INSTITUTO TECNOLÓGICO DE TUXTLA GUTIÉRREZ.

ING. ELECTRÓNICA

REPORTE TÉCNICO DE RESIDENCIA PROFESIONAL

REESTRUCTURACIÓN DE RED INALAMBRICA UNACH

INTEGRANTE:

ALAN RODRÍGUEZ DOMÍNGUEZ

9° SEMESTRE

ASESOR INTERNO.

M.C. RIGOBERTO JIMÉNEZ JONAPÁ

ASESOR EXTERNO

M.MARCOS PAUL GONZÁLES VÁZQUEZ

EMPRESA:

“UNACH, COORDINACION EN TECNOLOGIAS DE INFORMACION”

PERIODO:

ENERO-JUNIO 2014

TUXTLA GUTIERREZ, CHIAPAS

INDICE

Capítulo 1.

Capítulo 2

CAPITULO 1

Reporte de residencia

INTRODUCCIÓN

En la actualidad Cada vez son más usadas las conexiones inalámbricas para tener conexión de red. El uso de las Tecnologías de Información ha alcanzado rápidos cambios; Se evidencia que su aplicabilidad proporciona mejores construcciones de instrumentos para atender las actividades diarias que se desempeña en la universidad tanto alumnos como trabajadores. Desde este punto de vista, se puede visualizar la importancia presente y futura de esta tecnología.

El dominio de esta tecnología servirá para mejorar la calidad del servicio.
Es necesario que se realicen adaptaciones tecnológicas que permitan el único acceso a esta información hacia la comunidad universitaria. De esta manera se asegura de ampliar la capacidad de procesar y adaptarse a ello. Con ello también se necesitan innovaciones respecto a otros conjuntos de técnicas,

Distribuir esa tecnología es una labor importante y se requiere de distintos conocimientos para poder llevar a cabo esa función.
El poder distribuir, ordenar y sobre todo tener el control para poder administrar cada uno de las tecnologías requiere de un trabajo adecuado y lleva un largo proceso.

Sin lugar a dudas, estas denominadas tecnologías crean nuevos entornos, establecen nuevas formas de interacción de los usuarios con las herramientas donde cada uno desempeñan roles diferentes, y el conocimiento contextualizado en el saber, y el que hacer. En este sentido, el propósito de la residencia se orientó hacia instrumentos para lograr un mejor desempeño, aportar conocimientos tecnológicos para poder tener la mayor capacidad posible y que tenga un alto grado de fluidez. Al igual analizar y corregir ciertos factores que alteren la red. Que requieren conocimientos en el manejo de la red y de las tecnologías que se describirán a lo largo del reporte.

