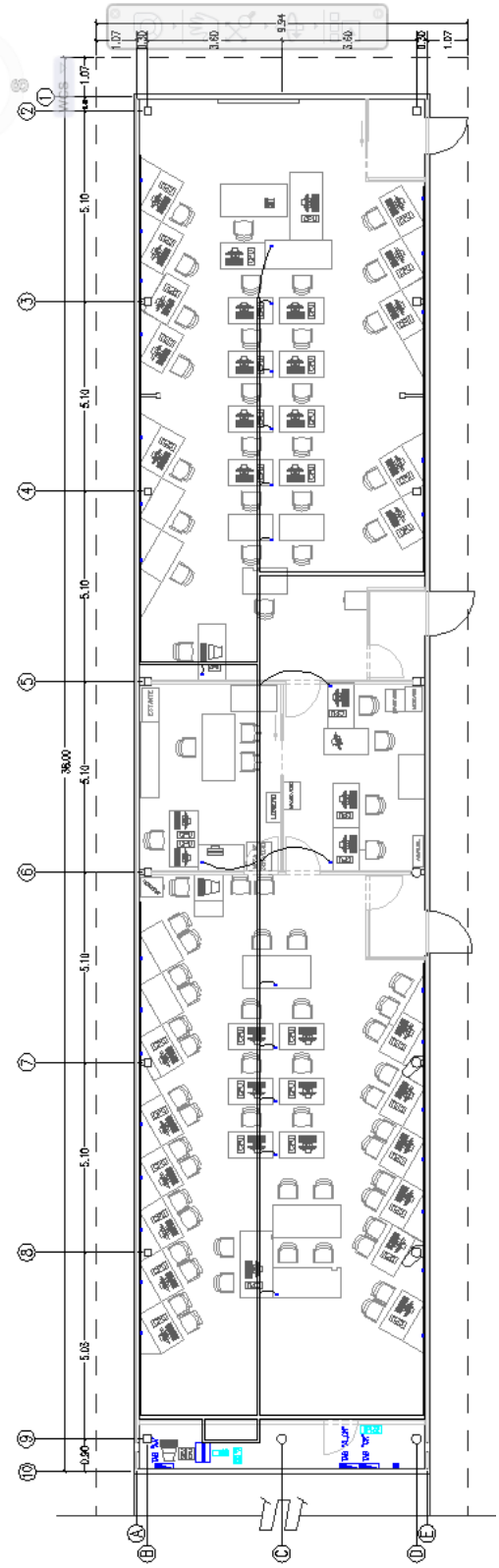


Figura 2. 26 Equipos finales y escritorios

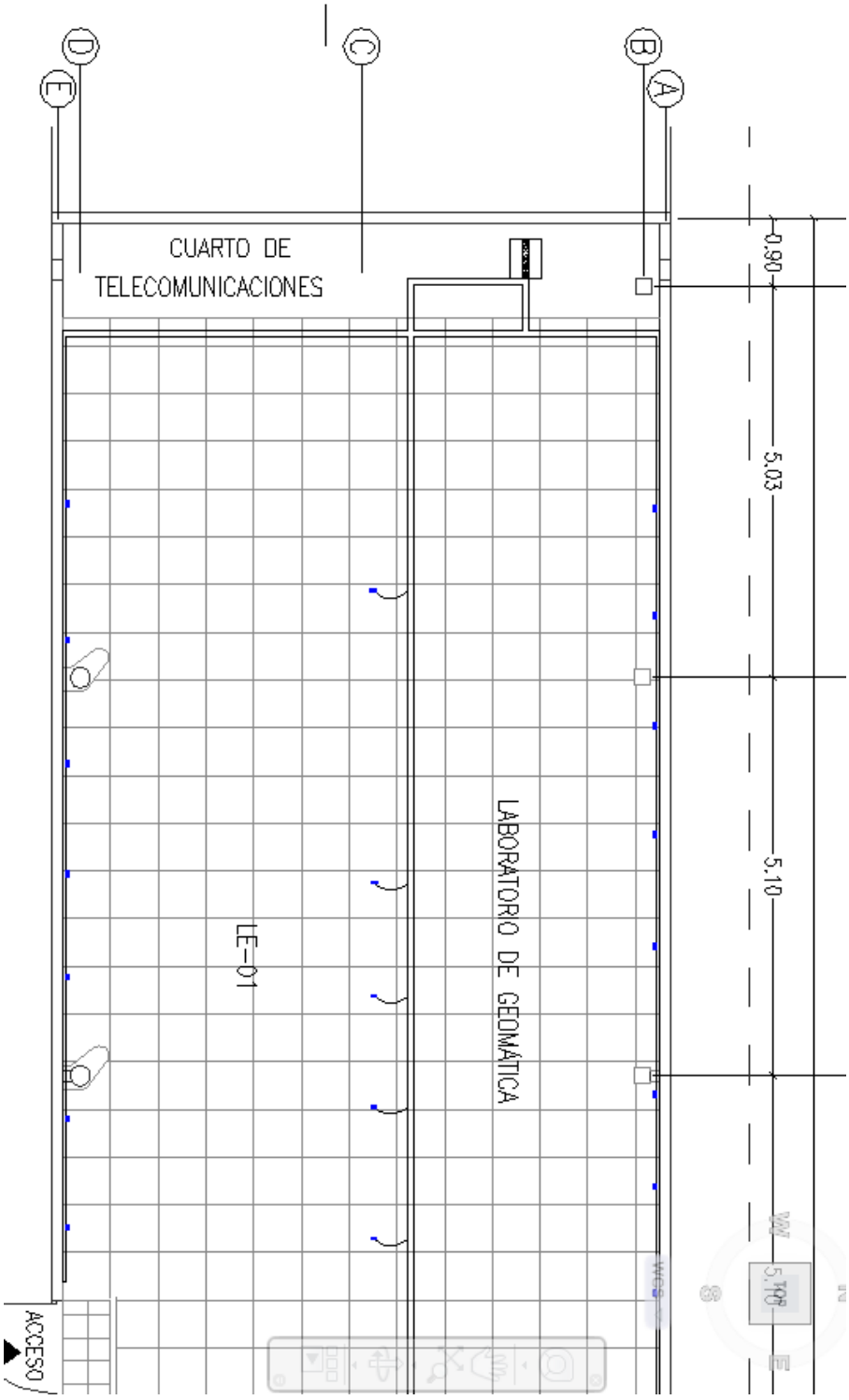


Figura 2. 27 Cuarto de Telecomunicaciones

En la vista del plano (*Figura 2.24)* se puede ver la totalidad de las instalaciones de red a escala. Se ilustran las canaletas laterales y la posición de las rosetas. Además en esta vista del plano se aprecia el tendido de la canaleta central que se localiza debajo del piso falso y su llegada al cuarto de telecomunicaciones.

Se etiquetan también las áreas de trabajo del laboratorio que en este capítulo se describieron.

En la segunda vista (*Figura 2.25)* se añade a la distribución del cableado el piso falso. La referencia que el piso falso proporciona para una rápida ubicación de la canaleta central es indispensable ya que de requerirse indicará que losetas deben removerse para tener acceso al cableado directamente.

En la tercera vista (*Figura 2.26)* se puede ver la distribución de los equipos finales en las 4 áreas de trabajo del laboratorio. Del mismo modo se conserva el tendido del cableado para identificar qué roseta suministra la conexión a la red de cada dispositivo final.

En la última vista (*Figura 2.27)* se hace un acercamiento a la sección del cuarto de telecomunicaciones en el que se muestra la llegada del cableado y la posición del rack.

La realización de estos planos busca dar al laboratorio las bases para el reconocimiento físico de la red, ubicación ágil del cableado y componentes de red, así como de los dispositivos finales.

2.3 Problemática de la red

Después de realizar el descubrimiento de la red tanto físico como lógico y el monitoreo, se pudieron detectar muchas fallas dentro del laboratorio. Existen fallas tanto físicas como de configuración, incumplimiento de normas y estándares internacionales de cableado estructurado y ausencia de una correcta administración de la red.

En este capítulo se detallarán todas las fallas que pudieron ser detectadas en la etapa de monitoreo y descubrimiento de la red, además de todas las detecciones de incumplimiento de normas y estándares internacionales de cableado estructurado.

2.3.1 Problemas físicos de la red

El laboratorio ha brindado servicio por más de 13 años sin recibir algún tipo de mantenimiento preventivo o correctivo, ni implementación de nuevas tecnologías. Hay un gran deterioro de los componentes de la red que afectan de manera importante las actividades que se llevan a cabo en el laboratorio. A continuación se describen los

componentes de la red que presentan problemas físicos y que afectan el desempeño de la red del laboratorio.

Rosetas de canaleta

Algunas de las rosetas que se encuentran instaladas en las canaletas laterales de los laboratorios presentan fallas. Los hilos de cobre del cable UTP que fueron ponchados en estos conectores se han desgastado a tal grado de quebrarse provocando un falso contacto. La disponibilidad de red de los equipos que se conectan a estas rosetas se ve afectada constantemente.

Rosetas de piso

Algunas de las rosetas centrales, instaladas en el piso del laboratorio, han sufrido un gran deterioro físico provocado principalmente por las pruebas físicas a las que son sometidas.

Al estar en el suelo, las rosetas son pisadas frecuentemente lo que ha provocado que los conectores se aflojen y los hilos de cobre que estaban ponchados se zafen. La disponibilidad de red de los equipos que se conectan a estas rosetas se ve afectada constantemente y en algunos casos han dejado de funcionar totalmente.

Cables UTP terminales (Patch cord)

Los cables UTP terminales que tienen como finalidad conectar las rosetas con los equipos de trabajo, tienen un gran deterioro provocado por su mal manejo.

Algunos de estos cables tienen flojos los conectores o plugs RJ-45 y esto provoca que constantemente el cable no cumpla con su función y se pierda la conectividad del equipo con la red.

Switches

Los equipos de interconexión, la base de la conectividad en el laboratorio, presentan muchas fallas físicas debido a que nunca han recibido algún tipo de mantenimiento.

Algunos puertos han dejado de funcionar irremediablemente, los ventiladores internos no pueden cumplir ya su función debido al bloqueo de las ventilas de los switches por el polvo y la humedad que hay en el cuarto de telecomunicaciones.

Internamente los switches están cubiertos por una densa capa de polvo, el calentamiento de los equipos es inevitable y esto provoca que constantemente entren en un modo de suspensión preventivo que obliga a su reinicio forzado manualmente.

Este es uno de los mayores problemas físicos que afecta la red del laboratorio, principalmente la disponibilidad y la calidad de servicio. Al estar los switches conectados en apilamiento, la falla de uno de los equipos que a su vez se apila con otro switch, provoca que el error extienda su dominio, afectando no solamente a los equipos finales que se conectan al switch que presenta la falla, sino también a los equipos conectados a los switches que dependen de la funcionalidad de éste.

La falla de los switches fue lo que provocó un mayor número de incidencias detectados en el monitoreo, dejando en algunas ocasiones sin servicio de red a la mitad del laboratorio.

Rack o gabinete

El rack o gabinete, donde están montados los switches, presenta de igual manera deterioro por la falta de mantenimiento. Está cubierto por una densa capa de polvo, los switches no están bien empotrados debido a que los tornillos utilizados no son los adecuados y los cables que se distribuyen del patch panel a los switches presentan fallas que provocan que algunos equipos pierdan la conexión constantemente.

2.3.2 Problemas de configuración de la red

Además de las fallas físicas que se detectaron en la red del laboratorio, también existen fallas provocadas por una mala configuración de la red.

Hay problemas provocados tanto por configuraciones lógicas como físicas. Desde la asignación de las direcciones lógicas o IP, hasta la incorrecta identificación de los nodos, rosetas y puertos del patch panel y switches.

Configuración de parámetros de red

Como se describió anteriormente en este capítulo, a la red del laboratorio se le asignó un segmento de red que está dado por la dirección IP de red: *192.168.199.0* con máscara de subred: *255.255.255.0.* Esto supone que puede haber 254 equipos conectados a este segmento de red, si la infraestructura física lo permitiera.

Pero hay una mala distribución de las direcciones lógicas en los dispositivos finales. De las 254 direcciones lógicas disponibles, no están definidos rangos de direcciones utilizables para cada una de las áreas de trabajo con que cuenta el laboratorio.

Los equipos de las secciones LE-01 y LE-02 tienen asignadas direcciones IP estáticas, pero no de manera ordenada. Se han asignado las direcciones IP de estos equipos en función de su número de mesa.

Las secciones administrativa y de servicio social no cuentan con direcciones IP asignadas ni correctamente registradas. Los prestadores de servicio social y personal administrativo utilizan equipos portátiles a los cuales se les configura la dirección IP de manera aleatoria, esto provoca que por la falta de conocimiento de las IP utilizadas y al no tener un rango de direcciones específico para cada sección, existan ocasiones en que se configuran IPs ya utilizadas provocando la duplicidad de direcciones lógicas en la red. Esto provoca que los equipos involucrados no puedan tener acceso a la red y en muchas ocasiones la falla tarde en detectarse.

Grupos de trabajo de Windows

Los grupos de trabajo que permite configurar el Sistema Operativo Windows, es la única configuración en los equipos que ofrece cierto nivel de seguridad a la hora de delimitar las áreas de trabajo en la red. Sin embargo, la configuración de este servicio está realizada de manera incorrecta ya que todos los equipos del laboratorio tienen asignado el mismo grupo de trabajo. Esto provoca que se tenga acceso a archivos no protegidos en los equipos desde cualquier otro dispositivo de la red.

Esto es un gran problema ya que en muchas ocasiones los profesores comparten con sus grupos exámenes y materiales con contenido que debe distribuirse de manera cuidadosa. La actual configuración de los dispositivos es una gran vulnerabilidad que puede permitir que estos recursos sean obtenidos por personas no autorizadas. Incluso los equipos del área administrativa y de servicio social son vulnerables en este sentido.

Software mal configurado o dañino

Existen programas instalados en los equipos de cómputo que realizan constantes descargas de actualizaciones o envío del estado de los equipos en segundo plano, lo cual consume recursos de la red además de ser una amenaza para la confidencialidad de los activos o información que pudiera verse comprometida al ser enviada a servidores remotos.

Programas como Ccleaner y TuneUP son utilizador para realizar mantenimiento lógico en el Sistema Operativo, pero las configuraciones en este tipo de software deben

realizarse con mucha precaución debido a que generalmente orillan al usuario a aceptar la instalación de componentes extras o plugins, compartición de la información del equipo, actualizaciones automáticas, modificación de archivos importantes, etc.

Etiquetado de rosetas

Inicialmente la configuración de las rosetas y patch panel era correcta, sin embargo, con el paso del tiempo y el intento por corregir fallas en la red de manera incorrecta se perdió la relación de puertos y la identificación de los nodos finales es difusa.

El etiquetado de las rosetas no corresponde en su totalidad con el etiquetado del patch panel, lo cual provoca que sea difícil identificar a qué roseta pertenece el cable que llega a un puerto del patch panel.

Ponchado de cables del patch panel a los switches

Los cables UTP que interconectan el patch panel y los switches no son los adecuados. Estos cables son demasiado largos, además de no llevar un orden, distribución correcta ni etiquetado.

Esto provoca que sea prácticamente imposible identificar de manera ágil la relación de puertos entre los switches y patch panel. Y todo esto, en conjunto con las fallas del etiquetado de las rosetas, hace muy complicado identificar a qué puerto del switch se conecta cada equipo en el laboratorio.

2.3.3 Normas, estándares y buenas prácticas que no se cumplen

Hay una gran cantidad de normas, estándares internacionales y buenas prácticas que no se cumplen en el laboratorio. Aunque muchas de ellas no son causantes de fallas en la red, si son aspectos que hay que considerar para evitar en mayor medida que se puedan presentar errores en la red o que existan vulnerabilidades que puedan ser explotadas.

Configuración del tipo de cableado

Por medio del descubrimiento de la red se detectó que el tipo de configuración de cableado que se implementó en el laboratorio es tipo “A”, el cual corresponde al estándar TIA/EIA 568-A. Inicialmente el laboratorio cumplía con este estándar en su totalidad, pero con el paso del tiempo y con las fallas de los cables terminales (patch cord) que se fueron presentando, se incluyeron algunos nuevos cables sin verificar si la configuración de éstos era la correcta.

De esta manera se consiguió que no se respetara el estándar, ya que existen cables con configuración tipo “A” directos, cables con configuración tipo “B” directos e incluso cables con configuración cruzada.

Aunque las nuevas tecnologías a nivel software y hardware permiten que aún sin utilizar los cables con configuración correcta se puedan enviar y recibir datos, es importante tener control de las configuraciones implementadas. Con esto se consigue garantizar la compatibilidad con todos los dispositivos, siendo este uno de los principales objetivos del seguimiento de estándares.

Tamaño de los cables terminales o patch cord

Además de haber irregularidades con el tipo de configuración de estos cables terminales, también hay irregularidades con su tamaño.

Algunos cables que se utilizaron para sustituir cables que dejaron de funcionar, no fueron creados con la finalidad de ser patch cord, por lo tanto tienen tamaños que no corresponden a los requeridos. Hay cables de más de 5 metros de largo e incluso un cable con más de 20 metros enrollado y conectado desde una rosea a una computadora.

