IMPLEMENTACION DE UN CONTROLADOR DE DOMINIO BAJO WINDOWS SERVER Y UN ROUTERBOARD DE MIKROTIK EN LA RED DE COMPUTADORES DE SYSTEM PLUS DE LA CIUDAD DE TUQUERRES.

WILSON EDUARDO BENITEZ PAZ
RICHARD ALFREDO MOLINA ESTRADA

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2016

IMPLEMENTACION DE UN CONTROLADOR DE DOMINIO BAJO WINDOWS SERVER Y UN ROUTERBOARD DE MIKROTIK EN LA RED DE COMPUTADORES DE SYSTEM PLUS DE LA CIUDAD DE TUQUERRES.

WILSON EDUARDO BENITEZ PAZ
RICHARD ALFREDO MOLINA ESTRADA

Trabajo de grado presentado como requisito parcial para optar al título de Ingeniero de Sistemas

Asesor:
Ing. Edgar Dulce Villarreal

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2016

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones aportadas en este Trabajo de Grado son Responsabilidad de los autores.

Artículo 1 del Acuerdo No. 324 de octubre 11 de 1966, emanado por el Honorable Consejo Directivo de la Universidad de Nariño.

“La Universidad de Nariño no se hace responsable de las opiniones o resultados obtenidos en el presente trabajo y para su publicación priman las normas sobre el derecho de autor”.

Artículo 13, Acuerdo N. 005 de 2010 emanado del Honorable Consejo Académico.

Nota de Aceptación:

_____
_____
_____
_____
_____
_____
_____

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

San Juan de Pasto, Febrero de 2016.

AGRADECIMIENTOS

Gracias a Dios, por acompañarme y guiarme a lo largo de mi carrera, por ser mi fortaleza en los momentos de debilidad y por brindarme una vida llena de aprendizajes, experiencias y sobretodo felicidad.

A mis padres, Alfredo Molina porque siempre me ha brindado su fuerza y apoyo; a mi madre Dilia Estrada por sus enseñanzas y su amor.

A mi esposa, Cristina Dueñas, por su comprensión y apoyo y por ser parte importante de mi vida

A mis hijas, por entender que su padre estaba haciendo una tarea muy importante y que esa tarea les estaba robando a su papito por muchas horas. Gracias hijas mías

Al Ingeniero Manuel Bolaños, por su apoyo y compromiso en el desarrollo y culminación de este trabajo.

A todos los ingenieros que fueron mis docentes a lo largo de mi carrera y a los que lo fueron en esta última etapa.

Richard Alfredo Molina

.

AGRADECIMIENTOS

Gracias a la Virgencita de las Lajas, por iluminarme en mi carrera y durante el tiempo que estuve como egresado, como también en mi vida laboral y familiar.

A mi Padre German Benítez García, sus valores inculcados hacen que cada día busque ser una mejor persona y porque a pesar de todos mis errores cometidos nunca dejaste de creer en mí hasta el día en que lamentablemente partiste.

A mi Madre Mariana Paz, me diste la vida y me enseñaste a vivirla, y con tu ejemplo de temple, perseverancia y fortaleza para salir airosa de los diferentes obstáculos que hemos tenido has hecho de mí una persona de bien. No hay palabras para agradecerte todo lo que has hecho por mí, Mamá.

A mi hermana Mónica Benítez y su esposo Miller Portilla, por su apoyo incondicional y económico en los momentos que lo necesité.

A mis hermanas, Cristina y Janeth Benítez, por su empeño y constancia para decirme que puedo ser mejor, por su apoyo desmedido y su inmenso amor hacia mis hijas.

A mis hijas, Brenda y Avril, por ser la base principal de mi vida; su amor, apoyo, comprensión y compañía hicieron que retome nuevamente este objetivo. Las Amo infinitamente.

A mi esposa, Constanza Molina, por su insistencia en mejorar para brindarles una vida mejor a nuestras hijas.

A todos los Ingenieros que directa o indirectamente participaron enseñando, corrigiendo y teniendo paciencia; principalmente al Ingeniero Manuel Bolaños, por crear y brindar nuevas oportunidades a los estudiantes para lograr terminar la carrera como Ingenieros.

A mi cuñado Richard Molina, porque a pesar de haber iniciado con proyectos diferentes, compartió conmigo la realización y culminación del trabajo de grado para lograr juntos un mismo objetivo.

Wilson Eduardo Benítez Paz

RESUMEN

Una Red es un organizado sistema de comunicaciones, permite comunicarse con otros usuarios y compartir archivos y periféricos para realizar un trabajo específico. Es decir es un sistema de comunicaciones que conecta varios dispositivos, tales como los computadores y que intercambian información. Conexiones que pueden ser a través de cableado, como también mediante el uso de láser, microondas y satélites de comunicación.

Siendo uno de los objetivos básicos el compartir recursos, haciendo que todos los programas, datos y equipos estén disponibles para cualquier momento en el que sean solicitados para realizar una tarea específica, sin tener en cuenta la ubicación del usuario y el recurso. Logrando realizar una determinada en menos tiempo.

La administración de redes es un conjunto de técnicas que buscan mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.

Por medio de Windows Server y herramientas como el RouterBoard, con su sistema operativo incluido RouterOS permitirán realizar dichas tareas, y así System Plus de Túquerres, podrá estar a la vanguardia en los últimos desarrollos tecnológicos en este aspecto.

Con la aplicación del trabajo, se logrará mejorar la administración de la red y los recursos informáticos en System Plus de Túquerres.

ABSTRACT

A network is an organized system of communications, allows us to communicate with other users and share files and peripherals to perform a specific job. I.e. it is a communication system that connects various devices, such as computers and allowing them to exchange information. Connections that may be through wiring, and also through the use of laser, microwave and satellite communication.

Being one of the main objectives to share resources, by making all programs, data and equipment available for any time which are requested to perform a specific task, regardless of the location of the user and the resource.

Network management is a set of techniques that seek to maintain a network operational, efficient, secure, constantly monitored and with planning suitable and properly documented.

Through Windows Server and tools as the RouterBoard, with its included operating system RouterOS will enable us to perform these tasks, and thus System Plus de Túquerres, you can be at the forefront in the latest technological developments in this regard.

With the implementation of the project, will be achieved to improve the administration of the network and computing resources in System Plus de Túquerres.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

- **Actualizar.** Sustituir el software o firmware existente con una versión más moderna.
- **Adaptador**. Dispositivo que añada funcionalidad de red a su equipo.
- **Ad-hoc.** Grupo de dispositivos inalámbricos que se comunican directamente entre ellos (punto a punto) sin la utilización de un punto de acceso.
- **Ancho de banda.** Capacidad de transmisión de un dispositivo o red determinado
- **Banda ancha**. Conexión a Internet de alta velocidad y siempre activa.
- **Base de datos**. Recopilación de datos que puede organizarse de forma que pueda sus contenidos puedan accederse, gestionarse y actualizarse fácilmente.
- **Bit (dígito binario)**. La unidad más pequeña de información de una máquina.
- **Byte**. Una unidad de datos que suele ser de ocho bits.
- **Cargar**. Transmitir un archivo a través de una red.
- **Conmutador**. Dispositivo que es el punto central de conexión de equipos y otros dispositivos de una red, de forma que los datos puedan transmitirse a velocidad de transmisión completa.
- **DNS (sistema dinámico de nombres de dominio)**. Permite albergar un sitio Web, servidor FTP o servidor de correo electrónico con un nombre de dominio fijo (por ejemplo, www.xyz.com) y una dirección IP dinámica.
- **Descargar**. Recibir un archivo transmitido a través de una red.

- **DHCP (protocolo de configuración dinámica de host)**. Protocolo que permite a un dispositivo de una red, conocido como servidor DHCP, asignar direcciones IP temporales a otros dispositivos de red, normalmente equipos.

- **Dirección IP**. Dirección que se utiliza para identificar un equipo o dispositivo en una red.

- **Dirección IP dinámica**. Dirección IP temporal que asigna un servidor DHCP.

- **Dirección IP estática**. Dirección fija asignada a un equipo o dispositivo conectado a una red.

- **DNS (Servidor de nombres de dominio)**. La dirección IP de su servidor ISP, que traduce los nombres de los sitios Web a direcciones IP.

- **DSL (Línea de suscriptor digital).** Conexión de banda ancha permanente a través de las líneas de teléfono tradicionales.

- **Enrutador**. Dispositivo de red que conecta redes múltiples, tales como una red local e Internet.

- **Ethernet**. Protocolo de red estándar de IEEE que específica la forma en que se colocan los datos y se recuperan de un medio de transmisión común.

- **Fibra óptica.** Medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

- **Firewall**. Elemento utilizado en redes de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas.

- **Firmware**. El código de la programación que ejecuta un dispositivo de red. Fragmentación Dividir un paquete en unidades menores al transmitirlas a través de un medio de red que no puede admitir el tamaño original del paquete.

- **FTP (Protocolo de transferencia de archivos).** Protocolo estándar de envío de archivos entre equipos a través de redes TCP/IP e Internet.

- **Gateway.** Equipo para interconectar redes.

- **Ghz**. Equivale a 109 hercios (1 millón). Se utiliza muy frecuentemente como unidad de medida de la frecuencia de trabajo de un dispositivo de hardware.

- **GPO**. **Group policy objects.** herramienta fundamental que nos da Microsoft para administrar la infraestructura de nuestro dominio. Básicamente las políticas dan el control de los equipos de la red, pudiendo establecer configuraciones para los distintos componentes de sistema operativo, para poder lograrlo se va a necesitar un Windows Server que tenga el servicio o rol de active directory, y se podrá aplicar la configuración a sitios, dominios, unidades organizativas. También se debe tener en claro que las políticas pueden aplicarse a equipos y usuarios.

- **Hardware**. El aspecto físico de equipos, telecomunicaciones y otros dispositivos de tecnologías de la información.

- **HTTP (protocolo de transferencia de hipertexto)**. Protocolo de comunicaciones utilizado para conectarse a servidores de la World Wide Web.

- **Hz (Hercio).** El hertz o hertzio (también se le puede llamar Hercio) es la unidad de frecuencia del Sistema Internacional de Unidades. Existe la división de este término en submúltiplos y múltiplos documentados en un Sistema Internacional de Unidades.

- **Infraestructura.** Equipo de red e informático actualmente instalado.

- **Inicio**. Iniciar un dispositivo y provocar que comience a ejecutar instrucciones.

- **IPCONFIG (Internet Protocol Configuration)**. Utilidad de los sistemas operativos Windows que muestra la dirección IP de un dispositivo de red concreto.

- **IPSec (Internet Protocol Security).** Protocolo VPN utilizado para implementar el intercambio seguro de paquetes en la capa IP.

- **Itinerancia**. Capacidad de transportar un dispositivo inalámbrico desde el alcance de un punto de acceso hasta otro sin perder la conexión.

- **Malware**. Software que tiene como objetivo infiltrarse en el sistema y dañar la computadora sin el conocimiento de su dueño.

- **Máscara de subred.** Código de dirección que determina el tamaño de la red.

- **Mbps (megabits por segundo).** Un millón de bits por segundo, unidad de medida de transmisión de datos.
- **Mhz**. Equivale a 106 hercios (1 millón). Se utiliza muy frecuentemente como unidad de medida de la frecuencia de trabajo de un dispositivo de hardware.

- **Módem de cable**. Un dispositivo que conecta una equipo a la red de la televisión por cable que a su vez se conecta a Internet.

- **Modo infraestructura.** Configuración en la que se realiza un puente entre una red inalámbrica y una red con cable a través de un punto de acceso.

- **Navegador**. Programa de aplicación que proporciona una forma de consultar e interactuar con la información de la World Wide Web.

- **Niveles de Servicio (SLA: service level agreement).** Contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad del servicio.

- **Nodo**. Unión de red o punto de conexión, habitualmente un equipo o estación de trabajo.

- **Paquete**. Un paquete es un pequeño bloque de datos transmitido en una red de conmutación de paquetes.

- **Phishing**. Tipo de delito encuadrado dentro del ámbito de las estafas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial.

- **PHP**. Lenguaje de programación interpretado, diseñado originalmente para la creación de páginas web dinámicas.

- **Ping (buscador de paquetes de internet)**. Utilidad de Internet que se utiliza para determinar si una dirección IP determinada está en línea.

- **Pirata informático**. Un término de jerga para un entusiasta informático. También hace referencia a los individuos que obtienen acceso no autorizado a sistemas informáticos con el fin de robar y corromper datos.

- **Piso falso antiestático** .Consiste en placas colocadas sobre pedestales apoyados en el firme o losa de concreto, a una altura que permita el ocultamiento de cables así como la alimentación de aire acondicionado a través del mismo.

- **PoE (alimentación a través de ethernet).** Tecnología que permite a un cable de red Ethernet transmitir tanto datos como corriente.

- **PPPoE (protocolo a través de ethernet punto a punto)**. Tipo de conexión de banda ancha que proporciona autenticación (usuario y contraseña) además de transporte de datos.

- **PPTP (protocolo de túnel punto a punto)**. Protocolo VPN que permite tunelar el protocolo Punto a punto (PPP) a través de una red IP. Este protocolo se utiliza también como tipo de conexión de banda ancha en Europa.

- **Puente**. Dispositivo que conecta dos tipos diferentes de redes locales, como por ejemplo una red inalámbrica a una red Ethernet con cable.

- **Puerta de enlace**. Un dispositivo que interconecta redes con protocolos de comunicaciones diferentes e incompatibles.

- **Puerta de enlace predeterminada.** Dispositivo que redirecciona tráfico de Internet desde su red de área local.

- **Puerto.** Punto de conexión en un equipo o dispositivo de red utilizado para conectar un cable o adaptador.

- **Punto de acceso.** Dispositivo que permite a los equipos y a otros dispositivos equipados con función inalámbrica comunicarse con una red con cable. También se utiliza para ampliar el alcance de una red inalámbrica.

- **Red**. Serie de equipos o dispositivos conectados con el fin de compartir datos, almacenamiento y la transmisión entre usuarios.

- **Red punto a punto**. Aquellas que responden a un tipo de arquitectura de red en las que cada canal de datos se usa para comunicar únicamente dos nodos.

- **Red punto a multipunto**. Aquellas en las que cada canal de datos se puede usar para comunicarse con diversos nodos.

- **Red troncal**. Parte de una red que conecta la mayoría de los sistemas y los une en red, así como controla la mayoría de datos.

- **Rendimiento**. Cantidad de datos que se han movido correctamente de un nodo a otro en un periodo de tiempo determinado.

- **Router**. Enrutador, es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Este dispositivo permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

- **RouterOS**. Es un sistema operativo de la empresa Mikrotik diseñado especialmente para el manejo de redes de computadores. Es un software propietario.

- **Routing**. El proceso de mover un paquete de datos de fuente a destino, normalmente se usa un “Router”.

- **Servidor**. Cualquier equipo cuya función en una red sea proporcionar acceso al usuario a archivos, impresión, comunicaciones y otros servicios.
.
- **Servidor de seguridad**. Un servidor de seguridad es cualquiera de los esquemas de seguridad que evitan a los usuarios no autorizados obtener acceso a una red de equipos o que supervisa la transferencia de información hacia y desde la red.

- **Servidor de seguridad SPI (Inspección de paquetes de datos)** Una tecnología que inspecciona los paquetes de información entrantes antes de permitirles que entren en la red.

- **Single Sign On.** Procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación.

- **Spam.** Se llama Spam, correo basura o SMS basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.

- **Spyware**. Software que se instala en una computadora para recopilar información sobre las actividades realizadas en ella.

- **SMTP (Simple mail transfer protocol)**. Protocolo de correo electrónico estándar de Internet.

- **SNMP (Simple network management protocol)**. Protocolo de control y supervisión de redes ampliamente extendido.

- **Software**. Instrucciones para el equipo. Se denomina programa al conjunto de instrucciones que realizan una tarea determinada.

- **SSID (service set identifier).** Nombre de su red inalámbrica.

- **Tasa TX**. Tasa de transferencia.

- **TCP (transport control protocol)**. Un protocolo de red para la transmisión de datos que requiere la confirmación del destinatario de los datos enviados.

- **TCP/IP (transport control protocol / internet protocol).** Protocolo de red para la transmisión de datos que requiere la confirmación del destinatario de los datos enviados.

- **Telnet**. Comando de usuario y protocolo TCP/IP que se utiliza para acceder a equipos remotos.

- **TFTP (trivial file transfer protocol)**. Versión del protocolo FTP TCP/IP que utiliza UDP y no dispone de capacidades de directorio ni de contraseña.

- **TKIP (temporal key integrity protocol)**. Protocolo de cifrado inalámbrico que cambia periódicamente la clave de cifrado, haciendo más difícil su decodificación.

- **TLS (transport layer security).** Protocolo que garantiza la privacidad y la integridad de los datos entre aplicaciones cliente/servidor que se comunican a través de Internet.

- **Topología.** Distribución física de una red.

- **UDP (user datagram protocol).** Protocolo de red para la transmisión de datos que no requieren la confirmación del destinatario de los datos enviados.

- **URL (user resource locator).** Dirección de un archivo situado en Internet.

- **VPN (red privada virtual).** Medida de seguridad para proteger los datos a medida que abandona una red y pasa otra a través de Internet.

- **WAN (wide area network).** Grupo de equipos conectados en red en un área geográfica extensa. El mejor ejemplo de WAN es Internet.

- **WEP (wired equivalent privacy).** Protocolo de seguridad para redes inalámbricas. El objetivo de WEP es proporcionar seguridad mediante el cifrado de datos a través de ondas de radio, de forma que estén protegidos a medida que se transmiten de un punto a otro. Para permitir la comunicación entre los equipos y el enrutador se utiliza una clave compartida (similar a una contraseña). WEP ofrece un nivel básico (pero satisfactorio) de seguridad para la transferencia de datos a través de redes inalámbricas.

- **Windows server**. es un software propietario de la empresa estadounidense microsoft para la administración de redes de computadores. Sucesor de

Windows NT. La versión que se usa para el proyecto es 2012. La última versión hasta el momento de la publicación de este proyecto es 2016.

- **Wireless.** Tipo de comunicación en la que no se utiliza un medio de propagación físico alguno esto quiere decir que se utiliza la modulación de ondas electromagnéticas.

- **WLAN (wireless local area network).** Grupo de equipos y dispositivos asociados que se comunican entre sí de forma inalámbrica.

- **WPA (wifi protected access).** Protocolo de seguridad para redes inalámbricas que se fundamenta en los cimientos básicos de WEP. Asegura la transferencia de datos de forma inalámbrica mediante la utilización de una clave similar a WEP. La robustez añadida de WPA es que la clave cambia de forma dinámica. La clave, en continuo cambio, dificulta que un pirata informático pueda conocer la clave y obtener acceso a la red.

- **WPA2 (wifi protected access 2).** Es la segunda generación de WPA y proporciona un mecanismo de cifrado más fuerte a través del Estándar de cifrado avanzado (AES), requisito para algunos usuarios del gobierno.

- **WPA-enterprise**. Versión de WPA que utiliza las mismas claves dinámicas que WPA-Personal y también requiere que todo dispositivo inalámbrico esté autorizado según lista maestra, albergada en un servidor de autenticación especial.

- **WPA-personal**. Versión de WPA que utiliza claves de cifrado en constante cambio y de mayor longitud para complicar el proceso de su decodificación.

INTRODUCCIÓN

Las redes de computadores actuales son una combinación de dispositivos, técnicas y sistemas de comunicación que han ido apareciendo desde finales del siglo XIX o, lo que es lo mismo, desde la invención del teléfono.

El teléfono se desarrolló exclusivamente para transmitir voz, hoy se utiliza, en muchos casos, para conectar ordenadores entre sí. Desde entonces han aparecido las redes locales, las conexiones de datos a larga distancia con enlaces transoceánicos o satélites, la telefonía móvil, etc. Mención especial merece la red Internet dentro de este mundo de las comunicaciones a distancia. Nadie duda de que hoy en día constituya una red básica de comunicación entre los humanos.

Con el avance tecnológico, nuevos sistemas operativos se han ido especializando en la administración de redes de computadores. Es así, como el tradicional Windows Server, ahora en su versión 2012, brinda un sinnúmero de herramientas para optimizar una red.

Merece atención también el sistema operativo RouterOS, acompañado de su hardware diseñados por Mikrotik para robustecer la red y al mismo tiempo simplificar su administración.

Con el presente trabajo se trata de dar a conocer algunos conceptos de redes, de los sistemas operativos antes mencionados para luego implementar un controlador de dominio, el cual a su vez se conecta a un RouterBoard de Mikrotik para hacer un mejor control en la red de System Plus de Túquerres, empresa tuquerreña que ya cumple 17 años impartiendo educación de calidad en el municipio y regiones aledañas.

TEMA

Título:

“IMPLEMENTACION DE UN CONTROLADOR DE DOMINIO BAJO WINDOWS SERVER Y UN ROUTERBOARD DE MIKROTIK EN LA RED DE COMPUTADORES DE SYSTEM PLUS DE LA CIUDAD DE TUQUERRES”.

Modalidad:

La modalidad para el presente trabajo de grado es Otros trabajos de Grado.

Línea de investigación:

La línea de investigación a seguir en este proyecto es OPTIMIZACIÓN DE SISTEMAS.

Alcance y delimitación:

El RouterBoard y el controlador de dominio se implementarán en la red de computadores de System Plus de Túquerres. Se tratará de brindar el servicio de Internet a los clientes a través de un RouterBoard para la parte inalámbrica a través de HotSpot y de un Servidor Windows Server 2012 para la red cableada. Para este proyecto, de aquí en adelante se hará referencia a este Servidor con el nombre de Orión. En el servidor Orión controlará el dominio systemplusdetuqueres.com. El Servidor se conectará directamente al RouterBoard.

En cuanto a la metodología escogida, en la fase 4: "Pruebas, Optimización y Documentación de la red", únicamente se realizará la optimización puesto que se trata de una monografía.

DESCRIPCIÓN DEL PROBLEMA

Planteamiento:

Reseña histórica: System Plus, empezó como una idea a finales de los ochenta, creando una cartilla como guía para la enseñanza de la computación. Muy pronto esa cartilla se convirtió en libros de diferentes temáticas, y en la actualidad son más de 100 ejemplares. La metodología utilizada se basa en el manejo de un libro, profesor y computador. Las empresas editoriales de la marca System Plus, se han puesto de acuerdo en programas, metodología y material didáctico.

En Nariño, se estableció en la ciudad de Pasto en el año de 1994, en el puerto marítimo de Tumaco en 1997 y en Túquerres en 1998, aproximadamente a una hora y cuarto de la capital. Durante este tiempo se ha trabajado arduamente formando a las personas como técnicos laborales en diferentes modalidades los cuales han aportado al desarrollo social y económico de esta ciudad y cerca de 10 poblaciones vecinas de la ex provincia de Túquerres y sus afluencias.

En cuanto a los valores misionales y de visión se presenta lo siguiente:

Misión: System Plus es una Institución Educativa, organizada como red nacional, que contribuye al desarrollo socio económico de las regiones donde se encuentra, capacitando a sus clientes para dar respuesta a las exigencias del mercado laboral, empresarial y social, en las áreas Gerencia, Comercial, Administrativa, talento humano y TIC, con actualización permanente, calidad y valores

humanistas, buscando el continuo progreso institucional y una retribución justa para sus accionistas, colaboradores y la sociedad en general.

Visión: ser para el 2020 una empresa líder, reconocida y competitiva, posicionada a nivel nacional, y con influencia internacional, con alto nivel de calidad en su talento humano, procesos y servicios, apoyado en las TIC, aportando al medio social, laboral y empresarial, personas con formación integral fundamentada en el sistema de competencias.

Políticas de calidad:

- System Plus es una institución de educación técnica en las áreas de una mipyme (gerencia, administración, mercadeo y TI) constituida desde hace 17 años, cuyo principal objetivo es la búsqueda del desarrollo y progreso del ser humano.

- Los estudiantes de SYSTEM PLUS tienen a su servicio una sede dotada con el recurso humano y técnico que garantiza su educación, como salas demostrativas y salas de informática con conexión permanente a Internet.

- Cuenta con un equipo que tiene interés genuino en cada estudiante, para guiarlo en la dirección correcta en cada uno de los desafíos que impone la nueva tecnología, acordes con los requisitos de la norma Colombiana Icontec 5555 de 2007 y mediante la mejora contínua de los procesos de la Institución.

Objetivos de System Plus:

- Desarrollar estrategias pedagógicas para la formación de técnicos laborales en las áreas de las mipymes, gerencia, administración, sistemas y mercadeo, con forme a las exigencias legales por ocupaciones.

- Elaborar planes de acción para la articulación de norma técnica Colombiana 5555 de ICONTEC, y establecer procesos de mejoramiento continuo de la calidad.

- Establecer convenios con el sector productivo para la realización de prácticas, y así estimular y promover la incorporación laboral de los estudiantes.

- Incrementar la satisfacción de los estudiantes, docentes, personal administrativo y socios de System Plus de Túquerres.

System Plus cuenta con una sala de informática, tres aulas de teoría, un aula para Mantenimiento y Redes, una oficina para Administración y un Área de

Sistemas con un Servidor Proxy, Modem de Movistar y un AccessPoint. En la sala de informática hay 14 computadores conectados a un Switch.

En cada aula de teoría hay un computador y un TV para el docente y en el área administrativa hay dos computadores, para la Secretaria y el Director.

Todos estos equipos se encuentran conectados a la red y acceden a Internet a través del servidor Proxy.

El servicio de Internet lo brinda Movistar con una velocidad de transmisión de 5Mbps. A la red inalámbrica se accede a través de un AccessPoint que se encuentra conectado directamente al módem de Movistar.

Se anexa el respectivo plano para mayor entendimiento de la situación actual de la red. Véase figura 1.

Figura 1. Plano de System Plus de Túquerres

Los computadores del aula de informática se encuentran conectados al Servidor Proxy. Desde allí se puede controlar el acceso a Internet de los alumnos pero no se puede proteger los equipos para que los estudiantes no instalen software.

La red inalámbrica tampoco se encuentra protegida, pues la persona que disponga de la clave de la red simplemente accede a ella sin ningún control, incluso estando fuera de las instalaciones. No se tiene control de las aplicaciones que ejecutan los alumnos ni mucho menos del ancho de banda al que cada estudiante tiene acceso.

Formulación del problema:

¿Cómo la implementación de un RouterBoard y un Controlador de Dominio en la red de computadores de System Plus de Túquerres, ayudarán a optimizar el tráfico y la seguridad de los datos que por dicha red circulan?

Sistematización del problema:

- ¿Se ha elaborado un diagnóstico de la situación actual de la red de System Plus?
- ¿Hay un nuevo diseño para el mejoramiento de la red de System Plus de Túquerres?
- ¿Se ha elaborado un plano del nuevo diseño para la red de System Plus de Túquerres?
- ¿Hay control sobre los usuarios que usan la red inalámbrica de System Plus de Túquerres?
- ¿System Plus cuenta con un dominio en la nube?
- Hay cuentas de usuario en un servidor para los estudiantes de System Plus de Túquerres?
- Existen en la red Servidores de DHCP y DNS?
- Hay restricciones para el ingreso de los usuarios a los equipos de la red de System Plus de Túquerres?

OBJETIVOS

Objetivo general

Optimizar el tráfico y brindar seguridad a los datos a través de la implementación de un RouterBoard y un Controlador de Dominio en la red informática de System Plus de Túquerres.

Objetivos específicos

- Elaborar un diagnóstico de la situación actual de la red de System Plus de Túquerres en cuanto a su infraestructura física.
- Diseñar una nueva red para System Plus de Túquerres implementando hardware y software de última tecnología para la administración de dicha red.
- Elaborar un plano de la nueva arquitectura de red para System Plus.
- Implementar un RouterBoard en la red System Plus de Túquerres para gestionar los usuarios que se conectan a la red inalámbrica.
- Adquirir un dominio para controlarlo desde un Servidor con Windows Server 2012.
- Crear cuentas de usuario para los estudiantes de System Plus de Túquerres
- Configurar un servidor DHCP y un servidor DNS en Windows Server para la red LAN.
- Configurar políticas de seguridad en el Servidor Orión para los equipos de la red de System Plus de Túquerres.

JUSTIFICACIÓN

El papel de las Instituciones Educativas o Centros de Formación, en un sentido genérico se han creado para educar, es decir, para adelantar el proceso de capacitación del individuo para actuar conscientemente frente a nuevas situaciones de la vida, aprovechando la experiencia anterior y teniendo en cuenta la integración, la continuidad y el progreso social. Todo ello de acuerdo con la realidad de cada uno, de modo que sean atendidas las necesidades individuales y colectivas.

Las Instituciones Educativas preparan las nuevas generaciones para recibir, conservar y enriquecer la herencia cultural de la humanidad, así mismo prepara

los procesos de subsistencia y organización de los grupos humanos, teniendo en cuenta las nuevas exigencias sociales, derivadas del crecimiento demográfico, el surgimiento de las TIC y de los nuevos conocimientos. También promueven el desenvolvimiento económico y social, disminuyendo los privilegios y proporcionando los beneficios de la civilización al mayor número posible de individuos.

En System Plus se pretende dar a conocer a sus estudiantes nuevas tecnologías, avances en las áreas de Informática, Redes de Computadores, Mantenimiento, Sistemas Operativos, Contabilidad, Técnicas de Oficina; usando siempre hardware y software de última tecnología. Lo anterior, entonces hace pensar que si se usa siempre nuevas tecnologías para la enseñanza por qué no entonces usarlas en la infraestructura de la institución, es decir, hacer que System Plus se convierta en un modelo en el aplicación de esas herramientas.