DATOS GENERALES DE LA EMPRESA

UNIVERSIDAD AUTONOMA DE CHIAPAS

COORDINACIÓN DE TECNOLOGIAS DE INFORMACION

DOMICILIO

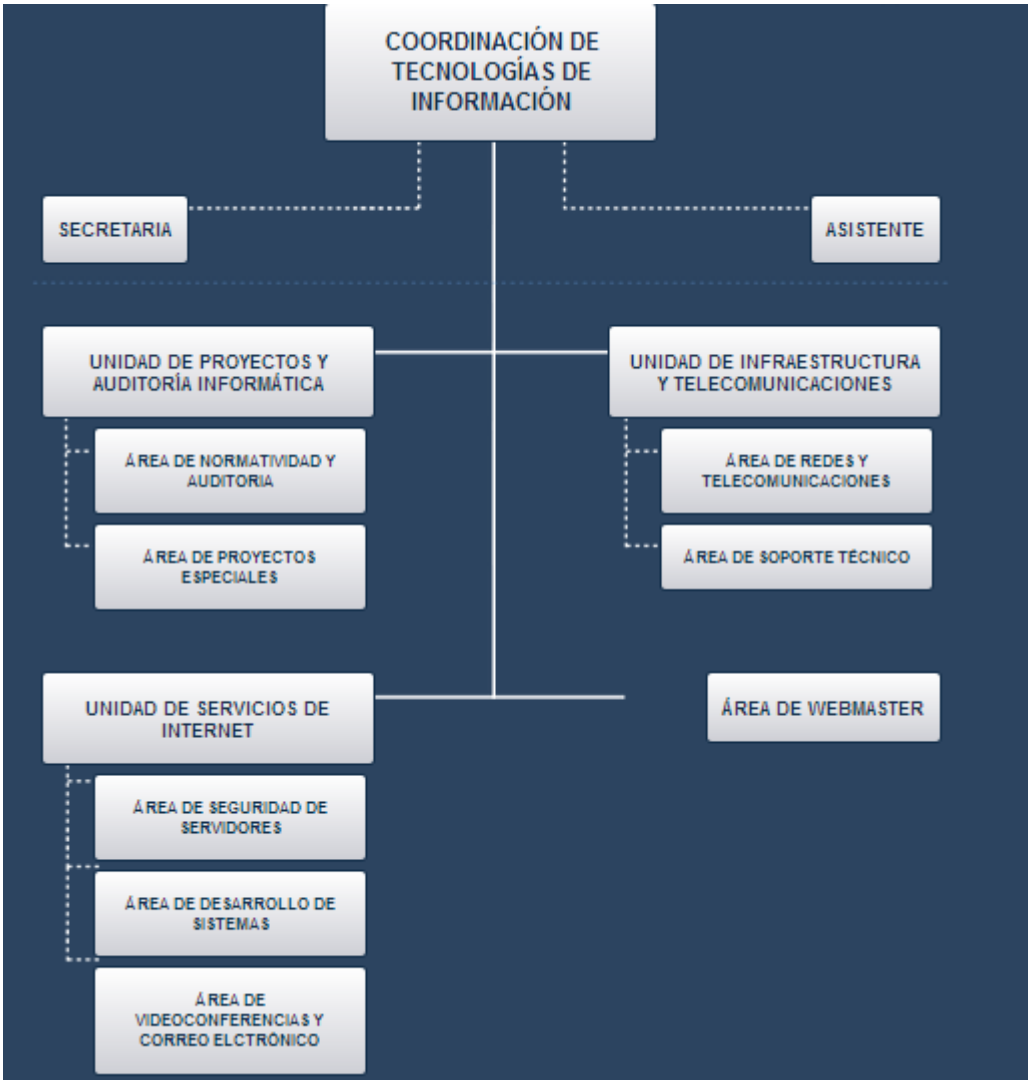
Boulevard Belisario Domínguez Km. 1081 Colina Universitaria S/N C.P. 29020

Tuxtla Gutiérrez, Chiapas.

GIRO

Publico.

ORGANIGRAMA



MISIÓN

Impulsar, fomentar y desarrollar aplicaciones y servicios tecnológicos que simplifiquen el intercambio de información y de comunicación en la comunidad universitaria, incorporando el conocimiento y los avances de la ciencia y la tecnología para potenciar su desarrollo y su capacidad de respuesta a las necesidades contemporáneas de la sociedad de la información y del conocimiento.

VISIÓN

Ser la entidad normativa del desarrollo tecnológico para la universidad que promueva soluciones integrales en la implementación de ambientes virtuales, gestión, aprendizaje y colaboración, impulsando la mejora continua de la comunidad universitaria.

DESCRIPCION DE LA EMPRESA

La Red Universitaria surge a raíz del proyecto RUTyC (Red universitaria de Teleinformática y Comunicaciones), propuesto a nivel nacional en el que se ofreció participar a la Universidad Autónoma de Chiapas, junto con la Universidad de Salamanca, la Secretaria de Educación Pública, la UNAM y Villahermosa. Durante la administración del Lic. Jorge Arias Zebadúa, es tomada la decisión de realizar el proyecto con el fin de ir a la vanguardia en la era de la información y evitar caer en la obsolescencia. Para el desarrollo e implantación de todo el proyecto, el capital fue aportado en su mayor parte por FOMES, seguidamente por la Universidad y a su vez del fideicomiso SEP-UNAM, para la capacitación de la formación de personal para operar la Red. En 1991 da inicio como un proyecto piloto, en el cual se instala la red Satelital, creándose a la vez las oficinas de la Red Universitaria, la cual va creciendo y ampliándose con la instalación de la fibra óptica y los nodos a Villa flores, Tapachula y San Cristóbal. El enlace Satelital era proporcionado por TELECOM, actualmente privatizado con el nombre de SATMEX. El proyecto era interconectarse a las Universidades mencionadas para compartir información y la base de conocimientos con los demás. Inicia como una Red local.