Cables demasiado largos pueden ser susceptibles a interferencias o fallas físicas debido a que son enrollados o doblados de manera incorrecta.

Canaletas compartidas con cables eléctricos

Como se muestra en las fotografías del descubrimiento de la red, el tendido del cableado se realiza por medio de canaletas tanto laterales como por debajo del piso falso. Dichas canaletas se comparten con las instalaciones eléctricas, lo cual es incorrecto debido a que las líneas eléctricas pueden provocar interferencia a las líneas de red.

Cuarto de telecomunicaciones

El cuarto de telecomunicaciones no cumple ciertas normas y estándares de cableado estructurado.

El espacio del cuarto de telecomunicaciones no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones. En el laboratorio el espacio designado para el cuarto de telecomunicaciones se comparte con los paneles eléctricos y reguladores, además este cuarto es utilizado como depósito de equipos de cómputo y muebles.

Además de comprometer las instalaciones de red, esto provoca que el cuarto de telecomunicaciones se vea altamente afectado por el polvo que, en conjunto con la humedad, ha deteriorado considerablemente los equipos de interconexión switches.

El sistema de ventilación no es el adecuado. Considerando la compartición de espacio con las instalaciones eléctricas, éste debería ser más eficiente para garantizar la correcta circulación de aire y así evitar la acumulación de polvo y presencia de humedad.

Aunque el acceso al laboratorio es controlado por el personal que ahí labora, la puerta del cuarto de telecomunicaciones no tiene control de acceso, no cuenta con llave.

La puerta no abre a ras de piso, debido a que el cuarto de telecomunicaciones se encuentra al nivel del piso real, mientras que las áreas de trabajo están a nivel del piso falso, varios centímetros por encima del piso real.

El desnivel del cuarto de telecomunicaciones lo hace susceptible a inundaciones, considerando que pudiesen existir filtraciones de agua en el techo debido a que el laboratorio se encuentra en el último piso.

Finalmente se puede mencionar que el espacio asignado para el cuarto de telecomunicaciones no es el adecuado. Es muy reducido y la movilidad dentro de él es complicada, además de que dos pilares de la estructura del edificio lo atraviesan reduciendo aún más el espacio dentro del cuarto.

El rack no tiene el espacio libre a su alrededor que se sugiere, el cual debe ser de 82 cm a partir de su perímetro. Esto provocado no por un mal posicionamiento del rack, si no que el cuarto de telecomunicaciones, como ya se ha mencionado, es muy reducido y es imposible proveer de esta característica al rack.

Etiquetas de identificación

La correcta identificación de los componentes del cableado y equipos finales se consigue con, además de un buen diseño de la red, el correcto etiquetado de rosetas, equipos finales y equipos de comunicación.

El laboratorio tiene etiquetadas las rosetas y los patch panels, pero la relación entre éstos se ha perdido debido a que se han realizado modificaciones descontroladas en los patch panels buscando la solución a problemas de disponibilidad en la red.

Actualmente no hay concordancia con el etiquetado que presentan las rosetas y el etiquetado del patch panel. Esto en conjunto con la incorrecta distribución de los cables

en el rack hace imposible saber a qué puerto de un switch se conecta cada equipo del laboratorio.

Segmentación por áreas

Identificadas y bien definidas las diferentes áreas de trabajo que se tienen en el laboratorio, es recomendable configurar la red para brindar ciertas delimitantes en cada una de éstas áreas. Con lo cual se busca controlar el envío y recepción de información, compartición de recursos y tráfico en la red.

En el laboratorio no existe ningún tipo de control sobre las 4 áreas de trabajo que tiene, ya que todas pertenecen a un mismo grupo de trabajo lo cual posibilita el acceso a información por parte de usuarios no autorizados; o incluso la difusión de algún tipo de malware o virus a todo el segmento de red, entre otras vulnerabilidades.

2.3.4 Tecnologías atrasadas

La red del laboratorio fue diseñada e implementada hace más de 13 años, desde ese entonces no se ha invertido en remodelar o actualizar los diversos componentes de la red, aun cuando ha presentado grandes fallas. Esto ha dejado al laboratorio desactualizado de las nuevas tecnologías que se han presentado y que sin duda alguna, mejoran el rendimiento y funcionalidad de las redes de datos.

La mayoría de los conectores y casi la totalidad del cableado son de categoría 5, actualmente se requieren implementaciones mínimo con la categoría 5e.

Los equipos switches no son administrables, y aunque cuentan con velocidades de transferencia de hasta 100Mbps, evidentemente tienen un rendimiento menor comparado con dispositivos actuales.

El firewall utilizado está instalado en un servidor poco robusto al cual no se tiene acceso ni se conocen las especificaciones de funcionalidad. Únicamente se detectó que tiene configuradas políticas o reglas de comunicación en las que se bloquean conexiones remotas a servidores FTP.

Otro punto a considerar es que la red del laboratorio no atiende una de las necesidades de conectividad que en la actualidad tiene alta demanda, la movilidad. El número de equipos en el laboratorio se ha vuelto insuficiente por lo que permitir que usuarios utilicen sus equipos personales sería una buena solución a esta problemática. Sería necesario acondicionar la infraestructura de red para poder brindar este servicio y permitir temporalmente el acceso a los recursos de la red a profesores y alumnos con sus equipos personales, todo esto sin afectar los servicios de la red.

CAPÍTULO III

Plan de mantenimiento a bajo costo aplicable en la red

En este capítulo se describen aquellas acciones correctivas y preventivas que se llevarán a cabo en el laboratorio con la finalidad de mejorar los servicios de red. Dichas acciones deberán ser realizarse de tal manera que no interrumpan los horarios programados en el laboratorio y en el menor tiempo posible, debido a que el estado actual de la red afecta de manera importante los servicios que el laboratorio brinda a profesores y alumnos y se tiene que dar solución a esta problemática lo antes posible.

No se cuenta con ningún tipo de presupuesto para la realización de este plan de mantenimiento, por lo que todas las acciones que se lleven a cabo se implementarán únicamente con las herramientas y materiales que hay en el laboratorio o que se hayan adquirido personalmente.

3.1 Descripción de problemas de la red a resolver

No es posible atender todas las fallas detectadas en la red del laboratorio debido a que muchas de ellas requieren de un presupuesto del cual no se dispone. Es por esto que se ha establecido el alcance de este plan de mantenimiento como la resolución de todas aquellas fallas de la red y aplicación de buenas prácticas que no requieran un costo monetario importante.

A continuación se describen aquellas acciones que han sido propuestas para ser aplicadas en este plan de mantenimiento.

3.1.1 Ponchado de rosetas

Dar mantenimiento a las rosetas que presentan fallas es posible debido a que no es necesario cambiar los conectores sino simplemente ponchar de nuevo los hilos de cobre en ellos. Afortunadamente al momento de la implementación de la red se consideró dejar cierta cantidad de cable extra en los conectores de los laboratorios, lo cual permite utilizar ese cable extra para volver a ponchar la roseta de forma adecuada.

Dar mantenimiento a las rosetas no afecta las actividades del laboratorio, ya que esta acción se realizará en cada roseta en el momento en que los equipos de cómputo no estén siendo utilizados y el proceso de ponchado de cada una de las rosetas no tardará más de 15 minutos, en un escenario sin contratiempos.

3.1.2 Ponchado de cables patch cord

Como se mencionó en el capítulo anterior, algunos de los cables patch cord o terminales presentan fallas. Los plugs RJ-45 de muchos de ellos se han aflojado provocando que los cables tengan falso contacto. Además, muchos de los cables que se utilizaron para

sustituir cables que dejaron de funcionar no respetan la configuración del tipo de cable que deberían y algunos otros tienen un tamaño incorrecto.

Dar mantenimiento a los cables patch cord es una actividad que sin duda debe realizarse, ya que se detectó que un número importante de fallas se debe a errores físicos en estos cables. Las actividades del laboratorio no se verían afectadas de ninguna manera ya que los cables que se requieran corregir se trabajarían uno por uno y si es necesario se podría utilizar un cable provisional para conectar la computadora mientras se repara el otro cable.

3.1.3 Configuración de direccionamiento de la red

La asignación de direcciones IP en todos los equipos se lleva a cabo manualmente y aunque inicialmente estaban bien distribuidas las direcciones, con el paso del tiempo y la incorrecta asignación de IPs a equipos nuevos o debido al proceso de clonación de equipos se han presentado problemas de duplicidad de direcciones IP, provocando que los equipos involucrados se desconecten de la red.

En este caso se considera necesario volver a realizar la distribución de direcciones IP, asignando ordenadamente rangos de direcciones del segmento para las distintas áreas del laboratorio. De igual manera se verificarán los demás parámetros de red como servidores DNS, ya que se detectó que se incluyeron servidores DNS como predeterminados pero dichos servidores no están activos, por lo que se realizan consultas a servidores inaccesibles y posteriormente a los servidores secundarios que sí funcionan.

Una vez realizada la propuesta de distribución de direcciones IP se llevará a cabo la configuración de todos los equipos. El proceso de modificación de los parámetros de red en cada equipo requerirá al menos de 10 minutos por cada uno, ya que hay que desactivar primero una aplicación que evita realizar cambios en el sistema y ésta requiere el reinicio de los equipos para aplicar las modificaciones realizadas.

Además es necesario que inicialmente todos los equipos se encuentren desconectados de la red, ya que si se configura alguna dirección que por algún motivo haya sido asignada a algún equipo anteriormente, el sistema operativo no permitirá realizar los cambios. Esto obliga a que la asignación de direcciones en los equipos se realice ordenadamente y en un periodo de tiempo ininterrumpido.

3.1.4 Optimización y configuración del Sistema Operativo

Los equipos de cómputo presentan fallas relacionadas con la sobrecarga del procesador, algunos de los programas que tienen instalados que se utilizan para dar mantenimiento no fueron configurados correctamente y realizan descargas automáticas, envían reportes de estado a servidores de la aplicación y demandan recursos de la red.

Se configurarán estas aplicaciones para garantizar que su función se limite a ejecutar las herramientas de mantenimiento, consiguiendo así disminuir la demanda de recursos tanto del equipo como de la red.

Así mismo se configurarán los grupos de trabajo que ofrece el sistema operativo Windows para delimitar de cierta manera el acceso a recursos que se compartan localmente en las áreas de trabajo del laboratorio.

Estas acciones se llevarán a cabo en los días que se realiza el mantenimiento de los equipos, además se debe confirmar que no hayan sido agendadas sesiones extra oficiales en el laboratorio para no interrumpir estas actividades.

3.1.5 Mantenimiento físico de Switches

Actualmente 3 de los 4 switches que hay en el laboratorio presentan múltiples fallas ocasionadas por las condiciones en las que se encuentran dentro del cuarto de telecomunicaciones y por el deterioro físico que han sufrido debido a todos los años que llevan brindando servicio.

Dar mantenimiento físico a estos equipos puede ayudar a que su desempeño mejore considerablemente. Las condiciones actuales de estos equipos provocan que múltiples estados de suspensión se presenten debido al sobrecalentamiento que es generado por la obstrucción de las zonas de ventilación de los switches.

Al entrar un switch en estado de suspensión repentinamente, deja sin servicio a todos los equipos que se conectan a él y además el problema se extiende si es un switch que tiene conexión en apilamiento con otros switches.

El mantenimiento físico de estos equipos consistirá en desmontar cada switch del rack, desarmarlo y limpiar sus componentes internos y armazón. Con esto se busca conseguir que los equipos sean menos propensos a sobre calentarse ya que su sistema de ventilación volvería a funcionar.

El mantenimiento de cada switch requerirá de al menos 2 horas de inactividad en el laboratorio, o al menos del área de trabajo que tiene sus equipos de cómputo conectados al switch que se esté desmontando.

3.1.6 Etiquetado de rosetas y conexiones del rack

El etiquetado de las rosetas y de las conexiones en el rack no es una acción que vaya a corregir fallas en la red, pero si permitirá que sea mucho más fácil identificar cómo está distribuido el cableado, a qué puerto de los switches se conecta cada puerto del patch panel y a qué roseta de las áreas de trabajo pertenece dicho puerto.

Dentro de este plan de mantenimiento a bajo costo no se considera el ponchado completo del rack, debido a que no se cuenta con todo el material necesario para realizar esta implementación.

El etiquetado de rosetas y de las conexiones del rack requerirá primero una etapa de identificación de las relaciones roseta - patch panel y patch panel – switches. Una vez identificadas todas las conexiones, se etiquetarán los cables del rack y se corregirán las etiquetas de las rosetas que estén mal.

3.2 Planificación de actividades

Todas las actividades que se llevarán a cabo en este plan de mantenimiento se programarán en horarios en los que no se interrumpan las actividades del laboratorio. El orden en que se realizarán estas acciones también deberá tener en cuenta la prioridad de resolución de las fallas detectadas.

Para la realización del plan de mantenimiento se ha desarrollado el siguiente cronograma el cual establece los días en los que se deberán llevar a cabo las actividades. El periodo de tiempo establecido para la aplicación de este plan de mantenimiento corresponde del 6 al 30 de Mayo del 2014, la distribución de fechas y actividades se presentan en la *Figura 3.1*.

Id	Nombre de tarea	Dur.	Comienzo	Fin	Predec.
1	Mantenimiento switches	1 día	vie 09/05/14	vie 09/05/14	
2	Mantenimiento switches	1 día	vie 16/05/14	vie 16/05/14	1
3	Ponchado de rosetas	4 días	mar 06/05/14	vie 09/05/14	
4	Ponchado de cables	5 días	lun 12/05/14	vie 16/05/14	3
5	Parámetros de red	1 día	vie 23/05/14	vie 23/05/14	4
6	Mantenimiento SO	1 día	vie 23/05/14	vie 23/05/14	5
7	Etiquetado conexiones	5 días	lun 26/05/14	vie 30/05/14	6

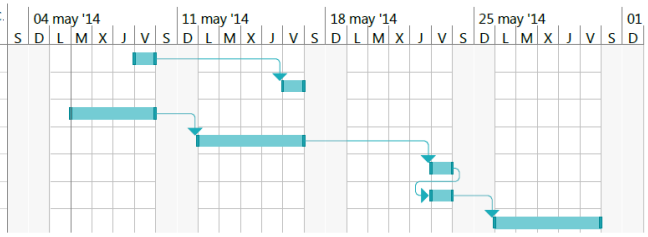


Figura 3. 1 Cronograma del plan de mantenimiento

Mantenimiento de switches

Esta actividad tiene prioridad sobre las demás, ya que el actual estado de los switches provoca que entren en estado de suspensión frecuentemente afectando el servicio de red.

Sin embargo para la realización del mantenimiento de los switches se requiere dar de baja temporalmente los servicios de red, por lo que se han establecido las fechas de realización de estas actividades los días viernes, en los cuales a partir de las 12:00 horas no hay clases regulares programadas en el laboratorio.

El mantenimiento de los switches se llevará a cabo en dos viernes consecutivos, en cada uno se desmontarán 2 switches y se les dará mantenimiento físico que consistirá en desarmar completamente los equipos, limpiarlos interna y externamente y tratar de detectar la presencia de fallas internas que puedan ser resueltas sin poner en riesgo el funcionamiento de los equipos.

El tiempo estimado para esta actividad es de 2 horas por cada switch, lo que significa que se estima un total de 8 horas para la realización del mantenimiento de los 4 switches.

Material necesario

- *Desarmador plano*
- *Desarmador de cruz*
- *Aire comprimido*
- *Brochas*
- *Franelas*

Ponchado de rosetas

El mantenimiento a las rosetas que se detectaron con fallas se llevará a cabo durante la primera semana del plan de mantenimiento que corresponde del 6 al 9 de Mayo, ya que es una actividad que no requiere de la suspensión los servicios de red, sino que se puede dar mantenimiento a cada roseta en los periodos de tiempo en que no haya actividad en el laboratorio.

Durante el análisis físico de la red se detectaron 12 rosetas que presentan fallas, de las cuales 3 no podrán ser reutilizadas. Se estiman entre 10 y 15 minutos de tiempo los que tomará dar mantenimiento a cada roseta.

Material necesario

- *Desarmador plano*
- *Desarmador de cruz*
- *Pinzas pela cables*
- *Pinzas de impacto*

Ponchado de cables patch cord

Esta actividad se llevará a cabo en la segunda semana del plan de mantenimiento que corresponde del 12 al 16 de Mayo. No requiere de la suspensión de los servicios de red

puesto que el ponchado de los cables se hará de manera ordenada dando mantenimiento a uno por uno.

El ponchado de cada cable no tardará más de 10 minutos por lo que esta actividad se puede llevar a cabo en periodos de tiempo en que no se utilicen los equipos y sea posible desconectar momentáneamente el cable de red. Esta actividad está condicionada a ser realizada una vez que se concluyó el mantenimiento de las rosetas.

Se detectaron un total de 19 cables que requerirán ser ponchados nuevamente, este total incluye los cables con algún fallo físico, con tamaño incorrecto o que no respetan la configuración del cableado.