METODOLOGÍA

La metodología que se va a usar es **TOP-DOWN NETWORK DESIGN.** Es una disciplina que creció del éxito de la programación de software estructurado y el análisis de sistemas estructurados[1].

El objetivo principal del análisis de sistemas estructurado es representar más exacto las necesidades de los usuarios que a menudo son lamentablemente ignoradas.

Otro objetivo, es hacer el proyecto manejable dividiéndolo en módulos que pueden ser más fáciles de mantener y cambiar. El diseño de red top-down es una metodología para diseñar redes que comienza en las capas superiores del modelo de referencia de OSI antes de mover a las capas inferiores. Esto se concentra en aplicaciones, sesiones, y transporte de datos antes de la selección de routers, switches, y medios que funcionan en las capas inferiores.

Se ha escogido esta metodología por la adaptabilidad a los cambios durante el proceso de desarrollo del proyecto y porque es recomendada para el desarrollo de proyectos a corto plazo.

Es una metodología que propone cuatro Fases, para el diseño de redes

- Fase1: Análisis de Negocios Objetivos y limitaciones
- Fase2: Diseño Lógico
- Fase3: Diseño Físico

[1] http://www.buenastareas.com/materias/proyecto-de-redise%C3%B1o-de-red-utilizando-la-metodologia-top-down/0

- Fase4: Pruebas, Optimización y Documentación de la red

1. RESULTADOS ESPERADOS

Con la elaboración de este proyecto se pretende hacer un control de los usuarios que usan la red tanto inalámbrica como cableada. Los usuarios que usarán la red deben estar previamente registrados en el servidor Orión o en el RouterBoard dependiendo de si el servicio se presta alámbrica o inalámbricamente.

Se pretende además asignar un ancho de banda a los usuarios para que se optimice el servicio de internet en la red de System Plus de Túquerres.

Se espera que el dominio www.systemplusdetuquerres.com.co se administre desde el servidor Orión.

Además, se entregará un documento final sobre el trabajo realizado.

2. RECURSOS

2.1 RECURSOS HUMANOS

• Diseñador de la red	Estudiantes a cargo del proyecto
• Encargado de pruebas (tester)	Coordinador académico de System Plus
• Clientes	Secretaria, coordinadora académico y representante legal de System Plus de Túquerres
• Asesor del proyecto	Docente de la Universidad de Nariño, Ing. Edgar Dulce

2.2 RECURSOS TECNOLÓGICOS

Entre los recursos tecnológicos, se tiene:

- Un computador con procesador AMD dual core a 2.2 GHz, 2GB de memoria RAM, disco duro de 120GB que se usará como servidor con Sistema operativo Windows Server 2012. Este computador será un servidor no dedicado.
- Un RouterBoard de Mikrotik Ref. hAP lite RB941 2nD
- Un AccessPoint de marca TP-LINK Ref. TL MR3220
- Un Switch de 24 puertos
- Todos los equipos se encuentran conectados a una red y ésta a internet con una velocidad de transmisión de 5Mbps

2.3 RECURSOS MATERIALES

CANTIDAD	DETALLE	VALOR
2	Cartuchos de tinta parta impresora HP negra	$ 110.000
2	Cartuchos de tinta para impresora HP de color	$ 130.000
1	RouterBoard de Mikrotik	$ 130.000
1	Memoria Flash USB de 8GB	$ 25.000
1	Caja de lapiceros	$ 8.500
1	Caja de lápices	$ 7.800
	Total	**$ 411.300**

2.4 RECURSOS FINANCIEROS

El costo de los recursos materiales fue asumido en su totalidad por los estudiantes encargados del proyecto.

System Plus de Túquerres por su parte se compromete a vincular laboralmente y de tiempo completo a los estudiantes cancelándoles un salario mínimo mensual vigente y las prestaciones sociales a que se dé lugar por un periodo de tres (3) meses a partir de la aprobación del trabajo.

3. MARCO TEÓRICO

3.1 MARCO REFERENCIAL

System Plus de Túquerres es una institución para el trabajo y el desarrollo humano que brinda educación de calidad a la población tuquerreña y municipios circunvecinos, aprobada mediante resolución de funcionamiento 3614 del 3 de noviembre de 2009 y Registro de programas mediante resolución 0606 de 28 de febrero de 2011. En Túquerres cumple ya 17 años y en Nariño 20 años.

En Túquerres se ubica en la Cra. 12 No. 18 - 13 Segundo piso. Actualmente cuenta con un Director, Coordinadora académica, Secretario, Asesora comercial y 6 profesores.

3.2 MARCO CONCEPTUAL

Computador[2]**.** Una computadora o un computador, (del latín computare -calcular), también denominada ordenador (del francés ordinateur, y éste del latín ordinator), es una máquina electrónica que recibe y procesa datos para convertirlos en información útil.

Red informática. Una red es un sistema donde los elementos que lo componen (por lo general ordenadores) son autónomos y están conectados entre sí por medios físicos y/o lógicos y que pueden comunicarse para compartir recursos. Independientemente a esto, definir el concepto de red implica diferenciar entre el concepto de red física y red de comunicación.

Información. En sentido general, la información es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Internet. Internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las

[2] http://zonasoftwareyhardware.blogspot.com.co/2011/05/computadora.html
http://www.monografias.com/trabajos40/redes-informaticas/redes-informaticas.shtml

redes físicas heterogéneas[3] que la componen funcionen como una red lógica única, de alcance mundial.

www. Es un conjunto de servicios basados en hipermedios, ofrecidos en todo el mundo a través de Internet, se lo llama WWW (World Wide Web - Telaraña de Cobertura Mundial).

Modem. Un módem es un dispositivo que sirve para enviar una señal llamada moduladora mediante otra señal llamada portadora.

Switch. Los switches son dispositivos que filtran y encaminan paquetes de datos entre segmentos (sub-redes) de redes locales. Operan en la capa de enlace del modelo OSI, debiendo ser independientes de los protocolos de capa superior.

Rack. Un rack es un bastidor destinado a alojar equipamiento electrónico, informático y de comunicaciones.

Patch panel. Los Patch Panel son paneles electrónicos utilizados en algún punto de una red informática o sistema de comunicaciones analógico o digital en donde todos los cables de red terminan.

Conector RJ45. Es una interfaz física muy utilizada para conectar redes de cableado estructurado, es utilizada como un estándar para definir las conexiones eléctricas. Una aplicación común es su uso en cables de red Ethernet donde usan cuatro pares o en terminaciones de teléfonos.

WLAN. Acrónimo de Wireless Local Área Network (Red inalámbrica de área local). WLAN es un sistema de comunicación de datos inalámbrico utilizado como alternativa a las redes LAN cableadas o como extensión de éstas.

LAN. Una red de área local, red local o LAN (del inglés local área Network) es la interconexión de varias computadoras y periféricos. Su extensión está limitada

[3] https://es.wikipedia.org/wiki/Informaci%C3%B3n
http://avata.utadeo.edu.co/portal/index.php?option=com_content&view=article&id=66:que-es-internet
http://www.matpec.com.ar/desde0/desde0-www.htm

físicamente a un edificio o a un entorno de 200 metros, con repetidores podría llegar a la distancia de un campo de 1 kilómetro.

Protocolo TCP/IP. [4]El TCP/IP es un protocolo que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local y área extensa.

Topología. La topología de red se define como la cadena de comunicación usada por los nodos que conforman una red para comunicarse[5].

3.3 MARCO CIENTÍFICO

3.3.1 Introducción a redes. Cada uno de los tres siglos pasados ha estado dominado por una sola tecnología. El siglo XVIII fue la etapa de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la época de la máquina de vapor. Durante el siglo XX, la tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, la instalación de redes telefónicas en todo el mundo, la invención de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de los computadores, así como a la puesta en órbita de los satélites de comunicación. A medida que crecen las habilidades para recolectar procesar y distribuir información, la demanda de más sofisticados procesamientos de información crece todavía con mayor rapidez.

La industria de ordenadores ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener un solo computador para satisfacer todas las necesidades de cálculo de una organización, se está reemplazando con rapidez por otro que considera un número grande de computadores separados, pero interconectados, que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de redes de computadores.

A lo largo de la historia los ordenadores han ayudado a realizar diversos tipos de aplicaciones, el hombre no satisfecho con esto, buscó más progreso, logrando implantar las Redes de Computadoras, hoy en día la llamada Internet, siendo esta la dueña de las Redes, en todo el mundo un ordenador se comunica, comparte

[4] https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local_inal%C3%A1mbrica
http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml
https://sanjuanboscoedu.files.wordpress.com/2011/03/topologia-de-redes1.pdf
[5] http://ti-prosoft.com/Docslink/Analisisred.pdf

datos, realiza transacciones en segundos y todo esto gracias a la existencia de las mismas.[6]

3.3.2 Concepto redes de computadores. Una red es una serie de ordenadores y otros dispositivos conectados por cables entre sí. Esta conexión les permite comunicarse entre ellos y compartir información y recursos. Las redes varían en tamaño; pueden reducirse a una oficina o extenderse globalmente. Una red conectada en un área limitada se conoce como Red de área local (LAN). Una LAN está contenida a menudo en una sola ubicación. Una Red de área extensa (WAN) es un grupo de dispositivos, o varias LAN, conectados en una área geográficamente mayor, a menudo por medio de líneas telefónicas u otro formato de cableado como puede ser una línea dedicada de alta velocidad, fibra o enlace vía satélite. Una de los mayores ejemplos de WAN es la propia Internet. Para comprender mejor véase la figura 2.

Figura 2. Redes de computadoras
Fuente: http://rockalaglam.galeon.com/

Es un conjunto de ordenadores conectados entre sí, permitiendo a la vez la comunicación y optimización de recursos.

3.3.3 Dispositivos de red. Los equipos que se conectan de forma directa a un segmento de red se denominan dispositivos. Estos dispositivos se clasifican en dos grupos:

[6] http://www.monografias.com/trabajos/introredes/introredes.shtml

3.3.3.1 Dispositivos de usuario final. Son aquellos dispositivos que conectan a los usuarios con la red también se conocen con el nombre de host (estación de trabajo). Los dispositivos de usuario final incluyen los computadores, impresoras, escáneres y demás dispositivos que brindan servicios directamente al usuario.

A. Dispositivos de Red. También conocidos como Elementos Activos, son dispositivos que se encargan de transportar los datos que deben transferirse entre dispositivos de usuarios final. Los dispositivos de red son todos aquellos que se conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación[7].

- **Switch**

Existen en el mercado una gran variedad de tipos de concentradores, desde los que sólo hacen funciones de concentración del cableado hasta los que disponen de mayor número de capacidades, como aislamiento de tramos de red, gestión remota, etc. Uno de sus ejemplares se puede observar en la **(Figura 3)**. La tendencia del mercado es la de ir incorporando cada vez más funciones dentro de los concentradores. No solo son capaces de determinar si los datos deben permanecer o no en la LAN, sino que pueden transferir los datos únicamente a la conexión que necesita esos datos. Otra diferencia entre un puente y un Switch es que un Switch no convierte formatos de transmisión de datos. Ver figura 3 - 4.

Figura 3.Switch
Fuente: http://nayeli-

[7] http://www.monografias.com/trabajos30/redes-de-datos/redes-de-datos.shtml

- **Modem ADSL**

Figura 4. Fotografía del modem ADSL de movistar

Es un router ADSL de fácil conexión, configuración y mantenimiento, como se muestra en la figura 5. Va a permitir que con una única línea telefónica, y con una sola cuenta de acceso a Internet, puedan conectarse todos los puertos de la LAN a Internet.

- **Router inalámbrico**

Figura 5. Fotografía del router inalámbrico TP-LINK
Fuente: http://www.tp-link.com/ar/products/details/cat-4691_TL-MR3220.html

Cumpliendo con el estándar IEEE 802.11n, el TL-MR3220 puede establecer una red inalámbrica con velocidades de transmisión de hasta 150 Mbps, mientras que la mitiga la pérdida de datos a largas distancias a través de obstáculos en una oficina pequeña o un apartamento grande, incluso en una de acero y edificio de concreto. Por encima de todo, los usuarios pueden fácilmente tomar su señal de

red inalámbrica a distancias más largas desde el router, donde con los productos 11g tendrían que estar mucho más cerca[8]. Ver figura 6.

- **RouterBoard hAP lite RB941 2nD**

.

Figura 6. RouterBoard de mikrotik
Fuente: http://routerboard.com/RB941-2nD

Se trata de un pequeño AccessPoint ideal para un apartamento, casa u oficina. Es compatible con WPS, por comodidad, tecnología que permite no tener que escribir una compleja contraseña cuando alguien quiere tener acceso inalámbrico a Internet. También puede ser usada en modo CAP y unirse a una red gestionada centralmente por CAPsMAN. Por supuesto, el dispositivo integra RouterOS con todas las características como balanceo de ancho de banda, firewall, control de acceso para usuarios y muchos otras. El hAP Lite está equipado con una potente CPU de 650MHz, 32MB de RAM, antena inalámbrica integrada de doble polaridad a 2.4GHz, cuatro puertos Fast Ethernet y licencia RouterOS L4.[9]

- **Topología de una red**

La topología de una red define únicamente la distribución del cable que interconecta los diferentes computadores, es decir, es el mapa de distribución del cable que forma la Intranet. Define cómo se organiza el cable de las estaciones de trabajo. A la hora de instalar una Red, es importante seleccionar la topología más adecuada a las necesidades existentes. Hay una serie de factores a tener en cuenta a la hora de decidirse por una topología de Red concreta, y éstas son:

- La distribución de los equipos a interconectar.
- El tipo de aplicaciones que se van a ejecutar.

[8] http://www.tp-link.com/co/products/details/cat-14_TL-MR3220.html
[9] http://routerboard.com/RB941-2nD

- La inversión que se quiere hacer.
- El coste que se quiere dedicar al mantenimiento y actualización de la red local.
- El tráfico que va a soportar la red local.
- La capacidad de expansión. Se debe diseñar una intranet teniendo en cuenta
- la escalabilidad.
- La arquitectura de una red engloba:
- La topología.
- El método de acceso al cable.
- Protocolos de comunicaciones.

Actualmente la topología está directamente relacionada con el método de acceso al cable, puesto que éste depende casi directamente de la tarjeta de red y ésta depende de la topología elegida.

b. Topología física

Es lo que hasta ahora se ha venido definiendo; la forma en la que el cableado se realiza en una red. Existen tres topologías físicas puras. Ver figura 7.

- **Topología en anillo**

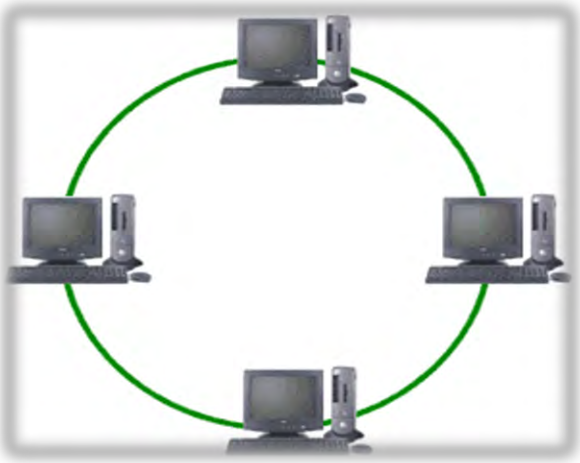

Figura 7. Topología en anillo
Fuente: http://ti-prosoft.com/Docslink/Analisisred.pdf

Tipo de LAN[10] en la que los computadores o nodos están enlazados formando un círculo a través de un mismo cable, como podemos observar en la figura 7. Las

[10] http://majo-flores.blogspot.com.co/2011/08/topologias-de-red.html

señales circulan en un solo sentido por el círculo, regenerándose en cada nodo. En la práctica, la mayoría de las topologías lógicas en anillo son en realidad una topología física en estrella.

Sus principales características, son:

- El cable forma un bucle cerrado formando un anillo.
- Todos los computadores que forman parte de la red se conectan a ese anillo.
- Habitualmente las redes en anillo utilizan como método de acceso al medio el modelo “paso de testigo”.

Los principales inconvenientes, son:

- Si se rompe el cable que forma el anillo se paraliza toda la red.
- Es difícil de instalar.
- Requiere mantenimiento.

- **Topología en bus**

Consta de un único cable que se extiende de un computador al siguiente de un modo serie. Los extremos del cable se terminan con una resistencia denominada terminadora, que además de indicar que no existen más computadores en el extremo, permiten cerrar el bus, como se refleja en la figura 8.

A diferencia del anillo, el bus es pasivo, no se produce regeneración de las señales en cada nodo. Como ejemplos de topología de bus tenemos 10BASE-2 y 10BASE-5. (Ver Figura 8).

Sus principales ventajas son:

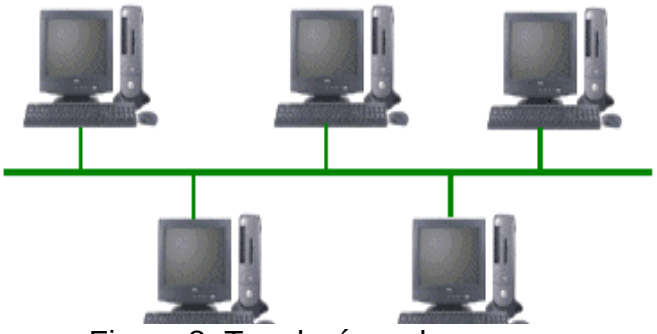

Figura 8. Topología en bus
Fuente: http://ti-prosoft.com/Docslink/Analisisred.pdf

- Fácil de instalar y mantener.
- No existen elementos centrales del que dependa toda la red, cuyo fallo dejaría
- Inoperativas a todas las estaciones.

Sus principales inconvenientes son: si se rompe el cable en algún punto, la red queda inoperativa por completo[11].

- **Red inalámbrica Wi-Fi**

Wi-Fi es una marca de la Wi-Fi Alliance (anteriormente la Wireless Ethernet Compatibility Alliance), la organización comercial que prueba y certifica que los equipos cumplen los estándares IEEE 802.11x.

Las nuevas redes sin cables hacen posible que se pueda conectar a una red local cualquier dispositivo sin necesidad de instalación, lo que permite que se pueda pasear libremente por la oficina con nuestro ordenador portátil conectado a la red o conectar sin cables cámaras de vigilancia en los lugares más inaccesibles. También se puede instalar en locales públicos y dar el servicio de acceso a Internet sin cables, como se puede ver en la figura 9.

La norma IEEE 802.11b dio carácter universal a esta tecnología que permite la conexión de cualquier equipo informático a una red de datos Ethernet sin necesidad de cableado, que actualmente se puede integrar también con los equipos de acceso ADSL para Internet. Ver figura 9.

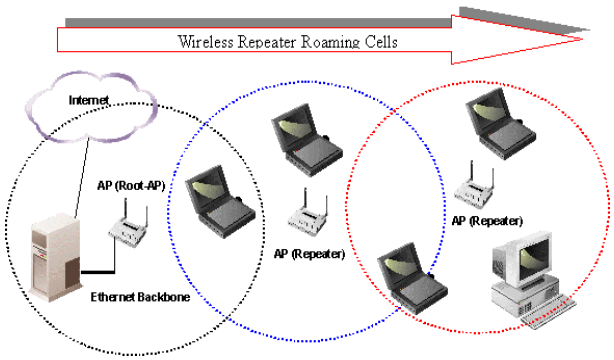

Figura 9. Topología de red inalámbrica Wifi
Fuente: http://ti-prosoft.com/Docslink/Analisisred.pdf

[11] http://cableadoestructurado.galeon.com/enlaces1685276.html

c. Seguridad

Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-Fi es la seguridad. Un muy elevado porcentaje de redes se han instalado por administradores de sistemas o de redes por su simplicidad de implementación, sin tener en consideración la seguridad y por tanto han convertido sus redes en redes abiertas, sin proteger el acceso a la información que por ellas circulan. Existen varias alternativas para garantizar la seguridad de estas redes, las más comunes son la utilización de protocolos de encriptación de datos como el WEP y el WPA, proporcionados por los propios dispositivos inalámbricos, o IPSEC (túneles IP) y 802.1x, proporcionados por o mediando otros dispositivos de la red de datos.

d. Topología en estrella

Lo más usual en ésta topología es que en un extremo del segmento se sitúe un nodo y el otro extremo se termine con un concentrador, como se puede visualizar en la figura 10. La principal ventaja de este tipo de red es la fiabilidad, dado que si uno de los segmentos tiene una rotura, afectará sólo al nodo conectado en él. Otros usuarios de los computadores de la red continuarán operando como si ese segmento no existiera. 10BASE-T Ethernet y Fast Ethernet son ejemplos de esta topología. Ver figura 10.

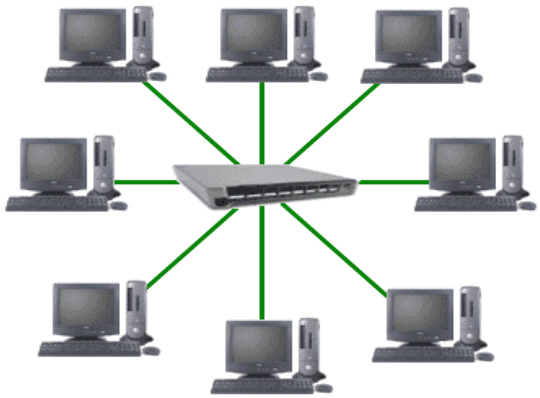

Figura 10. Topología en estrella
Fuente: http://ti-prosoft.com/Docslink/Analisisred.pdf

Sus principales características, son:

- Todas las estaciones de trabajo están conectadas a un punto central (concentrador), formando una estrella física.

- Habitualmente sobre este tipo de topología se utiliza como método de acceso al medio poolling, siendo el nodo central el que se encarga de implementarlo.
- Cada vez que se quiere establecer comunicación entre dos computadores, la información transferida de uno hacia el otro debe pasar por el punto central.
- Existen algunas redes con esta topología que utilizan como punto central una estación de trabajo que gobierna la red.
- La velocidad suele ser alta para comunicaciones entre el nodo central y los nodos extremos, pero es baja cuando se establece entre nodos extremos.
- Este tipo de topología se utiliza cuando el cambio de información se va a realizar ventajosamente entre el nodo central y el resto de los nodos, y no cuando la comunicación se hace entre nodos extremos.
- Si se rompe un cable sólo se pierde la conexión del nodo que interconectaba.
- Es fácil de detectar y de localizar un problema en la red.

e. Topología en árbol

La topología en árbol es similar a la topología en estrella extendida, salvo en que no tiene un nodo central. En cambio, un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos[12].

El enlace troncal es un cable con varias capas de ramificaciones, y el flujo de información es jerárquico generalmente se encuentra un host servidor. Ver figura 11.

Figura 11. Topología en árbol
Fuente:http://hugoenriquecastrocruz615.blogspot.com/2009/02/topologia

[12] http://galeon.com/jonatan11/equipo3/equipo3.htm

f. Topología lógica

Es la forma de conseguir el funcionamiento de una topología física cableando la red de una forma más eficiente. Existen topologías lógicas definidas:

- **Topología anillo - estrella**

Uno de los inconvenientes de la topología en anillo es que si el cable se rompe toda la red queda inoperativa; con la topología mixta anillo problemas quedan resueltos.

Las principales características, son:

Cuando se instala una configuración en anillo, se establece de forma lógica únicamente, ya que de forma física se utiliza una configuración en estrella. Se utiliza un concentrador, o incluso un servidor de red (uno de los nodos de la red, aunque esto es el menor número de ocasiones) como dispositivo central, de forma, si se rompe algún cable sólo queda inoperativo el nodo que conecta, y los demás pueden seguir funcionando.

El concentrador utilizado cuando se está utilizando esta topología se denomina MAU (Unidad de Acceso Multiestación), que consiste en un dispositivo que proporciona el punto de conexión para múltiples nodos. Contiene un anillo interno que se extiende a un anillo externo.

A simple vista, la red parece una estrella, aunque internamente funciona como un anillo**.**

Cuando la MAU detecta que un nodo se ha desconectado (por haberse roto el cable, por ejemplo), puentea su entrada y su salida para así cerrar el anillo.

- **Topología bus-estrella**

Este tipo de topología es en realidad una estrella que funciona como si fuese en bus. Como punto central tiene un concentrador pasivo (Hub) que implementa internamente el bus, y al que están conectados todos los computadores[13].

La única diferencia que existe entre esta topología mixta y la topología en estrella con hub pasivo es el método de acceso al medio utilizado.

La finalidad es dar a conocer la Red, como un mecanismo para compartir recursos, por lo cual se debe conectar físicamente los ordenadores. Para ello

[13] http://genesis.uag.mx/edmedia/material/comuelectro/uni1_2_7.cfm

debemos escoger entre las múltiples soluciones para conectar equipos físicamente en red.

3.3.3.2 Tipos de redes. Principales tipos de redes para soportar los sistemas distribuidos son:

a. Redes de área local:

Las redes de área local (local área Networks) llevan mensajes a velocidades relativamente grandes entre computadores conectados a un único medio de comunicaciones: un cable de par trenzado. Un cable coaxial o una fibra óptica. Un segmento es una sección de cable que da servicio y que puede tener varios computadores conectados, el ancho de banda del mismo se reparte entre dichas computadores. Las redes de área local mayores están compuestas por varios segmentos interconectados por conmutadores (switches) o concentradores (hubs). El ancho de banda total del sistema es grande y la latencia pequeña, salvo cuando el tráfico es muy alto.

b. Redes de área extensa

Estas pueden llevar mensajes entre nodos que están a menudo en diferentes organizaciones y quizás separadas por grandes distancias, pero a una velocidad menor que las redes LAN. El medio de comunicación está compuesto por un conjunto de círculos de enlazadas mediante computadores dedicados, llamados rotures o encaminadores. Esto gestiona la red de comunicaciones y encaminan mensajes o paquetes hacia su destino. En la mayoría de las redes se produce un retardo en cada punto de la ruta a causa de las operaciones de encaminamiento, por lo que la latencia total de la transmisión de un mensaje depende de la ruta seguida y de la carga de tráfico en los distintos segmentos que atraviese. La velocidad de las señales electrónicas en la mayoría de los medios es cercana a la velocidad de la luz, y esto impone un límite inferior a la latencia de las transmisiones para las transmisiones de larga distancia[14].

c. Redes de área metropolitana

Las MAN (Metropolitan Área Networks) se basan en el gran ancho de banda de las cableadas de cobre y fibra óptica recientemente instalados para la transmisión de videos, voz, y otro tipo de datos. Varias han sido las tecnologías utilizadas para implementar el encaminamiento en las redes LAN, desde Ethernet hasta ATM. IEEE ha publicado la especificación 802.6 [IEEE 1994], diseñado expresamente para satisfacer las necesidades de las redes WAN. Las conexiones de línea de

[14] http://informaciondet.blogspot.com.co/p/redes-de-computo.html

suscripción digital, DLS (digital subscribe line) y los MODEM de cable son un ejemplo de esto. DSL utiliza generalmente conmutadores digitales sobre par trenzado a velocidades entre 0.25 y 6.0 Mbps; la utilización de este par trenzado para las conexiones limita la distancia al conmutador a 1.5 kilómetros.

Una conexión de MODEM por cable utiliza una señalización análoga sobre el cable coaxial de televisión para conseguir velocidades de 1.5 Mbps con un alcance superior que DSL.

d. Redes inalámbricas

La conexión de los dispositivos portátiles y de mano necesitan redes de comunicaciones inalámbricas (Wireless Networks). Algunos de ellos son la IEEE802.11 (wave LAN) son verdaderas redes LAN inalámbricas (Wireless local área Networks; WLAN) diseñados para ser utilizados en vez de los LAN. También se encuentran las redes de área personal inalámbricas, incluida la red europea mediante el Sistema Global para Comunicaciones Móviles, GSM (Global System for Mobile Communication). En los Estados Unidos, la mayoría de los teléfonos móviles están actualmente basados en la análoga red de radio celular AMPS, sobre la cual se encuentra la red digital de comunicaciones de Paquetes de Datos Digitales Celular, CDPD (Cellular Digital Packet Data).

Dado el restringido ancho de banda disponible y las otras limitaciones de los conjuntos de protocolos llamados Protocolos de Aplicación Inalámbrica WAP (Wireless Aplication Protocol).

Uno de los sucesos más críticos para la conexión en red lo constituye la aparición y la rápida difusión de la red de área local (LAN) como forma de normalizar las conexiones entre las máquinas que se utilizan como sistemas ofimáticos. Como su propio nombre indica, constituye una forma de interconectar una serie de equipos informáticos[15].

A su nivel más elemental, una LAN no es más que un medio compartido (como un cable coaxial al que se conectan todas las computadoras y las impresoras) junto con una serie de reglas que rigen el acceso a dicho medio. La LAN más difundida, Ethernet, utiliza un mecanismo conocido como CSMA/CD. Esto significa que cada equipo conectado sólo puede utilizar el cable cuando ningún otro equipo lo está utilizando. Si hay algún conflicto, el equipo que está intentando establecer la conexión la anula y efectúa un nuevo intento más tarde.

3.3.3.3 Normas y estándares de red. Los creadores de estándares están siempre tratando de moldear un estándar en cemento, mientras los innovadores intentan

[15] http://datateca.unad.edu.co/contenidos/203532/Unidad_2/exelearning_leccion_Unidad

crear uno nuevo. Incluso una vez creados los estándares, son violados tan pronto como el proveedor agregue una nueva característica[16].

Los estándares oficiales creados por organizaciones tales como:

- **ANSI:** american National Standards Institute. Organización Privada sin fines de lucro fundada en 1918, la cual administra y coordina el sistema de estandarización voluntaria del sector privado de los Estados Unidos.