El proyecto no comprendía el enlace a la Red Mundial denominada Internet, pero debido a las ventajas y las nuevas tecnologías de comunicación y de los servicios que se obtienen, fue necesario estar conectados a esta nueva era de la información que hoy día es la base para poder comunicarse tanto a nivel nacional como mundial, unos de los beneficios que ha obtenido la Universidad con esta tecnología es darle a toda la comunidad universitaria la oportunidad de visitar lugares de interés, para realizar sus tareas y para su formación profesional como el servicio de E-mail y otras ventajas que nos ofrece el estar conectados a la Red mundial. En el año de 1994 recibe el nombre de Red Unach, y actualmente es administrada por la Unidad de Redes y Telecomunicaciones (URyT). Red Unach inicio con Redes locales de datos, en un principio se instalaron Redes Novell con el protocolo IPX, a raíz de que se realiza la conexión a Internet, se asigna un dominio ante NIC-México y una clase B. Se implanta el protocolo de comunicación TCP/IP para lo cual era necesario registrar un dominio ante NIC para obtener el rango de la dirección IP, que actualmente corresponde al dominio asignado. Actualmente los enlaces terrestres son proporcionados por TELMEX a Tapachula, San Cristóbal, Villa Flores. La salida actualmente a Internet es por medio de UNINET

Justificación

Las tecnologías de la información representan una herramienta cada vez más importante en las empresas, sin embargo el implementar un sistema de información de una empresa no garantiza que ésta obtenga resultados de manera inmediata y a largo plazo. La residencia se pretende hacer con la finalidad de mejorar la comunicación de los edificios de la UNACH Debido al aumento de usuarios y debido a diversidad de los equipos que maneja una sola persona en la actualidad, la demanda de la comunicación inalámbrica es mucho mayor y va en aumento. Es por eso tener en cuenta la configuración y el uso de equipos adecuados para poder responder a la necesidad de las diferentes áreas y brindarles el servicio adecuado para sus actividades para un mejor desempeño. Con el fin y único propósito de poder brindarles una mayor comodidad en el trabajo, tener la activa y completa comunicación entre áreas y tener así los beneficios de conectividad de red inalámbrica, cableado y servicio telefónico y así mantener la comunicación adecuada monitoreando los desperfectos y realizando un trabajo técnico óptimo para que el desempeño sea mayor y tenga un funcionamiento a largo plazo.

OBJETIVOS

Objetivo General.

Mantenimiento, reparación de la infraestructura de equipos de las áreas de punto de acceso para la comunicación entre las diferentes áreas de comunicación de la UNACH.

Objetivos específicos.

- Planificar, administrar, expandir y mantener la operatividad de la infraestructura de telecomunicaciones de la Universidad y del acceso a Internet, además organizar y realizar las actividades de soporte técnico en hardware y software.
- Administrar las direcciones IP y protocolos de red de la universidad, y coordinar con las dependencias y oficinas de la universidad para su distribución adecuada.
- Velar por el buen funcionamiento de la telefonía en servicio a la comunidad universitaria.

Problemas a resolver.