Material necesario

- *Pinzas ponchadoras RJ-45*
- *Pinzas pela cables*
- *Plugs RJ-45*
- *Tester de cables RJ-45*

Configuración de parámetros de red y mantenimiento del sistema operativo

Estas dos actividades se llevarán a cabo el día viernes de la tercera semana del plan de mantenimiento, debido a que es el único día de la semana en que pueden suspenderse los servicios de red en un periodo de tiempo prolongado.

Aunque ambas actividades se encuentran programadas el mismo día, primero se realizarán los ajustes de los parámetros de red en cada equipo y posteriormente se llevará a cabo el mantenimiento del sistema operativo, ya que esta segunda actividad se encuentra condicionada a realizarse una vez que se concluyan los ajustes de parámetros de red.

Todos los equipos del laboratorio, incluyendo las áreas de trabajo LE-01, LE-02, servicio social y administración recibirán la configuración de los parámetros de red. Por otra parte, únicamente a los equipos de trabajo que se encuentran en las áreas LE-01 y LE-02 se les realizarán los ajustes y mantenimiento del sistema operativo, ya que son estos equipos los que tienen instalados los programas de mantenimiento y otros tipos de software que provocan demanda excesiva de recursos en la red, realizan respaldos en servidores remotos y descargan actualizaciones en segundo plano.

Etiquetado de las conexiones de red

Durante la semana del 26 al 30 de Mayo, una vez concluidas todas las demás actividades del plan de mantenimiento, se llevará a cabo la identificación de las rosetas y su correspondiente puerto del patch panel y switch.

Esta actividad se llevará a cabo durante la semana en los periodos de tiempo en que las computadoras no estén en uso. Como las conexiones en el rack no están organizadas y los cables dificultan mucho identificar el origen de las conexiones, se realizarán pruebas de conectividad en las que una persona revisará el comportamiento de un equipo de cómputo y otra identificará el puerto del switch al que se conecta, desconectando momentáneamente cada puerto hasta que el equipo pierda conectividad. De esta forma se logrará identificar a qué puerto del switch se conecta cada roseta y por consiguiente el puerto del patch panel involucrado.

Al identificar cada roseta y su correspondiente conexión en el rack, se etiquetarán los cables que van del patch panel a los switches indicando de qué roseta vienen.

En esta actividad únicamente se etiquetarán los cables del rack pero no se llevará a cabo el ponchado de los cables en el mismo debido a que se requiere de una inversión mayor para llevar a cabo esta tarea.

Material necesario

- *Radios Walkie Talkie*
- *Cinta masking tape o etiquetas adhesivas*

3.3 Análisis de costo

Uno de los principales objetivos de este plan de mantenimiento es el bajo costo que debe tener para poder ser implementado debido a que no se cuenta con presupuesto para su realización. Por esta razón gran parte de los materiales y herramientas que se utilizarán serán con los que cuenta el laboratorio y algunos otros adquiridos personalmente.

Algunos de los materiales que se requieren para dar el mantenimiento al laboratorio deberán ser comprados, el costo de estos materiales será el único que se destinará para la realización de este proyecto.

En la *Tabla 11* se enlistan todos los materiales y herramientas que serán requeridos en este plan de mantenimiento, indicando si será necesaria su compra o si ya se cuenta con ellos.

Materiales y herramientas requeridos				
Nombre	Cantidad	Compra requerida	Costo pieza (MXN)	Costo total (MXN)
Desarmador plano	1	No	-	-
Desarmador cruz	1	No	-	-
Pinzas ponchadoras RJ-45	1	No	-	-
Pinzas pelacables	1	No	-	-
Pinzas de impacto	1	No	-	-
Probador de cableado (Tester)	1	No	-	-
Plug RJ-45	45	Si	4	180
Conector hembra RJ-45	3	Si	24	72
Aire comprimido	2	Si	58	116
Cinta masking tape	1	Si	12	12
Brocha	1	No	-	-
Franela	1	No	-	-
Par de Radios Walkie Talkie	1	No	-	-

Tabla 11 Materiales y herramientas requeridos en el plan de mantenimiento

Los cables UTP que serán corregidos no serán sustituidos en su totalidad, es decir, simplemente se poncharán nuevos conectores o plugs RJ-45 en dichos cables para reutilizarlos, esto debido a que el reemplazo del cableado significaría una inversión mayor la cual no puede ser costeada.

Con base en lo anterior se estima un costo para este plan de mantenimiento de $380.00 MXN, el cual se deriva únicamente de los materiales que requieren ser comprados.

Por otra parte, se presenta el estimado de tiempo a invertir en la realización de este plan de mantenimiento. Durante su implementación se contará con el apoyo de los prestadores de servicio social, a quienes se les asesorará y guiará durante la realización de las actividades, esto como requerimiento por parte del administrador del laboratorio.

Sin embargo, la planeación de las actividades del plan de mantenimiento no fue diseñada con base en las actividades y horarios de los prestadores de servicio social sino a los horarios disponibles en el laboratorio y del desarrollador de este proyecto. Esto debido a que la participación de los prestadores de servicio social tiene como principal objetivo que se familiarizasen con las instalaciones y con el mantenimiento que se lleva a cabo, ya que en su mayoría son alumnos de carreras distintas a computación.

En la *Tabla 12* se enlistan las actividades a realizar y el tiempo total de horas estimado que se invertirá en su realización, independientemente de la distribución de días en que están programadas dichas actividades.

Tiempo de realización de actividades			
Actividad	Cantidad	Tiempo por unidad (minutos)	Total tiempo
Mantenimiento switches	4	120	8 horas
Ponchado de rosetas	12	15	3 horas
Ponchado de cables	19	10	3 horas 10 minutos
Parámetros de red	40	10	6 horas 40 minutos
Mantenimiento SO	36	10	6 horas
Etiquetado conexiones	82	2	2 horas 44 minutos

Tabla 12 Tiempo estimado de la realización de las actividades

Por todo esto se estima un total de 29 horas y 34 minutos de tiempo efectivo que se invertirá en la realización de este plan de mantenimiento.

3.4 Resultados esperados

Con la aplicación de este plan de mantenimiento se espera conseguir una mejora notable en los servicios de red que se brindan en el laboratorio, especialmente en la disponibilidad de la red.

Durante el análisis físico de la red fue posible detectar una gran cantidad de fallas que se presentan en los diversos componentes de la red como lo es el cableado y los equipos de interconexión. El plan de mantenimiento diseñado tiene como principal objetivo atender dichas fallas y mejorar la disponibilidad de la red.

Son 12 rosetas las que presentan fallas físicas, las cuales representan el 14.63 % del total de rosetas existentes en el laboratorio, ya que éste cuenta con un total de 82 rosetas.

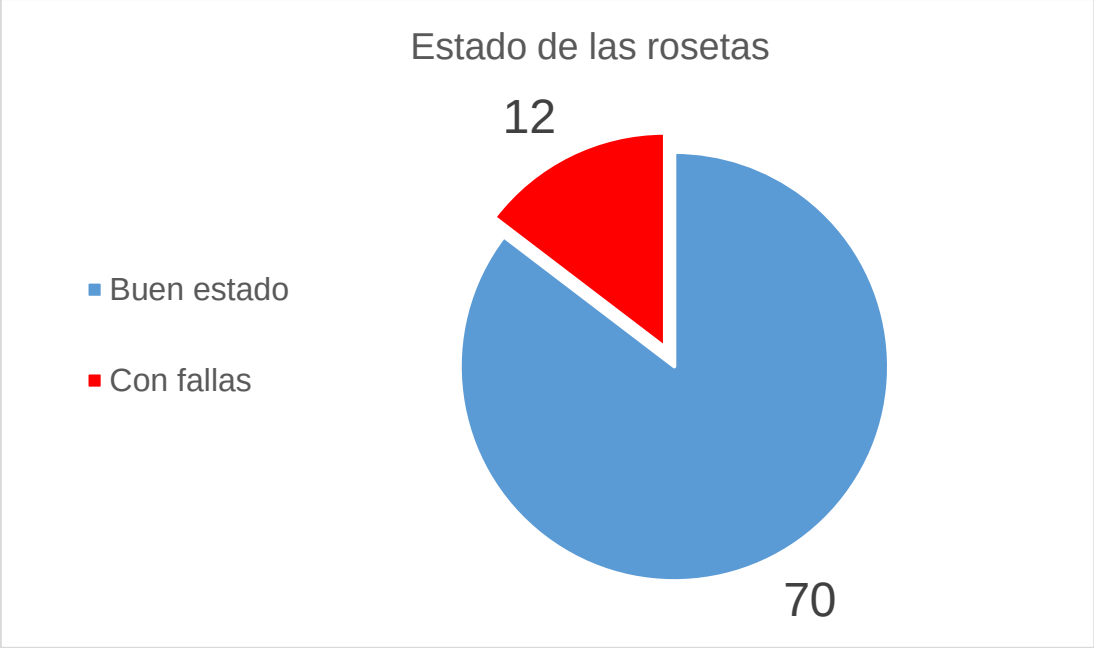


Figura 3. 2 Estado de las rosetas

Con la aplicación de este plan de mantenimiento se espera conseguir que la totalidad de rosetas del laboratorio funcionen correctamente y dejen de presentarse fallas de conectividad derivadas del estado actual de dichas rosetas.

Por otra parte, fueron detectados 19 cables terminales o patch cord que requieren ser ponchados nuevamente, 13 de estos cables presentan fallas físicas que provocan que los equipos pierdan conectividad constantemente.

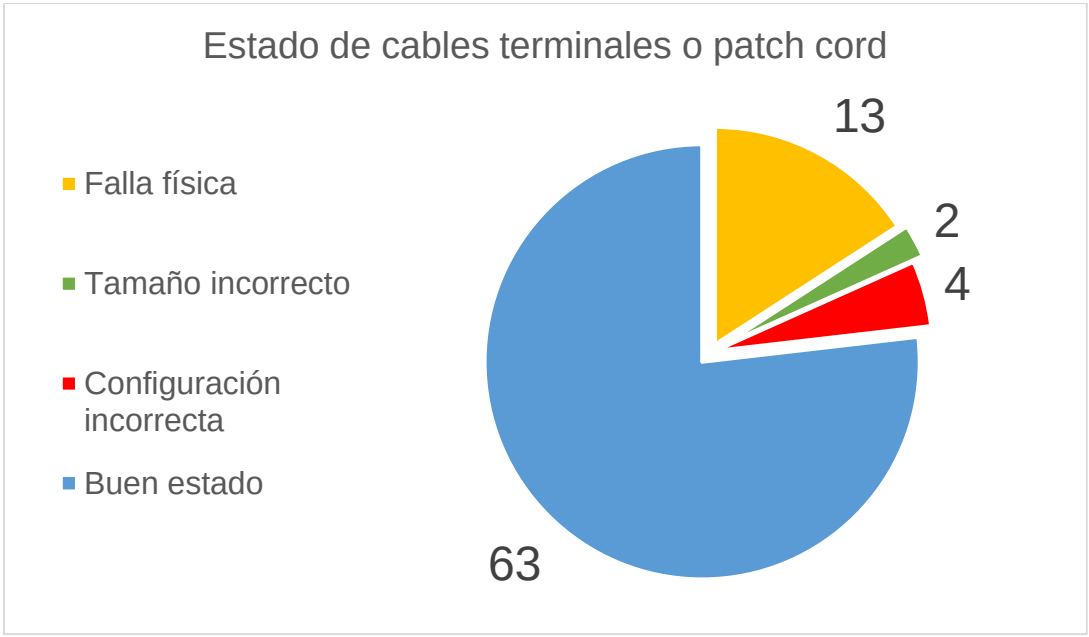


Figura 3. 3 Estado de cables terminales o patch cord

Mediante el plan de mantenimiento se busca conseguir que la totalidad de cables estén en perfecto estado y con la configuración y tamaño correctos. De esta forma se conseguirá que las fallas de conectividad disminuyan, esto debido a que los equipos que tenían cables en mal estado no presentarán más fallas.

La configuración del direccionamiento o parámetros de red en los equipos de trabajo en el laboratorio permitirá que no exista duplicidad de direcciones lógicas, el cual es un problema que actualmente se presenta con frecuencia y que provoca que los equipos involucrados pierdan conectividad en la red. La correcta distribución de direcciones IP permitirá que la asignación de direcciones a nuevos equipos se lleve a cabo de manera ordenada y que garantice que no afectará la configuración de ninguno de los demás equipos del laboratorio.

Además esta distribución de direcciones lógicas permitirá que la identificación de los equipos se pueda llevar a cabo de manera ágil, ya que dicho direccionamiento será asignado por bloques a las diferentes áreas del laboratorio.

Se espera que el mantenimiento del sistema operativo disminuya la sobrecarga del procesador de los equipos, ya que conseguirá que software instalado no realicé configuraciones y procesos en segundo plano, que no descargue contenido de internet y que no realice respaldos o envío de información a servidores remotos.

Además, con la configuración de grupos de trabajo de Windows se limitará de cierta forma el acceso a los recursos que se comparten en la red desde las distintas áreas de trabajo.

El mantenimiento físico de los switches es una de las actividades del plan de mantenimiento que tiene mayor importancia debido a que las fallas provocadas por estos equipos se presentan con mucha frecuencia y afectan de manera importante a un gran número de equipos de cómputo.

El estado actual de los switches es considerado como crítico debido a los múltiples estados de suspensión que presentan provocados por el sobrecalentamiento de los equipos.

Con el mantenimiento físico a estos equipos se espera que el sistema de ventilación pueda trabajar de forma correcta y así conseguir que disminuya la cantidad de veces que los switches entran en estado de suspensión, o que en el mejor de los casos se pueda erradicar este problema.

Tomando en cuenta que los switches, al igual que todo el cableado del laboratorio, han cumplido su tiempo de vida útil, dar el mantenimiento a estos equipos supone una mejora en su rendimiento y funcionalidad. Sin embargo no se puede garantizar que las acciones

correctivas y preventivas que se aplicarán en el plan de mantenimiento prolonguen el tiempo de vida de los equipos o que corrijan completamente las fallas que presentan.

Finalmente con el reconocimiento y etiquetado de las conexiones se tendrá una identificación más ágil de la distribución del cableado. Lo que permitirá conocer cómo están distribuidas las conexiones en el rack entre los switches, patch panel y rosetas.

CAPÍTULO IV

Implementación de plan de mantenimiento y resultados obtenidos

En este capítulo se describirán las actividades realizadas durante la implementación del plan de mantenimiento, se analizarán los resultados obtenidos y se describirán las condiciones de funcionalidad y operatividad de la red una vez finalizado el plan de mantenimiento.

4.1 Desarrollo de actividades del plan de mantenimiento

4.1.1 Mantenimiento físico de switches

El mantenimiento físico de los switches se llevó a cabo conforme a las fechas establecidas en el cronograma. Los equipos fueron desmontados del rack y se desarmaron completamente para limpiar todos sus componentes internos.

El sistema de ventilación de los todos los switches fue limpiado y revisado en busca de alguna falla física. Se limpiaron todos los orificios de las carcasas, mismos que obstruían la ventilación en algunos switches.

Figura 4. 1 Switch desmontado, previo al mantenimiento

Figura 4. 2 Switch desmontado, vista trasera

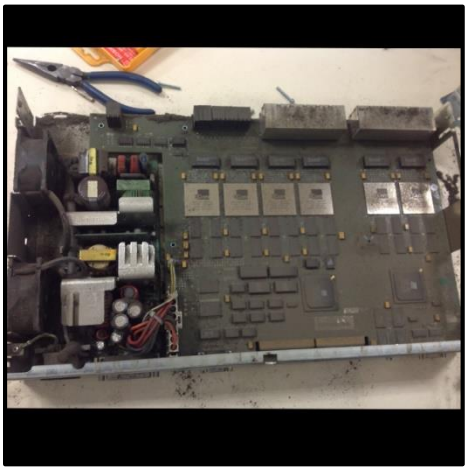


Figura 4. 3 Vista del interior del switch

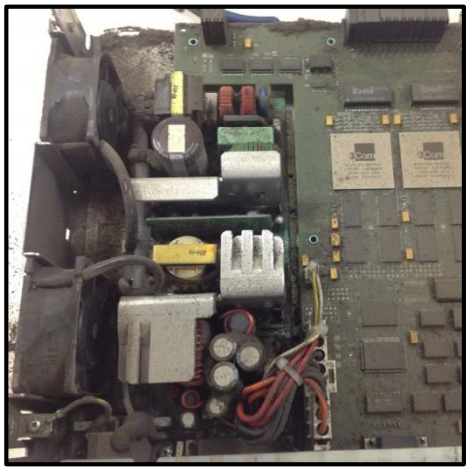


Figura 4. 4 Sistema de ventilación y fuente de poder del switch

Figura 4. 5 Vista de las interfaces del switch

Figura 4. 6 Ventilador del switch

Figura 4. 7 Orificios de ventilación obstruidos por el polvo

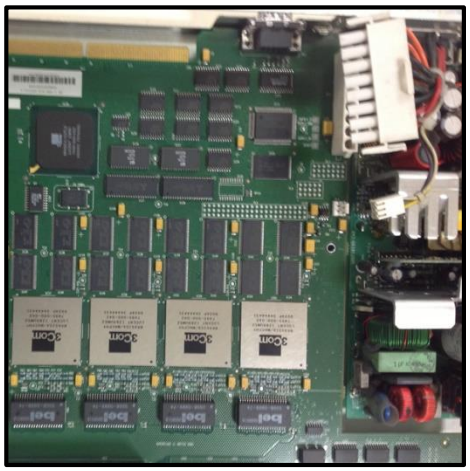


Figura 4. 8 Vista del interior del switch después del mantenimiento

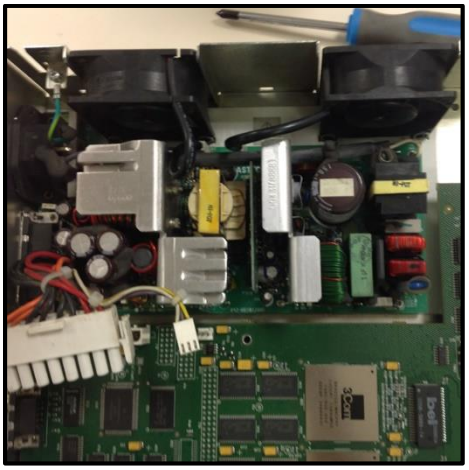


Figura 4. 9 Sistema de ventilación y fuente de poder después del mantenimiento

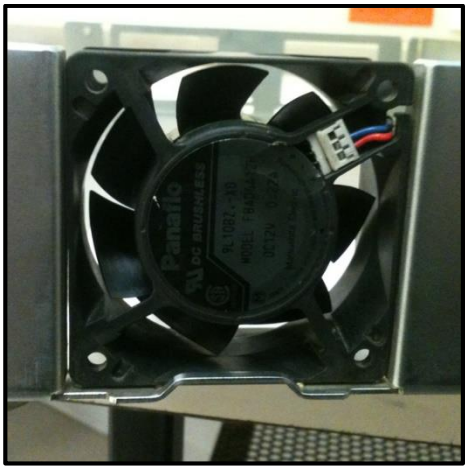


Figura 4. 10 Ventilador después del mantenimiento

Una vez realizado el mantenimiento físico de estos equipos, nuevamente fueron montados en el rack y puestos a funcionar.