- **EIA:** electronics Industry Association. Fundada en 1924. Desarrolla normas y publicaciones sobre las principales áreas técnicas: los componentes electrónicos, electrónica del consumidor, información electrónica, y telecomunicaciones.

- **TIA:** Telecommunications Industry Association. Fundada en 1985 después del rompimiento del monopolio de AT&T. Desarrolla normas de cableado industrial voluntario para muchos productos de las telecomunicaciones y tiene más de 70 normas reestablecidas.

- **ISO:** International Standards Organization. Organización no gubernamental creada en 1947 a nivel Mundial, de cuerpos de normas nacionales, con más de 140 países.

- **IEEE:** Instituto de Ingenieros Eléctricos y de Electrónica. Principalmente responsable por las especificaciones de redes de área local como 802.3 Ethernet, 802.5 Token Ring, ATM y las normas de Gigabite/Ethernet. El comité que se ocupa de los estándares de computadoras a nivel mundial es de la IEEE en su división 802, los cuales se dedican a lo referente de sistema de red están especificado los siguientes[17]:

  - ✓ **IEEE 802.3**: hace referencia a las redes tipo bus en donde se deben de evitar las colisiones de paquetes de información, por lo cual este estándar hace referencia el uso de CSMA/CD (Acceso múltiple con detención de portadora con detención de colisión).

  - ✓ **IEEE 802.4**: representa al método de acceso Token pero para una red con topología en anillo o la conocida como Token bus.

  - ✓ **IEEE 802.5**: hace referencia al método de acceso Token, pero para una red con topología en anillo, conocida como la Token Ring.

[16] http://redes5f.awardspace.com/Tarea%202.html

[17] http://datateca.unad.edu.co/contenidos/2150517/Exe_2150517/leccin_6_recoleccin_de_normas_vigentes.html

Las normas oficiales creados por organizaciones tales como:

- **ANSI/TIA/EIA-568-B.** Cableado de Telecomunicaciones en Edificios Comerciales. (Cómo instalar el Cableado)

- **TIA/EIA 568-B1.** Requerimientos generales

- **TIA/EIA 568-B2.** Componentes de cableado mediante par trenzado balanceado. Detalla los requerimientos específicos de los cables de pares trenzados balanceados, a nivel de sus componentes y de sus parámetros de transmisión

- **TIA/EIA 568-B3.** Componentes de cableado, Fibra óptica.

- **ANSI/TIA/EIA-569-A.** Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales (Cómo enrutar el cableado).

- **ANSI/TIA/EIA-570-A.** Normas de Infraestructura Residencial de Telecomunicaciones.

- **ANSI/TIA/EIA-606-A.** Normas de Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales.

- **ANSI/TIA/EIA-607.** Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales.

- **ANSI/TIA/EIA-758.** Norma Cliente-Propietario de cableado de Planta Externa de Telecomunicaciones estables, por lo menos durante un tiempo.

El cableado es una forma ordenada de conectar los cables para una red, basándose en normas EIA/TIA, establecidas a lo largo de todo el mundo, esto con el fin de establecer un orden en el mundo de la computación y las redes.

3.3.3.4 Tecnología de comunicación utilizada en redes. Las tecnologías utilizadas para la comunicación entre equipos pertenecientes a una red son las que indican la secuencia o protocolos utilizados para el transporte de la información a través del medio de transmisión utilizado. Se diferencian principalmente por la velocidad de transferencia de datos y por la configuración física de red que permiten. Las tecnologías más comunes son Ethernet, Token Ring, FDDI y ATM, sistemas que describimos a continuación:

a. Sistema ethernet

Este tipo de tecnología[18] más utilizada en redes de área local (LAN). La red Ethernet apareció por primera vez en 1970 desarrollado por la empresa Xerox, trabaja con el protocolo CSMA/CD con una velocidad de transmisión a ese entonces de 2.94 Mbps, velocidad muy alta para tal época, para conectar más de 100 estaciones de trabajo en un cable de 1 km.

Con el paso del tiempo esta tecnología ha sufrido varios cambios, de los cuales los más significativos son la velocidad de transferencia a 10 Mbps y la longitud máxima permitida entre los equipos. Las colisiones limitan la productividad máxima de la red al 30%. Existen versiones tanto con cable de cobre como con fibra óptica.

- **Especificación original de ethernet:**

Estándar IEEE 802.3 10Base5 cable coaxial grueso: Estos cables coaxiales permiten una transmisión de datos de mucha distancia sin debilitarse la señal, pero el problema es que, un metro de cable coaxial grueso pesa hasta medio kilogramo, y no puede doblarse fácilmente. Un enlace de coaxial grueso puede ser hasta 3 veces más largo que un coaxial delgado, para mayor detalle obsérvese la figura 12.

Algunas características de estos cables son:

- Conector BNC
- Longitud máxima de un segmento: 500 m.

Figura 12. Conector BNC
Fuente: http://www.videovigilancia.eu.com/components/com_ virtuemart/shop_image/product/BNC_ Female_Femmi_4bc4e55f47dec.jpg

[18] http://www.rediris.es/difusion/publicaciones/boletin/46-47/ponencia9.html

- Número máximo de segmentos interconectados por repetidores: 5
- Número máximo de conexiones por segmento: 100

Estándar IEEE 802.3 10 base2 cable coaxial fino: Este tipo de cable se le denomina delgado porque es menos grueso que el otro tipo de cable coaxial, debido a esto es menos rígido que el otro tipo, y es más fácil de instalar. Obsérvese la figura 13.

Figura 13. Cable coaxial grueso y delgado
Fuente: http://2.bp.blogspot.com/-9An4xC_Sgk/UGnfspDIOsI/AAAAAAAAABI/hKIoZsUkA8w/s1600/Outdoor_CATV_P3_500_Trunk_thick_coaxial_cable.jpg

Algunas características de estos cables son:

- Conector BNC
- Longitud máxima de un segmento: 185 m.
- Número máximo de segmentos interconectados por repetidores: 5
- Número máximo de conexiones por segmento: 30
- Separación mínima entre conexiones de 1,5 m. Ver figura 14.

802.3 10 baseT:

Figura 14. Conectores RJ-45 macho (M) y hembra (F)
Fuente: http://i00.i.aliimg.com/wsphoto/v1/321966878/-font-b-RJ45-b-font-font-b-Male-b-font-font-b-to-b-font.jpg

Las principales características, son:

- Cable de par trenzado, con conector RJ-45
- Cable de distintas categorías (normalizadas)
- No apantallado (UTP) o apantallado (STP)
- Dos pares de hilos en el cable (dos Tx y dos Rx)
- Se utiliza un concentrador (Hub) al que se conecta cada computador
- El concentrador hace las funciones de un repetidor pasivo

802.3 10baset SW

- Es conocido como Ethernet 10BaseT conmutado.
- Consiste en sustituir el concentrador por un conmutador (switch)
- Con las mismas restricciones que en 10BaseT
- Mejora el rendimiento: sólo se efectúa difusión cuando en necesario
- Los datos circulan por conexiones punto-punto.
- Es posible tener transferencias simultáneas entre distintos pares de nodos y filtrar tráfico.

Ethernet es una tecnología muy usada ya que su costo no es muy elevado

Evolución de ethernet: fast ethernet (IEEE 802.3U): Existen colisiones en el acceso al canal; la productividad máxima está en torno al 50%, las tarjetas y concentradores suelen ser duales.

Hay distintas especificaciones de nivel físico:

- Ethernet 802.3u 100BaseTX:
  - ✓ Cable de par trenzado UTP o STP de categoría 5 (dos pares), y conectores RJ-45
  - ✓ Longitud máxima enlace computador–concentrador: 100 m
- Ethernet 802.3u 100BaseFX:
  - ✓ Utiliza cable de fibra óptica multimodo, similar a FDDI
  - ✓ Longitud máxima enlace computador–concentrador: 400 m
- Ethernet 802.3 100BaseT4:
  - ✓ Utiliza cable de par trenzado de categoría 3 con 4 pares, y conectores RJ-45
  - ✓ Longitud máxima enlace computador–concentrador:100 m7

b. Sistema token ring.

La tecnología Token Ring[19] fue creada por IBM y está destinada al uso con redes en anillo aunque realmente el alambrado es hecho en forma de estrella por medio de unas unidades especiales denominadas MAU o unidad de acceso multiestacionario.

El Token Ring viaja a través de la red por cada una de las estaciones y es el encargado de asignar los permisos para transmisión de datos. Si una estación desea transmitir información debe esperar el turno hasta que el Token Ring pase por allí y la habilite para tal operación. Con este método se elimina la posibilidad de colisión ya que siempre existe una única estación que puede transmitir en determinado momento.

Dentro de este sistema se puede describir algunas de sus características principales:

- Utiliza una topología lógica en anillo, aunque por medio de una unidad de acceso de estación múltiple (MSAU), la red puede verse como si fuera una estrella. Tiene topología física estrella y topología lógica en anillo.

- Utiliza cable especial apantallado, aunque el cableado también puede ser par trenzado.

- La longitud total de la red no puede superar los 366 metros.

- La distancia entre una computadora y el MAU no puede ser mayor que 100 metros.

- A cada MAU se pueden conectar ocho computadoras.

- Estas redes alcanzan una velocidad máxima de transmisión que oscila entre los 4 y los 16 Mbps.

- Posteriormente el High Speed Token Ring (HSTR) elevó la velocidad a 110 Mbps pero la mayoría de redes no la soportan.

[19] http://tecnologia-celulares-smartphones.blogspot.com.co/2015/01/protocolos-de-comunicacion-de-redes.html

c. Sistema ATM (asinchronous transfer mode)

Modo de Transferencia Asíncrona[20], es una tecnología de red diseñada para alta velocidad de transferencia de datos. ATM define una estructura física de 53 bytes, denominada celda, la cual puede ser usada para transmitir voz, datos y vídeo en tiempo real, todo sobre el mismo cable en forma simultánea.

La tecnología ATM básica viaja a 155 Mbps pero algunas versiones permiten 660 Mbps. Inclusive, en pruebas de laboratorios se han alcanzado velocidades mucho más altas. Este sistema de transmisión ha sido denominado de tercera generación debido a que se ambiaron los esquemas tradicionales de transmisión de información a través de la red.

El Sistema ATM es una tecnología de conmutación excelente, a continuación se destaca algunos de sus beneficios:

- Una única red ATM dará cabida a todo tipo de tráfico (voz, datos y video). ATM mejora la eficiencia y manejabilidad de la red.

- Capacita nuevas aplicaciones, debido a su alta velocidad y a la integración de los tipos de tráfico, ATM capacita la creación y la expansión de nuevas aplicaciones como la multimedia.

- Compatibilidad, porque ATM no está basado en un tipo especifico de transporte físico, es compatible con las actuales redes físicas que han sido desplegadas. ATM puede ser implementado sobre par trenzado, cable coaxial y fibra óptica.

- Simplifica el control de la red. ATM está evolucionando hacia una tecnología estándar para todo tipo de comunicaciones. Esta uniformidad intenta simplificar el control de la red usando la misma tecnología para todos los niveles de la red.

- Largo periodo de vida de la arquitectura. Los sistemas de información y las industrias de telecomunicaciones se están centrando y están estandarizando ATM.

3.3.3.5 Protocolos de red[21]. Es una descripción formal de un conjunto de reglas y convenciones que rigen un aspecto particular de cómo los dispositivos de una red se comunican entre sí, que posibilitan la comunicación de red desde un host hacia otro host. Los protocolos determinan el formato, la sincronización, la

[20] http://html.rincondelvago.com/atm.html
[21] http://www.monografias.com/trabajos30/redes-de-datos/redes-de-datos.shtml

secuenciación y el control de los errores en la comunicación de datos. Sin protocolos, la computadora no puede armar o reconstruir el formato original del flujo de bits entrantes desde otra computadora. Los protocolos controlan todos los aspectos de la comunicación de datos, que incluye lo siguiente:

- Cómo se construye la red física.
- Cómo los computadores se conectan a la red.
- Cómo se formatean los datos para su transmisión.
- Cómo se envían los datos.
- Cómo se manejan los errores.

Un protocolo de red es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red, además es una convención o estándar que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales. Permite establecer, mantener y finalizar una comunicación.

3.3.3.6 Modelo OSI:

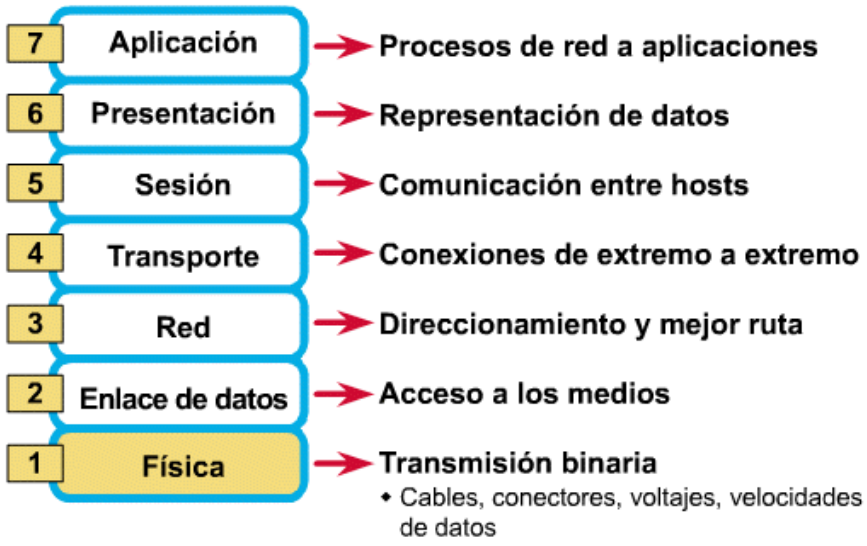

Figura 15. Las capas del modelo OSI
Fuente: http://2.bp.blogspot.com/-t8ZNB75xYqg/TcTRF7yRORI/AAAAAAAAAOE/GBrWCWWVOSI/s1600/OSI.gif

El modelo OSI (*Open Systems Interconnection*, interconexión de sistemas abiertos) fue un intento de la Organización Internacional de Normas (ISO) para la creación de un estándar que siguieran los diseñadores de nuevas redes. Se trata

de un modelo teórico de referencia: únicamente explica lo que debe hacer cada componente de la red sin entrar en los detalles de implementación.

El modelo divide las redes en capas. Cada una de estas capas debe tener una función bien definida y relacionarse con sus capas inmediatas mediante unos interfaces también bien definidos. Esto debe permitir la sustitución de una de las capas sin afectar al resto, siempre y cuando no se varíen los interfaces que la relacionan con sus capas superior e inferior. El sistema de comunicaciones del modelo OSI estructura el proceso en varias capas que interaccionan entre sí. Una capa proporciona servicios a la capa superior siguiente y toma los servicios que le presta la siguiente capa inferior.

a. Normalización dentro del modelo OSI

El proceso de descomposición del problema de comunicaciones en capas hace posible la normalización de cada capa por independiente y la posible modificación de una capa sin afectar a las demás.

Es preciso el empleo de normalizaciones para que dos sistemas puedan conocerse y poder comunicarse con plena exactitud, sin ambigüedades.

Para que dos capas de dos sistemas se puedan comunicar es necesario que estén definidas las mismas funciones en ambos, aunque el cómo se implementen en la capa inferior de cada sistema sea diferente.

b. Primitivas de servicio y parámetros[22]

Las capas inferiores suministran a las superiores una serie de funciones o primitivas y una serie de parámetros. La implementación concreta de estas funciones está oculta para la capa superior ésta sólo puede utilizar las funciones y los parámetros para comunicarse con la capa inferior (paso de datos y control).

El gráfico anterior figura 15 se muestran las 7 capas del modelo OSI. Las tres primeras capas se utilizan para mover la información de unas redes a otras. En cambio, las capas superiores son exclusivas de los nodos origen y destino. La capa física está relacionada con el medio de transmisión (cableado concreto que utiliza cada red). En el extremo opuesto se encuentra la capa de aplicación: un programa de mensajería electrónica, por ejemplo. El usuario se situaría por encima de la capa 7. La figura 16 muestra el flujo de información entre capas.

[22] http://www.monografias.com/trabajos14/tipos-redes/tipos-redes.shtml

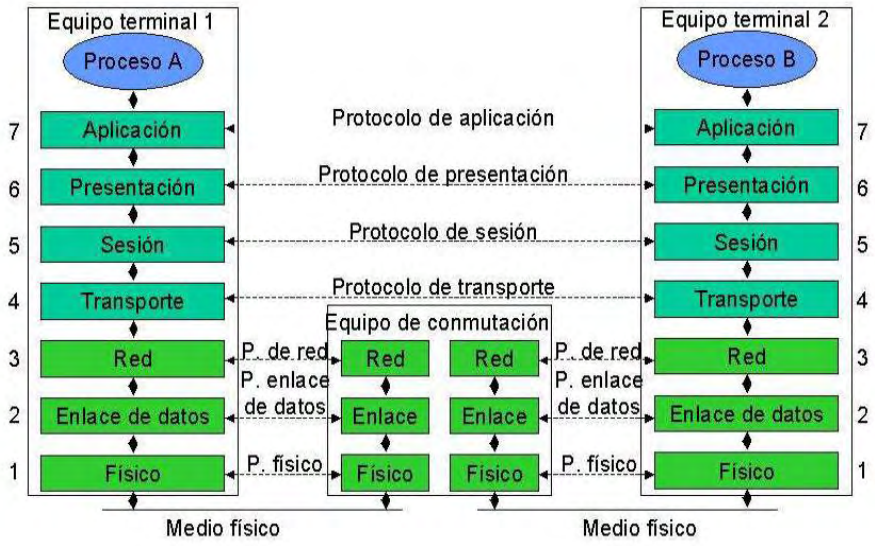

Figura 16. Esquema con los 7 niveles del modelo de referencia

Fuente: http://ariadna.ii.uam.es/wiki/wiki_ar1/doku.php?id=introduccion

El host A es el nodo origen y el host B, el nodo destino. Nótese que estos papeles se intercambian continuamente en cualquier comunicación. Mediante este modelo se envía un mensaje al usuario del host B. El mensaje son los "datos" que están por encima de la capa Estos datos van descendiendo de capa en capa hasta llegar a la capa física del host A. Cada capa añade un encabezado (C = cabecera) a los datos que recibe de la capa superior antes de enviárselos a su capa inferior. En la capa de enlace de datos existen una serie de códigos al final de la secuencia (F = final) para delimitar no sólo el comienzo sino también el final de un paquete de datos. La capa física no entiende de datos ni de códigos: únicamente envía una secuencia de bits por el medio de transmisión (un cable).

Estos bits llegarán, probablemente pasando por varios encaminadores intermedios, hasta la capa física del host destino. A medida que se van recibiendo secuencias de bits, se van pasando a las capas superiores. Cada capa elimina su encabezado antes de pasarlo a una capa superior. El mensaje que envía cada capa del host A a su capa inferior es idéntico al que recibe la capa equivalente del host B desde una capa inferior. Finalmente los datos llegarán a la capa de aplicación, serán interpretados y mostrados al usuario del host B.

Los paquetes de datos de cada capa suelen recibir nombres distintos. En la capa de enlace de datos marcos o tramas; en la capa de red, de paquetes o

datagramas. En la capa de transporte, en ocasiones se utiliza el término segmento.

Cada capa se comunica con la capa equivalente de otro host (por ejemplo, la capa de red de un host se entiende con la capa de red de otro host). Sin embargo, la comunicación realmente desciende capas en el host origen, transmitiendo por el medio físico y aumentando capas en el host destino. Cada capa añade algo nuevo a la comunicación, como a continuación:

- **Capa física[23].** Se encarga de la transmisión de bits por un medio de transmisión, ya sea un medio guiado (un cable) o un medio no guiado (inalámbrico). Esta capa define, entre otros aspectos, lo que transmite cada hilo de un cable, los tipos de conectores, el voltaje que representa un 1 y el que representa un 0. La capa física será diferente dependiendo del medio de transmisión (cable de fibra óptica, cable par trenzado, enlace vía satélite, etc). No interpreta la información que está enviando: sólo transmite ceros y unos.

- **Capa de enlace de datos.** Envía tramas de datos entre hosts (o routers) de una misma red. Delimita las secuencias de bits que envía a la capa física, escribiendo ciertos códigos al comienzo y al final de cada trama. Esta capa fue diseñada originalmente para enlaces punto *a* punto, en los cuales hay que aplicar un control de flujo para el envío continuo de grandes cantidades de información. Para las redes de difusión (redes en las que muchos ordenadores comparten un mismo medio de transmisión) fue necesario diseñar la llamada subcapa de acceso al medio. Esta subcapa determina quién puede acceder al medio en cada momento y cómo sabe cada host que un mensaje es para él, por citar dos problemas que se resuelven a este nivel.

- **Capa de red.** Se encarga del encaminamiento de paquetes entre el origen y el destino, atravesando tantas redes intermedias como sean necesarias. Los mensajes se fragmentan en paquetes y cada uno de ellos se envía de forma independiente. Su misión es unificar redes heterogéneas: todos los host tendrán un identificador similar a nivel de la capa de red (en Internet son las direcciones IP) independientemente de las redes que tengan en capas inferiores (Token Ring con cable coaxial, Ethernet con cable de fibra óptica, enlace submarino, enlace por ondas, etc.).

- **Capa de transporte[24].** Únicamente se preocupa de la transmisión origen/destino. Esta capa canaliza fiablemente la unión de un proceso de un host con otro proceso de otro host. Un host puede tener varios procesos ejecutándose: uno para mensajería y otro para transferir archivos, por ejemplo. No se preocupa del camino intermedio que siguen los fragmentos de los

[23] http://www.monografias.com/trabajos14/tipos-redes/tipos-redes.shtml
[24] http://es.slideshare.net/arbolita/deber2-34974464

mensajes. Integra control de flujo y control de errores, de forma que los datos lleguen correctamente de un extremo a otro.

- **Capa de sesión.** Se encarga de iniciar y finalizar las comunicaciones. Además proporciona servicios mejorados a la capa de transporte como, por ejemplo, la creación de puntos de incronismo para recuperar transferencias largas fallidas.

- **Capa de presentación.** Codifica los datos que recibe de la capa de aplicación a un sistema convenido entre emisor y receptor, con el propósito de que tanto textos como números sean interpretados correctamente. Una posibilidad es codificar los textos según la *tabla ASCII* y los números en complemento a dos.

- **Capa de aplicación.** Aquí se encuentran los protocolos y programas que utiliza el usuario para sus comunicaciones en red. Esta capa tendrá que ser adaptada para cada tipo de computador de forma que sea posible el envío de un correo electrónico (u otros servicios) entre sistemas heterogéneos como Macintosh, Linux o Windows.

Sin embargo, la idea de la división por capas del modelo OSI es realmente valiosa. Esta misma idea se aplica a todas las redes actuales, incluyendo Internet. OSI es un modelo teórico general que da preferencia a un buen diseño en papel, antes que a la implementación de los protocolos. El modelo TCP/IP se hizo justamente al revés: primero vinieron los protocolos y, después, se pensó en sus especificaciones.

De tal forma, que el modelo TCP/IP únicamente es aplicable para la pila de protocolos TCP/IP.

La comunicación según el modelo OSI siempre se realizará entre dos sistemas. Supóngase que la información se genera en el nivel 7 de uno de ellos, y desciende por el resto de los niveles hasta llegar al nivel 1, que es el correspondiente al medio de transmisión (por ejemplo el cable de red) y llega hasta el nivel 1 del otro sistema, donde va ascendiendo hasta alcanzar el nivel 7. En este proceso, cada uno de los niveles va añadiendo a los datos a transmitir la información de control relativa a su nivel, de forma que los datos originales van siendo recubiertos por capas de datos de control.

3.3.3.7 El protocolo TCP/IP. El Internet [25]es una red de computadores conectados juntos a través de redes de comunicaciones. Esta red consiste en enlaces de fibra óptica, satélite, radio y las líneas telefónicas.

[25] http://recursostic.educacion.es/usuarios/web/ayudas/54-conexiones-a-internet-bis

El sistema tiene computadores de todos los tipos y funcionamiento todo el tipo de sistemas operativos. Todos utilizan el TCP/IP como lenguaje común.

a. Concepto

Cuando se habla de TCP/IP, se relaciona automáticamente como el protocolo sobre el que funciona la red Internet. Esto, en cierta forma es verdad, ya que se le llama TCP/IP, a la familia de protocolos que permite estar conectados a la red Internet. Este nombre viene dado por los dos protocolos estrella de esta familia:

- **Protocolo TCP**, funciona en el nivel de transporte del modelo de referencia OSI, proporcionando un transporte fiable de datos.

- **Protocolo IP**, funciona en el nivel de red del modelo OSI, que nos permite encaminar nuestros datos hacia otras computadoras.

Pero un protocolo de comunicaciones debe solucionar una serie de problemas relacionados con la comunicación entre computadores, además de los que proporciona los protocolos TCP e IP.

TCP/IP se basa en software utilizado en redes. Aunque el nombre **TCP/IP** implica que el ámbito total del producto es la combinación de dos protocolos: Protocolo de Control de Transmisión y Protocolo Internet.

El término **TCP/IP** no es una entidad única que combina dos protocolos, sino un conjunto de programas de software más grande que proporciona servicios de red, como registro de entrada remota, transferencia de archivo remoto y correo electrónico, etc., siendo TCP/IP un método para transferir información de una máquina a otra. Además TCP/IP maneja los errores en la transmisión, administra el enrutamiento y entrega de los datos, así como controlar la transmisión real mediante el uso de señales de estado predeterminado.

b. Requisitos del protocolo TCP/IP[26]

Para poder solucionar los problemas que van ligados a la comunicación de computadores dentro de la red Internet, se tienen que tener en cuenta una serie de particularidades sobre las que ha sido diseñada TCP/IP:

- Los programas de aplicación no tienen conocimiento del hardware que se utilizara para realizar la comunicación (módem, tarjeta de red...).

[26] http://recursostic.educacion.es/usuarios/web/ayudas/54-conexiones-a-internet-bis

- La comunicación no está orientada a la conexión de dos computadoras, eso quiere decir que cada paquete de información es independiente, y puede viajar por caminos diferentes entre dos computadoras.

- La interfaz de usuario debe ser independiente del sistema, así los programas no necesitan saber sobre qué tipo de red trabajan.

- El uso de la red no impone ninguna topología en especial (distribución de los distintos computadores).

De esta forma, dos redes están interconectadas, si hay un computador común que pase información de una red a otra. Además, también una red Internet virtual realizara conexiones entre redes, que ha cambio de pertenecer a la gran red, colaboraran en él trafico de información procedente de una red cualquiera, que necesite de ella para acceder a una red remota. Todo esto independiente de las computadoras que implementen estas funciones, y de los sistemas operativos que estas utilicen.

c. La Estructura de TCP/IP

El modelo de comunicaciones de OSI está definido por siete capas a diferencia del modelo TCP que define cuatro. Véase la relación entre capas en la figura 17.

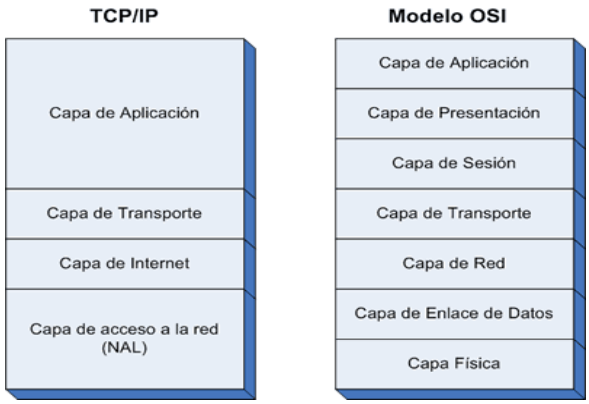

Figura 17. Capas TCP/IP vs OSI
Fuente: http://www.textoscientificos.com/imagenes/redes/tcp-ip-osi.gif

- Capa de aplicación.
- Capa de transporte.

- Capa de red o de internet.
- Capa de enlace o capa de acceso a la red.

d. Descomposición en niveles de TCP/IP

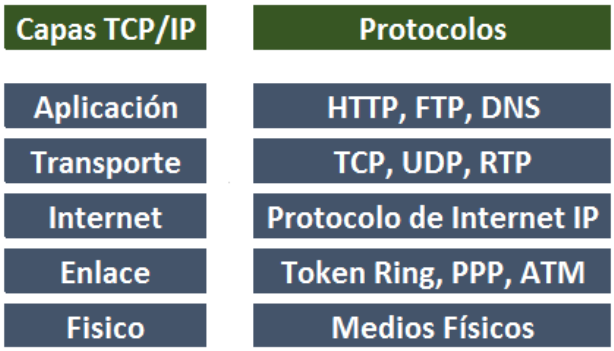

Figura 18. Capas del modelo TCP/IP y sus Protocolos
Fuente: Autores del proyecto

Toda arquitectura de protocolos se descompone en una serie de niveles, usando como referencia el modelo OSI. Esto se hace para poder dividir el problema global en sus problemas de más fácil solución.
A diferencia del OSI, formado por una torre de siete niveles, TCP/IP se descompone en cinco niveles, cuatro niveles software y un nivel hardware. En la figura 18 se describe los niveles software, los cuales tienen cierto paralelismo con el modelo OSI como se mostró en la figura 17.