1. Mantenimiento a los equipos de comunicación y de conectividad inalámbrica
2. Realizar diagnóstico de los equipos que no tenga una buena operatividad para realizar nueva configuración o reparación, debido al mal funcionamiento.
3. Ver el tendido de cableado de red así como de telefonía y observar si presenta algún daño o si requiere de un nuevo cableado, dependiendo de dónde se requiera hacer el tendido de cable, analizar qué tipo de cable es el adecuado.
4. Mala configuración de los equipos y también observar el área donde se encuentra instalado para ver su seguridad y que esté protegido contra descargas que dañen los equipos.
5. Mala recepción en algunas áreas y proseguir con la nueva reubicación del ap.
6. Mal funcionamiento de equipos de conectividad, router, switch, analizar para solución o un posible cambio de equipo.

CAPITULO 2

MARCO TEORICO

REDES DE COMPUTADORAS

1. Concepto de red.

En esencia, una red es un conjunto de equipos informáticos interconectados entre sí. En toda red, hay una parte física y otra parte lógica. La parte física, está compuesta por todos los elementos materiales (hardware), y los medios de transmisión. La parte lógica (software), son los programas que gobiernan o controlan esa transmisión y la información o datos que es transmitida.

De este modo, una red de ordenadores puede ser entendida desde dos vertientes distintas:

- Conjunto de equipos interconectados con el fin de compartir recursos y transmitir información.
- Sistema de comunicación de datos entre equipos distintos.

Una red es, en definitiva, como un sistema de dos o más ordenadores autónomos que, mediante una serie de protocolos, dispositivos y medios físicos de interconexión, son capaces de comunicarse con el fin de compartir datos, hardware y software, proporcionando así acceso a un mayor número de recursos con un menor coste económico y facilitando su administración y mantenimiento.

La existencia de las redes de computadores ha facilitado enormemente el trabajo colaborativo y el uso de recursos compartidos, además de crear mecanismos de comunicación mucho más rápidos y eficientes. Para los centros docentes supone un gran ahorro de material puesto que permite disponer de periféricos y recursos de hardware más potentes y con mejores prestaciones. Todo ello realizado de forma transparente para el usuario de la red.

2. Elementos de una red

Para determinar los elementos que componen una red debemos diferenciar entre los elementos físicos y los componentes lógicos. Entendemos por componentes físicos todo el hardware y medios físicos necesarios para la comunicación entre ordenadores. Los componentes lógicos son los protocolos de comunicación y el software que permite esa comunicación. Resulta evidente que, dependiendo del tamaño de la red y las prestaciones que deseemos que nos ofrezca, estos componentes pueden aumentar en número y complejidad. Para facilitar su comprensión, vamos a centrarnos inicialmente en una red formada por dos ordenadores:

Elementos físicos:

- Dos equipos.
- Una entrada y salida física de comunicación entre cada uno de los equipos y el medio físico de comunicación.
- Un medio físico para la transmisión de datos.

Elementos lógicos:

- Software.
- Protocolos de comunicación.

La unión física entre ambos ordenadores podrá realizarse a través de puerto serie, del paralelo, a través de USB o, como es más habitual, a través de un cable de red conectado a un concentrador, aunque si se tratara de dos equipos sólo, se puede hacer a través de un cable de red de tipo cruzado. Esta comunicación entre ordenadores puede acoger tecnologías de última generación como las redes inalámbricas basadas en el estándar 802.11x o las basadas en bluetooth.

Cuando nos encontramos con redes constituidas por más de dos equipos, debemos empezar a emplear otros tipos de mecanismos de interconexión. En estos casos, la red estaría constituida por:

- Ordenadores autónomos.
- Elementos de interconexión:

-Puertos o adaptadores de red. Permiten la comunicación entre el equipo y el medio físico de comunicación.

-Medio físico para el transporte de datos.

-Medios guiados: cable coaxial, par trenzado, fibra óptica.

-Medios no guiados: ondas de radio, infrarrojos, etc.

-Mecanismos de interconexión: concentradores, conmutadores, puentes, enrutadores, cortafuegos, transceptores, MODEM, MSAU, etc. Los mecanismos de interconexión aparecen cuando es necesaria la comunicación de varios equipos con un nivel de eficiencia alto.

-Otros: terminales, acopladores, repetidores, conector RJ45, BNC, etc.

- Software de conexión y protocolos de comunicación.