4.1.2 Ponchado de rosetas

Durante la primera semana del plan de mantenimiento se realizó el ponchado de las 12 rosetas que habían sido identificadas con problemas físicos. Esta actividad no requería de suspender los servicios de red del laboratorio, debido a que el mantenimiento de cada roseta se podía llevar a cabo en periodos de tiempo en que no hubiera clases o que el equipo que se conecta a la roseta no estuviera siendo utilizado.

Tres de los doce conectores hembra RJ-45 que recibieron mantenimiento fueron sustituidos debido a que presentaban fallas físicas irreparables.

En esta actividad además de verificar la funcionalidad física de los conectores, se respetó el tipo de configuración de cableado que originalmente se implementó en el laboratorio, por lo que el ponchado de rosetas se realizó con la configuración TIA/EIA 568-A.

Una vez que las rosetas eran ponchadas y armadas, se conectaba de nuevo el equipo para verificar que había conectividad.

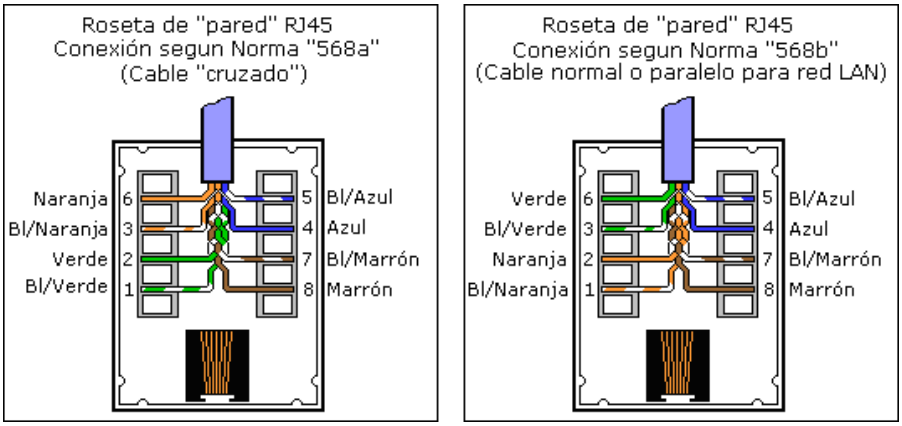


Figura 4. 11 Configuración de conexiones, conectores hembra RJ-45

4.1.3 Ponchado de cables patch cord

Como se había establecido en el cronograma, durante la segunda semana del plan de mantenimiento se llevó a cabo el ponchado de cables terminales o patch cord. Un total de 19 cables fueron ponchados nuevamente debido a que presentaban fallas físicas, de tamaño o de configuración.

Cada uno de estos cables fue corregido cambiando sus conectores RJ-45, respetando la configuración del tipo de cable TIA/EIA 568-A y proporcionándoles el tamaño correcto según su ubicación y la de su correspondiente roseta.

Para corroborar el correcto ponchado de los cables, fue diseñado un tester basado en un circuito básico implementado en una protoboard, el circuito se ilustra en la *Figura 4.12*. Con este tester se verifica el correcto ponchado de los cables ya que cuenta con 2 conectores hembra RJ-45 en los cuales se conecta el cable ponchado cerrando el circuito y encendiendo un led por cada par de pines de los conectores. El correcto funcionamiento de un cable se verifica al visualizar todos los leds encendidos.

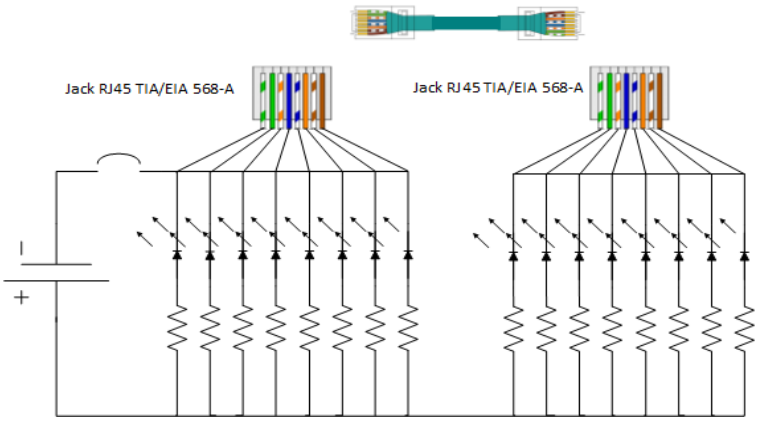


Figura 4. 12 Diagrama de circuito eléctrico de tester RJ45

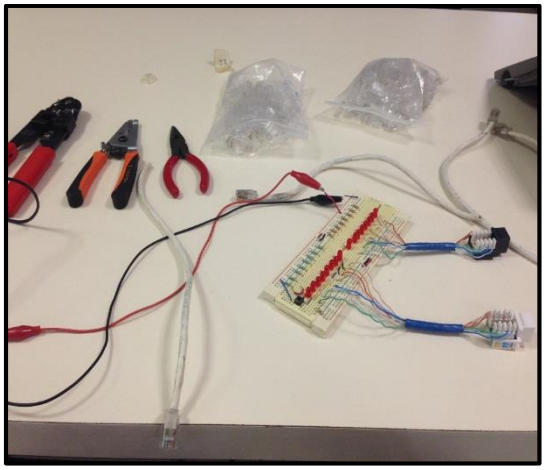


Figura 4. 13 Herramientas utilizadas para el ponchado de cables

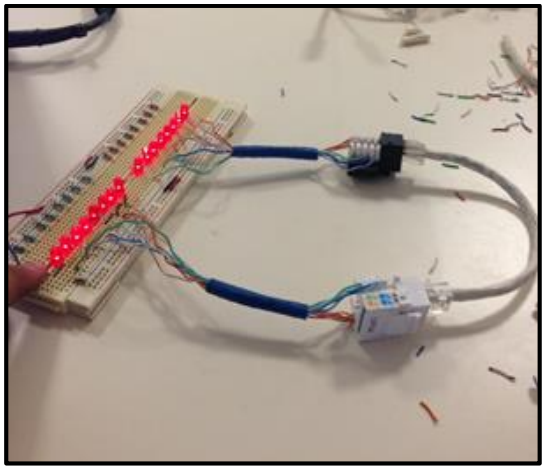


Figura 4. 14 Uso del tester para probar el ponchado de un cable

4.1.4 Configuración de parámetros de red y mantenimiento del sistema operativo

Conforme a las fechas establecidas en el cronograma del plan de mantenimiento se llevó a cabo la configuración de red de los equipos de cómputo y el mantenimiento del sistema operativo.

Se realizó la distribución de direcciones IP por áreas de trabajo, es decir, del segmento de red ***192.168.199.0/24*** se asignaron rangos de direcciones IP para cada área de trabajo en específico.

La distribución de direcciones IP que se diseñó se presenta en la *Tabla 13*:

	Rango de direcciones asignadas	
Área de trabajo	**Primera dirección utilizable**	**Última dirección utilizable**
LE-01	192.168.199.1	192.168.199.49
LE-02	192.168.199.50	192.168.199.98
Administración	192.168.199.99	192.168.199.109
Servicio social	192.168.199.110	192.168.199.130
Sin asignar	192.168.199.131	192.168.199.244
Equipos de red	192.168.199.245	192.168.199.253

Tabla 13 Distribución de direcciones IP por área de trabajo

La asignación de direcciones IP se realiza de manera manual ya que no se cuenta con un servidor DHCP, además de que es requerido tener identificado cada equipo con un nombre y dirección únicos.

Durante el análisis de la red se descubrió que los equipos de cómputo tenían configurados como servidores DNS por defecto algunas direcciones IP sin servicio. Durante los ajustes de los parámetros de red en cada equipo, se eliminaron dichos servidores y se asignaron únicamente dos, el principal que corresponde a un servidor DNS público de la UNAM que tiene la dirección IP ***132.248.10.2*** y como secundario el DNS público de google con la dirección IP ***8.8.8.8***, el cual fue elegido debido a su alta disponibilidad y a los niveles de seguridad con que cuenta, siendo así uno de los servidores DNS más confiable y conocido.

En los equipos de cómputo de las áreas de trabajo LE-01 y LE-02 se realizó la configuración de los grupos de trabajo que proporciona el sistema operativo Windows, esto permitió limitar la compartición de archivos en la red a únicamente los equipos que pertenezcan al mismo grupo de trabajo.

Una vez configurados los parámetros de red de todos los equipos, se realizaron modificaciones en las configuraciones de algunas aplicaciones que se había detectado descargaban actualizaciones automáticas y enviaban reportes de actividad a servidores remotos.

Las aplicaciones identificadas con esta problemática fueron ***TuneUp Utilities, CCleaner y Deep Freeze.*** Estas aplicaciones son utilizadas para dar mantenimiento y limpieza al sistema operativo.

Se configuraron dichas aplicaciones para que no buscaran ni descargaran actualizaciones automáticas, además de restringir el análisis automático del sistema operativo y de aplicaciones. Con esto se consiguió disminuir la cantidad de tareas en segundo plano que generaban estas aplicaciones consumiendo recursos tanto de la red como de las computadoras.

4.2 Análisis de resultados

La implementación del plan de mantenimiento dio como resultado una mejora significativa en los servicios de la red del laboratorio, especialmente en cuanto a la disponibilidad, la cual se veía gravemente afectada antes del plan de mantenimiento aplicado.

El mantenimiento dado a las rosetas del laboratorio ha erradicado las fallas físicas que estos componentes de la red presentaban anteriormente, las cuales provocaban que los equipos de cómputo perdieran conectividad constantemente. Otro beneficio obtenido con

el mantenimiento de las rosetas es haber conseguido estandarizar las configuraciones de los conectores hembra RJ-45 en todo el laboratorio, los cuales ahora respetan la norma TIA/EIA 568-A sin excepción.

Por otra parte, el mantenimiento que se dio a los cables terminales o patch cord de las áreas de trabajo también dio solución a los problemas de conectividad que presentaban algunos equipos debido a que el cable que tenían asignado tenía fallas físicas. Con esto se consiguió que la totalidad de cables patch cord del laboratorio sean funcionales, además de tener el tamaño adecuado y respetar la configuración del cableado establecido por la norma TIA/EIA 568-A.

La correcta distribución de direcciones IP en los equipos del laboratorio ha permitido que no existan más problemas de duplicidad de direcciones en la red. Ahora la asignación de direcciones en los equipos se basa en los rangos establecidos para cada área de trabajo, lo cual permite, entre otras cosas, identificar de manera rápida cada equipo, además de tener un orden a la hora de asignar nuevas direcciones a dispositivos que se integren a la red del laboratorio.

Actualmente todos los equipos del laboratorio tienen configurados los parámetros de red de forma correcta, únicamente tienen un servidor DNS primario y un secundario, los cuales se han verificado están activos y son accesibles desde la red del laboratorio.

La correcta configuración del software instalado en los equipos impide que se realicen tareas en segundo plano que anteriormente demandaban recursos tanto del equipo como de la red. Al ser software utilizado para dar mantenimiento al sistema operativo, no era requerida la descarga de actualizaciones automáticas ni envío de reportes del estado del equipo a servidores remotos, por lo cual fue bloqueado el acceso a internet desde el firewall del propio sistema operativo a estas aplicaciones.

La configuración de los grupos de trabajo que permite realizar el sistema operativo Windows ha limitado el acceso a recursos compartidos en la red. Anteriormente todos los equipos del laboratorio tenían acceso a cualquier recurso que fuera compartido; mediante la configuración de los grupos de trabajo los recursos que comparte un equipo de cómputo únicamente son accesibles desde los equipos pertenecientes al mismo grupo de trabajo.

Anteriormente 3 de los 4 switches con que cuenta el laboratorio presentaban fallas en las que el equipo entraba en estado de suspensión provocado por el sobrecalentamiento. Esta problemática se presentaba de manera aleatoria pero con mayor ocurrencia en tiempos en que la red tenía más actividad. Una vez realizado el mantenimiento físico de los cuatro switches se presentó una mejora notable en el rendimiento de los equipos.

Tres de los switches no presentan fallas de sobrecalentamiento y su funcionamiento es adecuado. Sin embargo uno de los equipos, a pesar de que ha disminuido la frecuencia en que presenta esta falla, sigue entrando en estado de suspensión provocado por el sobrecalentamiento.

4.2.1 Monitoreo de la red

El análisis anterior se sustenta en los resultados obtenidos durante el monitoreo de la red que se realizó después de la aplicación del plan de mantenimiento.

Este monitoreo se llevó a cabo bajo las mismas condiciones que el anterior, es decir, durante un periodo de tiempo de 3 semanas en las cuales se monitorearon un total de 9 sesiones de una hora y media cada uno de los cuatro escenarios posibles.

Escenario 1			
Cantidad de equipos monitoreados	Horas de monitoreo	Evento	Cantidad de Incidencias
36	13 hrs. 30 min.	Falla en red	0
36	13 hrs. 30 min.	Sobrecarga CPU	0
36	13 hrs. 30 min.	Uso de memoria	0
36	13 hrs. 30 min.	Interfaz de Windows	0

Tabla 14 Registro de eventos de segundo monitoreo E1

Escenario 2			
Cantidad de equipos monitoreados	Horas de monitoreo	Evento	Cantidad de Incidencias
17	13 hrs. 30 min.	Falla en red	0
17	13 hrs. 30 min.	Sobrecarga CPU	1
17	13 hrs. 30 min.	Uso de memoria	0
17	13 hrs. 30 min.	Interfaz de Windows	0

Tabla 15 Registro de eventos de segundo monitoreo E2

Escenario 3			
Cantidad de equipos monitoreados	Horas de monitoreo	Evento	Cantidad de Incidencias
19	13 hrs. 30 min.	Falla en red	0
19	13 hrs. 30 min.	Sobrecarga CPU	2
19	13 hrs. 30 min.	Uso de memoria	0
19	13 hrs. 30 min.	Interfaz de Windows	0

Tabla 16 Registro de eventos de segundo monitoreo E3

Escenario 4			
Cantidad de equipos monitoreados	Horas de monitoreo	Evento	Cantidad de Incidencias
36	13 hrs. 30 min.	Falla en red	8
36	13 hrs. 30 min.	Sobrecarga CPU	1
36	13 hrs. 30 min.	Uso de memoria	0
36	13 hrs. 30 min.	Interfaz de Windows	0

Tabla 17 Registro de eventos de segundo monitoreo E4

Como se puede apreciar en las tablas *14, 15, 16 y 17* hubo una disminución considerable en cuanto a fallas de red detectadas. En el monitoreo realizado antes de la aplicación del plan de mantenimiento se detectaron fallas de red en los cuatro escenarios, esto debido a que constantemente se presentaban fallas provocadas por problemas físicos en las rosetas, cables y switches.

Únicamente fueron detectados 8 eventos en los cuales equipos del laboratorio tuvieron fallas de conectividad, las cuales corresponden al escenario 4 en el cual se presenta la mayor actividad en la red del laboratorio. Los 8 eventos detectados corresponden al momento en que el único switch que siguió presentando fallas provocadas por sobrecalentamiento entró en estado de suspensión y por consiguiente los 8 equipos conectados a él perdieron conectividad.