- **Capa de aplicación**

Constituye el nivel más alto de la torre TCP/IP. Se trata de un nivel simple en el que se encuentran las aplicaciones que acceden a servicios disponibles a través de Internet. Estos servicios están sustentados por una serie de protocolos que los proporcionan. Por ejemplo, se tiene:

- **TELNET.** El programa Telnet [27]proporciona capacidad de registro de entrada remoto. Esto permite a un usuario de una computadora, registrarse en otra computadora, y actuar como si estuviera directamente frente a la segunda computadora. La conexión puede hacerse en cualquier sitio del mundo, siempre y cuando el usuario tenga permiso para registrarse en el sistema remoto.

[27] https://docs.google.com/document/d/1wsT0cGae0nYiN4ZG5rS-tXZ-X202wP_pDDQZqZuTf0/edit

- **FTP.** Protocolo de Transferencia de Archivos. (File Transfer Protocol) permite que un archivo de un sistema se copie a otro sistema. No es necesario que el usuario se registre como usuario completo en la computadora a la que desea tener acceso, como en el caso de Telnet, en vez de ello se puede valer del programa FTP para lograr el acceso.

- **SMTP.** Protocolo Simple de Transferencia de Correo (Simple Mail Transfer Protocol). Se utiliza para transferir correo electrónico. Transparente para el usuario, SMTP conecta distintas computadoras y transfiere mensajes de correo, de una manera similar a como FTP transfiere archivos.

- **Kerberos.** Es un protocolo de seguridad de amplio soporte que utiliza un dispositivo especial conocido como servidor de autenticación. Este revalida contraseñas y esquemas de encriptado. Kerberos es uno de los sistemas de encriptamiento más seguros utilizados en comunicaciones.

- **DNS**. Servidor de Nombre de Dominio. (Domain Name Server). habilita un dispositivo con un nombre común para que sea convertido a una dirección especial de red. Por ejemplo, no se puede tener acceso a un sistema llamado geo_laptop desde una red del otro lado del país, al menos que éste disponible algún método de verificación de los nombres de las computadoras locales. DNS proporciona la conversión del nombre común local a la dirección física única de la conexión de red del dispositivo.

- **SNMP.** Protocolo Simple de Administración de Red**.** (Simple Network Management protocol). Utiliza como mecanismo de transporte el Protocolo de Datagrama de Usuario (UDP). Emplea términos diferentes de TCP/IP, como administradores y agentes en vez de clientes y servidores. Un agente proporciona información sobre un dispositivo, en tanto que el administrador se comunica a través de la red.

- **TFTP**. Protocolo Trivial de Transferencia de Archivos. (Trivial File Transfer Protocol). Es un protocolo muy sencillo, sin complicaciones, que carece totalmente de seguridad.utiliza al UDP como transporte.

- **Capa de transporte**

Este nivel proporciona una comunicación [28]extremo a extremo entre programas de aplicación. La computadora remota recibe exactamente lo mismo que le envió la computadora origen. En este nivel el emisor divide la información que recibe del nivel de aplicación en paquetes, le añade los datos necesarios para el control de

[28] https://docs.google.com/document/d/1wsT0cGae0nYiN4ZG5rS-tXZ-X202wP_pDDQZqZuTf0/edit

flujo y control de errores, y se los pasa al nivel de red junto con la dirección de destino.

En el receptor este nivel se encarga de ordenar y unir las tramas para generar de nuevo la información original.

Para implementar el nivel de transporte se utilizan dos protocolos:

UDP. El protocolo UDP (User Datagram Protocol) está orientado a transacciones pero a lo contrario del TCP no está orientado a la conexión y no tiene fiabilidad ninguna, como el protocolo IP, no garantiza de que los datagramas lleguen a su destino ni que lleguen ordenadamente. No abarca ningún tipo de control de errores ni de flujo, cuando se detecta un error en uno de sus datagramas se elimina pero no se notificará su extravío. La aplicación que se apoye en este protocolo deberá tener en cuenta de que toda información que se le envía no debe ser imprescindible para su funcionamiento, por lo tanto, normalmente se utilizará para enviar mensajes relativamente cortos y no cruciales.

Es un protocolo del tipo best-effort porque hace todo lo que puede para transmitir los datagramas, de forma más óptima que el TCP, pero en contra no garantiza que lleguen a su destino, lleguen duplicados o desordenados.

Además, cada datagrama UDP pueden procesarse independientemente de los datagramas que le siguen. En el caso de una conexión TCP desde que recibe el primer datagrama deberá quedarse paralizado sin procesar los datagramas hasta que no le llegue la respuesta de confirmación de recepción completa por parte de la computadora remota.

Los mensajes UDP son más rápidos, todo lo que se envía llega junto al destino. Pero si no llega tampoco dejará al equipo remoto a la espera de que llegue y por lo tanto irá procesando los mensajes que vaya recibiendo sin que los que se pierdan sean cruciales para su funcionamiento. Utilizan aplicaciones como NFS y RPC, pero sobre todo se emplea en tareas de control.

TCP. Es el Protocolo de Control de Transporte. (Transport Control Protocolo). Es el protocolo que proporciona un transporte fiable de flujo de bits entre aplicaciones. Está pensado para poder enviar grandes cantidades de información de forma fiable, liberando al programador de aplicaciones de la dificultad de gestionar la fiabilidad de la conexión (retransmisiones, pérdidas de paquete, orden en que llegan los paquetes, duplicados de paquetes...) que gestiona el propio protocolo. Pero la complejidad de la gestión de la fiabilidad tiene un coste en eficiencia, ya que para llevar a cabo las gestiones anteriores se tiene que añadir bastante información a los paquetes a enviar. Debido a que los paquetes a enviar tienen un tamaño máximo, como más información añada el protocolo para su gestión, menos información que proviene de la aplicación podrá contener ese

paquete. Por eso, cuando es más importante la velocidad que la fiabilidad, se utiliza UDP, en cambio TCP asegura la recepción en destino de la información a transmitir.

- **Capa de red**[29]

También recibe el nombre de nivel Internet. Coloca la información que le pasa el nivel de transporte en datagramas IP, le añade cabeceras necesarias para su nivel y lo envía al nivel inferior. En este nivel se emplea el algoritmo de encaminamiento, al recibir un datagrama del nivel inferior decide, en función de su dirección, si debe procesarlo y pasarlo al nivel superior, o bien encaminarlo hacia otra computadora.

Para implementar esta capa se utilizan los siguientes protocolos:

- **IP** (Internet Protocol): es un protocolo no orientado a la conexión, con mensajes de un tamaño máximo. Cada datagrama se gestiona de forma independiente, por lo que dos datagramas pueden utilizar diferentes caminos para llegar al mismo destino, provocando que lleguen en diferente orden o bien duplicados. Es un protocolo no fiable, eso quiere decir que no corrige los anteriores problemas, ni tampoco informa de ellos. Este protocolo recibe información del nivel superior y le añade la información necesaria para su gestión (*direcciones IP, checksum*).

- **ICMP** (*Internet Control Message Protocol*). Proporciona un mecanismo de comunicación de información de control y de errores entre computadoras intermedias por las que viajaran los paquetes de datos. Estos datagramas los suelen emplear las computadoras (gateways, host,...) para informarse de condiciones especiales en la red, como la existencia de una congestión.

  Se utiliza por las siguientes razones:

  - ✓ Cuando no se puede enviar mensajes.
  - ✓ Para que los routers encaminen el tráfico de los paquetes por rutas más cortas.
  - ✓ Cuando un router no dispone de suficiente memoria para almacenar paquetes recibidos que esperan se notifique al propietario de los paquetes del problema.

  Para deshacerse de los paquetes que permanecen demasiado tiempo en la red, la existencia de errores y las posibles peticiones de cambios de ruta. Los mensajes de ICMP están encapsulados en datagramas IP.

[29] http://rinalo.tripod.com/paginaTE/capas_protocolo.html

- **IGMP** (*Internet Group Management Protocol*). Este protocolo está íntimamente ligada a IP. Se emplea en computadoras que utilizan IP multicast. El IP multicast es una variante de IP que permite emplear datagramas con múltiples destinatarios.

  También en este nivel tiene una serie de protocolos que se encargan de la resolución de direcciones.

- **ARP.** (*Address Resolution Protocol*). [30]Cuando una computadora desea ponerse en contacto con otra conoce su dirección IP, entonces necesita un mecanismo dinámico que permite conocer su dirección física. Entonces envía una petición ARP por broadcast (o sea a todas las computadoras). El protocolo establece que solo contestará a la petición, si ésta lleva su dirección IP. Por lo tanto, solo contestará la computadora que corresponde a la dirección IP buscada, con un mensaje que incluya la dirección física. El software de comunicaciones debe mantener una cache con los pares IP-dirección física. De este modo la siguiente vez que hay que hacer una transmisión a esa dirección IP, ya se conoce la dirección física.

- **RARP.** (*Reverse Address Resolution Protocol*). A veces el problema es al revés, o sea, una computadora solo conoce su dirección física, y desea conocer su dirección lógica. Esto ocurre, por ejemplo, cuando se accede a Internet con una dirección diferente, en el caso de PC que acceden por módem a Internet, y se le asigna una dirección diferente de las que tiene el proveedor sin utilizar. Para solucionar esto se envía por broadcast una petición RARP con su dirección física, para que un servidor pueda darle su correspondencia IP.

- **BOOTP.** (*Bootstrap Protocol*). El protocolo RARP resuelve el problema de la resolución inversa de direcciones, pero para que pueda ser más eficiente, enviando más información que meramente la dirección IP, se ha creado el protocolo BOOTP.

- **IPX.** El protocolo de Novell para el encaminamiento de paquetes.

- **Capa de enlace**[31]

Este nivel se limita a recibir datagramas del nivel superior (nivel de red) y transmitirlo al hardware de la red. Pueden usarse diversos protocolos: DLC (IEEE 802.2), Frame Relay, X.25, etc.

[30] https://es.wikipedia.org/wiki/Protocolo_de_resoluci%C3%B3n_de_direcciones
[31] http://www.edu.xunta.es/centros/iesfelixmuriel/system/files/IP_m%C3%A1scara_Red.pdf

La interconexión de diferentes redes genera una red virtual en la que las computadoras se identifican mediante una dirección de red lógica. Sin embargo, a la hora de transmitir información por un medio físico se envía y se recibe información de direcciones físicas. Un diseño eficiente implica que una dirección lógica sea independiente de una dirección física, por lo tanto es necesario un mecanismo que relacione las direcciones lógicas con las direcciones físicas. De esta forma se cambia la dirección lógica IP conservando el mismo hardware, se cambia una tarjeta de red, la cual contiene una dirección física, sin tener que cambiar la dirección lógica IP.

El conjunto de protocolos TCP/IP ha sido de vital importancia para el desarrollo de las redes de comunicación, sobre todo para Internet. El ritmo de expansión de Internet también es una consecuencia de estos protocolos, sin los cuales, conectar redes de distintas naturalezas (diferente Hardware, sistema operativo, etc.), hubiera sido mucho más difícil, por no decir imposible. Así pues, se puede decir que los protocolos TCP/IP fueron y son el motor necesario para que las redes en general, e Internet en particular.

e. Medios de transmisión

La capa física determina el soporte físico o medio de transmisión por el cual se transmiten los datos. Estos medios de transmisión se clasifican en *guiados* y *no guiados.*

En el diseño de sistemas de transmisión es deseable que tanto la distancia como la velocidad de transmisión sean lo más grandes posibles. Hay una serie de factores relacionados con el medio de transmisión y con la señal que determinan tanto la distancia como la velocidad de transmisión:

- **El ancho de banda:** si todos los otros factores se mantienen constantes, al aumentar el ancho de banda de la señal, la velocidad de transmisión se puede incrementar.
- **Dificultades en la transmisión:** las dificultades, como, por ejemplo, la atenuación, limitan la distancia. En los medios guiados, el par trenzado sufre de mayores adversidades que el cable coaxial, que a su vez, es más vulnerable que la fibra óptica.

- **Interferencias:** las interferencias resultantes de la presencia de señales en bandas de frecuencias próximas pueden distorsionar o destruir completamente la señal. Las interferencias son especialmente relevantes en los medios no guiados, pero a la vez son un problema a considerar en los medios guiados.

- **Número de receptores:** un medio guiado se puede usar tanto para un enlace punto a punto como para un enlace compartido, mediante el uso de múltiples

conectores. En este último caso, cada uno de los conectores utilizados puede atenuar y distorsionar la señal, por lo que la distancia y/o la velocidad de transmisión disminuirá.

- **Medios de transmisión guiados**[32]

Son aquellos que utilizan un medio sólido (un cable) para la transmisión En los medios de transmisión guiados, la capacidad de transmisión, en términos de velocidad de transmisión o ancho de banda, depende drásticamente de la distancia y de si el medio se emplea para un enlace punto a punto o por el contrario para un enlace multipunto, como, por ejemplo, en redes de área local (LAN).

Par trenzado: un par de cables trenzados es un par de alambre que se cruzan o trenzan entre sí para minimizar la interferencia electromagnética entre los pares de cables. Cada par de cables conforman un enlace para transmisión de señales de datos completos. El flujo de corrientes produce campos electromagnéticos que pueden introducir ruido a los pares vecinos. De todos modos los campos correspondientes a cada par de cables tienen polaridades opuestas. Trenzando los cables entre sí, los campos magnéticos de cada uno se cancelan mutuamente, lo cual minimiza el ruido y/o la interferencia generada por cada par de cables.

El par trenzado es el medio guiado más económico y a la vez más usado. En la figura 19 se puede observar claramente el Cable Par Trenzado.

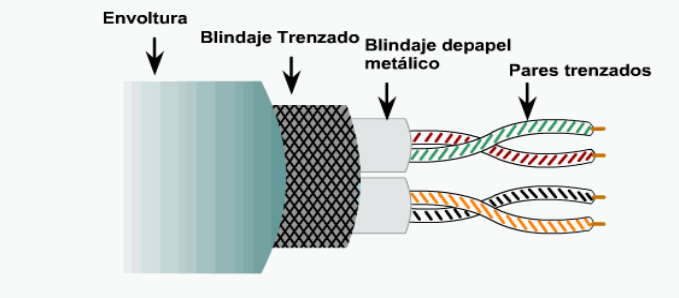

Figura 19. Cable de par trenzado
Fuente: http://2.bp.blogspot.com/-0vfYa4bZcRA/TsKy_oSOzxI/AAAAAAAAAAc/A8w6QXMfrcA/s1600/Image42.gif

Descripción física: el par trenzado consiste en dos de cables de cobre embutidos en un aislante, entrecruzados en forma de espiral. Cada par de cables constituye

[32] http://e.se-todo.com/doc/4910/index.html?page=5

sólo un enlace de comunicación. Normalmente, se utilizan haces en los que se encapsulan varios pares mediante una envoltura[33] protectora. En aplicaciones de larga distancia, la envoltura puede contener cientos de pares. El uso del trenzado tiende a reducir las interferencias electromagnéticas (diafonía) entre los pares adyacentes dentro de una misma envoltura. Para este fin, los pares adyacentes dentro de una misma envoltura protectora se trenzan con pasos de torsión diferentes. Para enlaces de larga distancia, la longitud del trenzado varía entre 5 y 15 cm. Los conductores que forman el par tienen un grosor que varía entre 0,4 y 0,9 mm. La impedancia característica del mismo es de 10 Ohms y la longitud máxima de cada segmento de 100m. Para el caso de datos de los cuatro pares posibles se usan 2, uno para la transmisión y otro para recepción, quedando dos libres.

Aplicaciones: generalmente, los pares trenzados se utilizan para las conexiones al conmutador digital o a la PBX digital (PBX, Private Branch Exchange), con velocidades de 64 kbps. El par trenzado se utiliza también en redes de área local dentro de edificios para la conexión de computadores personales. La velocidad típica en esta configuración está en torno a los 10 Mbps. No obstante, recientemente se han desarrollado redes de área local con velocidades entre 100 Mbps y 1 Gbps mediante pares trenzados, aunque estas configuraciones están bastante limitadas por el número de posibles dispositivos conectados y extensión geográfica de la red. Para aplicaciones de larga distancia, el par trenzado se puede utilizar a velocidades de 4 Mbps o incluso mayores.

Características de transmisión: los cables de pares se pueden usar para transmitir tanto señales analógicas como señales digitales. Para señales analógicas, se necesitan amplificadores cada 5 o 6 km. Para transmisión digital (usando tanto señales analógicas como digitales), se requieren repetidores cada 2 o 3 km.

Pares trenzados blindados y sin blindar:

Figura 20. Cables STP y UTP
Fuente: http://ti-prosoft.com/Docslink/Analisisred.pdf

33 http://www.profesores.frc.utn.edu.ar/electronica/ElectronicaAplicadaIII/PlantelExterior/Introducables

Hay dos variantes de pares trenzados: blindado y sin blindar. El par trenzado no blindado (UTP, Unshielded Twisted Pair) es el medio habitual en telefonía. No obstante, actualmente es práctica habitual en el cableado de edificios, muy por encima de las necesidades reales de telefonía. Esto es así ya que hoy por hoy, el par sin blindar es el menos caro de todos los medios de transmisión que se usan en las redes de área local, además de ser fácil de instalar y de manipular. El par trenzado sin blindar puede ser afectado por interferencias electromagnéticas externas, incluyendo interferencias con pares cercanos y fuentes de ruido. Una manera de mejorar las características de transmisión de este medio es embutiéndolo dentro de una malla metálica, reduciéndose así las interferencias.
Una variación de este cable es el que se conoce como STP (Shield twisted pair).que es el mismo cable UTP pero con blindaje externo, generalmente un papel de aluminio. Si bien puede disminuir aún más la interferencia obliga a tener un sistema de masas donde en ningún caso existan más de 3 Ohms entre los conectores y la masa del sistema. El STP proporciona mejores resultados a velocidades de transmisión bajas. Ahora bien, este último es más costoso y difícil de manipular que el anterior.

En la figura 20 se muestra tanto el Cable UTP como el Cable STP con sus respectivas características.

UTP Categoría 5e y categoría 6: en la mayoría de los edificios se hace una pre-instalación con un par trenzado de 100 ohmios denominado calidad telefónica («voice-grade»). Por tanto, este tipo de reinstalaciones se debe considerar siempre como una alternativa bastante atractiva y poco costosa para las LAN.

No obstante, hay que tener en cuenta que las velocidades de transmisión y las distancias que se pueden alcanzar con este medio no siempre cubren las necesidades típicas. En 1991, la EIA (Electronic Industries Association) publicó el estándar EIA-568, denominado «Commercial Building Telecommunications Cabling Standard», que define el uso de pares trenzados sin blindar de calidad telefónica y de pares blindados como medios para aplicaciones de transmisión de datos en edificios, como se puede observar en la figura 21. Por aquel tiempo, las características de dichos medios eran suficientes para el rango de frecuencias y velocidades típicas necesarias en entornos ofimáticas. Es más, en esa época el objetivo diseño en las LAN tenía velocidades de transmisión comprendidas entre 1 y 16 Mbps. Con el tiempo, los usuarios han migrado tanto a estaciones de trabajo como a aplicaciones de mayores prestaciones. Como consecuencia, ha habido un interés creciente en las LAN que proporcionen hasta 100 Mbps sobre medios no costosos. Como respuesta a esa necesidad, en 1995 se propuso el EIA-568A. En esta especificación se consideran tanto cables de pares blindados a 150 ohms como pares no blindados de 100 ohms.

En el estándar EIA-568-A se consideran tres tipos o categorías de cables UTP:

- **CAT. 1:** utilizado para líneas telefónicas ya que únicamente soporta voz.

- **CAT. 2:** puede transportar datos hasta 4Mbps. Utilizado para LocalTalk.

- **CAT. 3:** transmisión de datos de hasta 10Mbps. Utilizado para Ethernet. Por lo general cuenta con cuatro pares de hilos.

- **CAT. 4:** transmisión de datos de hasta 20Mbps o 16Mbps en Token Ring. Por lo general, el cable tiene cuatro pares de hilos. Este grado de UTP no es frecuente.

- **CAT. 5:** [34]transmisión de datos de hasta 100Mbps. Utilizado en Fast Ethernet. Por lo general, el cable tiene cuatro pares de hilos de cobre y tres trenzados por pie. El cable UTP de categoría 5 es el tipo de cable que más se utiliza en instalaciones nuevas.

- **CAT. 5e:** es una categoría 5 mejorada. Minimiza la atenuación y las interferencias. Esta categoría no tiene estandarizadas las normas aunque si esta diferenciada por los diferentes organismos. Está definido para un ancho de banda de 1 a 250 MHz.

- **CAT. 6:** esta estandarizada y actualmente se está utilizando. Se definen sus características para un ancho de banda de 250 MHz.

- **CAT. 7:** no está definida y mucho menos estandarizada. Se definen para un ancho de banda de 600 MHz.

De entre los anteriores, CAT. 5e y 6 son los más utilizados en los entornos LAN.

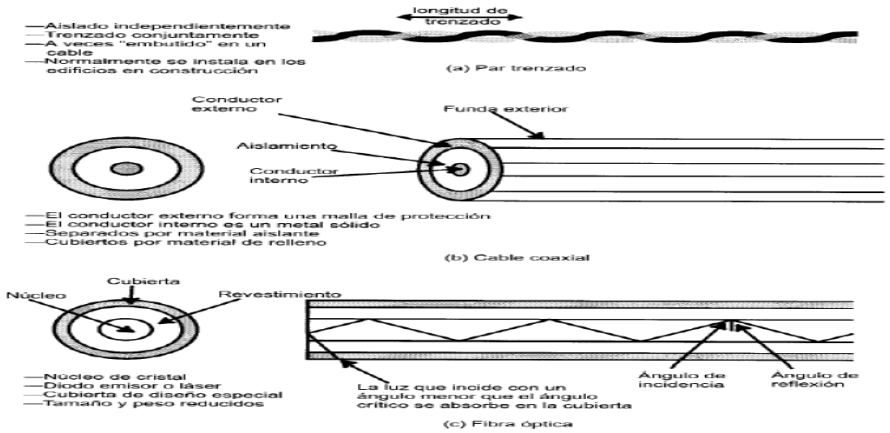

Figura 21. Medios de transmisión guiados

34 Fuente: http://ti-prosoft.com/Docslink/Analisisred.pdf

http://www.profesores.frc.utn.edu.ar/electronica/ElectronicaAplicadaIII/PlantelExterior/Introducables

CAT. 3 corresponde a los cables de calidad telefónica que existen en la mayoría de las edificaciones.

Con un diseño apropiado y a distancias limitadas, con cables CAT. 3 se pueden conseguir velocidades de hasta 16 Mbps. El CAT. 5 («data-grade») es un cable de mejores características para la transmisión de datos, y cada vez se está utilizando más y más como pre-instalación en los nuevos edificios de reciente construcción. Con un diseño apropiado y a distancias limitadas, con CAT. 5 se pueden alcanzar 100 Mbps.

La diferencia esencial entre los cables CAT. 3 y 5 están en el número de trenzas por unidad de distancia. La longitud de la trenza en el CAT. 5 es del orden de 0,6 a 0,85, 71 cm., mientras que el CAT. 3 tiene una trenza de 7,5 o 10 cm. El trenzado del CAT. 5 es por supuesto más caro, ahora bien proporciona prestaciones superiores que el de CAT. 3.Los cables: UTP CAT. 3 y UTP CAT. 5, así como el cable STP especificado en el EIA-568-A.

El primer parámetro para establecer la comparativa es la atenuación. La energía de la señal decrece con la distancia recorrida en el medio de transmisión. En medios guiados la atenuación obedece a una ley logarítmica, por tanto, se expresa como un número constante de decibelios por unidad de longitud.

Como se puede observar en la figura 22 la comparación entre par trenzados

		Atenuación (dB por 100 m)			Diafonía en el extremo final (dB)		
	Frecuencia (MHz)	UTP tipo 3	UTP tipo 5	STP 150 ohmios	UTP tipo 3	UTP tipo 5	STP 150 ohmios
	1	2,6	2,0	1,1	41	62	58
	4	5,6	4,1	2,2	32	53	58
	16	13,1	8,2	4,4	23	44	50,4
	25	-	10,4	6,2	-	41	47,5
	100	-	22,0	12,3	-	32	38,5
	300	-	-	21,4	-	-	31,3

Figura 22. Comparación de pares trenzados
Fuente: http://ti-prosoft.com/Docslink/Analisisred.pdf

La diafonía que sufren los sistemas basados en pares trenzados es debida a la inducción que provoca un conductor en otro cercano. Por conductor debe entenderse tanto los pares que forman el cable, como los «pines» (patillas metálicas) del conector.

Este tipo de diafonía se denomina cercana al extremo porque la señal transmitida en el enlace se acopla en un conductor cercano e induce una señal en sentido contrario (es decir, la energía transmitida es capturada por un par de recepción).

El UTP CAT 5 es un cable diseñado específicamente para la transmisión de datos y se basa en pares de alambres de cobre de 0.5mm de diámetro, retorcidos mediante una hélice en sentido antihorario y una vuelta de 5 a15 cm.(a mayor cantidad de vueltas por cm. es de mayor calidad, pero también más difícil de manipular).

3.3.3.8 Elementos para el cableado de red:

a. Elementos pasivos

- **Cable**

A la hora de elegir el cable a usar, habrá que tener en cuenta:

- Cuántos equipos hay que conectar
- Su distribución física: distancia que los separa, si están en el mismo edificio o en varios.
- El ancho de banda que se necesite.
- La existencia de redes ya montadas o de equipos con tarjetas de red aprovechables.
- Las condiciones ambientales de los edificios: temperaturas, humedad, etc.

El cable UTP está compuesto por cuatro pares de hilos trenzados, individualmente y entre ellos con un ciclo de trenzado de menos de 38 mm, como se muestra en la figura 23.

El hilo usado es de 0'5 mm y está indicado para ser utilizado a temperaturas entre 10ºC a 60ºC. Los colores con los que se identifican cada uno de los pares, son:

- Par 1: blanco – azul / azul
- Par 2: blanco - naranja / naranja
- Par 3: blanco – verde / verde
- Par 4: blanco – café / café

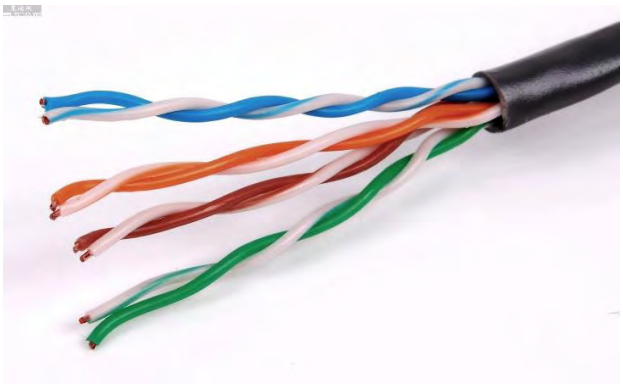

Figura 23. Cable UTP CAT. 6
Fuente: http://image.made-in-china.com/2f0j00GSNQYJlnLgqy/4-Pairs-CAT6-UTP-Cable-Panduit-Cable.jpg

- **Rosetas**

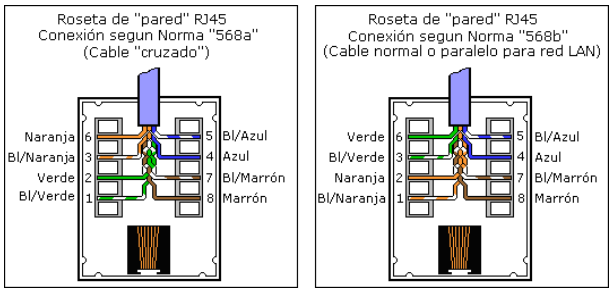

Figura 24. Rosetas RJ-45
Fuente: http://www2.configurarequipos.com/imgdocumentos/codigocolorescablesred/7.gif

En el mercado existen varios tipos de muestra de ello se puede visualizar en la figura 24.

Habrá que vigilar a la hora de escoger cualquiera de ellas, que cumplan con la reglamentación y la mejor forma de hacerlo es comprobar que sea de categoría 5e. La mayoría necesitan de herramientas adicionales para su conexionado.

- **Conectores**

Figura 25. Conectores RJ-45
Fuente:
http://micompusa.com/image/cache/data/Conector%20rj%2045-600x600.jpg

Es importante saber que en el mercado existen conectores de varias calidades y que en muchos casos, un mal contacto producido por un mal conector, puede bajar el rendimiento de una LAN, en la figura 25 se muestra la Fotografía del conector.

Se pueden destacar las siguientes características:

- La calidad de sus contactos es alta.

- El conector tiene una capucha para la sujeción final del cable, que ayuda a hacer más solidario el cable al conector.

- Dispone de un contacto de tierra para conseguir más protección de datos ante interferencias externas.

- **Canaletas**

Las canaletas hay de dos cavidades con un tabique central para poder separar en dos grupos los cables que van por su interior, véase en la siguiente figura 26.

- **Patch cord (cable de enlace)**

Se le llama Patch Cord al cable (UTP, FO, etc.) que se usa en una red para conectar un dispositivo electrónico con otro, obsérvese en la figura 27.

Figura 26. Patch cord para cable UTP
Fuente. http://4.bp.blogspot.com/_3N-vMzD6cZM/TU2A2VXcJNI/AAAAAAAAABk/S37ZGq8IaII/s1600/PART+CORD.jpg

Figura 27. Canaletas
Fuente: http://www.eletroamerica.com.br/images/canaletas-e-acessorios/qdro_dutopiso.jpg

- **Patch panel**

Conocido también como Centro de empalme, es el lugar donde llegan todos los cableados para conexión a la infraestructura de Red. Como se puede apreciar en la figura 28.

Figura 28. Patch Panel
Fuente: http://es.excel-networking.com/_assets/images/Cat6A_PreTerm_0005.jpg

b. Elementos activos

Los constituyen todos los equipos mencionados en la sección siguiente de este capítulo.