3. Compartición de recursos.

La arquitectura cliente-servidor es la base para la utilización de los recursos disponibles en una red:

- Cliente: entendemos como tal cualquier ordenador, conectado a una red, de cualquier tipo.
- Servidor: es también, un ordenador, conectado a una red, pero que tiene algún recurso que puede ofrecer a la red.

El cliente solicita algún recurso y el servidor los ofrece. Es un proceso cooperativo entre cliente y servidor. Normalmente, el servidor es un ordenador más potente y con más recursos que el cliente, pero no siempre es así.

Entendemos por recurso:

- Hardware: distintos periféricos de entrada o salida, impresoras, escáneres, cámaras, sistemas de almacenamiento de datos, etc.
- Software: cualquier tipo de aplicaciones, paquetes de programas, programas, etc.
- Información: todo tipo de datos; de texto, numéricos, bases de datos, imágenes, audio, etc.

Compartición de Recursos.

Como ya hemos indicado, una red de ordenadores es, “un conjunto de ordenadores conectados entre sí y que pueden compartir información y recursos”. Es decir, los recursos instalados en un equipo pueden ser utilizados por el resto de equipos y usuarios de la red. Para limitar los accesos de los usuarios se pueden aplicar permisos y políticas.

a) Principales recursos para compartir.

Conviene destacar que, de todos los recursos que pueden ser utilizados en una red local, los que nos van a ofrecer mayores ventajas a la hora de ser compartidos son:

Unidades de almacenamiento:

En una red pueden compartirse, discos duros, unidades de CD-ROM, particiones de disco, etc. Proporcionándonos un gran ahorro en la adquisición de estos materiales. Sin embargo, más importante que este ahorro, es el poder tener la información centralizada, evitando la repetición y la dispersión de estos archivos. Esto facilita el trabajo en común, ahorrando esfuerzo y costos a la vez que se garantiza la seguridad ante pérdidas o deterioro de la información, ya que al estar centralizada, las copias de seguridad son más sencillas de realizar.

Servidor de aplicaciones:

En lugar de tener una misma aplicación instalada en cada ordenador, es mejor tener una única para todos los que la utilicen. Con esto ahorraremos costes y facilitaremos el mantenimiento reparaciones, actualizaciones, etc. En este sentido, son muy importantes las aplicaciones tipo groupware, que son aquellas que se utilizan para trabajar en grupo, por ejemplo: calendarios de grupo, planificación de trabajos de grupo, correo electrónico, etc. El incremento de productividad que esta forma de trabajar conlleva, es obvio.

Impresoras:

Las impresoras, son uno de los elementos más caros de los periféricos de una red informática, por tanto el hecho de poder minimizar el número de ellas, redunda en un importante ahorro de costes al realizar un uso más racional en la adquisición de este tipo de recursos. Evitamos tener que trasladarnos con la información de un equipo a otro y ahorramos tiempo y espacio en nuestra aula, centro, etc. Así, podremos adquirir mejores impresoras en lugar de disponer de un mayor número de ellas, aunque de menor calidad.

Acceso compartido a Internet.

Otra de las grandes ventajas de una red es el poder acceder a Internet a través de un servidor o mediante un acceso compartido. Todos los equipos, empleando una única conexión: RTB, RDSI, ADSL, etc. pueden obtener las ventajas de los servicios de Internet: correo electrónico, FTP, news, WWW, etc. Cuando disponemos de un acceso a Internet de este tipo, podemos, además, establecer una serie de medidas de seguridad mediante un cortafuego que evite el acceso a contenidos inadecuados para el ámbito educativo a la vez que protegemos nuestra red del ataque de intrusos.

b) Recursos según la organización de la red.

Según su tipo de organización, podemos tener una red:

- Distribuida: en este caso los recursos estarán distribuidos entre los distintos ordenadores que conforman la red y cada uno podrá, o no, ofrecer a los demás los recursos de que disponga.
- Centralizada: en este caso los recursos estarán centralizados en un ordenador servidor, y los demás ordenadores accederán a él solicitando sus recursos.
- Mixta: es una mezcla de ambas, con parte distribuida y parte centralizada. El grado de centralización puede ser variable en cada caso.