4.3 Conclusiones de implementación de plan de mantenimiento

La aplicación del plan de mantenimiento a bajo costo permitió corregir fallas físicas en los componentes del cableado estructurado de la red, tales como rosetas y cables terminales o patch cord. Tres de los cuatro switches actualmente funcionan con normalidad, únicamente uno de ellos sigue presentando fallas provocadas por el sobrecalentamiento aunque con menor frecuencia.

La disponibilidad de la red mejoró considerablemente después de la aplicación del plan de mantenimiento. El tiempo de vida útil de los componentes del cableado estructurado y de los equipos de interconexión ha sido alcanzado y esto se veía reflejado en las condiciones físicas de dichos componentes que afectaban gravemente la disponibilidad de la red.

Se consiguió estandarizar la configuración del cableado bajo la norma TIA/EIA 568-A, característica que con el paso del tiempo se había perdido. Todas las rosetas y cables terminales del laboratorio respetan esta norma sin excepción.

Se corrigió la distribución de direcciones IP en la red, actualmente está basada en rangos de direcciones IP específicos para cada una de las áreas de trabajo del laboratorio. Además la configuración de parámetros de red en cada equipo del laboratorio se realizó de manera correcta.

Software instalado en los equipos del laboratorio no genera más tareas en segundo plano, no realiza descargas automáticas de internet ni compromete la información almacenada en los equipos.

La implementación del plan de mantenimiento no afectó en ningún momento las actividades programadas en el laboratorio, éste era uno de los principales objetivos debido a que el laboratorio tiene una gran demanda de actividades que diariamente debían ser atendidas.

No se presentaron contratiempos durante la implementación del plan de mantenimiento, las actividades programadas en el cronograma se realizaron conforme a las fechas establecidas.

Aunque los resultados de la aplicación del plan de mantenimiento muestran una gran mejora en los servicios de la red, no es posible garantizar que los componentes del cableado estructurado o equipos de interconexión seguirán funcionando de manera correcta un largo tiempo debido a que, como se ha mencionado anteriormente, han alcanzado su tiempo de vida útil lo cual se ve reflejado en sus condiciones físicas.

CAPÍTULO V
Propuesta de implementaciones en la red del laboratorio

Hace más de 10 años la red del laboratorio fue diseñada para atender las necesidades básicas de los usuarios. Actualmente la distribución de los equipos de cómputo, su direccionamiento, sus configuraciones y los equipos de red implementados no permiten brindar los servicios requeridos por los usuarios, servicios que evidentemente han cambiado desde que la red fue implementada hace más de 13 años.

En este capítulo se presenta una propuesta de nuevas implementaciones en la red del laboratorio, la cual tiene como principal objetivo mejorar los servicios de red que se ofrecen a profesores y alumnos, además de implementar nuevos servicios que brinden a los usuarios, entre otras cosas, mayor seguridad y movilidad; también se busca mejorar los mecanismos de control de acceso a los recursos de la red interna y de internet.

5.1 Actualización de cableado y conectores a categoría 6

Se propone la sustitución de todo el cableado y conectores de la red del laboratorio a categoría 6 (Cat 6).

Actualmente todo el cableado del laboratorio es categoría 5, esta categoría de cable se considera desactualizada a pesar de la funcionalidad que pueda seguir ofreciendo en las redes de datos.

Beneficios de actualización a categoría 6:

- Soporte de red:

  El cableado Cat 6 soporta transferencia de datos desde 10 hasta 1000 Mbps a diferencia de la Cat 5 que soporta únicamente hasta 100 Mbps. El cableado Cat 6 es completamente compatible con versiones anteriores, y se puede utilizar en cualquier aplicación en la que se suele utilizar cable Cat 5.

- Reducción de crosstalk:

  Diafonía es la interferencia eléctrica que se produce cuando los efectos de señal de un cable interfieren con la señal de otro cable. El cable Cat 6 se ha mejorado con respecto al cable Cat 5 en este aspecto, la diafonía se ha reducido considerablemente.

- Ancho de Banda:

  Esto está directamente relacionado a la red de apoyo, en el sentido de que el ancho de banda es la capacidad de transportar información de un sistema. Cuanto mayor sea el ancho de banda, mayor será la capacidad de transportar información en un período dado de tiempo. El cable Cat 6 tiene una potencia de 350 MHZ y es este aumento de ancho de banda que le permite soportar Ethernet Gigabit.

Sustituir el cableado del laboratorio es una acción que deberá realizarse próximamente debido a las condiciones físicas de los componentes que operan actualmente. La implementación de cableado Cat 6, además de los beneficios anteriormente mencionados, permitirá al laboratorio posibles nuevas implementaciones de equipos con mejores características, mayor velocidad de transferencia y ancho de banda.

Cantidad de material[1] requerido:

- Cable UTP Cat 6:
  - Tendido horizontal
  - Patch cords
  - Rack

Total: 2,145 metros de cable Cat 6

- Conectores hembra RJ-45 (jacks) Cat 6:
  - 80 conectores

- Conectores RJ-45 (plugs) Cat 6:
  - 500 conectores

- Patch panel de 24 puertos Cat 6:
  - 4 Unidades

Costo estimado de material para cableado					
Material (Cat 6)	Cantidad requerida	Unidad de venta	Costo por unidad de venta (MXN)	Unidades de venta requeridas	Costo total (MXN)
Cable UTP	2,145 metros	Bobina de 300 mts.	$920.00	8	$7,360.00
Conectores hembra RJ-45	80 unidades	Individual	$39.00	80	$3,120.00
Conectores macho RJ-45	500 unidades	Paquete de 100 piezas	$165.00	5	$825.00
Patch Panel 24 Puertos	4 unidades	Individual	$630.00	4	$2,520.00

Tabla 18 Costo de material para cableado Cat 6

5.2 Equipos de interconexión Switches

Los equipos de interconexión switches que actualmente operan en la red del laboratorio son de tipo plug-and-play, es decir no son administrables. Únicamente se conectan a sus

[1] Material Cableado Categoría 6. Proveedor PCdigital, precio al 4 de Noviembre de 2014. http://www.pcdigital.com.mx/

interfaces los equipos pertenecientes a la red y al tener configurada una dirección IP del mismo segmento, los equipos de cómputo tendrán conectividad.

A pesar de las facilidades de implementación y de operatividad que poseen este tipo de switches, al no ser administrables limitan las configuraciones y adaptación a las necesidades de la red en que se implementen.

Un switch administrable permite implementar tecnologías como las redes virtuales o VLANs que ayudan a optimizar el tráfico de la red y mejoran la seguridad y el acceso a los recursos, entre otros beneficios. Con la implementación de switches administrables se puede reaccionar ante el crecimiento de la red, y mejorar la confiabilidad y disponibilidad de la misma.

El estado físico de los switches que actualmente son utilizados en la red del laboratorio es malo, a pesar del mantenimiento dado a dichos equipos no hay garantía de que sigan funcionando correctamente. Existe un riesgo constante de falla en estos equipos que, en caso de presentarse, atentaría contra la disponibilidad de la red completamente.

Se propone la adquisición de nuevos switches administrables que, además de brindar los servicios básicos de interconexión, permitan la implementación de otras tecnologías como VLANs, configuración de puertos espejo (port mirroring) para monitorear el tráfico de la red, y calidad de servicio.

El modelo de switches propuesto para esta implementación es el NETGEAR FS726T, el cual cuenta con las siguientes características técnicas:

Ficha técnica Switch NETGEAR FS726T	
Compatibilidad de protocolos y estándares	– IEEE 802.3 10BASE-T – IEEE 802.3u 100BASE-TX – IEEE 802.3ab 1000BASE-T – IEEE 802.3z 1000BASE-X – IEEE 802.3x full-duplex flow control
Puertos de red	24 Puertos Fast Ethernet 10/100 Mbps con auto-sensing. 2 Puertos Gigabit Ethernet 10/100/1000 Mbps con auto-sensing. 1 slot SFP slot SFP Módulos GBIC.
LED	Por puerto: (10/100 and Gigabit): Link/ Activity, Speed Por dispositivo: Power
Administración	– IEEE 802.1Q VLAN estática (64) – VLAN basada en puerto (26) – IEEE 802.1p Class of Service (CoS) – QoS basada en puerto

	– DSCP, QoS Capa 3 – IEEE 802.3ad – IEEE 802.1D Spanning Tree Protocol – RFC 1157 SNMP v1* – RFC 1213 MIB II – RFC 1643 Ethernet Interface MIB – RFC 1493 Bridge MIB – RFC 2131 DHCP Cliente – Static IGMP e IGMP Snooping v1 – Private Enterprise MIB – Soporte para puerto espejo – Configuración basada en interfaz web – Configuración de respaldo y restauración – Control de acceso por password e IP – Control de tormenta broadcast – Actualización de firmware

Tabla 19 Ficha técnica de switches propuestos

El costo[2] por dispositivo es de $3,010.90, son requeridos 4 switches para el laboratorio haciendo un total de $12,043.00 MXN.

5.3 Firewall

Con la finalidad de gestionar y filtrar la totalidad de tráfico entrante y saliente de la red del laboratorio se propone la implementación de un dispositivo firewall.

Con la correcta instalación y configuración de un firewall en el laboratorio se podrá restringir el acceso a diversos sitios web y servicios que están prohibidos en el laboratorio, además este control se puede implementar a nivel local si en conjunto con los switches administrables se configuran VLANs.

Tener la posibilidad de controlar el tráfico entrante y saliente de la red traería muchos beneficios en cuanto a su administración. Actualmente no existe un mecanismo que prohíba el acceso a páginas no permitidas en el laboratorio como redes sociales, sitios de descargas, juegos en línea o páginas para adultos por lo que el área que administra el laboratorio debe estar revisando presencialmente que los alumnos no accedan a este tipo de sitios.

La red del laboratorio puede considerarse relativamente pequeña, la cantidad de hosts activos en la red no supera los 50, esto es un factor importante a considerar al momento

[2] NETGEAR FS726T. Proveedor e-office, precio al 4 de Noviembre de 2014. https://www.e-office.com.mx/shop/redes/switches/netgear/47/

de proponer un firewall ya que éste debe cumplir con ciertas características de funcionalidad y operatividad requeridas en la red en que será implementado.

Se propone el firewall FortiGate 60C, el cual es un dispositivo diseñado para redes medianas y pequeñas, las características de este dispositivo se describen en el Anexo II.

El costo[3] de este dispositivo a precio de lista es de $6,341.00 MXN.

Este dispositivo permite su configuración vía web o mediante el software FortiExplorer incluido en la compra del equipo. Entre las funcionalidades con que cuenta este firewall y que se consideran aplicables a la red del laboratorio están:

- **Definición de políticas de navegación:** Son las reglas que definen qué tipo de tráfico de entrada y salida está o no permitido en la red. Es mediante estas políticas de navegación que se define por ejemplo a qué sitios en específico no se permite el acceso, o inclusive pueden definirse los servicios que deben ser bloqueados como SSH o FTP por ejemplo.

- **Definición de interfaces internas:** La definición de interfaces internas permite que el dispositivo reciba paquetes etiquetados pertenecientes a VLANs. Al definir interfaces internas con la información de las VLANs que debe permitir el firewall, este dispositivo aplicará a dichas interfaces las políticas que les sean definidas y les brindará servicios como DHCP, DNS e incluso podrá realizar el direccionamiento entre VLANs si así se configura.

- **Generación de bitácoras:** El firewall genera bitácoras en las que se registran los eventos ocurridos detectados por el firewall. Entre estos eventos pueden estar inicios de sesión al firewall, bloqueos de conexiones o servicios en específico, detección de posibles ataques a la red, etc. Estas bitácoras pueden ser consultadas a través de la interfaz web o mediante el software FortiExplorer.

- **Monitor de actividad:** Este servicio muestra estadísticas de conexiones realizadas a nivel local y remoto. Se pueden enlistar los sitios web y servicios a los que se han accedido en determinado tiempo.

- **Servidor DHCP:** Este servicio permite configurar dinámicamente los parámetros de red en los equipos. Se pueden configurar de manera general o únicamente en algunas de las interfaces internas que se hayan definido en el firewall. Por ejemplo este servicio podría habilitarse únicamente en una interfaz interna que sea definida para una VLAN dedicada a conectividad inalámbrica.

[3] FortiGate 60-C. Proveedor AVFirewalls, precio al 4 de Noviembre de 2014. http://www.avfirewalls.com/FortiGate-60C.asp

- **Definición de usuarios:** Este dispositivo permite definir varios usuarios a los cuales se les puede dar acceso a toda la administración del dispositivo o únicamente a algunas secciones de la interfaz web o software FortiExplorer. De esta manera se podrán crear usuarios que únicamente puedan estar monitoreando la actividad detectada por el firewall o las políticas que se han aplicado pero no podrán modificarlas.

En la *Figura 5.1* se muestra el diagrama lógico de la red que se tiene actualmente en el laboratorio:

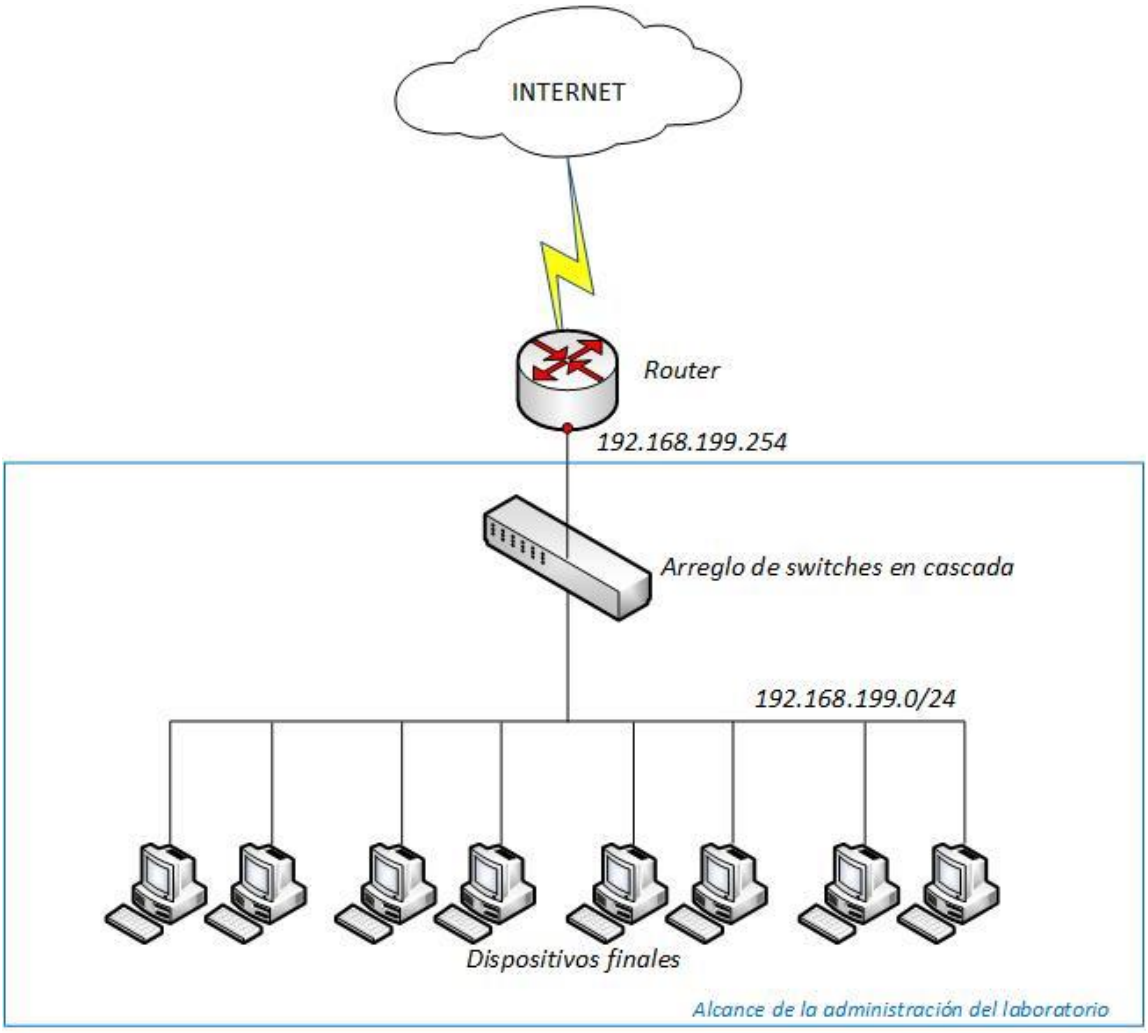


Figura 5. 1 Diagrama lógico de la red actual.

El alcance de la administración de la red está limitado por el recuadro azul, es decir, únicamente se tiene control sobre la red interna a partir de los switches y hasta los dispositivos finales.

De acuerdo a lo anterior, la ubicación del firewall se propone entre el router y el switch ilustrados en el diagrama. De esta manera el dispositivo puede ser administrado desde la red interna del laboratorio además podrá filtrar el tráfico de salida y de entrada sin inconvenientes.