3.3.3.9 DNS. Un servidor DNS[35] sirve para transformar la IP de un servidor web en un dominio. Para que se pueda entender que es un servidor DNS, se explica mediante la figura 29, como se compone la estructura de Internet para una página web cualquiera:

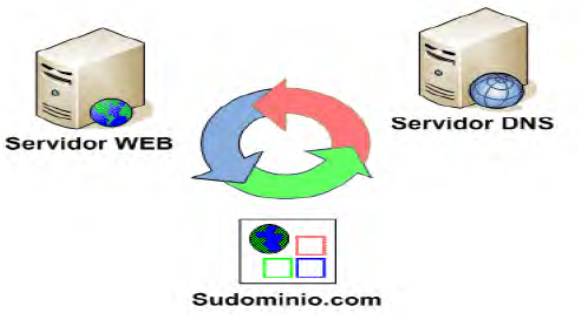

Figura 29. Estructura de Internet
Fuente: http://ti-prosoft.com/Docslink/Analisisred.pdf

[35] https://blog.smaldone.com.ar/2006/12/05/como-funciona-el-dns/

Como se puede ver en la figura 29, existen tres elementos indispensables en Internet para que ésta sea posible.

- **Servidor web:** es un servidor que está acondicionado para servir páginas web las 24 horas del día.

- **Dominio:** es el nombre con el cual la gente busca en Internet, al escribir en la barra de direcciones del navegador.

- **Servidor DNS:** es el encargado de transformar la IP de un servidor web, en el nombre del dominio.

El funcionamiento[36] es el siguiente: Cuando se escribe por ejemplo, systemplusdetuquerres.com.co en la barra del explorador, este realiza la consulta en Internet de cómo está configurado este dominio. El servidor DNS le indica a nuestro explorador que tiene que ir a buscar la información de la página web a la IP del servidor web.

Figura 30. Funcionamiento del servidor DNS
Fuente: http://ti-prosoft.com/Docslink/Analisisred.pdf

El explorador envía la petición de la página web al servidor web, indicándole el nombre del dominio que desea. El servidor web sirve la página web y el explorador la muestra. Todo esto pasa en cuestión de milésimas de segundo, para hacerse una idea mejor ver la figura 30 y 31, se da una pequeña explicación del funcionamiento del Servidor DNS.

[36] https://blog.smaldone.com.ar/2006/12/05/como-funciona-el-dns/

Figura 31. Funcionamiento del servidor DNS
Fuente: http://ti-prosoft.com/Docslink/Analisisred.pdf

3.3.3.10 Servicios de internet. Las posibilidades que ofrece Internet se denominan servicios. Cada servicio es una manera de sacarle provecho a la Red independiente de las demás.

Una persona podría especializarse en el manejo de sólo uno de estos servicios sin necesidad de saber nada de los otros. Sin embargo, es conveniente conocer todo lo que puede ofrecer Internet, para poder trabajar con lo que más interese. En la actualidad, los servicios más usados en Internet son: Correo Electrónico, World Wide Web, FTP, Grupos de Noticias, Chats, Servicios de Telefonía, Redes Sociales.

3.3.3.11 Antivirus. Hoy en día, el uso de un software antivirus es tan importante que nadie debería atreverse a utilizar una computadora sin la protección de este software para mayor seguridad.

El software antivirus intenta cubrir las principales formas de ataque a un computador. Las consecuencias que suelen ocurrir después de un ataque pueden ser graves.

Un antivirus actúa de la siguiente forma:

- Inspecciona (Scan) todos los e-mail que se reciben en la computadora y busca virus para remover.

- Monitoriza los archivos de la computadora a medida que van siendo abiertos o creados para garantizar que no estén infectados. Esta es una protección en tiempo real, que puede afectar el computador.

- Inspecciona periódicamente todo el computador para verificar si existen archivos corruptos y remover los virus existentes.

El servicio de protección de antivirus está gestionado de manera corporativa, para lo cual se debe instalar en el servidor y en cada una de los clientes una aplicación antivirus y antispam.

Las actualizaciones de las definiciones de virus se realizan diariamente en el servidor y los usuarios automáticamente en el momento de iniciar una sesión.

3.3.3.12 Seguridad. Se toma en cuenta tanto la seguridad física de los equipos como de la seguridad de la información que circula en la Red o se almacena en los diferentes repositorios como son bases de datos, estaciones de trabajo, impresoras, etc.

- **Seguridad física.** Para la seguridad física de los equipos la Institución cuenta con un vigilante quien brinda resguardo las 24 horas.

Para complementar la seguridad física se recomienda:

- **Seguridad de la Información.** Otro punto de seguridad es el que ese refiere a la seguridad de la información, tanto la almacenada en el servidor y las PCs. Como la que circula por el canal de la Red.

- **Seguridad para el acceso a internet.** Se recomienda utilizar listas de acceso o ACL, en las cuales se define el orden de navegación y las redes que están autorizadas para navegar por Internet, además de mantener filtros de contenidos y direcciones Web (URL).

- **Seguridad en el router.** El Router[37] es un equipo que une la red local con el Internet, por esta razón, se constituye en el primer filtro de seguridad desde el Internet hacia la Red Local; para ello se deben declarar ACL's, en las cuales se configuran para que en las redes estén permitidas el tráfico; los protocolos y puertos que se pueden utilizar para la transmisión de información.

[37] http://datateca.unad.edu.co/contenidos/CCNA4/ARCHIVOS/MODULO%20CCNA4%20EXPLORATION.pdf

3.3.3.13 Red inalámbrica:

a. Introducción

En los últimos años se ha producido un crecimiento espectacular en lo referente al desarrollo y aceptación de las comunicaciones móviles y en concreto de las redes inalámbricas de área local (WLANs). La función principal de este tipo de redes es la de proporcionar conectividad y acceso a las tradicionales redes cableadas (Ethernet, Token Ring...), como si de una extensión de éstas últimas se tratara, pero con la flexibilidad y movilidad que ofrecen las comunicaciones inalámbricas. El momento decisivo para la consolidación de estos sistemas fue la conclusión del estándar IEEE 802.11 en 1997.

En este estándar se encuentran las especificaciones técnicas que se deben tener en cuenta a la hora de implementar una red de área local inalámbrica WLAN.

Las redes inalámbricas de área local se diferencian de las redes de área local tradicionales en que los terminales no están interconectados físicamente mediante un cable, sino que se utilizan ondas de radio para este fin. Esto es posible, en gran parte, a que los organismos internacionales que establecen el reparto de las frecuencias han dejado libres varias franjas para uso personal o privado. Estas frecuencias son usadas, por ejemplo, por teléfonos fijos inalámbricos, walkie-talkies etc. En cambio y en contra de lo que se piensa comúnmente, los aficionados a la radio-afición cuentan con unas frecuencias por las que tienen que abonar unos cánones.

Desde hace poco, existe una nueva tecnología que hace uso de las frecuencias libres de licencia: las redes de área local inalámbricas o redes Wireless. Las LAN inalámbricas utilizan básicamente longitudes de onda correspondientes a las microondas (2,4 GHz y 5 GHz) y permiten tener anchos de banda apreciables (desde 1 MB/s en las primeras versiones hasta llegar a los 54 MB/s de los últimos estándares).

También es verdad que aunque la banda alrededor de los 5 GHz es abierta en todo el mundo, el ancho de banda que se puede ocupar depende de la situación particular que haya impuesto cada legislador. Es por ello que en Europa se pueden utilizar hasta 455 MHz, mientras que en Norteamérica el ancho de banda se restringe a 300 MHz y en Japón a 100 MHz.

En muchos sitios, las redes Ethernet de cable tradicional han sido ampliadas con la implantación de este tipo de redes inalámbricas. La interconexión de varias redes locales (como por ejemplo en el caso de redes inalámbricas que se extienden en todo el campus universitario) ha propiciado que algunos visionarios hayan visto la posibilidad de crear una red metropolitana con gran ancho de banda y con la posibilidad de acceso a Internet, de forma que se pudiera acceder a

cualquier servicio de los que comúnmente se utilizan en Internet (correo, web, ftp, etc.) desde cualquier lugar dentro del ámbito metropolitano. La figura 32 muestra una red inalámbrica.

Figura 32. Red inalámbrica
Fuente: http://www.citypassenger.com/wp-content/uploads/2014/10/WIFICENTRAL-en2.png

b. Componentes y topologías de una red inalámbrica

Una red local 802.11 está basada en una arquitectura celular donde el sistema está dividido en células, denominadas Conjunto de Servicios Básicos (BSS), y cada una de estas células está controlada por una estación base denominada Punto de Acceso (AP)[38].

Aunque una red Wireless puede estar formada por una única célula (incluso sin utilizar un punto de acceso), normalmente se utilizan varias células, donde los puntos de accesos estarán conectados a través de un Sistema de Distribución (DS), generalmente Ethernet y en algunos casos sin usar cables.

La red Wireless completa, incluyendo las diferentes células, sus puntos de acceso y el sistema de distribución, puede verse en las capas superiores del modelo OSI como una red 802 clásica, y es denominada en el estándar como Conjunto Extendido de Servicios (ESS).

La siguiente figura muestra una red 802.11 clásica, con los componentes descritos previamente:

[38] http://ieeestandards.galeon.com/aficiones1573328.html

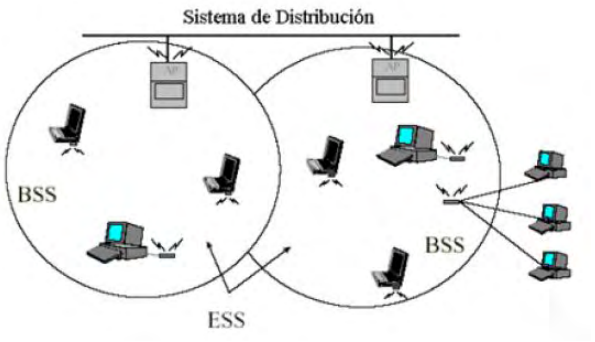

Figura 33. Sistema de distribución
Fuente: http://ti-prosoft.com/Docslink/Analisisred.pdf

c. Topologías

Existen dos modos diferentes de operación para los dispositivos 802.11: Ad Hoc (Juego de Servicios Independientes Básicos- Independent Basic Service Set, IBSS) o Infraestructura (Juego de Servicios Extendidos, ESS)[39].

Una red Ad Hoc es usualmente aquella que existe por un tiempo limitado entre dos o más dispositivos inalámbricos que no están conectados a través de un punto de acceso (Access Point - AP) a una red cableada.

Por ejemplo, dos usuarios de laptop que deseen compartir archivos podrían poner una red ad hoc usando NICs compatibles con 802.11 y compartir archivos a través del medio inalámbrico (WM) sin la necesidad de usar medios externos (por ejemplo discos floppy, tarjetas flash). Véase figura 34.

Figura 34. Red Ad Hoc
Fuente: http://lh6.ggpht.com/-B5lv_ZkocBg/UXwZRkAj6GI/AAAAAAAAA8E/h1h-VHNzi1Y/Rede%252520Ad%252520Hoc_thumb%25255B3%25255D.png?imgmax=800

[39] http://ieeestandards.galeon.com/aficiones1573328.html

El modo de Infraestructura asume la presidencia de uno o más APs puenteando el medio inalámbrico al medio cableado. El AP maneja la autentificación de la estación y la asociación con la red inalámbrica. Múltiples APs conectados por un sistema de distribución (DS) puede extender el alcance de la red inalámbrica a un área mucho mayor de la que puede ser cubierta por un solo AP. En instalaciones típicas, el DS es simplemente la infraestructura de la red IP existente. Para propósitos de seguridad, LANs virtuales (VLANs) son usadas con frecuencia para segregar el tráfico inalámbrico de otro tráfico en el DS. Aunque 802.11 permite que las estaciones inalámbricas conmuten de forma dinámica la asociación de un punto de acceso a otro (tal sería el caso de un usuario de un PDA caminando a través de un campus), no gobierna como esto deberá ser logrado.

Figura 35. Infraestructura BSS
Fuente: http://4.bp.blogspot.com/-FKQJrHX_nx4/TpkUeCmVudI/AAAAAAAAACs/EI7HGmVnKv0/s1600/adhoc1.jpg

Como resultado de esto, las implementaciones de los diferentes vendedores son incompatibles en este sentido, así como por ejemplo tiene la figura 35.

Dentro de los PAs (actualmente ya se puede comenzar a aplicar también a los TRs) se puede modificar enormemente la capacidad de TX/RX gracias al uso de antenas especiales. Estas antenas se pueden dividir en:

- Direccionales
- Omnidireccionales

Las antenas Direccionales envían la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se escucha nada, no se puede establecer comunicación entre los interlocutores.

Las antenas Omnidireccionales envían la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales.

d. Estándares y procesos de desarrollo de la IEEE

IEEE es uno de los fabricantes de estándares líder en el mundo. La IEEE desarrolla sus estándares trabajando a través de la asociación de estándares IEEE-SA. Los estándares IEEE afectan a las industrias de alto rango incluyendo energía, biomédica, salud, información, telecomunicaciones transportes, nanotecnologías y muchas otras.

En el 2005, IEEE tenía cerca de 900 estándares activos, con 500 estándares en desarrollo. Uno de los estándares IEEE más notables es el IEEE 802 LAN/MAN grupo de estándares que incluye el estándar IEEE 802.3 Ethernet y el estándar IEEE 802.11 para redes inalámbricas.

- **IEEE 802.11 - wireless networking**

El protocolo IEEE 802.11 o WI-FI [40]es un estándar de protocolo de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.

La familia 802.11 actualmente incluye seis técnicas de transmisión por modulación que utilizan todos los mismos protocolos. El estándar original de este protocolo data de 1997, era el IEEE 802.11, tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2,4 GHz. En la actualidad no se fabrican productos sobre este estándar. El término IEEE 802.11 se utiliza también para referirse a este protocolo al que ahora se conoce como "802.11legacy." La siguiente modificación apareció en 1999 y es designada como IEEE 802.11b, esta especificación tenía velocidades de 5 hasta 11 Mbps, también trabajaba en la frecuencia de 2,4 GHz. También se realizó una especificación sobre una frecuencia de 5 Ghz que alcanzaba los 54 Mbps, era la 802.11a y resultaba incompatible con los productos de la b y por motivos técnicos casi no se desarrollaron productos. Posteriormente se incorporó un estándar a esa velocidad y compatible con el b que recibiría el nombre de 802.11g.

En la actualidad la mayoría de productos son de la especificación b y de la g (Actualmente se está desarrollando la 802.11n, que se espera que alcance los 500 Mbps). La seguridad forma parte del protocolo desde el principio y fue mejorada

[40] https://es.wikipedia.org/wiki/IEEE_802.11

en la revisión 802.11i. Otros estándares de esta familia (c–f, h–j, n) son mejoras de servicio y extensiones o correcciones a especificaciones anteriores. El primer estándar de esta familia que tuvo una amplia aceptación fue el 802.11b. En 2005, la mayoría de los productos que se comercializan siguen el estándar 802.11g con compatibilidad hacia el 802.11b.

- **Estándares IEEE 802.11**

Las redes están de moda y los cables no. Pero no solo los propietarios de equipos portátiles con capacidades WLAN prefieren no usar cables. Muchos hogares necesitan conectar más de un ordenador a la red, y aparatos electrónicos como equipos de música o vídeos cada vez disponen de más conectividad LAN. La conectividad inalámbrica es preferible al menos que quiera tirar cables por toda la casa.

Esta tendencia se refleja en el tremendo incremento en ventas que han sufrido las ventas de equipos de red inalámbricos. El negocio está en auge para los fabricantes de chips y componentes WLAN. Solo en Europa se esperó que el beneficio alcance la mágica cifra del billón de dólares en 2007. Esta tendencia también es buena para los consumidores, debido a que el incremento de cantidades significa una rápida caída en los precios de equipos WLAN.

En lugar de un único y por tanto fiable estándar (IEEE 802.11), hay una completa sopa de alfabetos distintos entre los que elegir. 802.11a, b, g y h compiten por ser los preferidos de los usuarios de tecnologías básicas y 802.11n que aparecerá pronto.

11c, d, e, f e i le añaden un poco de salsa al asunto. Los usuarios potenciales están normalmente confusos por la variedad de opciones: ¿11 ó 54 Mbps? ¿2.4 ó 5 GHz? ¿WEP, WPA o 802.11i? A continuación se despejaran estas dudas recorriendo el alfabeto WLAN.

Principales estándares IEEE 802.11:[41]

- **802.11ª.** Estándar de comunicación en la banda de los 5 Ghz, ya descrito

- **802.11b.** Estándar de comunicación en la banda de los 2.4 Ghz, ya descrito.

- **802.11c.** Estándar que define las características que necesitan los APs para actuar como puentes (bridges).Ya está aprobado y se implementa en algunos productos.

[41] https://es.wikipedia.org/wiki/IEEE_802.11

- **802.11d.** Estándar que permite el uso de la comunicación mediante el protocolo 802.11 en países que tienen restricciones sobre el uso de las frecuencias que éste es capaz de utilizar. De esta forma se puede usar en cualquier parte del mundo.

- **802.11e.** Estándar sobre la introducción del QoS en la comunicación entre PAs y TRs. Actúa como árbitro de la comunicación. Esto permitirá el envío de vídeo y de voz sobre IP.

- **802.11f.** Estándar que define una práctica recomendada de uso sobre el intercambio de información entre el AP y el TR en el momento del registro a la red y la información que intercambian los APs para permitir la interportabilidad. La adopción de esta práctica permitirá el Roamming entre diferentes redes.

- **802.11g.** Estándar que permite la comunicación en la banda de los 2.4 Ghz, ya descrito.

- **802.11h.** Estándar que sobrepasa al 802.11a al permitir la asignación dinámica de canales para permitir la coexistencia de éste con el HyperLAN. Además define el TPC (Transmit Power Control) según el cual la potencia de transmisión se adecúa a la distancia a la que se encuentra el destinatario de la comunicación.

- **802.11i.** Estándar que define la encriptación y la autentificación para complementar completar y mejorar el WEP. Es un estándar que mejorará la seguridad de las comunicaciones mediante el uso del Temporal Key Integrity Protocol (TKIP).

- **802.11j.** Estándar que permitirá la armonización entre el IEEE, el ETSI HyperLAN2, ARIB e HISWANa.

- **802.11m.** Estándar propuesto para el mantenimiento de las redes inalámbricas

Principales estándares 802.11

- **802.11 Legacy.** La versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión teóricas de 1 y 2 mega bit por segundo (Mbit/s) que se transmiten por señales infrarrojas (IR) en la banda ISM a 2,4 GHz. IR sigue siendo parte del estándar, pero no hay implementaciones disponibles.

Estándares 802.11a, 802.11b y 802.11g:[42]

Como probablemente saben, 802.11a y b, cada una define una capa física diferente 802.11b, transmite a 2.4Ghz y envía datos a 11 Mbps usando una secuencia DSSS mientras tanto 502.11a transmite a 5Ghz y envía datos a 54 Mbps usando OFDM.

Por supuesto el desempeño superior del 802.11a ofrece excelente soporte para aplicaciones que requieran un amplio ancho de banda; pero la alta frecuencia de operación equivale a un rango de acción relativamente corta. Se han visto demostraciones de 802.11a entregando 54 Mbps a distancias de hasta 20 mts que es mucho menos que los 100 mts de cobertura de 802.11b. En comparación necesitaría muchos más AP en 802.11a para cubrir un área específica, especialmente si esta es muy grande.

La diferencia en la frecuencia y modulación de 802.11b causa que no sean interoperativas por ejemplo un usuario con una tarjeta 802.11a no será capaz de conectarse con una AP 802.11b.

El estándar 802.11 no ofrece soluciones de interoperabilidad entre las diferentes capas físicas. En 2002 y 2003 los productos que soportaban el nuevo estándar 802.11g empezaron a aparecer en escena. 802.11g intenta combinar lo mejor de las dos normas anteriores, soporta un ancho de banda de 54 Mbps y usa la banda de 2.4 Ghz para obtener un mayor rango. 802.11g es por lo tanto compatible con 802.11b.

Lineamientos de decisión:

Cuando se tome la decisión de ir con 802.11 a o b, se debe pensar en desempeño, rango e interoperabilidad.

Se debe considerar usar 802.11b si:

- Los requerimientos de cobertura son significativos como por ej. Almacenes de cadena
- Ya ha hecho una inversión en dispositivos 802.11b.
- Los usuarios finales están distribuidos ampliamente. Si hay pocos usuarios finales y están distribuidos en un área muy amplia, muy probablemente 802.11b cumpla con los requerimientos porque habrán menos usuarios compitiendo por un AP.

Se debe considerar usar 802.11ª, sí:

[42] https://es.wikipedia.org/wiki/IEEE_802.11

- Necesita un mayor desempeño, por ej. Aplicaciones que cubran video, voz y transmisión de archivos o imágenes grandes.
- Interferencia significativa de la banda de 2.4Ghz.
- Hay una alta densidad de usuarios finales como aeropuertos centros de convenciones y lugares públicos.

Se debe considerar usar 802.11g, teniendo en cuenta:

Ventajas

- Mayor velocidad de transferencia.
- Soporta más usuarios simultáneos.
- Su señal es mejor y no es fácilmente obstruible.

Desventajas

- Mayores costos que 802.11b
- Puede recibir interferencias de fuentes no reguladas.

Las redes inalámbricas se reparten entre dos clases principales subdivididas por la banda de frecuencia. Las primeras tecnologías usaban la banda de 2.4 GHz mientras que las más modernas usan la de 5 GHz (más ancha). La primera incluye los estándares del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) 802.11b (11 Mbps) y es compatible con su sucesor (802.11g a 54 Mbps). Esta primera opción es la más común actualmente.

Por otro lado, tanto 802.11a como 802.11h, que operan en la banda de 5 GHZ, consiguen un rendimiento nominal de 54 Mbps. 802.11h, referida en Estados Unidos como “de compatibilidad en Europa”, es la variante Europea del estándar Americano.

Sus dos características más importantes son la selección dinámica y la potencia de transmisión variable, obligatorias para el mercado Europeo según el Instituto Europeo de Estándares de Comunicación (ETSI) con el fin de asegurar que los sistemas tengan una capacidad de transmisión razonable.

IEEE 802.11c, especifica métodos para la conmutación inalámbrica, o lo que es lo mismo, métodos para conectar diferentes tipos de redes mediante redes inalámbricas.

El 802.11d normalmente se le conoce como el “Método Mundial” y se refiere a las diferencias regionales en tecnologías como a cuántos y cuáles son los canales disponibles para usarse en las distintas regiones del mundo. Como usuario sólo

necesitamos especificar el país en el que queremos usar la tarjeta WLAN y el controlador se ocupa del resto.

El protocolo **IEEE 802.11e** define la calidad del servicio y las extensiones para el flujo de medios para 802.11a/h. El objetivo es ajustar las redes de 54 Mbps para aplicaciones multimedia y de voz sobre IP, o lo que es lo mismo, telefonía a través de redes IP e Internet. La red debe soportar valores de transmisión de datos garantizados para servicios individuales o retrasos de propagación mínimos para que sean útiles con multimedia o voz.

El protocolo **802.11f** describe como se tratan los estándares de las comunicaciones de clientes de móviles fuera de zona entre puntos de acceso ("Roaming") con IAPP, el Protocolo de Puntos de Acceso manejando de los detalles.

3.3.4 Sistemas operativos para red:

3.3.4.1 RouterOS[43]**.** RouterOS es el sistema operativo de la empresa Mikrotik. Este sistema viene preinstalado en un RouterBoard. También se puede instalar en un PC y se convertirá en un router con todas las características necesarias: ruteado, cortafuegos, gestión de ancho de banda, AccessPoint, HotSpot, Gateway, servidor VPN y más. RouterOS es un sistema operativo autónomo basado en el kernel de Linux v2.6, y la meta de Mikrotik es proporcionar todas estas características con una instalación rápida y sencilla y una interfaz fácil de usar.

Se puede probar RouterOS, para ello dirigirse a www.mikrotik.com y descargar la imagen del CD de instalación. La prueba gratuita ofrece todas las características sin limitaciones.

RouterOS soporta varios métodos de configuración, acceso local con teclado y monitor, consola de serie con una aplicación de terminal, Telnet y acceso seguro SSH en redes, una herramienta de configuración de GUI personalizada llamada Winbox, una sencilla interfaz de configuración basada en Web y una interfaz de programación de API para la construcción de su propia aplicación de control. En caso de que no haya acceso local, y haya un problema con las comunicaciones de nivel de IP, RouterOS también soporta una conexión basada en nivel de MAC con las herramientas de Winbox. RouterOS ofrece una potente, pero fácil de aprender interfaz de configuración de línea de comandos con capacidades de scripts integradas:

- GUI Winbox sobre IP y MAC.

[43] https://es.wikipedia.org/wiki/MikroTik

- CLI con Telnet, SSH, Consola Local y consola serie.
- API para programar tu propia herramienta.
- Interfaz Web.

3.3.4.2 Microsoft windows server 2012[44]**.** Es un sistema Operativo propietario de la empresa estadounidense Microsoft diseñado para la administración de redes informáticas. Posee un excelente soporte de hardware.

Permite la instalación y administración de servicios de red como DHCP, DNS, VPN, IIS entre otros. Además posee una herramienta propia que es el Directorio Activo, este último para la administración de árboles de dominios.

Tiene una herramienta llamada **administrador del servidor**, la cual es una consola de administración en Windows Server 2012 que ayuda a los profesionales de TI a aprovisionar y administrar los servidores locales y remotos basados en Windows desde los escritorios, sin necesidad de tener acceso físico a los servidores ni de habilitar conexiones de Protocolo de escritorio remoto (RDP) para cada servidor.

Windows server 2012 R2[45] es actualmente la versión de Windows Server más moderna y mejorada. Las ediciones de Windows Server 2012 R2 siguen siendo optimizadas y simplificadas para que los administradores puedan elegir más fácilmente la edición que más les convenga de acuerdo con sus necesidades, a continuación una descripción general del enfoque de cada versión.

- **Windows server 2012 R2 datacenter**: Para un entorno altamente virtualizado que requiera características de alta disponibilidad, incluida la agrupación en clústeres.

- **Windows server 2012 R2 standard**: Para un entorno no virtualizado o poco virtualizado en el que se desee incluir características de alta disponibilidad, incluida la agrupación en clústeres.

- **Windows server 2012 R2 essentials**: Para pequeñas empresas con hasta 25 usuarios, especialmente aquellas empresas que quieran implementar su primer servidor.

- **Windows server 2012 R2 foundation**: Para pequeñas empresas con hasta 15 usuarios (solo disponible a través de partners OEM directos).

[44] https://es.wikipedia.org/wiki/Microsoft
[45] http://www.internetya.co/versiones-y-caracteristicas-de-windows-server-2012-r2/

Dentro de las principales características se encuentran:

a. Nuevo server manager: para crear manager server groups

Una de las ventajas de la nueva interface de Server Manager es la capacidad de crear grupos de servidores, que son colecciones de servidores que ya existen en la red, y se pueden gestionar a través de la nueva experiencia de usuario. La creación de nuevos grupos de servidores permite gestionar las tareas entre cada servidor con atributos comunes -un grupo de servidores que contiene todos los equipos que ejecuten IIS, por ejemplo; un grupo de todos los servidores de bases de datos, y así sucesivamente-, y proporcionar información específica sobre cualquiera de ellos como desee. Esta es una gran bendición para las organizaciones sin software de monitoreo dedicado.

b. Mejor edición, selección SKU

El sistema operativo es ahora el mismo, y la edición que compre -Standard o Datacenter- depende de si desea ejecutar hasta dos máquinas virtuales como invitadas, o si quiere virtualización ilimitada de invitados. No hay edición Enterprise que estanque los trabajos.

c. Una línea de comandos primero, una segunda mentalidad de interface gráfica

Para Windows Server el énfasis ha cambiado de una filosofía pensada primero en la interface gráfica de usuario (GUI), a una interfase gráfica de usuario opcional. De hecho, la primera vez que instale el sistema operativo, tendrá que elegir entre una instalación completa o de núcleo. De núcleo es la opción preferida. Una vez que instale una versión de núcleo de Windows Server 2012, puede volverla una interfase gráfica de usuario con solo instalar la función GUI y, a continuación, puede optar por despegar sin una reinstalación completa.

d. Replicación Hyper-V

La característica Hyper-V[46] Replica permite replicar una máquina virtual de una locación a otra con Hyper-V y una conexión de red -y sin ningún tipo de almacenamiento compartido. Este es un gran problema en el mundo de Microsoft para la recuperación ante desastres, alta disponibilidad y mucho más. VMware hace esto también, pero el vendedor cobra por las licencias extra de tal capacidad.

Esto hace que mantener en pie las instancias de servicios en todo el mundo sea un asunto de uno o dos clics (suponiendo que existe conectividad de red). Las nuevas interfaces de Hyper-V Replica dentro de Hyper-V Manager incluyen una

[46] https://es.wikipedia.org/wiki/Microsoft_Windows

interface mucho más simple para la creación de una secuencia de replicación, y un mejor control del proceso y de la salud general de los sistemas y socios de replicación.

e. Ampliación de las capacidades de PowerShell

Hay cientos de cmdlets más en la última versión de Windows Server. Esto hará que la vida sea más fácil, ya que PowerShell es esencialmente el método preferido para la gestión de todas las cargas de trabajo que se pueden ejecutar en el sistema operativo.

f. Storage spaces, espacios de almacenamiento

Storage Spaces es una característica innovadoras que básicamente lleva los productos básicos de almacenamiento -drivers baratos y sus controladores, como JBOD (lenguaje informal para muchos discos)-, y se convierte en una piscina de almacenamiento que se divide en espacios que a su vez son utilizados como discos regulares.

g. DirectAccess: una VPN sin el dolor de una VPN

DirectAccess permite un túnel seguro tipo VPN[47] desde cualquier extremo de vuelta a la red corporativa, sin la sobrecarga y el impacto en el rendimiento de una VPN verdadera. Tampoco, hay un agente de gestión en el cliente. Cuando la tecnología está configurada correctamente, trabaja -los usuarios tienen conectividad permanente con los recursos compartidos de archivos, equipos en las instalaciones y otros recursos como si estuvieran en el campus corporativo.