4 Arquitectura cliente-servidor.

La arquitectura de tipo Cliente-Servidor, se caracteriza porque tiene sus recursos distribuidos entre los distintos ordenadores que forman la red y cada uno podrá, o no, ofrecer a los demás los recursos que posea. El grado, menor o mayor, en que estén distribuidos, puede ser muy variable. Esto implica un tráfico por la red, de todo tipo de objetos, no sólo datos. La red se convierte así en un elemento crítico y, con ella, la figura de administrador de la red. El objetivo es proporcionar más potencia al usuario final, con el objetivo de aumentar la operatividad. El hecho de adoptar este tipo de arquitectura, aparte de afectar al entramado de hardware y software, supone cambios en la estructura de funcionamiento de un sistema de información.

La arquitectura Cliente-Servidor supone, normalmente, una mezcla de hardware, software y componentes de red, de distintos fabricantes. Por tanto tienen que ser arquitecturas de sistemas abiertos, capaces de utilizar hardware y software de distintos fabricantes, en contraste con los sistemas cerrados, o de un sólo fabricante. Si se quieren minimizar los costes de software y mantenimiento, el software debería residir en el servidor y, cuando el cliente lo ejecute, cargarlo en su memoria.

a) Seguridad.

Un tema importante en este modelo es la seguridad. Normalmente los servidores, debidamente configurados por el administrador, son los encargados de pedir las passwords necesarias, de identificar a los usuarios, de conceder los permisos pertinentes para acceder a los distintos recursos, etc. La seguridad es un tema clave a la hora de determinar una arquitectura. Cuando utilizamos un modelo centralizado garantizamos la seguridad desde todos los puntos de vista, sin embargo, cuando empleamos redes entre iguales obtendremos un nivel de seguridad mucho más bajo.

b) Modelos de arquitectura cliente-servidor.

- Modelo basado en servidor: en este modelo los datos residen en el servidor, pero además, hay una serie de procesos que se ejecutan también en él. Las aplicaciones cliente-servidor, en realidad se componen de dos partes, aplicación cliente, que se ejecuta en él, y aplicación servidor, que se ejecuta en el servidor.
- Las redes “punto a punto”, se pueden considerar un caso particular de este tipo de redes. Estas redes no tienen servidores, propiamente dichos, aunque, cada ordenador puede tener algunos recursos y puede ofrecerlos al resto de los ordenadores, o a algunos. En este sentido, se les puede considerar servidores. Aquí, los ordenadores pueden ser tanto clientes como servidores, dependiendo de que soliciten u ofrezcan algún recurso.
- Basada en correo electrónico (e-mail): todas las funciones son ejecutadas por el cliente y sólo las funciones de mensajería están en el servidor.
- Base de datos compartida: todas las funciones son ejecutadas por el cliente, pero los datos están en el servidor. El cliente carga la aplicación en su memoria y esta aplicación hace las llamadas necesarias al servidor de datos.

5. Tipos de Redes.

Hay varios criterios por los que se pueden clasificar las redes de ordenadores, según su tecnología, su tamaño, su topología

Por su tecnología de transmisión.

Básicamente hay dos tipos de tecnologías de transmisión: redes broadcast o de difusión y redes punto a punto.

a) Redes de difusión.

En las redes broadcast hay un único canal de comunicación, compartido por todos los ordenadores de la red. Los ordenadores envían mensajes cortos, denominados tramas, que llegan al resto de los ordenadores de la red (con las salvedades que estudiaremos más adelante. Sin embargo, esto no quiere decir que todos los mensajes tengan como destinatarios, siempre, la totalidad de los ordenadores de la red.

Los protocolos que se utilizan en estas redes deben permitir determinar cuándo un mensaje se envía a todos los computadores o cuándo lo hacen únicamente a uno, del mismo modo, deben preocuparse de controlar que no se produzcan colisiones. En la trama, aparte de la información propiamente dicha, hay un campo que indica el origen y el destino de dicha información. Pudiendo determinarse si el mensaje se envía a todos, a uno, o varios ordenadores en concreto.