La *Figura 5.2* muestra el diagrama lógico de la red con la propuesta de la implementación del firewall:

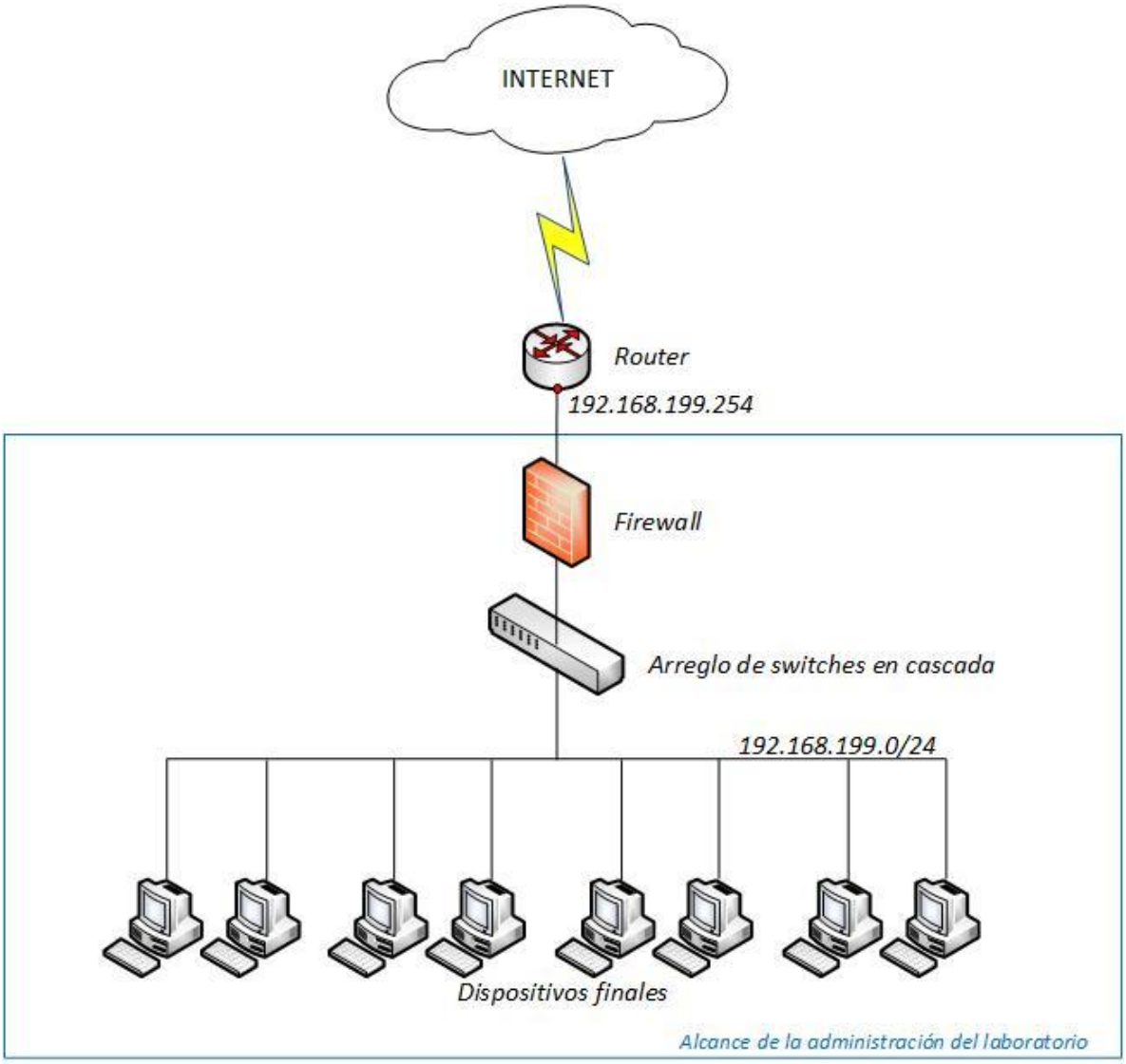


Figura 5. 2 Diagrama lógico, implementación de Firewall.

5.4 VLANs

Actualmente toda la red del laboratorio pertenece al mismo segmento de red, es decir, todos los equipos del laboratorio forman parte de la misma red independientemente del área de trabajo a la que pertenezcan. Esto genera la problemática de que todos los dispositivos conectados a la red pueden comunicarse entre sí, lo que implica que si se comparten recursos en alguna área de trabajo todos los equipos podrán acceder a esos recursos indistintamente.

Para resolver esta problemática se propone la implementación de redes virtuales o VLANs, las cuales segmentarán de manera lógica la red brindando los siguientes beneficios:

- **Mayor seguridad:** Las distintas áreas de trabajo del laboratorio quedarán seccionadas cada una por una VLAN, de esta manera aquellas áreas que tengan datos sensibles se separarán del resto de la red, disminuyendo la posibilidad de que se tenga acceso a información confidencial desde distintas VLANs.

- **Mejor rendimiento:** Poder dividir la actual red plana de capa 2 en múltiples grupos lógicos de trabajo reduce el tráfico innecesario en la red e incrementa el rendimiento.

- **Reducción de dominio Broadcast:** Dividir la red en VLANs reducirá la cantidad de dispositivos que pueden participar en una tormenta broadcast.

- **Adaptabilidad:** Al tener definida una VLAN para cada área de trabajo ésta será acondicionada según las necesidades de los usuarios que deban pertenecer a la VLAN.

Para poder configurar VLANs en la red del laboratorio es necesario contar en primera instancia con switches administrables que permitan esta tecnología. Los switches propuestos en este proyecto son los NETGEAR FS726T, estos switches permiten la configuración de VLANs estáticas, es decir, cada puerto del switch es configurado para pertenecer a una VLAN.

Adicionalmente es requerido un dispositivo de capa 3 que pueda direccionar las tramas etiquetadas de las VLANs para permitir la comunicación entre ellas y dar salida a internet. Idealmente un dispositivo router es quien puede ser configurado para realizar estas funciones pero en este caso se puede implementar el firewall FortiGate 60C propuesto en este proyecto debido a que también permite realizar estas funciones.

El siguiente diagrama lógico de la red presentado en la *Figura 5.3* muestra la implementación de las VLANs en conjunto con el arreglo de los switches propuestos y el firewall:

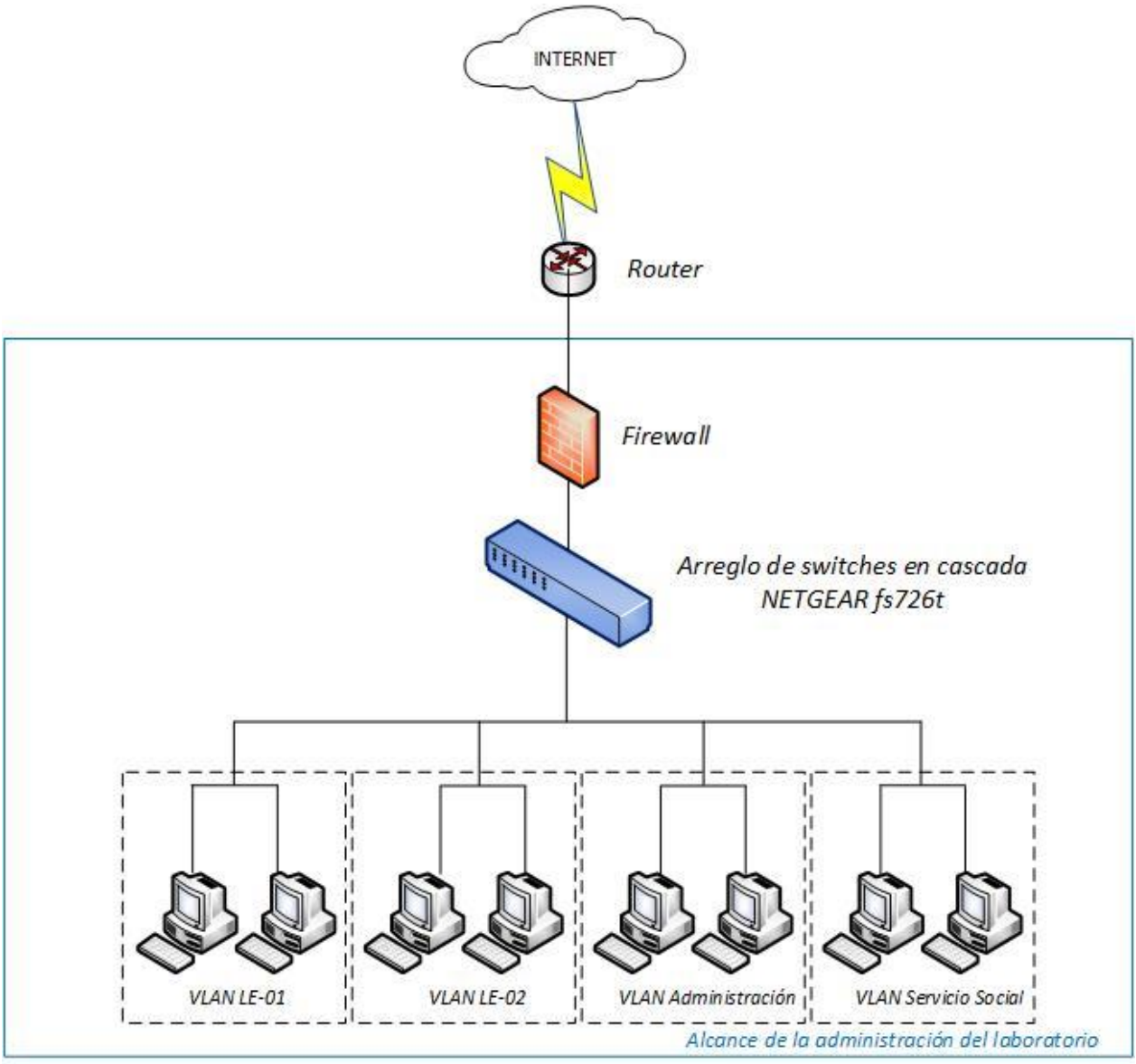


Figura 5. 3 Diagrama lógico, implementación de VLANs.

5.5 Red inalámbrica

En la actualidad, la cantidad de equipos con que cuenta el laboratorio son insuficientes puesto que el número de alumnos que conforman los grupos que acuden al él ha aumentado considerablemente en los últimos años.

Esto ha provocado que los alumnos se vean motivados en llevar sus equipos personales o laptops para poder trabajar dentro de la red del laboratorio. Sin embargo, la infraestructura de la red no permite que estos usuarios tengan acceso de manera ágil puesto que no existen rosetas disponibles ni espacios dedicados para estos usuarios.

Para cubrir estos requerimientos se propone la implementación de una red inalámbrica dentro del laboratorio. Un Access Point es el dispositivo que permitirá conectar de manera inalámbrica los equipos de los alumnos a la red del laboratorio.

La red inalámbrica conformaría una nueva área de trabajo la cual tendría un rango de direcciones IP asignado y pertenecería a una VLAN. La cantidad máxima de equipos que se estima podrían estar conectados a la red inalámbrica en el laboratorio es de 30, por lo cual se propone un rango de 40 direcciones IP para cubrir la cantidad estimada y tener direcciones de reserva.

La propuesta de distribución final de direcciones IP dentro del laboratorio se muestra en la *Tabla 20.*

	Rango de direcciones asignadas	
Área de trabajo	**Primera dirección utilizable**	**Última dirección utilizable**
LE-01	192.168.199.1	192.168.199.49
LE-02	192.168.199.50	192.168.199.98
Administración	192.168.199.99	192.168.199.109
Servicio social	192.168.199.110	192.168.199.130
Red inalámbrica	192.168.199.131	192.168.199.170
Sin asignar	192.168.199.171	192.168.199.244
Equipos de red	192.168.199.245	192.168.199.253

Tabla 20 Distribución final de direcciones IP por área de trabajo.

Es requerido que la red inalámbrica sea capaz de cubrir toda el área del laboratorio para que pueda garantizar la conectividad en las áreas de trabajo. Considerando que un Access Point ofrece cobertura en forma radial, será requerido que el dispositivo emita la señal de al menos 18 metros desde su ubicación.

En la *Figura 5.4* se muestra el área que debe cubrir el Access Point dentro de todo el laboratorio:

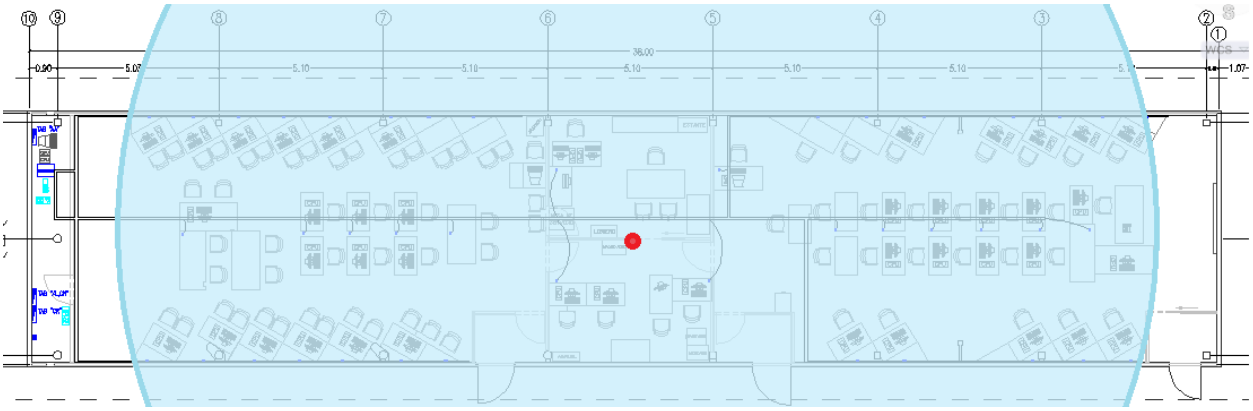


Figura 5. 4 Área de cobertura del Access Point.

El equipo propuesto para la implementación de la red inalámbrica es el Access Point WAP300N de Linksys Cisco. Este dispositivo cuenta con las siguientes características técnicas:

Ficha técnica Access Point WAP300N de Linksys Cisco	
Velocidad del puerto Ethernet	10/100 Mbps (Fast Ethernet)
Radiofrecuencia	2,4 y 5 GHz
Número de antenas	2
Tipo de antena	Antena dipolo externa con conector R-SMA
Desmontable	Sí
Puertos	Power (Alimentación), Ethernet
Botones	Reset (Reinicio), Wi-Fi Protected Setup™ (Configuración Wi-Fi protegida), Power (Alimentación) (solo el modelo europeo)
LED	Alimentación, configuración Wi-Fi protegida, Ethernet, conexión inalámbrica
Funciones de seguridad inalámbrica	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2), filtrado de direcciones MAC inalámbrico
Bits de clave de seguridad	Cifrado de hasta 128 bits
Alcance	De 30 a 40 metros a partir de su ubicación.

Tabla 21 Ficha técnica de Access Point propuesto.

El costo[4] del Access Point WAP300N de Linksys Cisco es de $1,065.00 MXN. La administración del dispositivo se realiza mediante una interfaz web y permite realizar un respaldo de la configuración del equipo.

[4] Access Point WAP300N Linksys Cisco. Proveedor PCEL, precio al 4 de Noviembre de 2014. http://pcel.com/Linksys-WAP300N-100580

El alcance de la señal que brinda este dispositivo supera el requerido en el laboratorio, además incluye una función de seguridad que puede ser implementada en la red del laboratorio para restringir el acceso a la red inalámbrica, el filtrado de direcciones MAC.

Este filtrado utiliza una lista de direcciones MAC que son introducidas manualmente, cada dirección corresponde a un dispositivo, ya sea una computadora, laptop, celular, tablet, etc. Tomando en cuenta esta lista, hay dos modos en los que se puede configurar el filtrado MAC:

1. **Permitir la conexión a los dispositivos añadidos a la lista de direcciones MAC.** Mediante este modo de configuración, únicamente aquellos dispositivos que se encuentren en la lista de direcciones podrán conectarse a la red inalámbrica. A todo aquel dispositivo que no se encuentre en la lista de direcciones no le será permitido conectarse a la red.

2. **Denegar la conexión a los dispositivos que aparecen en la lista de direcciones MAC.** Con este modo de configuración, cualquier equipo podrá conectarse a la red inalámbrica del laboratorio excepto todos aquellos dispositivos cuya dirección MAC se encuentre en la lista.

En el laboratorio será necesario que los usuarios que requieran acceso a la red inalámbrica del laboratorio registren sus equipos, de esta manera serán introducidas las direcciones MAC de estos equipos en la lista de filtrado del Access Point y se configurará de tal manera que solo tengan acceso a la red inalámbrica los equipos que se encuentren en la lista.

Esta red inalámbrica propuesta está destinada a todos los usuarios que requieren acceso a internet desde la red del laboratorio, incluyendo alumnos, profesores, prestadores de servicio social, invitados. Por esta razón dicha red inalámbrica pertenecería a una VLAN independiente para poder administrar desde el firewall el acceso a los diferentes recursos disponibles en la red.