Además, se aplican los objetos de la política de grupo y los administradores pueden gestionar las máquinas estén donde estén, y no solo cuando llegan a la sede o al conectarse a la VPN. Esta tecnología había sido difícil de establecer, pero en Windows Server 2012, funciona en gran medida.

H. Dynamic access control: nueva forma de pensar

Los Dynamic Access Control (DAC) son un conjunto de instalaciones que realmente mejoran la forma en que se puede controlar el acceso a la información. Ya no se trata de tomar decisiones sobre los archivos o carpetas: “Sí, esta gente puede” y “no, esta gente no puede”.

[47] http://cioperu.pe/articulo/11028/diez-caracteristicas-de-windows-server-2012-para-los/

i. Sistema de archivos resilientes2: Una evolución de NTFS

El sistema de archivos “resiliente” (ReFS, por sus siglas en inglés) fue diseñado como una evolución del New Technology File System (NTFS) con un enfoque en la disponibilidad y la integridad. Refs escribe en diferentes ubicaciones del disco de manera atómica, lo que mejora la capacidad de recuperación de datos en caso de una falla de alimentación durante la escritura, e incluye la nueva característica “integrity streams” que utiliza sumas de comprobación y asignación de tiempo real para proteger la “secuenciación” y el acceso al sistema y a los datos de usuario.

j. Gestión de dirección IP fuera de la caja

En la caja de Windows Server 2012, encontrará una suite IPAM completa. Esto es algo a lo que muchas pequeñas y medianas empresas simplemente no tienen acceso. Con la suite IPAM puede asignar, agrupar, rentar, y renovar las direcciones IP de forma organizada, así como integrarla con el DHCP en la caja y los servidores DNS para descubrir y administrar dispositivos que ya están en la red. Si no ha probado los servicios IPAM de Nortel u otros, esto es una inclusión muy interesante y útil al producto -y ya que es libre con la licencia del sistema operativo, vale la pena su precio.

4. DESARROLLO DEL TRABAJO

4.1 METODOLOGÍA

Las metodologías son necesarias para desarrollar cualquier tipo de proyecto de forma ordenada y eficaz, razón por la que la metodología utilizada para la realización del presente proyecto en System Plus de Túquerres. es **Top-Down Network Design.**

Para alcanzar los objetivos propuestos, se utilizó la metodología de tipo empírico, porque se realiza recolección y análisis de datos, además se toma como fuente primaria de información la observación directa por parte del estudiante, también, se estudian y aplican conceptos y esquemas teóricos. Cabe mencionar que esta metodología clasifica dentro del tipo de investigación aplicada, ya que todas las recomendaciones finales deberán ser aplicadas para tener un funcionamiento de calidad.

Se aplican entonces las fases de la metodología que se escogió:

- Fase1: Análisis de Negocios Objetivos y limitaciones
- Fase2: Diseño Lógico
- Fase3: Diseño Físico

- Fase4: Pruebas, Optimización y Documentación de la red

4.1.1 Fase1. Análisis de Negocios Objetivos y limitaciones. Para el desarrollo del presente proyecto se presenta en esta fase un plano de System Plus y el diseño lógico de la red actual.

Como se aprecia en la figura 36 se tiene inicialmente un Modem de Movistar, con IP para la LAN 192.168.1.1. A él se conecta un Computador el cual tiene instalado un Servidor Proxy. El Servidor Proxy tiene un Procesador AMD Phenom X3 con 4GB de memoria RAM y un disco duro de 200GB.

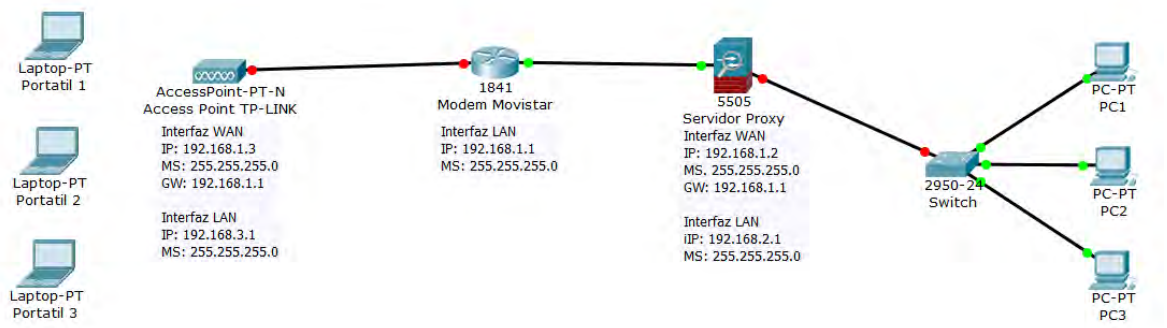

Figura 36. Red de System Plus antes de la ejecución del proyecto.

El equipo tiene instalado dos tarjetas de red. La una para la WAN, es decir, para la entrada del servicio de Internet y la otra para la LAN, es decir, para la conexión de la red local de System Plus. Véase figura 37.

La tarjeta de red WAN del servidor Proxy tiene IP 192.168.1.2. Obviamente está en el mismo rango de la IP del Modem de Movistar.

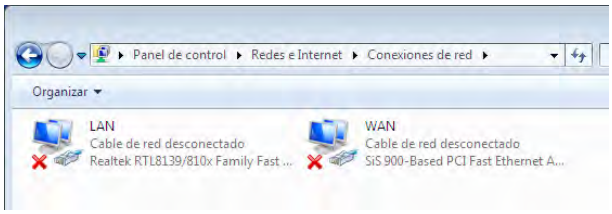

Figura 37. Conexiones de red del servidor proxy

Por otra parte, la tarjeta de red LAN del Servidor Proxy tiene IP 192.168.2.1. Esta será la puerta de enlace de los equipos que se conecten a la LAN de System Plus.

El aula de informática de System Plus está dotada de 14 computadores de escritorio. La IP de ellos se asigna de forma estática desde 192.168.2.101 hasta 192.168.2.114. En el navegador de cada computador se debe especificar la IP o el nombre del Servidor Proxy.

El software Proxy que se usa es CCProxy. Este software es de la empresa Youngzsoft y se puede descargar una versión libre para tres usuarios en la página web http://www.youngzsoft.net/ccproxy/proxy-server-download.htm. Figura 38.

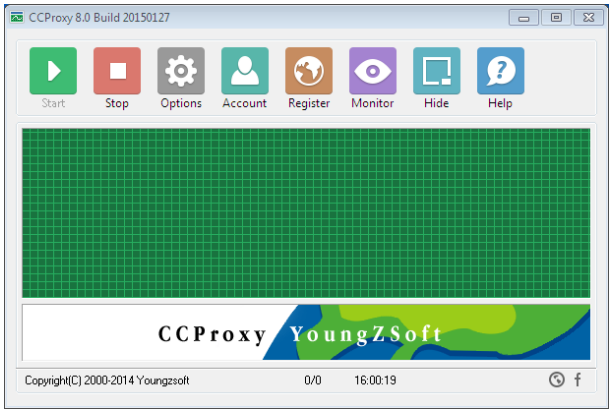

Figura 38. Pantalla inicial de CCProxy

CCProxy permite la creación de cuentas. Los clientes se pueden autenticar mediante MAC, IP o Contraseña o con la combinación de los mismos como se muestra en la figura 39.

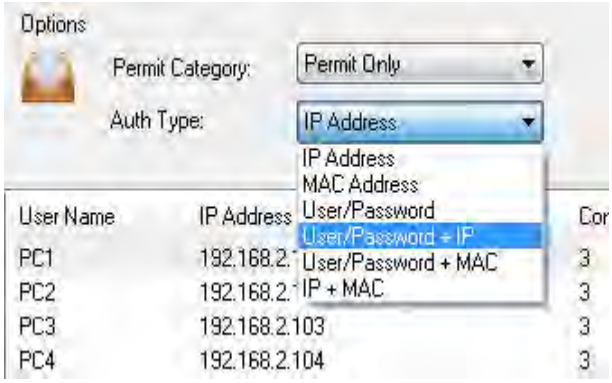

Figura 39. Tipos de autenticación en CCProxy

CCProxy permite además la restricción de páginas web, el establecimiento de horarios, restricción de servicios, control del ancho de banda.. A cada cliente se le asigna un nombre y una IP. Los clientes se pueden asociar en grupos para facilidad de administración de las cuentas. Véase figura 40 y 41.

Figura 40. Cuentas en CCProxy

En la figura 41 se puede apreciar que el PC1 tiene asignado un ancho de banda de 2000 Kbps para Tx y 300Kbps para Rx. Además el cliente tiene un filtro de web para Facebook.

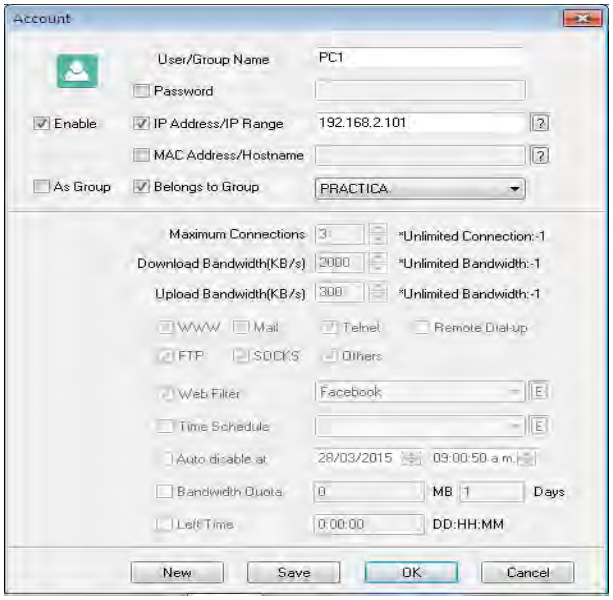

Figura 41. Cuenta del PC1 en CCProxy

Los clientes como son Dirección, Secretaría, Teoría 1, Teoría 2 y Teoría 3 se conectan a la red inalámbricamente.

En la red además hay un AccessPoint que es quien provee la Red Inalámbrica. A él se conectan 5 computadores portátiles que pertenecen a System Plus y los portátiles que algunos docentes y estudiantes llevan para sus clases. A la red inalámbrica también se conectan los teléfonos celulares de la comunidad de System Plus. Los PC de Redes y Mantenimiento se conectan por cable directamente al Modem de Movistar. Es importante anotar que desde aquí NO se genera ningún tipo de control. Véase Plano en la figura 42.

Figura 42. Plano de la red de System Plus

4.1.2 Fase 2: diseño lógico de la nueva red:

4.1.2.1 Configuración del routerboard:

a. Generalidades

Tal y como se indicó en los alcances del proyecto, se instaló un RouterBoard después del Modem de Movistar. El RouterBoard que se adquirió tiene referencia hAP lite RB941 2nD, posee 4 puertos de red 10/100 Ethernet y una interfaz inalámbrica. Véase en la figura 43 sus especificaciones.

Product specifications

Details	
Product code	RB941-2nD
CPU nominal frequency	650 MHz
CPU core count	1
Size of RAM	32 MB
10/100 Ethernet ports	4
Wireless chip model	QCA9531-BL3A-R
Wireless standards	802.11b/g/n
Power Jack	1
Supported input voltage	5 V - 5 V
License level	4
Antenna gain DBI	1.5
CPU	QCA9531-BL3A-R
Max Power consumption	3W
Number of chains	2
Suggested price	$21.95

Figura 43. Especificaciones routerboard hAP lite RB941 2nD
Fuente: http://routerboard.com/RB941-2nD

Para este ítem es importante explicar cómo se hace la administración de un RouterBoard. Como cualquier Router, para ingresar a él se necesita estar conectado al mismo para hacerlo. La ventaja es que se puede hacerlo con la IP o por medio de la MAC.

Es decir, si el RouterBoard está configurado con una IP, y el equipo que está conectado a él no tiene una IP en la misma subred, simplemente se puede acceder por medio de la MAC. Véase figura 44.

Para acceder a la configuración del RouterBoard se puede hacerlo de varias formas:

- Mediante la herramienta Winbox que se descarga desde la página oficial de Mikrotik

- Digitando la IP del RouterBoard en el navegador. Se necesita que la IP del equipo esté en la misma subred del RouterBoard.

- Usando la herramienta Netinstall que también se descarga desde la página oficial de Mikrotik.

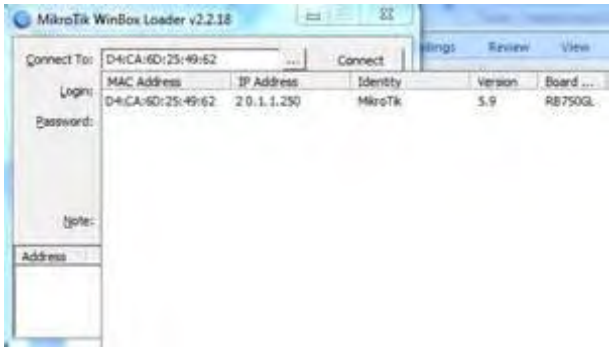

Figura 44. Login para el routerboard

Para el desarrollo de este trabajo se usará Winbox.

Un RouterBoard nuevo por defecto viene con la IP 192.168.88.1. Si se resetea toda configuración se puede acceder por la dirección MAC.

b. Nombramiento de Interfaces y asignación de IP

A continuación, se indica cómo se usaron las interfaces del RouterBoard:

- La primera interfaz se usó para conectar el Modem de Movistar. Es decir corresponde a la WAN del RouterBoard.

- La segunda interfaz se usó para conectar el Servidor con Windows server 2012.

- La tercera interfaz se usó para conectar un Router TP-Link. En esta interfaz se configuró un HotSpot.

- El cuarto puerto queda libre y se usará para labores de administración del RouterBoard.

La descripción anterior se observa en la figura 45.

Se empezó por la asignación de la IP de la primera interfaz. Esta IP debe estar en el mismo rango de la IP del Modem de Movistar, es decir, el Modem de Movistar tiene IP 192.168.1.1, la interfaz WAN del RouterBoard tendrá entonces 192.168.1.2. Véase figura 46.

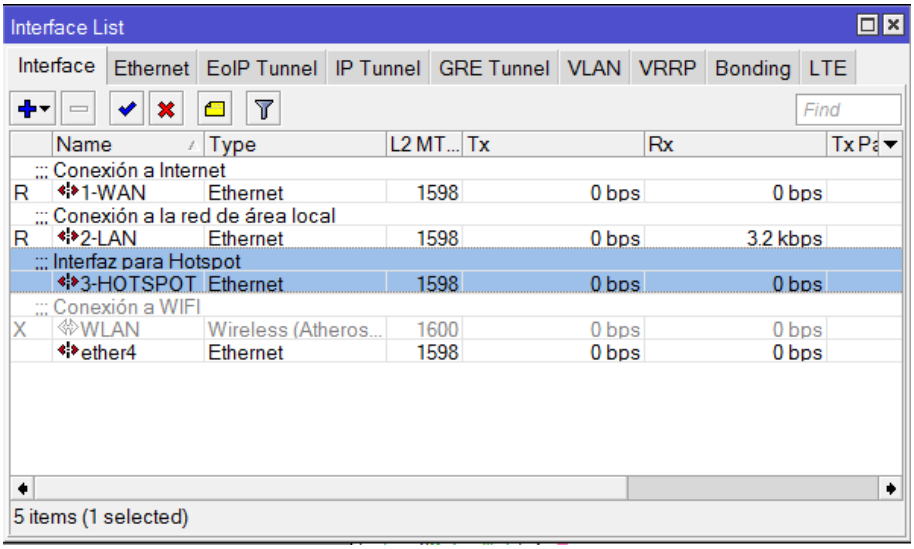

Figura 45. Interfaces del routerboard

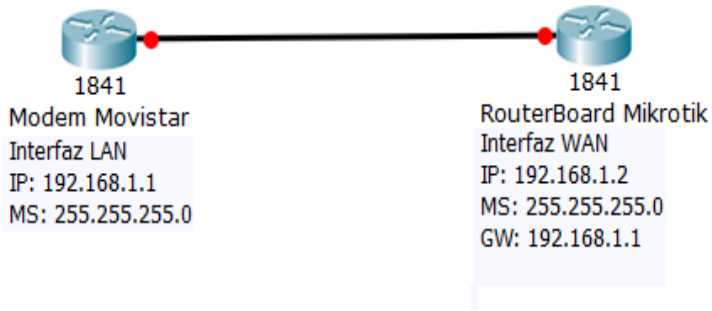

Figura 46. Conexión modem movistar – routerboard

Ahora se procede a asignar las demás IP a cada interfaz del RouterBoard. La segunda interfaz tendrá IP 192.168.2.1/30. A este puerto solamente se conectará el servidor con Windows Server 2012.

La tercera interfaz tendrá 192.168.3.1/30. El único host que se conectará directamente a este puerto será el AccessPoint TP-Link. Esta interfaz se la usará para configurar un HotSpot para la red inalámbrica. A este puerto se conectará el AccessPoint que se mencionó antes y desde este último se administrará la red inalámbrica. La interfaz WLAN del RouterBoard no se habilitará. Para un mejor entendimiento véase figura 47.

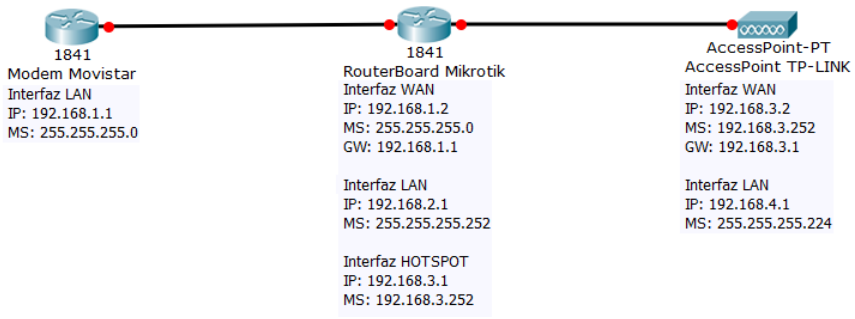

Figura 47. Diseño lógico inicial de la nueva red

Continuando con la configuración del RouterBoard, se procedió a renombrar las interfaces para una mejor comprensión a la hora de administrar el Router. Ahora ya tienen nombre e IP. Véase figura 48.

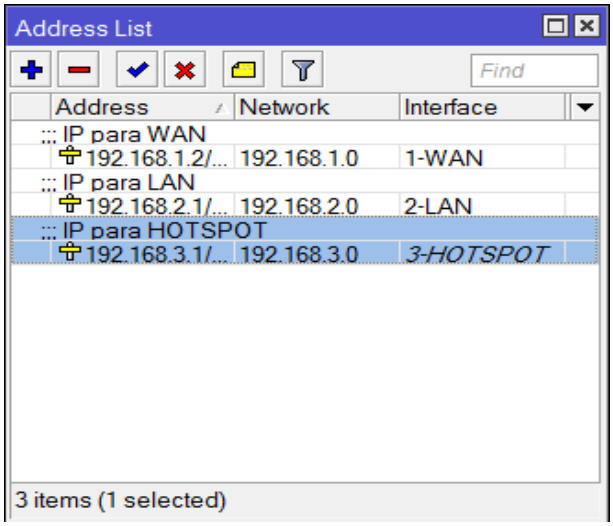

Figura 48. Interfaces con nombres

c. Configuración de DNS

Ahora se debe configurar los servidores DNS que usará el RouterBoard para conectarse a Internet. Se pueden usar DNS 's universales como los de Google: 8.8.8.8 y 8.8.4.4 o los DNS 's que asigna el ISP que está brindando el servicio de Internet. En este caso movistar usa: 200.21.200.10 y 200.21.200.80. Se usaron los del ISP. Véase la figura 49.

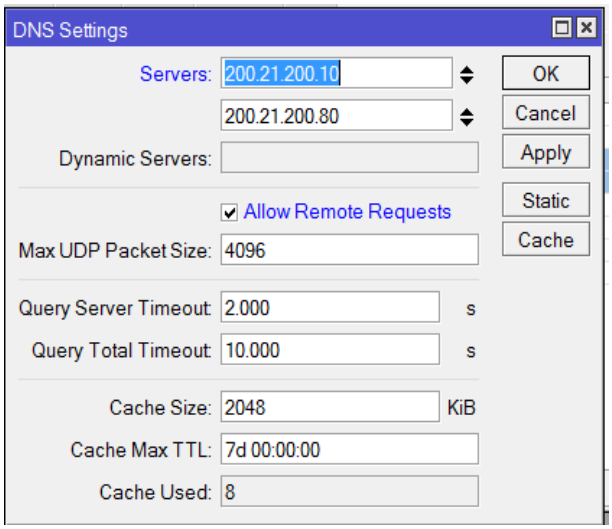

Figura 49. DNS
Fuente: Autores del Proyecto

d. Asignación de la puerta de enlace

Seguidamente habrá que asignar la puerta de enlace para el RouterBoard, es decir, la IP que servirá de enlace entre el RouterBoard y el Módem de Movistar. Véase figura 50.

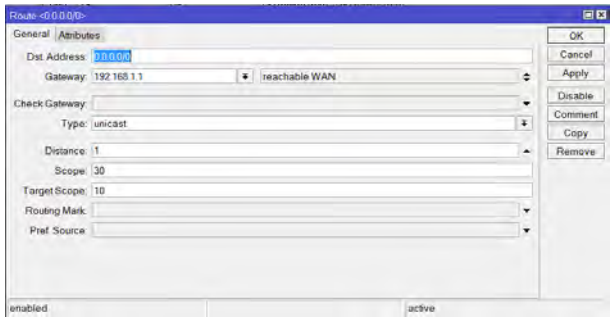

Figura 50. Asignación de la puerta de enlace

f. Configuración de NAT

Se necesita ahora configurar un NAT para Internet, es decir para que los equipos de la red LAN ya puedan navegar. Véase figura 51.

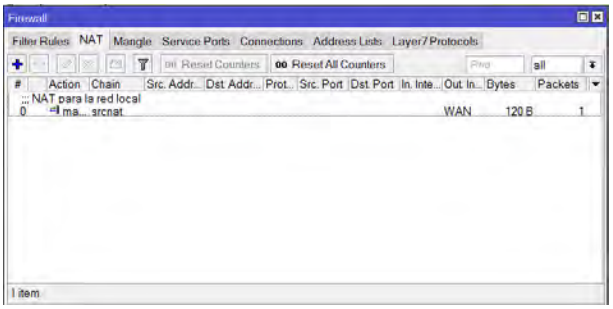

Figura 51. NAT para la red local

Para efectos de prueba se pondrá una IP en la misma subred al computador para verificar si hay navegación. Es importante anotar que el RouterBoard en el momento no tiene configurado el servicio DHCP, por tanto la IP para el equipo se debe asignar manualmente. Hay que recordar que la IP de la red LAN es 192.168.2.0, siendo 192.168.2.1 la puerta de enlace. Véase figura 52.

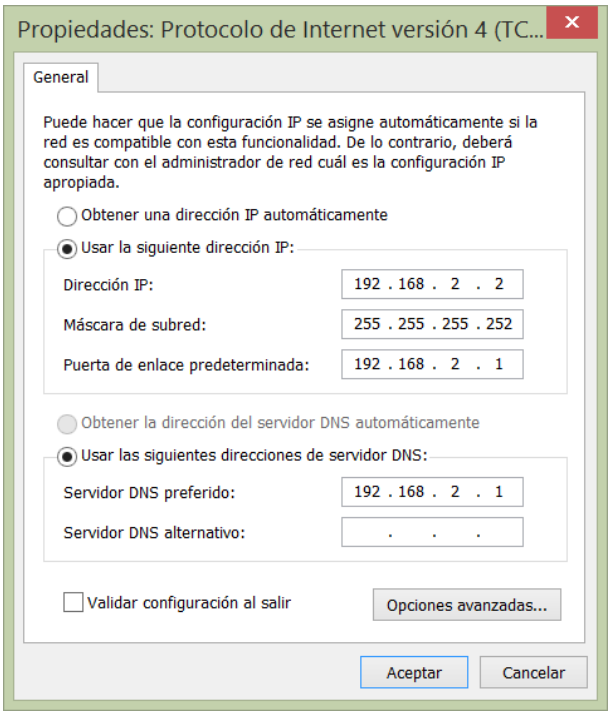

Figura 52. IP para prueba de navegación

En la figura 53 se comprueba que el equipo cliente ya está navegando.

Figura 53. Prueba de navegación

g. Configuración de HotSpot[48]

Continuando con la configuración del RouterBoard, se procede a configurar el HotSpot.

Un HotSpot es un sistema que permite capturar el tráfico http (web) de los clientes y re direccionarlo a un Portal para fines de autenticación. Una vez el cliente es autenticado, este puede acceder a todos los servicios de internet con normalidad.
La configuración estándar de Mikrotik HotSpot es muy fácil de configurar, pero hay que hacer ciertas modificaciones para evitar tener problemas en la red si es que se utiliza AP's o Routers modo cliente. Hay que tener en cuenta que un HotSpot está pensado para ser utilizado en lugares relativamente "pequeños", y que además los clientes NO se conectarán a través de AP's o Routers modo cliente.

Muchos usan Mikrotik HotSpot en redes Wireless extensas como único sistema de seguridad, dejando la señal abierta (sin encriptación), teniendo la creencia que este sistema es inviolable, lo es bastante falso. Sin contar que se esta dejando la puerta abierta para que cualquier persona malintencionada haga un gran alboroto en la red.

La configuración del HotSpot se hará de la siguiente manera:

- Ir a IP/HotSpot
- Ubicarse en la pestaña Servers
- Click en HotSpot Setup.

[48] http://www.ryohnosuke.com/foros/index.php?threads/334/

Al igual que la configuración del servidor DHCP de Mikrotik, se sigue el asistente de configuración automática para así configurar correctamente el HotSpot, inclusive ambos son muy parecidos.

- ***HotSpot interface.*** Aquí se debe especificar la interfaz donde se configurará el HotSpot Server, obviamente se debe elegir la interfaz de red LAN o tarjeta de red de los clientes, que en este caso es *HOTSPOT (Interface 3)*.

- ***Local address of network***. Aparecerá automáticamente la puerta de enlace de los clientes, que en este caso es *192.168.3.1*; claro, está tomando los datos del IP de la interface 3 que se especificó en el paso anterior.

- ***Masquerade network***. Hay que desmarcar ya que se tiene el servidor funcionando, por lo tanto, ya se cuenta con el enmascarado. Si se activa este check creará *otro* enmascarado.

- ***Address pool of network.*** Aparecerá un rango de IP's que serán asignados a los clientes para que así obtengan un IP automáticamente. Si no se tiene un servidor DHCP funcionando, este paso activaría uno obligatoriamente. Ya más adelante se podrá deshabilitarlo.

- **Select certificate**. A momento sólo se va a elegir none, ya que no se cuenta con un certificado SSL. Estos certificados son utilizados para validar una página web cuando se utiliza el protocolo https y así encriptar las conexiones entre el cliente y servidor, muy utilizado en las páginas de los bancos ya que así ofrecen seguridad respecto a las claves y los movimientos. La dirección IP del servidor SMTP, se deja tal como está: 0.0.0.0 ya que no se cuenta con un servidor SMTP.

- ***DNS servers***. Como ya se tiene configurado el DNS Cache estos valores aparecen automáticamente, sino, pues se tendrá que agregar manualmente.

- ***DNS name***. Aquí se coloca un DNS para la red de HotSpot; para mayor claridad, cuando HotSpot ya esté funcionando y se quiere abrir una página, este re direccionará al portal cautivo para que autenticarse con el usuario y clave asignados. Este portal tendrá dirección http://login.hot.net/ ya que ese es el DNS que se escribió; en todo caso, si este valor se deja en blanco, HotSpot usará directamente la puerta de enlace de los clientes, o sea, 192.168.3.1.

- ***Name of local hotspot user***. Por defecto, el nombre de usuario administrador para el logueo en el HotSpot es ***admin***, aunque si se quiere cambiar.

- ***Password for the user***. La contraseña de logueo, se podrá cambiar en cualquier momento.

Así deberá quedar la ventana de HotSpot una vez terminado el asistente de configuración. Véase figura 54.

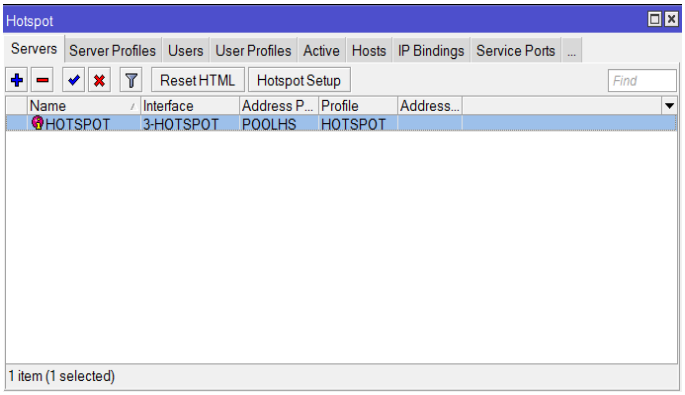

Figura 54. HotSpot ya configurado

Una vez hecho esto saldrá un mensaje que el HotSpot fue configurado satisfactoriamente; luego, si WinBox estaba conectado al servidor Mikrotik por IP, seguramente se desconectará. Si la conexión es por MAC, seguirá conectado. En todo caso, el servidor HotSpot ya está configurado, y si se intenta abrir una nueva página, este mostrará el portal cautivo de Mikrotik.