Es importante entender que las redes de difusión se caracterizan por tener a todos los equipos compartiendo el mismo medio por lo que se deben establecer mecanismos que controlen el acceso de los ordenadores. Este medio compartido permite el envío de mensajes de Broadcast. De ahí que a las redes de difusión también se les denomine redes de Broadcast.

Cuando el mensaje se dirige teniendo como remitentes al resto de los equipos de la red estamos enviando un mensaje de Broadcast. En el caso de que un host realice esta operación, todos los ordenadores reciben el mensaje y lo procesan. Sin embargo, si el mensaje no es de Broadcast, al ser un medio compartido y, dependiendo del dispositivo de interconexión, puede que todos los equipos lo reciban, pero, en este caso, si la trama no iba dirigida a él, la ignora. En una red se producen mensajes de broadcast en situaciones muy diversas, por ejemplo cuando un ordenador se conecta a una red envía un mensaje de este tipo en busca de un servidor que le pueda asignar una dirección IP, también, cuando desconoce una dirección MAC dirección de la tarjeta de red del host de destino de un equipo, envía otro mensaje de Broadcast al resto de los host de su red para que alguno le pueda proporcionar esta información. En definitiva, al tratarse de un medio compartido, todos los equipos reciben los mensajes enviados por el resto, sin embargo, estos mensajes pueden estar, efectivamente, dirigidos a todos, el mensaje de Broadcast o sólo a uno de ellos, en cuyo caso el resto de los equipos ignoraría la trama recibida.

Para enviar un mensaje de broadcast es necesario utilizar un código de dirección especial, ésta es la dirección de la red, con los campos que corresponden a los host puestos a 1. Así, la dirección IP más alta que puede tener un host de una red se reserva a los mensajes de Broadcast. También es posible, enviar mensajes a un grupo de ordenadores, esto se conoce como mensaje multicast.

La diferencia entre los mensajes de Unicast, Multicast y Broadcast

En terminología de redes y comunicaciones hay que tener claro la diferencia entre estos tres términos relacionados con el envío de paquetes.

Unicast

El término unicast hace referencia al envío de paquetes o información desde un único emisor a un único receptor. Ejemplos básicos de aplicaciones unicast son los protocolos http, smtp, ftp o telnet. Actualmente es la forma predominante de transmisión en Internet.

En términos cotidianos, una comunicación unicast podría ser por ejemplo una llamada telefónica entre dos personas.

Multicast

Multicast (multidifusión) es el envío de información en una red a múltiples receptores de forma simultánea, un emisor envía un mensaje y son varios los receptores que reciben el mismo.

Si antes hablábamos de que una comunicación unicast era una llamada telefónica entre dos personas, podemos decir que una comunicación multicast podría ser una conferencia, en la que son varias las personas que se comunican entre sí. Un ejemplo claro de comunicación Multicast en Internet es un IRC.

Broadcast

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

En la vida cotidiana, un ejemplo de comunicación Broadcast es el de una emisora de radio, que emite señales sin saber quien la recibe, el receptor decide si recibirla o no, al igual que la señal de la televisión, que se envía a todos los receptores.

Para pensar: Si en una localidad cada coche pudiera circular únicamente por una serie de calles, nunca encontraría atascos ni otros vehículos que obstruyeran sus vías, pero tal vez, las carreteras estarían infrautilizadas.

En este tipo de redes, el problema principal, es la asignación del canal, ya que éste es único, y debe ser compartido por todos los ordenadores. Para solucionar esto, se han creado múltiples protocolos, que pertenecen al nivel MAC (Control de Acceso al Medio).