Implementar una red inalámbrica en el laboratorio traería muchos beneficios para los usuarios que requieren de los servicios ofrecidos en la red del laboratorio. Los usuarios tendrían acceso a la red desde sus equipos personales lo cual resolvería el problema de la falta de equipos instalados en el laboratorio. Con la implementación del filtrado MAC del Access Point y las políticas de navegación del firewall, se controlaría el acceso a la red inalámbrica y además el acceso a los recursos a los cuales estos usuarios temporales tienen permitido ingresar.

En la *Figura 5.5* se muestra el diagrama lógico de la red que incluye la implementación del Access Point, con esto se presenta el diagrama lógico de la red final basado en las propuestas mencionadas en este capítulo:

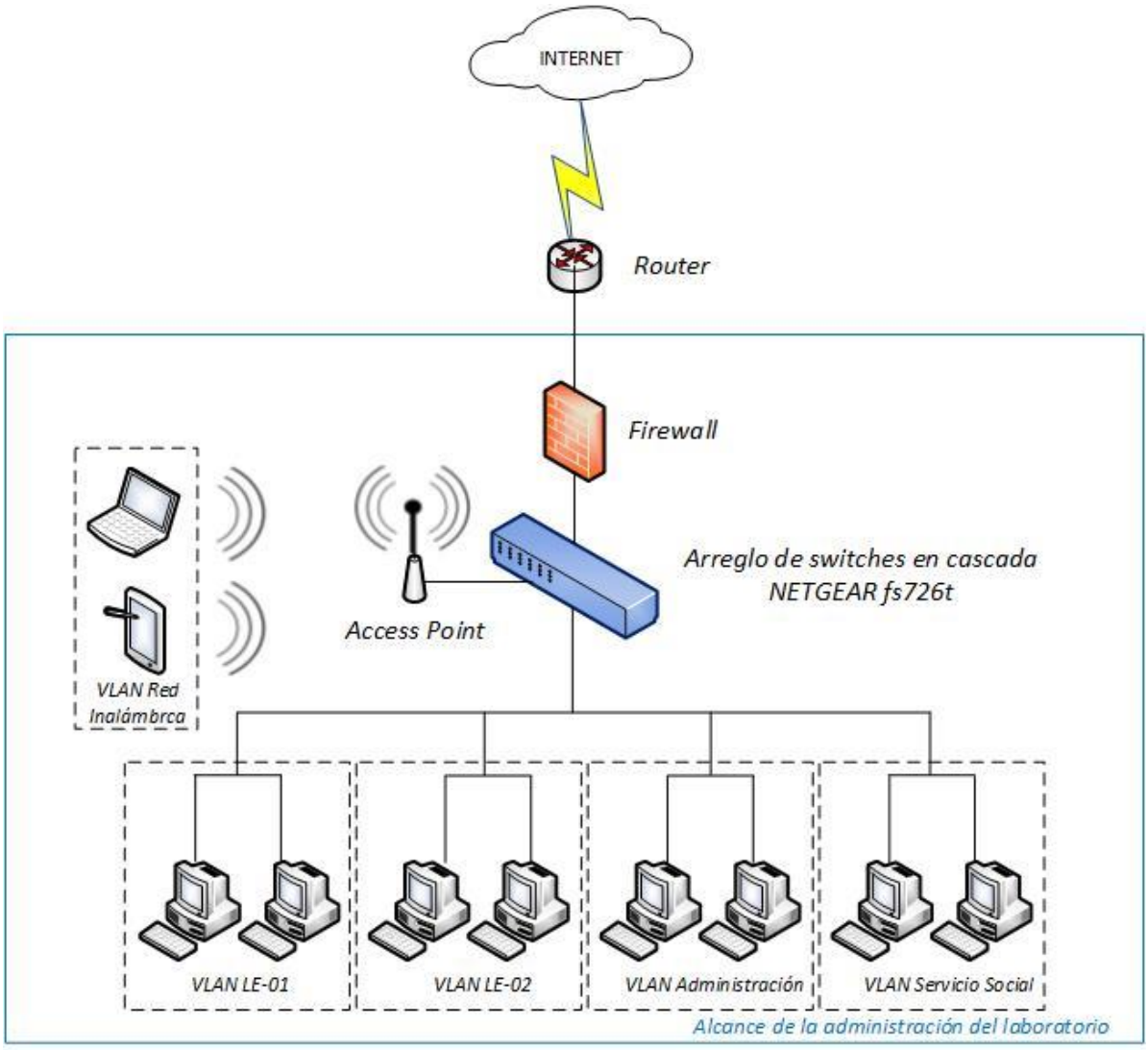


Figura 5. 5 Diagrama lógico de la red final

5.6 Resumen de la propuesta

La implementación de esta propuesta significaría la renovación de la red del laboratorio, no únicamente de los componentes del cableado ni equipos de interconexión, sino de la distribución y operatividad de la red misma. Esta propuesta está compuesta por:

1. Actualización de cableado y conectores a categoría 6
2. Equipos de interconexión Switches administrables
3. Firewall
4. Implementación de VLANs
5. Red inalámbrica

Entre los principales beneficios que obtendría la red del laboratorio se encuentran:

- Mayor disponibilidad en la red
- Velocidades de transferencia de datos desde 10 hasta 1000 Mbps
- Mayor ancho de banda y reducción de crosstalk
- Segmentación lógica de la red
- Mayor seguridad en la red
    - Definición de políticas de navegación
    - Monitoreo de la red
    - Definición de alcance de segmentos lógicos
    - Generación de bitácoras
- Servicio DHCP
- Mejor rendimiento
- Acceso inalámbrico controlado
- Posibilidad de integrar nuevas tecnologías y dispositivos en la red
- Identificación ágil de equipos en la red y de la distribución del cableado

En la *Tabla 22* se muestran los costos estimados de las propuestas de actualización de componentes de red y nuevas implementaciones en el laboratorio. Los costos estimados consideran el precio del material y dispositivos requeridos en cada propuesta detallada en este capítulo:

Resumen de costos	
Propuesta	Costo total estimado MXN
Actualización de cableado y conectores a categoría 6	$13,825.00
Equipos de interconexión switches NETGEAR FS726T	$12,043.00
Firewall FortiGate 60C	$6,341.00
Access Point WAP300N de Linksys Cisco	$1,065.00
Total	**$33,247.00**

Tabla 22 Resumen de costos estimados

CONCLUSIONES

Con base en los objetivos planteados al inicio de este proyecto de tesis, los cuales están encabezados por la corrección de fallas físicas y lógicas de la red del laboratorio de Geomática y Especialidades de Civiles mediante la implementación de un plan de mantenimiento a bajo costo, seguido de la propuesta de correcciones y nuevas implementaciones a la red se puede afirmar que dichos objetivos fueron alcanzados satisfactoriamente.

La implementación del plan de mantenimiento a bajo costo significó un gran desafío por dos aspectos principalmente. El primero de ellos fue la limitante económica que se tuvo para la realización de este plan de mantenimiento, la cual obligó a la reutilización de materiales y el uso de las pocas herramientas con que se cuenta en el laboratorio. Por otra parte, la asignación de tiempos a las distintas actividades programadas del plan de mantenimiento sin afectar los horarios de clases también fue complicada, debido a la alta demanda de actividades que tiene el laboratorio diariamente.

Los resultados obtenidos una vez finalizado el mantenimiento a bajo costo de la red del laboratorio demuestran el impacto que dicho mantenimiento tuvo en cuanto a la disponibilidad de la red, operatividad e identificación de los componentes y estructura física y lógica que se tienen. Este plan de mantenimiento permitió identificar claramente cuáles son aquellos aspectos que provocan que los servicios de red que se ofrecen a profesores y alumnos de la Facultad de Ingeniería se vean afectados. El estado físico de los componentes de red tales como el cableado, conectores y equipos de interconexión, es el factor de mayor importancia en cuanto a las diferentes fallas que se presentan en la red.

Otro de los beneficios obtenidos de la implementación del plan de mantenimiento a bajo costo y del análisis del estado de la red, fue la identificación de todos los componentes de red con que se cuentan, la elaboración de los planos del cableado estructurado y la documentación del estado de la red y de las configuraciones que se tienen.

A pesar de que se identificó que el estado físico de los componentes de la red del laboratorio era la principal causa de las fallas que se presentaban diariamente, también se observó que las configuraciones de los equipos de cómputo y la asignación desordenada de direcciones IP provocaba problemas en la red del laboratorio. Esta problemática logró resolverse al configurar manualmente todos los equipos de la red del laboratorio, documentando dichas configuraciones y registrando la asignación de direcciones IP con cada equipo del laboratorio para así evitar duplicidad de direcciones lógicas, problema que se presentaba frecuentemente en el laboratorio.

La propuesta de nuevas implementaciones y actualizaciones de los componentes de la red presentada en esta tesis, tiene como principal objetivo mejorar los servicios de red que se ofrecen diariamente en el laboratorio. Esta propuesta supone la reingeniería de la red del Laboratorio de Geomática y Especialidades de Civiles puesto que proyecta la migración de una red plana, insegura, físicamente deteriorada y que no se adapta a las

necesidades de los usuarios a una red segmentada lógicamente, con mayor seguridad, mayor disponibilidad, capaz de integrar nuevas tecnologías y de adaptarse a las necesidades de los usuarios y a las políticas de uso de la red establecidas en el laboratorio.

Gracias al proceso de desarrollo de este trabajo de tesis y al seguimiento dado por el coordinador del laboratorio, el Ingeniero Francisco López Mendieta, fue posible implementar una parte de la propuesta presentada, dicha implementación se describe en el Anexo I. De esta manera se pusieron en práctica los conocimientos y habilidades que fueron adquiridos a lo largo de la carrera en la Facultad de Ingeniería y junto con esta oportunidad se adquirió también la responsabilidad y compromiso de desarrollar, en la medida de lo posible, las implementaciones sin afectar las actividades del laboratorio.

ANEXO I
Implementaciones

Con base en la propuesta presentada, fueron adquiridos los switches NETGEAR FS726T, de los cuales a continuación se presentan imágenes del proceso de instalación junto con el ponchado del rack y el etiquetado de las conexiones en la red del laboratorio.

Los equipos adquiridos fueron:

- 3 Switches NETGEAR FS726T
- 1 Switch JFS524 (No administrable)

La instalación de estos equipos se realizó junto con el ponchado del rack y el etiquetado de las conexiones. Debido a que no era posible suspender las actividades en el laboratorio, el proceso de instalación fue dividido en 4 días, en cada uno de ellos se realizó el montaje de un switch y el ponchado de los cables del patch panel junto con el etiquetado. Estas actividades se realizaron en un horario vespertino, en el cual no se interrumpieron las clases programadas en el laboratorio.

Los switches fueron conectados en cascada. Las conexiones entre el patch panel y el switch se etiquetaron de tal manera que fuera posible identificar de manera clara y rápida de qué roseta proviene el cable ponchado en el patch panel y por consiguiente, a qué puerto del switch se conecta finalmente. Para el ponchado del rack fueron requeridos un total de 82 cables directos con configuración TIA/EIA 568-A.

Las siguientes imágenes muestran el proceso de la instalación de los equipos y el ponchado del rack junto con el etiquetado de las conexiones:

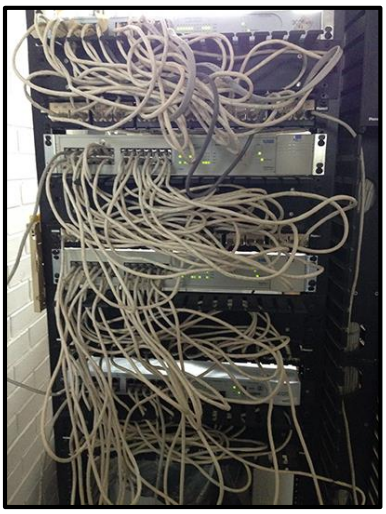


Figura 6. 1 Instalaciones previas en el rack

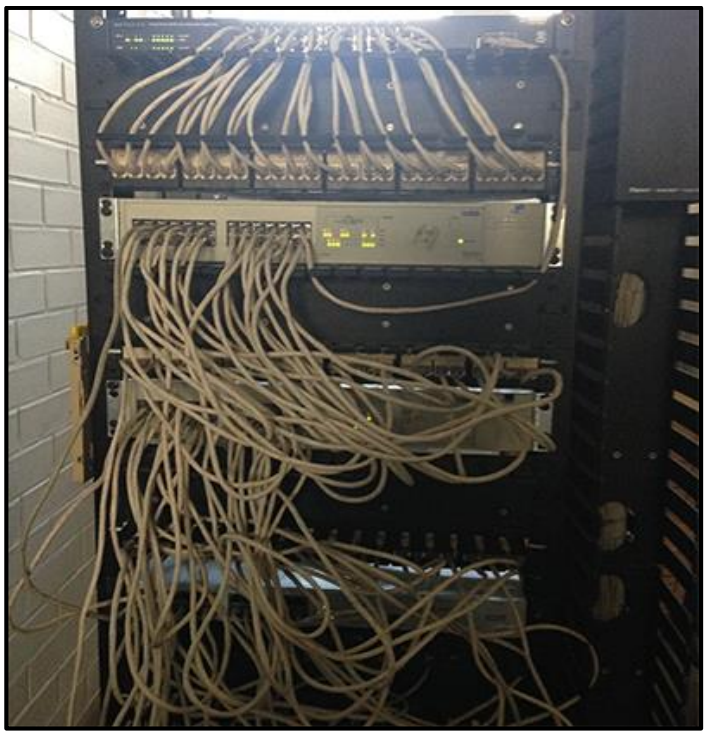


Figura 6. 2 Instalación del primer switch

Figura 6. 3 Instalación del segundo switch

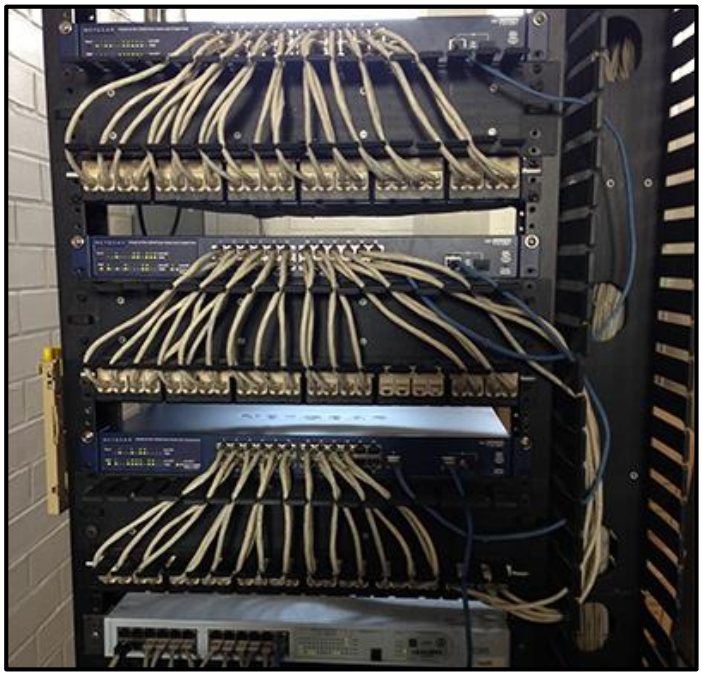


Figura 6. 4 Instalación del tercer switch

Figura 6. 5 Instalación del cuarto switch

Figura 6. 6 Etiquetado de conexiones del primer switch

Figura 6. 7 Etiquetado de conexiones del segundo switch

Figura 6. 8 Etiquetado de conexiones del tercer switch

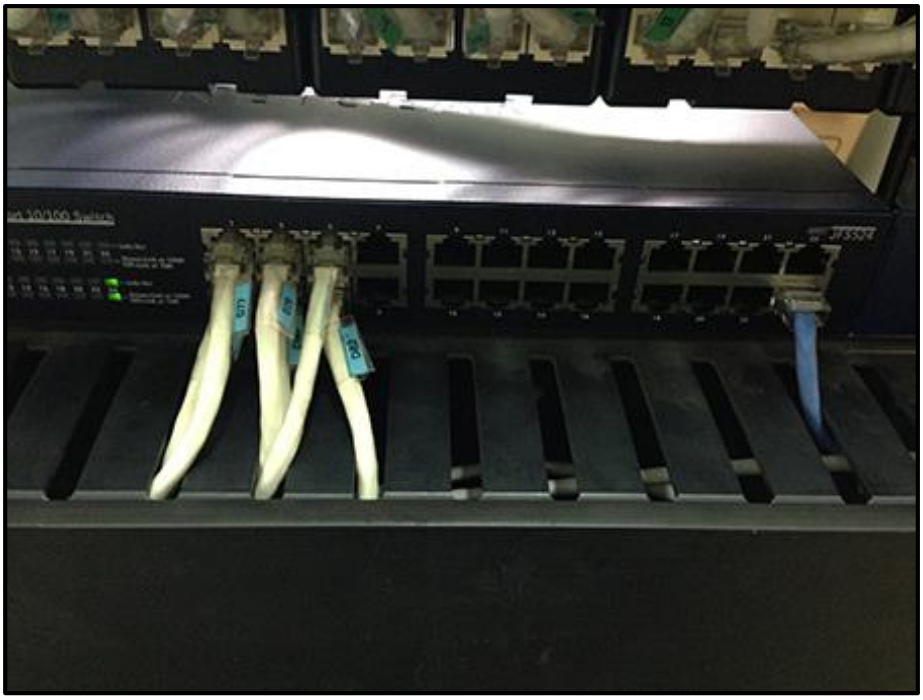


Figura 6. 9 Etiquetado de conexiones del cuarto switch

Figura 6. 10 Instalación final de equipos y conexiones en el rack

ANEXO II
Comparativa de Firewalls

A continuación se presentan los tres dispositivos Firewall que fueron analizados para la propuesta de nuevas implementaciones en la red del laboratorio. Los dispositivos propuestos son desarrollados por la empresa privada Estadounidense Fortinet que se especializa en el diseño y la fabricación de componentes y dispositivos de seguridad de redes. La fácil administración e implementación de estos equipos los hacen ideales para su instalación en la red del laboratorio, además de presentar características y funcionalidades que se ajustan a las necesidades requeridas en esta red.