Una vez que se vea el portal cautivo, se autentica con el usuario y contraseña que se configuró previamente. Una vez autenticados, HotSpot[49] dará un mensaje de bienvenida y se tendrá internet normalmente. Sin esta autenticación no hay absolutamente ningún servicio disponible que dependa de internet.

Ahora sigue la creación de perfiles de usuarios en el HotSpot. Se crean en la pestaña **Users Profiles.** Son grupos de usuarios a los cuales se les puede limitar su velocidad (sin utilizar Simple Queue), enviar mensajes a los clientes, controlar el tiempo para que al cliente le vuelva a aparecer el portal cautivo, etc.

Después de crear los perfiles de usuario, se crean los usuarios. Cada uno pertenecerá a un perfil de usuario. Cada usuario tendrá un nombre y una contraseña. Véase figuras 55 y 56.

[49] http://www.ryohnosuke.com/foros/index.php?threads/334/

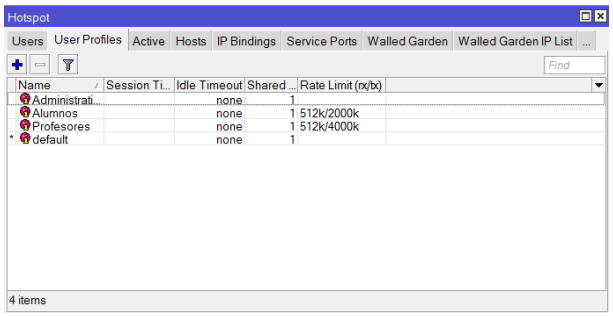

Figura 55. Perfiles de usuarios de hotspot

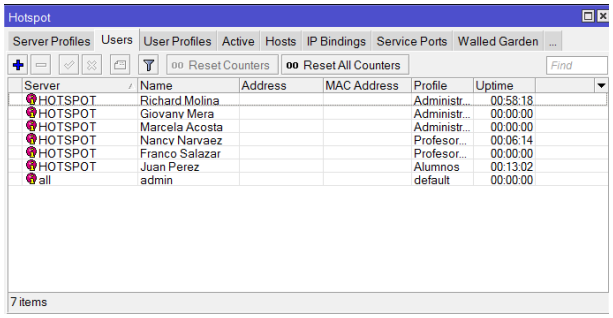

Figura 56. Usuarios de hotspot

4.1.2.2 Configuración de servidor orión. Orion, es el servidor que alojará un Sistema Operativo Windows Server 2012. El servidor tiene un procesador AMD Phenom X3 con 4GB de memoria RAM y un disco duro de 200GB.

Este servidor tiene dos tarjetas de red, una para conectarse a internet y otra para conectarse a la red local. La tarjeta de red WAN del Servidor Orión estará conectada al RouterBoard en su interface LAN. Véase figura 57.

A. Instalación del sistema operativo windows server 2012

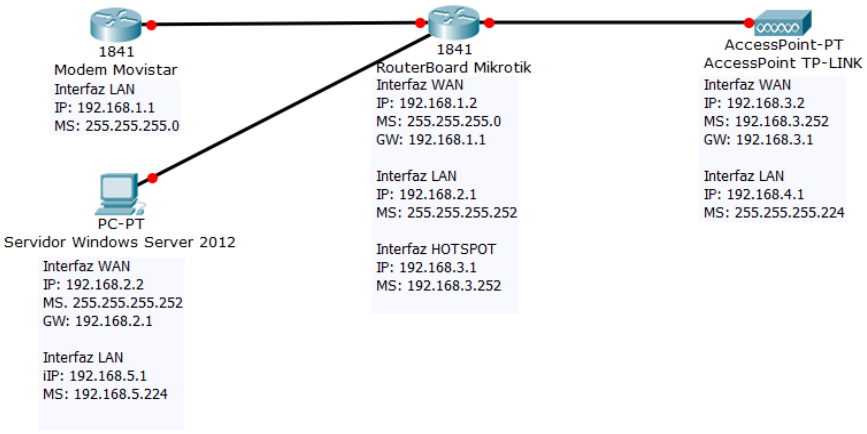

Figura 57. Conexión del servidor orión a la red de system plus

Al igual que en la instalación de cualquier sistema operativo de Microsoft, una vez, arranca la instalación se debe escoger el idoma, form ato de hora y moneda y la distribución del teclado, tal y como se ve en la figura 58.

Figura 58. Instalando windows server 2012 en orion
Fuente: http://i.ytimg.com/vi/YBgXdT9m-tw/maxresdefault.jpg

Después de esto, el instalador del sistema operativo prepara el disco duro para la instalación. Comienza entonces la descomprensión de los archivos como se ve en la figura 59.

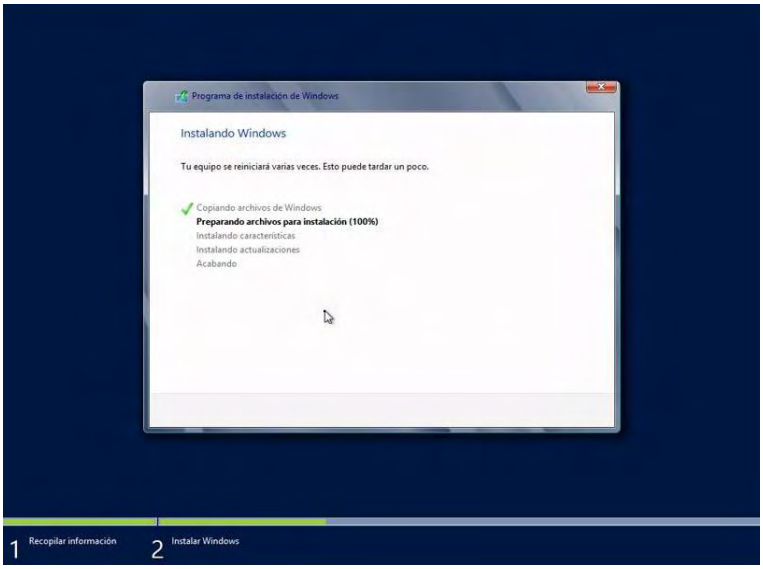

Figura 59. Preparando archivos para instalación

Se necesita ahora crear las particiones donde se instalará el sistema operativo. Véase figura 60.

Ya para finalizar la instalación el sistema operativo solicita una contraseña para el administrador. Véase figura 61.

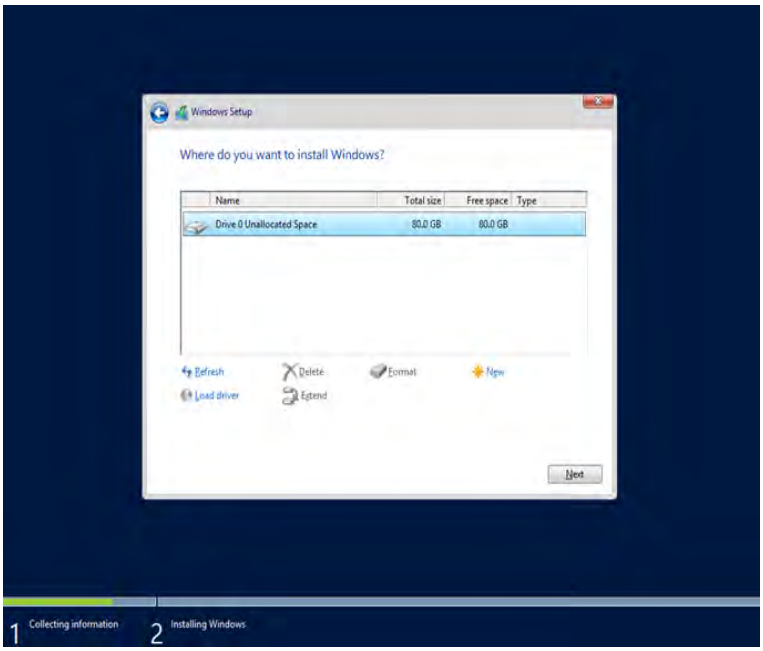

Figura 60. Creando las particiones
Fuente: https://www.tectimes.net/wp-content/uploads/2013/08/081913_1840_TUTORIALWin9.png

Figura 61.Solicitando contraseña para administrador

Una vez terminada la instalación, el sistema operativo se inicia por primera vez. Se ve en la figura 62 el Administrador del Sistema.

b. Configuración de las conexiones de red

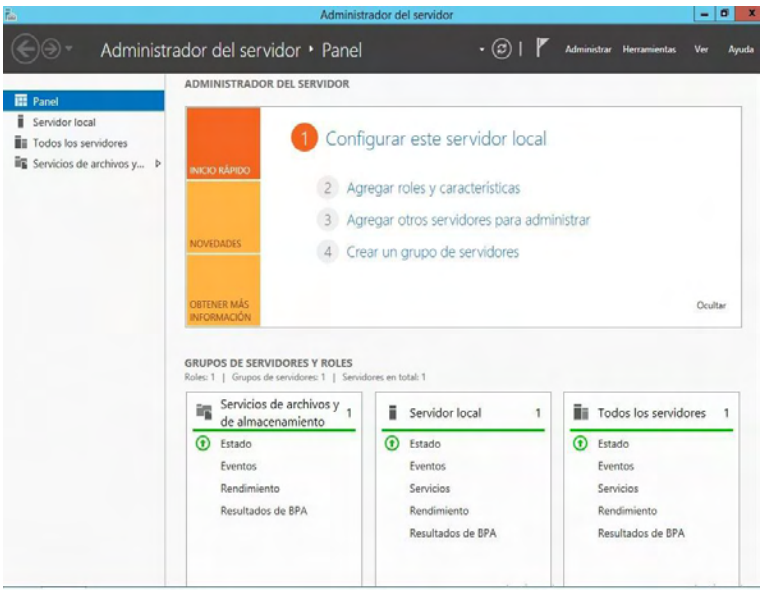

Figura 62. Administrador del servidor
Fuente: http://i0.wp.com/www.jfabello.es/wp-content/uploads/2015/05/Principal.jpg

Como se indica en las figuras 63 y 64, el servidor Orión tiene dos tarjetas de red. Las conexiones se renombran para facilidad en la administración.

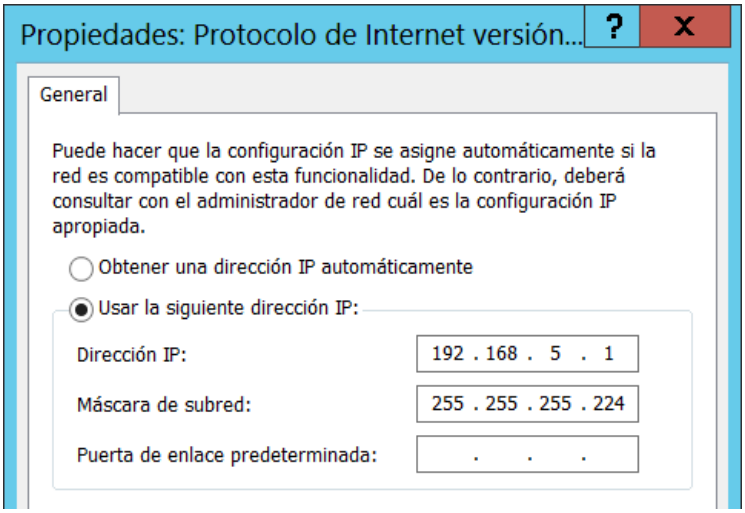

Figura 63. Conexión LAN

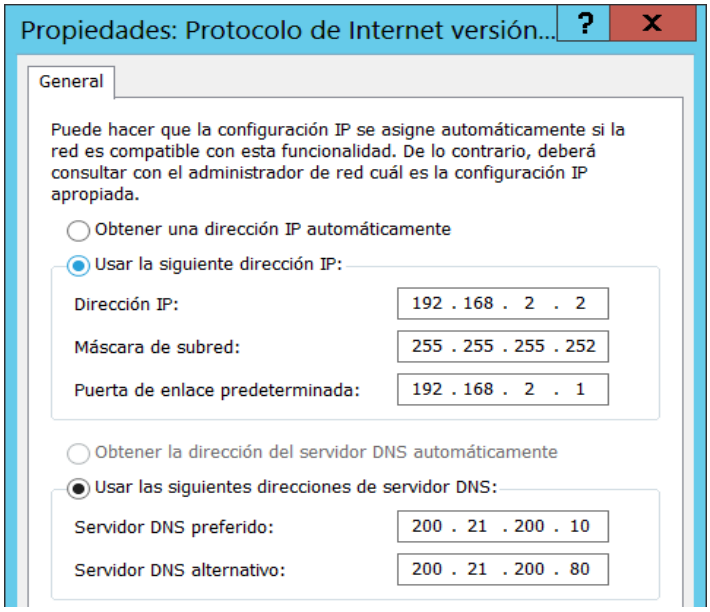

Figura 64. Conexión WAN

c. Instalación del directorio activo

El Directorio Activo es la representación lógica de una organización o empresa. El directorio activo permite asignar un dominio al Servidor para que sea controlado. Orión será entonces un controlador de dominio. El dominio de System plus es systemplusdetuquerres.com.co.

Se empieza con la instalación del directorio activo. Para ello se va al Administrador del servidor, se abre Agregar roles y características y de allí se elige Servicio de Dominio de Active Directory. La instalación no es complicada. Véase figura 65.

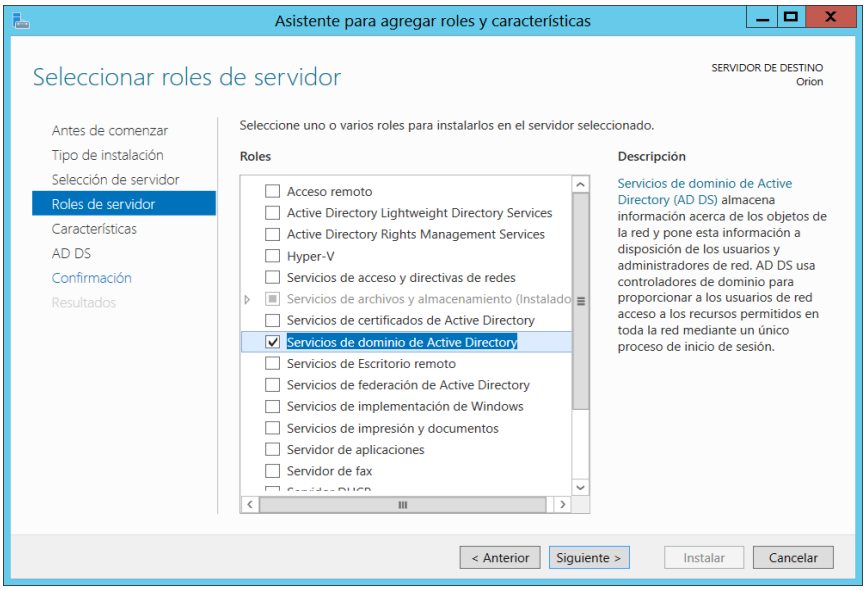

Figura 65. Agregando servicios de dominio de active directory

Hay que elegir: agregar un nuevo bosque. El dominio es systemplusdetuquerres.com.co. Véase figura 66.

Ahora Orión ya es un controlador de Dominio. Véase en el Administrador del Servidor como la ficha AD DS ya se encuentra en el panel. Figura 67.

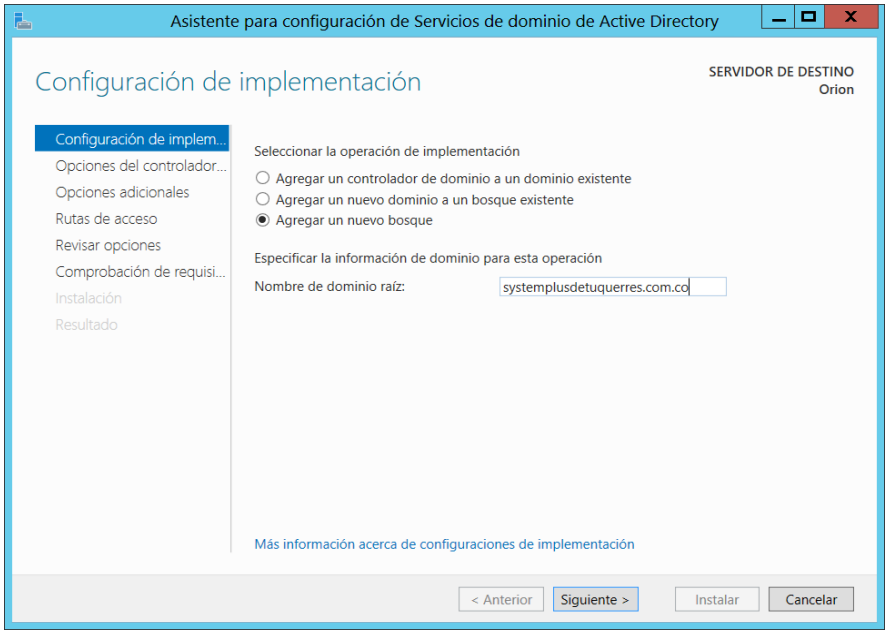

Figura 66. Agregando el dominio

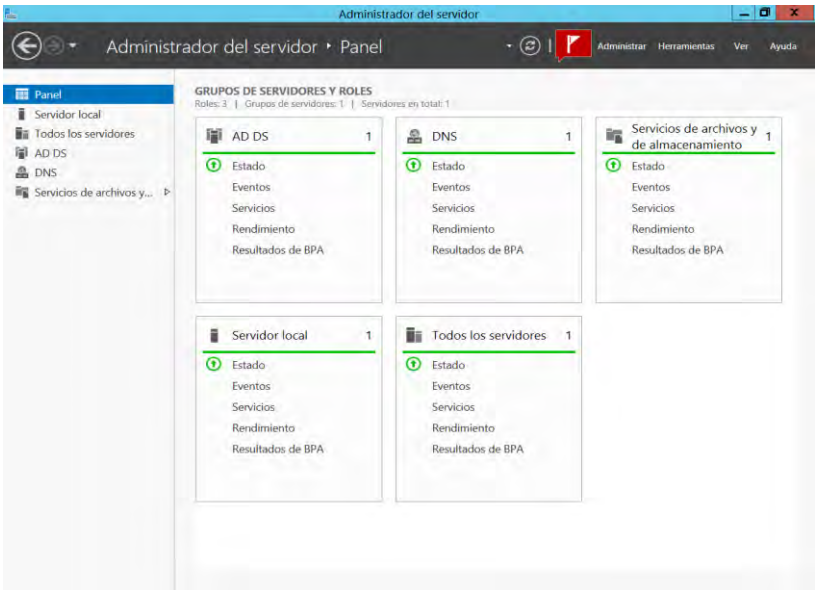

Figura 67. Active directoy instalado.

d. Adición de unidades organizativas y usuarios.

Las Unidades Organizativas son representaciones lógicas de los diferentes departamentos dentro de la empresa.

Para System Plus se crearon las siguientes Unidades Organizativas:

- Dirección
- Secretaría
- Docentes
- Alumnos
- Ventas

Para crear unidades organizativas y usuarios se abre **Usuarios y equipos de Active Directory** en la pestaña **Herramientas** del Administrador del servidor.

Véase en la figura 68 como se crean las unidades organizativas.

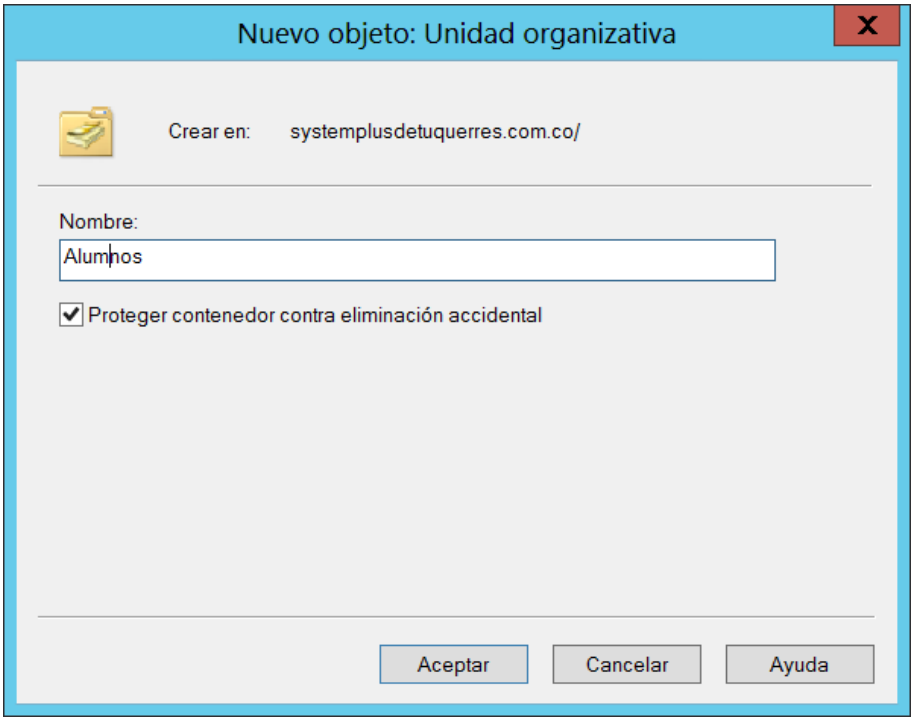

Figura 68. Creando unidades organizativas.

Los usuarios se crean dentro de cada una de las unidades organizativas.
En la siguiente lista se muestra la jerarquía que para ejemplo se creó en la red de System Plus.

- Dirección
- ✓ Richard Molina

- Secretaría
✓ Giovanny Mera

- Docentes
✓ Franco Salazar
✓ Nancy Narváez
✓ Nancy Delgado
✓ Hugo Benavides
✓ Javier Pérez

- Alumnos
✓ Juan Pérez
✓ Nelcy Chamorro
✓ Duván Ramírez
✓ Luis Suarez
✓ Pedro Carvajal

- Ventas
✓ Marcela Acosta

En la figura 69 se muestran las unidades organizativas ya creadas.

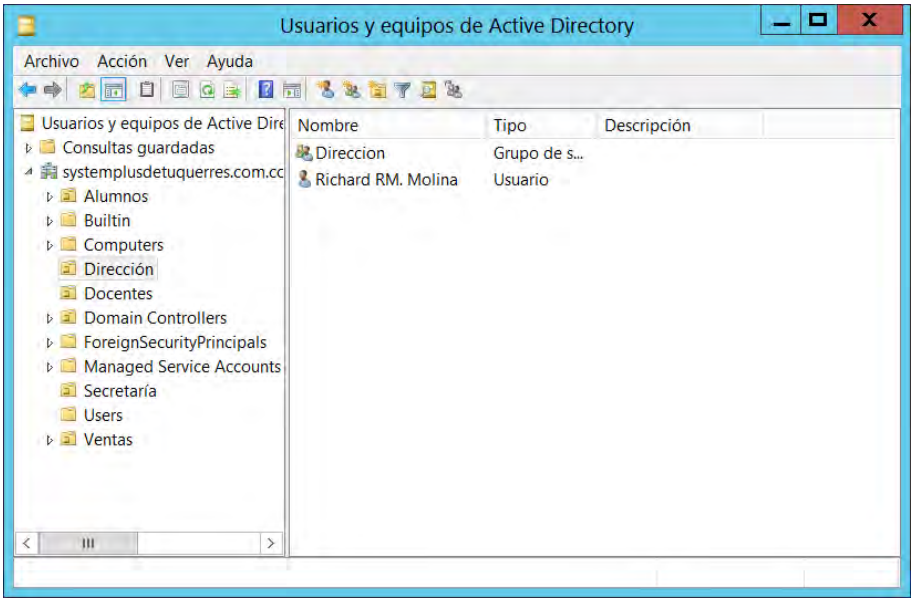

Figura 69. Unidades organizativas en el dominio

e. Instalación del servicio de enrutamiento

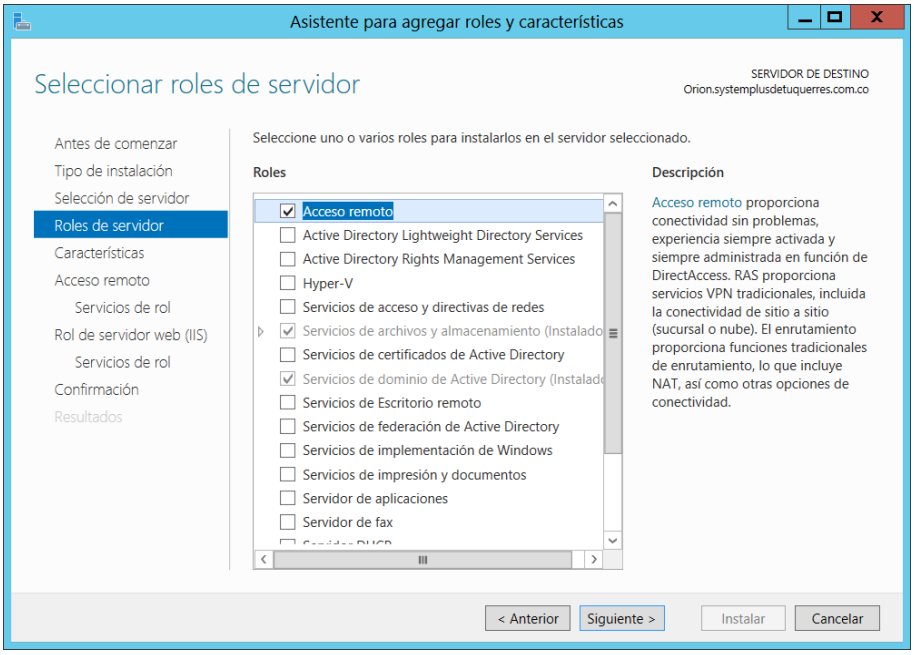

Figura 70. Instalando servicio de enrutamiento

Este servicio permite enrutar el servicio de Internet desde la conexión LAN del Orión hacia la conexión WAN del mismo servidor. Es decir, todos los computadores de la red LAN acceden a Internet por la misma conexión WAN. Específicamente esto lo hace el servicio NAT.

La instalación de este servicio se hace agregando un rol llamado Acceso Remoto. Véase figura 70.

Al configurar este servicio se debe escoger NAT para permitir que la red interna tenga acceso a Internet a través de una IP pública. Véase figura 71.

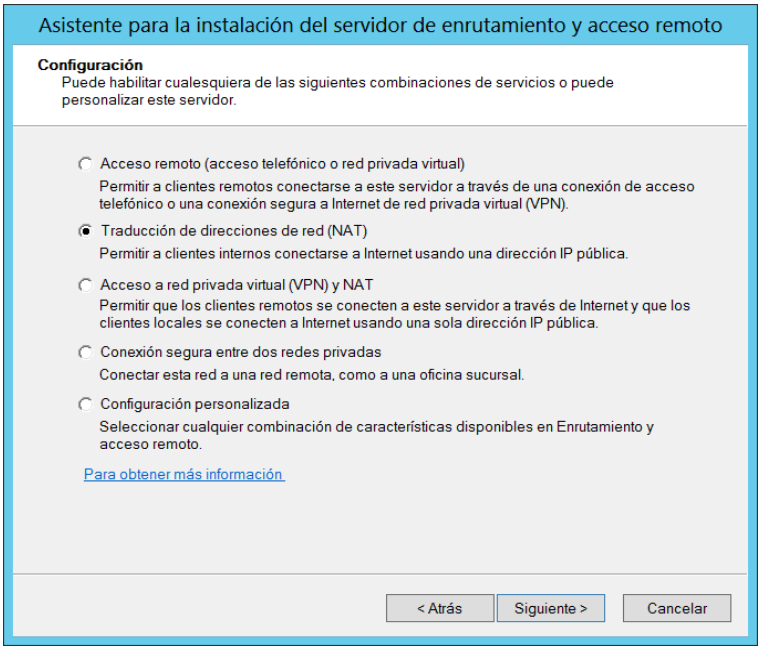

Figura 71. Instalando NAT

f. Adición de un computador con Windows 8.1 al dominio

En este momento los clientes ya pueden acceder a Internet. Lo que hay que hacer es asignar una IP al cliente que se encuentre en el rango de la tarjeta de red LAN de Orión. Hay que recordar que Orión tiene dos tarjetas de red. La IP de la LAN es 192.168.5.1/27. El computador que se unirá para las pruebas al dominio es el PC13 de la sala de informática. Este equipo tendrá la IP 192.168.5.13/27. Véase figura 72.

Ahora hay que unir el equipo al dominio. Para ello se accede a las propiedades del equipo y en lugar de dejarlo haciendo parte de un grupo de trabajo se escogerá la opción Dominio y allí se escribirá systemplusdetuquerres.com.co. Véase figura 73.

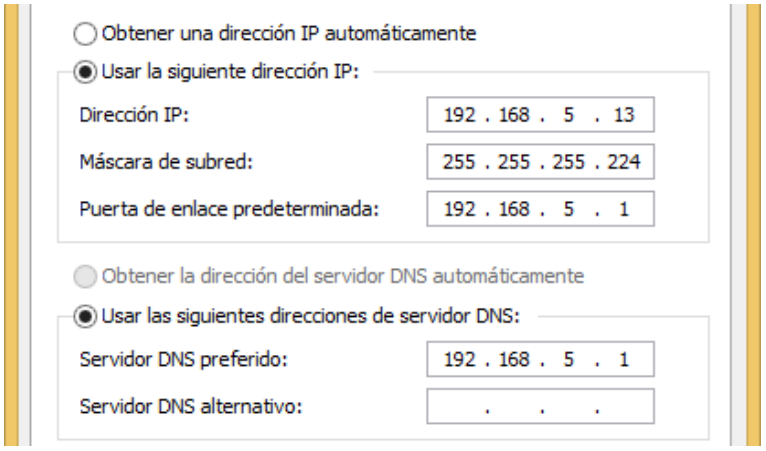

Figura 72. IP para el PC 13

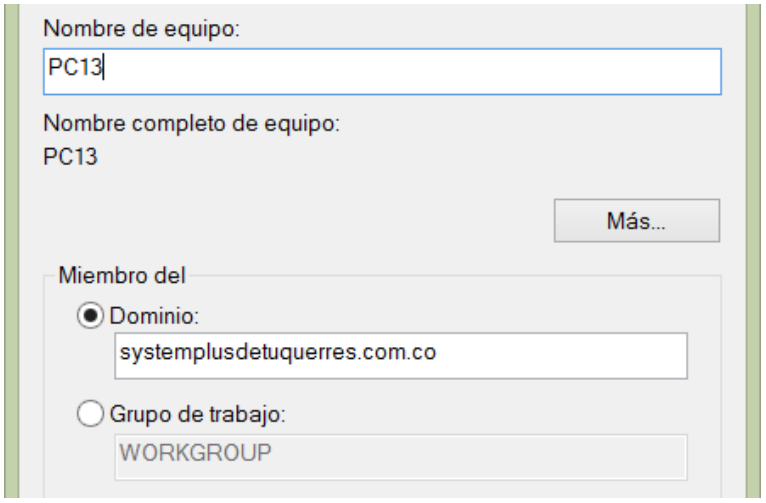

Figura 73. Uniendo el PC13 al dominio

Con os pasos anteriores el PC13 ya se encuentra en el dominio y tiene conexión a Internet.

g. Instalación del servicio DHCP

El servidor DHCP permite que el controlador de dominio asigne direcciones IP dinámicas a los clientes que así lo soliciten. Para ello se debe agregar el rol Servidor DHCP. Véase figura 74.

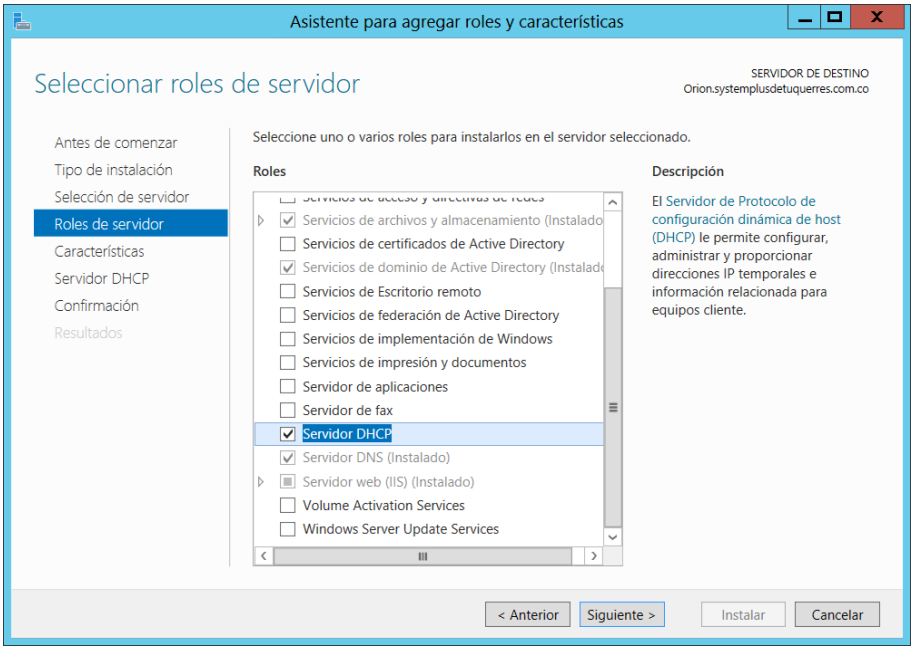

Figura 74. Agregando servidor DHCP

Una vez instalado se debe configurar el servicio. Se debe agregar un ámbito. Un *ámbito* es una agrupación administrativa de direcciones IP para equipos de una subred que usan el servicio DHCP (protocolo de configuración dinámica de host). Se crea primero un ámbito para cada subred física y, a continuación, se usa el ámbito para definir los parámetros usados por los clientes. Un ámbito tiene las siguientes propiedades:

- Un intervalo de direcciones IP desde el que incluir o excluir las direcciones usadas para las ofertas de concesión de servicio DHCP.

- Una máscara de subred, que determina la subred para una dirección IP determinada.
- Un nombre de ámbito.

- Valores de duración de la concesión, asignados a los clientes DHCP que reciben las direcciones IP asignadas dinámicamente.

- Todas las opciones de ámbito DHCP configuradas para la asignación a clientes DHCP, por ejemplo, servidor DNS (sistema de nombres de dominio), dirección IP de enrutador y dirección de servidor WINS (Servicio de nombres Internet de Windows).

- Reservas, usadas opcionalmente para garantizar que un cliente DHCP reciba siempre la misma dirección IP[50].

h. Políticas de grupo – GPO

Una GPO es una herramienta que permite asignar algunas políticas para los usuarios o equipos de un dominio con Active Directory.

Las **Directivas de grupo** (en adelante *GPO*) permiten implementar configuraciones específicas para uno o varios usuarios y/o equipos.

Para la configuración de GPO que sólo afecten a un usuario o equipo local se puede utilizar el editor de directivas locales ***gpedit.msc***. En este caso se accederá en el entorno de Servicios de Dominio de Active Directory, con la consola de administración ***gpmc.msc***.

Las GPO permiten administrar objetos de usuarios y equipos, aplicando la más restrictiva en caso de existir más de una política. Se puede usar una GPO para casi cualquier cosa, como indicar qué usuario o grupo tiene acceso a una unidad de disco, o limitar el tamaño máximo que puede tener un archivo.

Las GPO se pueden diferenciar dependiendo del objeto al que configuran y se pueden entender en distintos niveles:

- **Equipo Local:** tan solo se aplican en el equipo que las tiene asignadas independientemente del dominio al que pertenezca.
- **Sitio:** se aplican a los equipos y/o usuarios de un sitio, independientemente del dominio.
- **Dominio:** se aplican a todos los equipos y/o usuarios de un dominio.
- **Unidad Organizativa (*OU*):** se aplican únicamente a los equipos y/o usuarios que pertenecen a la OU.

Dentro de la configuración de directiva se puede acceder a lo siguiente:

- Configuración de equipo
- Configuración de usuario

[50] https://technet.microsoft.com/es-es/library/dd759218.aspx

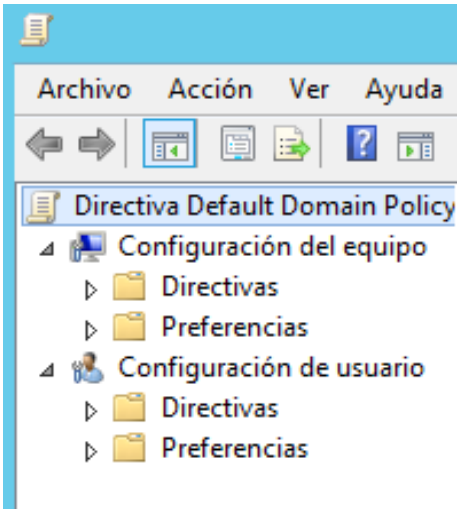

Figura 75. Menús de las directivas de grupo
Fuente: https://cetatech.ceta-ciemat.es/wp-content/uploads/2014/12/gpedit.png

- **Creación de una GPO**

Para la creación de una GPO se debe ingresar a administración de directivas de grupo de Windows Server. Véase figura 76.

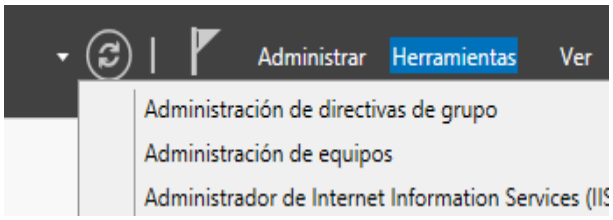

Figura 76. Directivas de grupo
Fuente: : https://cetatech.ceta-ciemat.es/wp-content/uploads/2014/12/gpedit.png

Aparecen las GPO del dominio.

Para crear una nueva GPO desde cero, pulsar en **Objetos de directiva de grupo** con el botón derecho y seleccionar **Nuevo.**

Ahora se debe dar el nombre a la nueva GPO. Véase **(Figura 77)**.

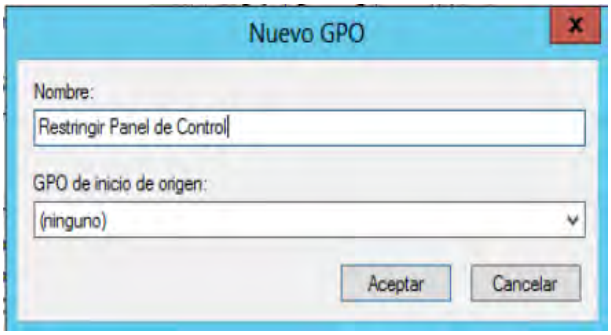

Figura 77. Creando una GPO

Si se quiere que la GPO solo afecte a una UO se debe crear esa GPO dentro de esa unidad haciendo el vínculo correspondiente.

Ahora se debe editar la GPO. Véase **(Figura 78).**

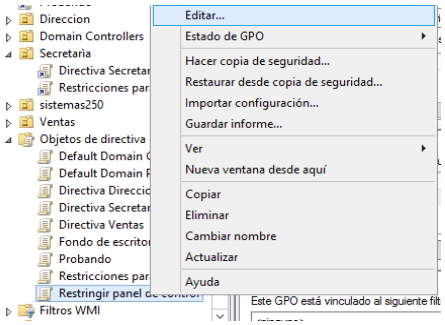

Figura 78. Editar la GPO

- ✓ **GPO para restringir el acceso al panel de control**

Para el caso de restringir a los usuarios el acceso al panel de control se debe acceder a ***Configuración de Usuario – Directivas – Plantillas Administrativas – Panel de Control*** y habilitar la GPO para el elemento ***Prohibir el Acceso a Configuración de PC y Panel de Control*.** Véase figura 79.

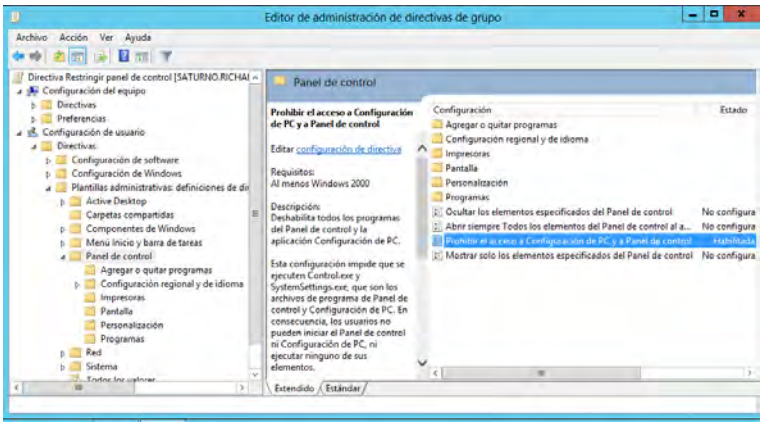

Figura 79. GPO para restringir acceso al panel de control

✓ **GPO para fondo de pantalla**

Para usar un mismo fondo de pantalla para los usuarios del domino se debe acceder a la siguiente ruta: ***Configuración de Usuario – Directivas – Plantillas Administrativas – Active Desktop – Active Desktop.*** Allí se deben habilitar tres elementos:

- Habilitar Active Desktop
- No permitir cambios, y
- Tapiz del escritorio

En este último se debe indicar la ruta donde se encuentra la imagen JPG que se va a usar como fondo de escritorio. Esta imagen se debe previamente almacenar en una carpeta compartida para todos los usuarios del dominio con permisos de solo lectura. Véase figura 80.

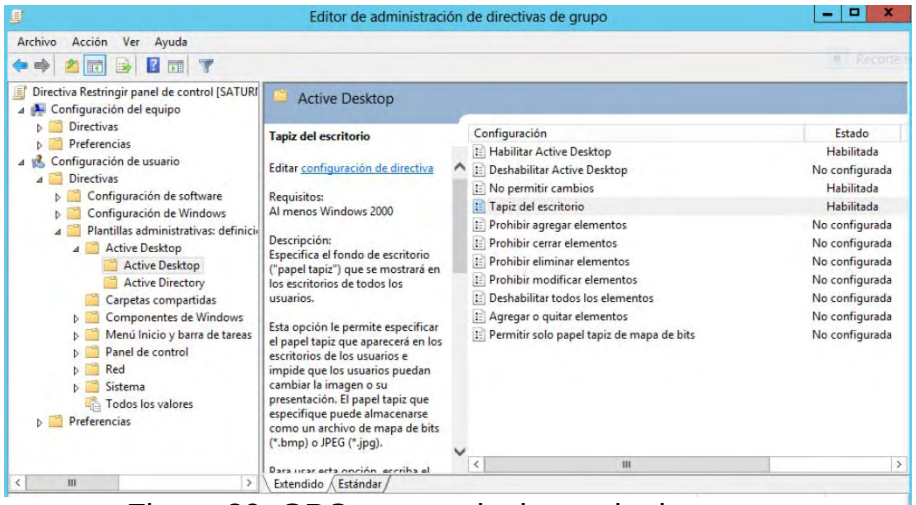

Figura 80. GPO para tapiz de escritorio

Es importante tener en cuenta que para que las GPO se apliquen es necesario

Actualizar las directivas de grupo mediante el comando gpupdate /force tanto en el servidor como en los equipos clientes.

4.1.2.3 Configuración del accesspoint TP-LINK. Se había explicado en apartes anteriores que la red inalámbrica no se administrará desde el RouterBoard sino desde el AccessPoint. El AccessPoint se conectará al RouterBoard en la interfaz 3, es decir, la interfaz del HotSpot. Esto se hace para que los usuarios de la red inalámbrica se autentiquen en un Portal Cautivo. De todas maneras la red estará protegida por una contraseña con seguridad WPA2.

Es importante recordar que el HotSpot tiene dirección de red 192.168.3.0. La interfaz HotSpot tiene IP 192.168.3.1/24 y la interfaz WAN del AccessPoint 192.168.3.2/24. Véase figura 81.

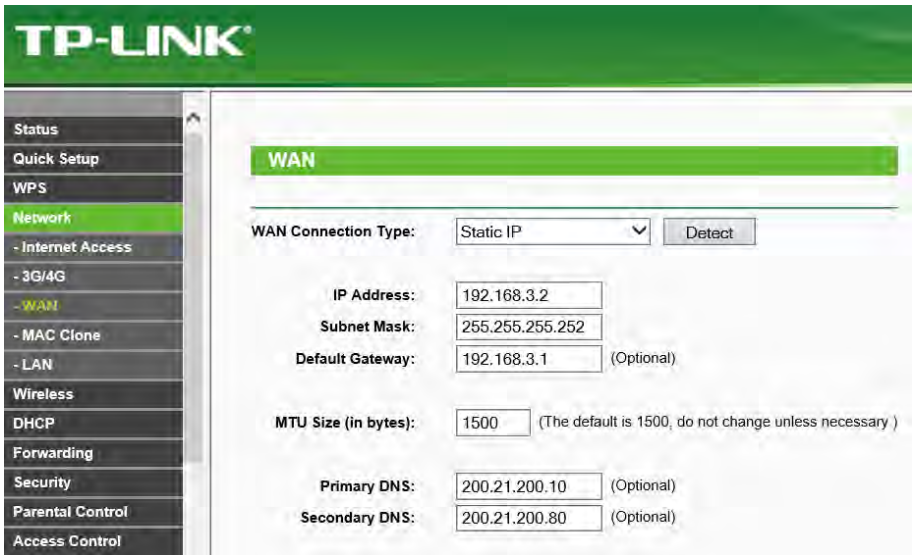

Figura 81. Configuración WAN del accesspoint

La configuración LAN del AccessPoint será el rango de red que tomarán los clientes de la red inalámbrica. El rango está en la red 192.168.4.0. La IP de la interfaz LAN del AccessPoint será 192.168.4.1/27. Véase figura 82.

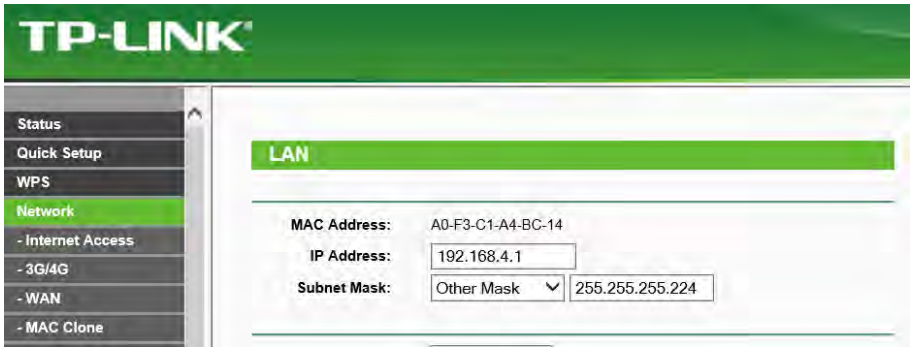

Figura 82. Configuración LAN del ACCESSPOINT

Ahora solo queda realizar la configuración inalámbrica del AccessPoint. La red se llamará System Plus. Véase figura 83.

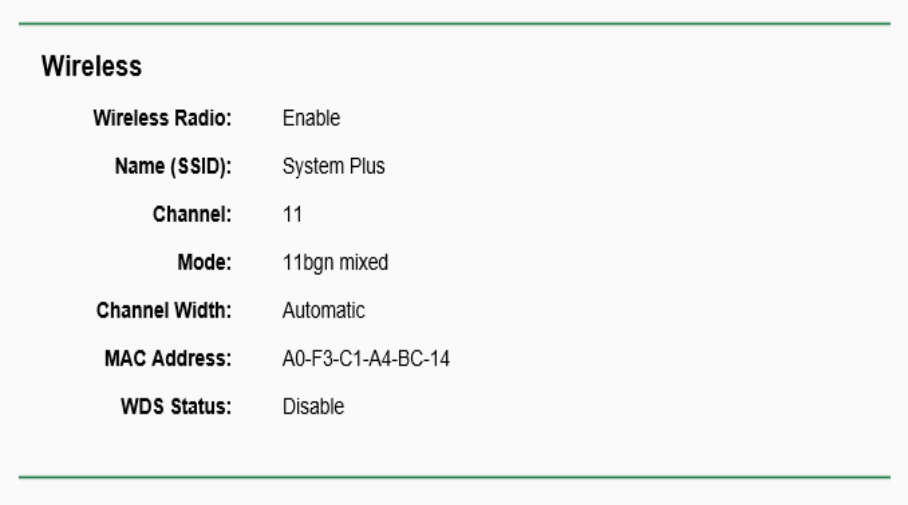

Figura 83. Configuración de la red inalámbrica del ACCESSPOINT TP-LINK

4.1.3 Fase 3. Diseño Físico de la red de System Plus. Para el diseño físico de la red hay que tener en cuenta que se parte de la red existente. Lo que se va a agregar a la red es un RouterBoard y un Servidor con Windows Server 2012.

Lo que cambiará en la red es la forma como los clientes se autentiquen en el servidor. Antes lo hacían ante un servidor Proxy. Ahora lo hacen ante un Servidor con Windows Server 2012 quienes se conectan por cable y ante un RouterBoard quienes se conecten de forma inalámbrica.

La ventaja es que todos los usuarios que usen la red deben estar registrados en el dominio o en el RouterBoard. Véase el nuevo plano de la red en la figura 84.

Figura 84. Nuevo plano de la red de system plus

Para mayor entendimiento se anexa la imagen del área de sistemas. Véase figura 85.

Figura 85. Área de sistemas

4.1.4 Fase 4. Pruebas, Optimización y Documentación de la red. Es importante recordar que en los alcances del proyecto se delimita la cuarta fase de la metodología a realizar simplemente la optimización de la red.

Para optimizar la red lo que se hizo fue hacer una revisión minuciosa de los puntos de red. Los puntos que estaban en mal estado, se volvió a poncharlos.

Igualmente se volvió a distribuir los dispositivos de red para una mejor organización y entendimiento sobre el funcionamiento de la red de System Plus de Túquerres. Véase figuras 86, 87 y 88.

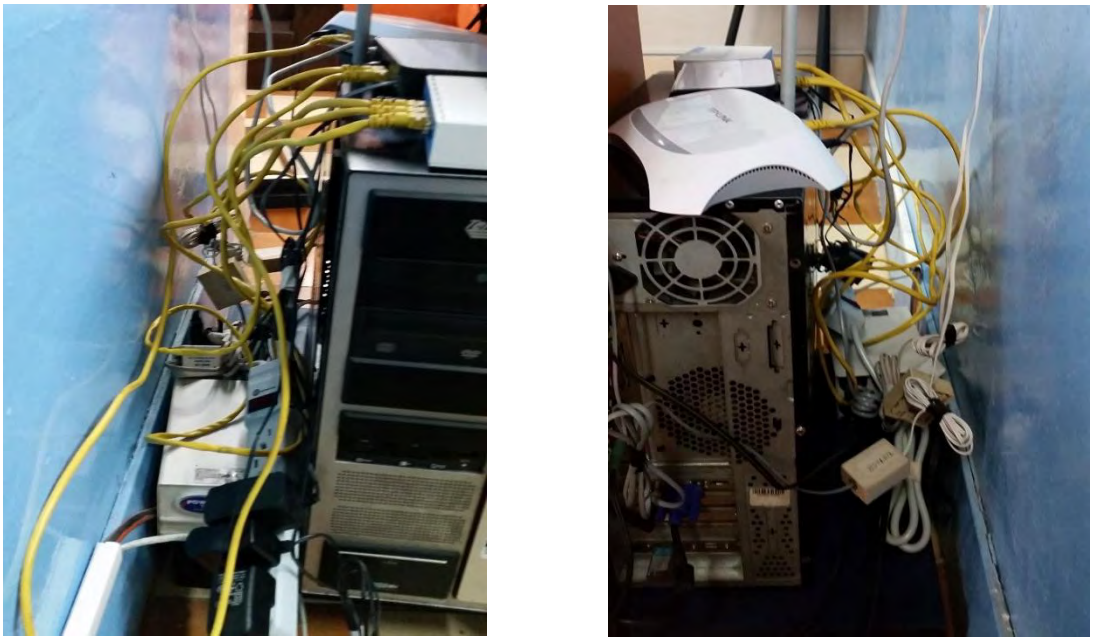

Figura 86. Conexión de los dispositivos de red antes de la implementación del proyecto

Figura 87. Conexión de los dispositivos de red después de la implementación del proyecto

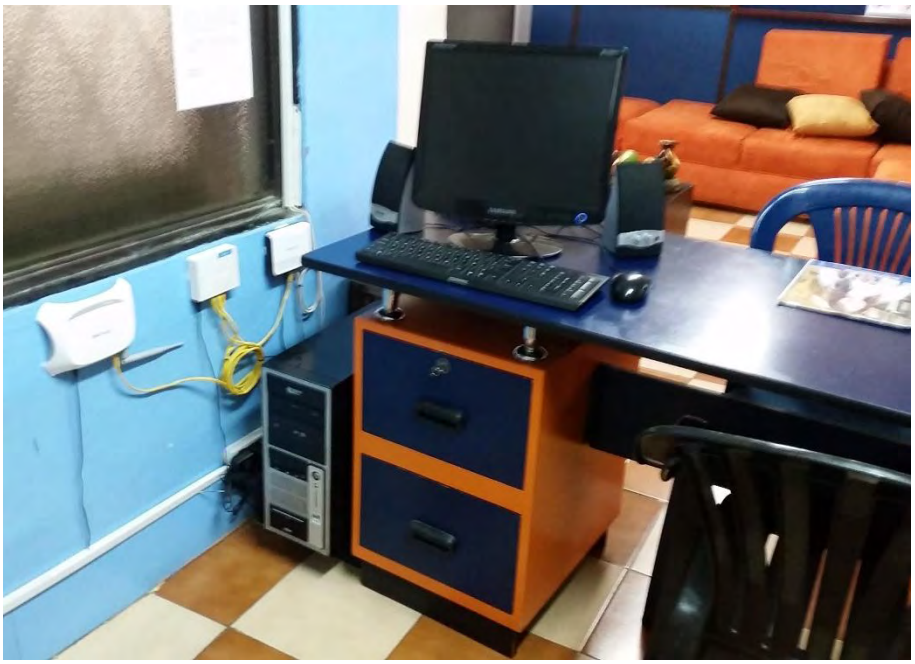

Figura 88. Área de Sistemas en system plus de Túquerres

A continuación se muestran algunas fotografías de System Plus de Túquerres para hacerse una idea de cómo está la institución en la actualidad.

Véase figuras 89, 90, 91, 92, 93 y 94.

Figura 89. Aula de teoría 1

Figura 90. Aula de teoría 2

Figura 91. Área de sistemas. Vista frontal

Figura 92. Aula de práctica. Vista 1.

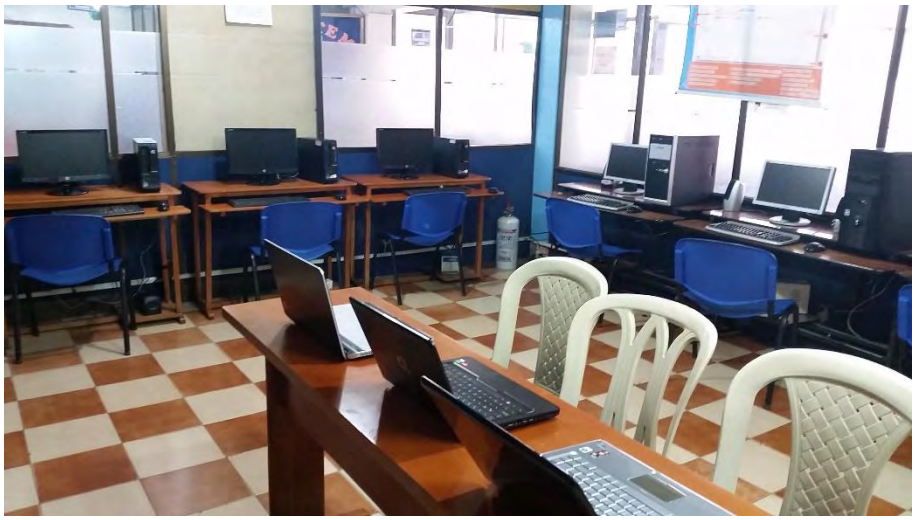

Figura 93. Aula de práctica. Vista 2.

Figura 94. Sala de estar

5. CONCLUSIONES

Se mejoró la distribución física de los dispositivos, logrando optimizar la red informática de System Plus de Túquerres.

Se implementó un RouterBoard de Mikrotik para hacer un mejor control de los usuarios que usan la red, específicamente se configuró un HotSpot para autenticar los usuarios en un portal cautivo.

El presente trabajo realizado en la empresa System Plus de Túquerres permitió realizar un diagnóstico de la situación de la red antes de implementar este proyecto, encontrando deficiencias a la hora de controlar los usuarios que acceden a la red tanto por cable como a la red inalámbrica.

Con el uso de nuevos dispositivos en la red de System Plus de Túquerres, tal es el caso de un RouterBoard, se puede afirmar que los nuevos sistemas operativos diseñados para redes permiten simplificar significativamente las tareas a la hora de configurar y administrar una red.

RouterOS es un sistema operativo para redes basado en Linux, que proporciona un alto grado de seguridad a la red.

6. RECOMENDACIONES

- Cambiar, si se requiere, los componentes de hardware y actualizar RouterOS a la última versión, para estar a la vanguardia de la tecnología.

- Aumentar el ancho de banda, para brindar un mejor servicio en System Plus de Túquerres.

- Asignar los diferentes tipos de velocidad que se relacionen a grupos específicos, es una buena alternativa para la eficiente administración de ancho de banda en el Hotspots y así brindar a cada usuario lo que va a necesitar para realizar una determinada tarea.

BIBLIOGRAFÍA

Consultas a las páginas Web:

- Análisis, Diseño e Implementación de una Red LAN por medios guiados y no guiados en el Colegio Técnico Semi-Presencial Intercultural Bilingüe “Rumiloma”; http://ti-prosoft.com/Docslink/Analisisred.pdf Fecha de consulta 12 de diciembre del 2015.

- Mikrotik; Routers y Wireless; http://www.mikrotik.com/; Fecha de consulta 17 de diciembre de 2015.

- Routerboard.com; http://routerboard.com/RB941-2nD; Fecha de consulta 15 de diciembre de 2015.

- Ryohnosuke.com; Configurar Mikrotik Routerboard HotSpot – Portal cautivo; http://www.ryohnosuke.com/foros/index.php?threads/334/; Fecha de consulta 16 de diciembre de 2015.

- Sopoerteti.com; Administración de Windows Server 2012; https://blog.soporteti.net/; Fecha de consulta 18 de diciembre de 2015.