El dispositivo seleccionado para la propuesta de nuevas implementaciones en la red del laboratorio es el FortiGate 60C, el cual cuenta con las siguientes características:

Ficha técnica FortiGate 60C	
Especificaciones de Hardware	
Interfaces WAN 10/100/1000	2
Interfaces Switch 10/100/1000	5
Interfaces DMZ 10/100/1000	1
Interfaz USB (Cliente/Servidor)	1
Ranura para tarjeta ExpressCard	1
Especificaciones del Sistema	
Rendimiento Firewall (paquetes por segundo)	1.5 Mpps
Sesiones TCP concurrentes	400,000
Nuevas sesiones por segundo (TCP)	3,000
Cantidad de políticas configurables	5,000
Rendimiento IPSec VPN	70 Mbps
Rendimiento IPS	135 Mbps
Rendimiento Antivirus	20/24 Mbps
Dominios virtuales	10/10
Configuraciones de alta disponibilidad	Si
Interfaz de configuración Web	Si
Filtrado Web	Si

Tabla 23 Ficha técnica de firewall FortiGate 60-D

Este dispositivo además de permitir la configuración de políticas que restrinjan el acceso a recursos de la red local e internet, permitirá llevar a cabo el direccionamiento entre las VLANs del laboratorio, la cual es una característica que ahorraría la implementación de un dispositivo de capa 3 como un router para llevar a cabo esta función. Este dispositivo está diseñado para redes medianas y cubre los requerimientos de funcionalidad y operatividad de la red del laboratorio.

Otro de los dispositivos que fueron analizados para su posible propuesta, fue el FortiGate 100-D, cuyas características se presentan a continuación:

Ficha técnica FortiGate 100-D	
Especificaciones de Hardware	
Interfaces WAN 10/100/1000	2
Interfaces Switch 10/100/1000	14
Interfaces DMZ 10/100/1000	1
Interfaz Administración 10/100/1000	1
Puertos de Alta Disponibilidad (HA)	2
Puerto Consola	1
Puertos USB	2
Puerto USB (Administración)	1
Puertos de Intercambio	4
Ranura para tarjeta ExpressCard	1
Especificaciones del Sistema	
Rendimiento Firewall (paquetes por segundo)	300 Kpps
Sesiones TCP concurrentes	3 Millones
Nuevas sesiones por segundo (TCP)	22,000
Cantidad de políticas configurables	10,000
Rendimiento IPSec VPN	450 Mbps
Rendimiento IPS	950 Mbps
Rendimiento Antivirus	300/650 Mbps
Dominios virtuales	10/10
Configuraciones de alta disponibilidad	Si
Interfaz de configuración Web	Si
Filtrado Web	Si

Tabla 24 Ficha técnica de firewall FortiGate 100-D

Es un dispositivo diseñado para redes medianas y grandes, por lo que sus características sobre pasan las necesidades del laboratorio y de igual manera incrementan considerablemente el costo del dispositivo.

Por último, el tercer dispositivo analizado para la propuesta fue el FortiGate 140-D, cuyas características se muestran a continuación:

Ficha técnica FortiGate 140-D	
Especificaciones de Hardware	
Interfaces WAN 10/100/1000	1
Interfaces Switch 10/100/1000	36
Interfaces DMZ 10/100/1000	2
Interfaz Administración 10/100/1000	1
Puertos de Alta Disponibilidad (HA)	1
Puerto Consola	1
Puertos USB	1
Puerto USB (Administración)	1

Especificaciones del Sistema	
Rendimiento Firewall (paquetes por segundo)	300 Kpps
Sesiones TCP concurrentes	3 Millones
Nuevas sesiones por segundo (TCP)	22,000
Cantidad de políticas configurables	10,000
Rendimiento IPSec VPN	450 Mbps
Rendimiento IPS	950 Mbps
Rendimiento Antivirus	300/650 Mbps
Dominios virtuales	10/10
Configuraciones de alta disponibilidad	Si
Interfaz de configuración Web	Si
Filtrado Web	Si

Tabla 25 Ficha técnica de firewall FortiGate 140-D

Al ser un dispositivo de la familia FortiGate serie D, cuenta con características muy similares al modelo FortiGate 100-D, con diferencias únicamente en cuanto a especificaciones de hardware. Es un dispositivo que está diseñado para redes medianas y grandes, pero que por sus características y su precio, sobre pasan las necesidades de la red del laboratorio.

GLOSARIO

Access Point. Es un dispositivo de red que a partir de la conexión alámbrica con un dispositivo de comunicación forma una red inalámbrica, a la cual se conectan dispositivos móviles o equipos con tarjetas de red inalámbricas.

ANSI. (American National Standards Institute). Instituto Nacional Estadounidense de Estándares es una organización sin fines de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos.

Apache. Es un servidor web, conocido por ser un proyecto de código abierto y uso gratuito, multiplataforma, muy robusto y que destaca por su seguridad y rendimiento.

AutoCAD. Autodesk AutoCAD es un software CAD utilizado para dibujo 2D y modelado 3D.

Broadcast. Es una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

CCIA. (Computer and Communication Industry Association). Asociación de la industria de Comunicaciones Computacionales.

Ccleaner. Herramienta de limpieza y optimización del sistema operativo.

CPU. (Central Processing Unit). Unidad central de procesamiento, es el hardware dentro de una computadora u otros dispositivos programables, que interpreta las instrucciones de un programa mediante la realización de las operaciones básicas aritméticas, lógicas y de entrada/salida del sistema.

Crosstalk. Es un disturbio en un circuito o cableado, causado por interferencia electromagnética

CSMA/CA. (Carrier Sense Multiple Access with Collision Avoidance). Acceso múltiple con detección de portadora y evasión de colisiones.

CSMA/CD. (Carrier Sense with Multiple Access with Collision Detection). Acceso múltiple con detección de portadora y detección de colisiones.

Deep Freeze. Programa que permite crear una imagen del sistema operativo y restaurarlo a partir de dicha imagen al reinicio del sistema.

DHCP. (Dynamic Host Configuration Protocol). Protocolo de configuración de host dinámico. Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) de forma dinámica.

DNS. (Domain Name System). Servidor de Nombres de Dominio. Resuelve direcciones IP en nombres de dominio y viceversa.

EIA. (Electronic Industries Alliance). Alianza de Industrias Electrónicas, conocida como Electronic Industries Association hasta 1997, es una organización formada por la asociación de las compañías electrónicas y de alta tecnología de los Estados Unidos, cuya misión es promover el desarrollo de mercado y la competitividad de la industria de alta tecnología de los Estados Unidos con esfuerzos locales e internacionales de la política.

Ethernet. Es un estándar de redes de área local para equipos con acceso al medio por detección portadora y con detección de colisiones (CSMA/CD).

Firewall. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre redes y equipos finales, tomando como base un conjunto de normas y otros criterios.

FTP. Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

Full-Duplex. La transmisión Full-Duplex es el canal de comunicación en el que se pueden enviar y recibir datos de manera simultánea.

Gateway. Puerta de enlace o gateway es el dispositivo que permite interconectar redes de computadoras con protocolos y arquitecturas diferentes a todos los niveles de comunicación.

Gbps. Un Gigabit por segundo es una unidad que se usa para cuantificar un caudal de datos equivalente a 1024 Mbps.

Half-Duplex. La transmisión Half-Duplex es el canal de comunicación que permite alternar la trasmisión de dos direcciones, pero no en ambas direcciones simultáneamente.

Hardware. Todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

Host. Equipos conectados a una red, que proveen y utilizan servicios de ella.

IEEE. (The Institute of Electrical and Electronics Engineers). Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas.

IETF. (Internet Engineering Task Force). Grupo de Tareas de Ingeniería de Internet es una organización de técnicos que administran tareas de ingeniería de telecomunicaciones, principalmente de Internet.

IP. (Internet Protocol). Es un protocolo utilizado para la comunicación de datos a través de una red de paquetes combinados.

Jack. Conector hembra, frecuentemente relacionado con el conector RJ-45 en cableado estructurado.

Kernel. El kernel o núcleo de linux se puede definir como el corazón de este sistema operativo. Es el encargado de que el software y el hardware la computadora puedan trabajar en conjunto.

LAN. (Local Area Network). Redes de Área Local. Es un sistema de comunicación entre computadoras que permite compartir información, con la característica de que la distancia entre las computadoras debe ser pequeña.

LE-01. Laboratorio de Geomática.

LE-02. Laboratorio de Especialidades de Civil.

Led. Es un componente optoelectrónico pasivo y, más concretamente, un diodo que emite luz.

MAC. Identificador único del dispositivo o interfaz de red de una computadora. Se representa como una serie de 12 dígitos hexadecimales agrupados en pares.

Máscara de red. Combinación de bits que sirve para delimitar el ámbito de una red de computadoras. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

Mbps. Un megabit por segundo es una unidad que se usa para cuantificar un caudal de datos equivalente a 1024 kbps.

Modelo OSI. Es el modelo de red descriptivo, que fue creado en el año 1980 por la Organización Internacional de Normalización (ISO, International Organization for Standardization).

Modelo TCP/IP. Es un modelo para ser implementado en cualquier tipo de red. Facilita el intercambio de información independientemente de la tecnología y el tipo de subredes a atravesar, proporcionando una comunicación transparente a través de sistemas heterogéneos.

Nagios. Es un sistema de monitoreo de redes ampliamente utilizado, de código abierto, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado.

Nodo. Es todo aquel dispositivo conectado en una red (computadora, servidor, teléfono VoIP, impresora, etc.).

NSClient++. Es un cliente para monitoreo utilizado por Nagios.

Patch cord. Cable terminal utilizado para conectar un dispositivo electrónico con otro.

Patch Panel. Elemento encargado de recibir todos los cables del cableado estructurado. Sirve como organizador de las conexiones de la red y además ayuda a prevenir daños en las interfaces de los equipos de red activos que son provocados por el constante trabajo de retirar e introducir los conectores en sus puertos.

PDU. (Protocol Data Unit). Unidad de datos del protocolo. Se refiere a la información que es entregada como una unidad entre entidades de una red y que pueden contener información de control, información de direcciones o datos.

PHP. Es un lenguaje de programación de uso general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico.

Plugins. Son herramientas que extienden la funcionalidad de una aplicación.

Protoboard. Es una placa de pruebas con orificios conectados eléctricamente entre sí, habitualmente siguiendo patrones de líneas, en el cual se pueden insertar componentes electrónicos y cables para el armado y prototipado de circuitos electrónicos y sistemas similares.

Rack. Es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones.

RAM. Memoria que se utiliza como memoria de trabajo de computadoras para el sistema operativo, los programas y la mayor parte del software.

RFC. (Request For Comments). Significa solicitud de comentarios y consiste en un documento que puede ser escrito por cualquier persona y que contiene una propuesta para una nueva tecnología, información acerca del uso de tecnologías y/o recursos existentes, propuestas para mejoras de tecnologías, proyectos experimentales y demás.

RJ-45. Interfaz física comúnmente utilizada para conectar redes de computadoras con cableado estructurado (categorías 4, 5, 5e, 6 y 6a).

Router. Es un dispositivo de interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

Servidor. Son equipos que dentro de una red brindan uno o varios servicios a los dispositivos finales.

Software. Es todo programa o aplicación desarrollada para realizar tareas específicas.

STP. (Spanning Tree Protocol). Es un protocolo de red de nivel 2 del modelo OSI (capa de enlace de datos). Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes.

Switch. Es un dispositivo que sirve para conectar varios elementos dentro de una red. Estos pueden ser un una computadora, una impresora, teléfonos VoIP, o cualquier aparato que tenga una tarjeta Ethernet.

TIA. (Telecomunications Industries Association). Asociación de la Industria de las Telecomunicaciones. Es una organización que desarrolla los estándares que se relacionan con las tecnologías de telecomunicaciones.

TuneUp. Es un paquete de aplicaciones para optimizar, personalizar y corregir fallos del sistema operativo.

VLAN. (Virtual Local Area Network). Tecnología que segmenta las redes de forma virtual.

VoIP. Se refiere al método utilizado para transportar llamadas telefónicas sobre una red IP de datos, ya sea que se trate de Internet o una red interna.

WAN. (Wide Area Network). Redes de Amplia Cobertura. Son redes que cubren una amplia región geográfica, a menudo un país o un continente.

REFERENCIAS

Bibliografía

- **Redes Cisco. Guía de estudio para la certificación CCNA 640-802 2da Edición.**
  Tema de Redes de Datos.
  Autor: ARIGANELLO, ERNESTO.
  Editorial: Alfaomega Grupo Editor, México 2011.

- **Instalación y mantenimiento de redes para transmisión de datos.**
  Tema de implementación de cableado estructurado en las redes de datos.
  Autor: BERRAL MONTERO, ISIDORO.
  Editorial: Paraninfo, 2014.

- **Comunicaciones y Redes de Computadores 7ª Edición.**
  Tema de Redes de Datos y fundamentos teóricos.
  Autor: STALLINGS, WILLIAM.
  Editorial: Pearson Prentice Hall, 2004.

- **CISCO CCNA Exploration 4.0.**
  Programa de estudios CISCO CCNA Exploration.
  Autor: CISCO NETWORKING ACADEMY.

Referencias electrónicas (Última revisión: 22/02/2015)

- **Configuración TCP/IP. Sistema Operativo Windows 7.**
  Liga: http://windows.microsoft.com/es-mx/windows/change-tcp-ip-settings
  Consultado: Noviembre de 2014.

- **Definición de las siete capas del modelo OSI y explicación de las funciones.**
  Liga: https://support.microsoft.com/kb/103884/es
  Consultado: Febrero de 2015.

- **Red LAN inalámbrica.**
  Liga: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vlans.html#wp1032048
  Consultado: Marzo de 2015.

- **El cableado estructurado y sus estándares.**
  Liga: http://www.revista.unam.mx/vol.5/num5/art28/art28-1.htm
  Consultado: Enero de 2015.

- **Tipos de redes.**
  Autor: Laboratorio de redes y seguridad. Facultad de Ingeniería, UNAM.
  Liga: http://redyseguridad.fi-p.unam.mx/proyectos/Wi/redes/tipos/tipos.html
  Consultado: Febrero de 2015.

- **Nagios, sitio oficial.**
  Liga: http://www.nagios.org/
  Consultado: Diciembre de 2014.

- **Comunidad Nagios.**
  Liga: http://community.nagios.org/
  Consultado: Diciembre de 2014.

- **Instalación de Nagios, Linux.**
  Liga: http://agcapa.es/instalacion-de-nagios-en-linux/
  Consultado: Enero de 2015.

- **Normas sobre Cableado Estructurado.**
  Liga: http://unitel-tc.com/normas-sobre-cableado-estructurado/
  Consultado: Febrero de 2015

- **ANSI. American National Standards Institute.**
  Liga: http://www.ansi.org/
  Consultado: Marzo de 2015.

- **TIA. Advancing Global Communications.**
  Liga: http://www.tiaonline.org/
  Consultado: Marzo de 2015.

- **¿Qué es un Firewall? CERT-UNAM.**
  Autor: CERT UNAM
  Liga: http://www.seguridad.unam.mx/descarga.dsc?arch=422
  Consultado: Febrero de 2015.

- **Firewalls, controlando el acceso a la red.**
  Autor: CERT UNAM
  Liga: http://revista.seguridad.unam.mx/numero-04/firewalls-controlando-el-acceso-la-red
  Consultado: Marzo de 2015.

- **VLAN, Red de Área Local Virtual.**
  Autor: DGTIC, UNAM.
  Liga: http://www.enterate.unam.mx/Articulos/2004/noviembre/vlan.htm
  Consultado: Enero de 2015.

  Redes virtuales y configuraciones básicas.
  Liga:
  http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/VLANs.html
  Consultado: Enero de 2015.

- **NETGEAR. Equipos.**
  Liga: http://www.netgear.mx/
  Consultado: Febrero de 2015.

- **Pruebas de conectividad.**
  Liga: http://norfipc.com/redes/usar-comando-ping.html
  Consultado: Diciembre de 2014.

- **Administración de Redes.**
  Autor: Laboratorio de redes y seguridad. Facultad de Ingeniería, UNAM.
  Liga: http://redyseguridad.fi-p.unam.mx/proyectos/admonredes/PHP/capitulo1.html
  Consultado: Marzo de 2015.