Hay dos métodos:

- Asignación estática: usa la multiplexación, para dividir el ancho de banda del canal entre los ordenadores que lo usan. Es decir, si un canal posee 100 Mb de ancho de banda y disponemos de diez host conectados al medio, éste es dividido en diez partes de 10 Mb, reservando una de ellas para cada uno de los host. Este sistema de asignación permite que cada ordenador no dependa del resto para comunicar aunque, si sólo necesita enviar datos uno de ellos, los otros 90 Mb están desaprovechados. Su mayor ventaja es que se evitan las interferencias y colisiones.
- Asignación dinámica: que permite gestionar la utilización de un único medio en función de las necesidades de comunicación de los equipos en cada momento; reparte el ancho de banda más eficazmente.

En este tipo de asignación se parte de los siguientes supuestos:

- Existe un número de equipos indefinido.
- Sólo se dispone de un canal de comunicación.
- Si se envían dos mensajes a la vez (tramas) se produce una colisión.
- Cualquier equipo puede comunicar en cualquier momento o se debe ajustar a unos intervalos determinados.
- Los host pueden observar la red y comprobar si el canal está ocupado. También se puede establecer un sistema en que esto no sea necesario.

En función de estos supuestos se han creado distintos protocolos de acceso al medio, en redes Ethernet uno de los protocolos más usados, es CSMA/CD (Carrier Sense Multiple Access with Collision Detection). El ordenador que quiere transmitir, examina si el canal lo está usando otro, en este caso espera para transmitir. Si hubiera un choque, la transmisión se detendría. El conjunto de normas IEEE 802.3, siguen este protocolo.

b) Redes punto a punto.

La otra tecnología, son las redes punto a punto. En este caso, las conexiones son punto a punto, entre pares de ordenadores. Se establece una comunicación directa entre los dos ordenadores. Hasta que un mensaje llega a su destino, puede pasar por varios nodos intermedios. Dado que normalmente, existe más de un camino posible, hay algoritmos de encaminamiento (routing), que lo gobiernan.

Este tipo de redes, usa dos tecnologías diferentes:

- Conmutación de circuitos: en las que se establece un “circuito” entre los dos puntos, mientras dura la conexión.
- Conmutación de paquetes: en las que el mensaje se divide en partes, denominadas paquetes, que se envían independientemente unos de otros, incluso desordenados y por distintos caminos, hasta su destino, donde se debe reordenar y recomponer el mensaje.

c) Diferencias entre las dos tecnologías.

Generalmente, las redes de área local (LAN), suelen usar la tecnología broadcast, mientras que las redes más extensas (WAN), suelen usar la tecnología punto a punto.

Las diferencias fundamentales entre las redes que usan tecnología broadcast y punto a punto son:

Broadcast

- Fundamentalmente empleada en redes locales (LAN)
- El software es más simple puesto que no necesita emplear algoritmos de routing y el control de errores es de extremo a extremo.
- Para que la estación reciba el mensaje, debe reconocer su dirección en el campo de destino.
- Un único medio de transmisión debe soportar todos los mensajes de la red, por lo que son necesarias líneas de alta velocidad (>1 Mbps)
- Los principales retrasos son debidos a las esperas para ganar el acceso al medio.
- El medio de transmisión puede ser totalmente pasivo y por ello más fiable.
- Se necesitaría duplicar las líneas en caso de que se quiera asegurar la funcionalidad ante fallos.
- Los costes de cableado de la red son menores. Sólo es necesaria una tarjeta de interface por estación.

Punto a punto

- Fundamentalmente empleada en redes de largo alcance (WAN)
- Los algoritmos de routing pueden llegar a ser muy complejos. Se necesitan dos niveles de control de errores: entre nodos intermedios y entre extremos.
- La información se recibe. Una vez leído el mensaje se procesa si va dirigido a la estación, o se reenvía si tiene un destino diferente.
- Varias líneas de comunicación pueden funcionar en paralelo, por lo que pueden usarse líneas de baja velocidad (2-50 Kbps)
- Los principales retardos son debidos a la retransmisión del mensaje entre varios nodos intermedios.
- El medio de transmisión incluye nodos intermedios por lo que es menos fiable.
- La redundancia es inherente siempre que el número de conexiones de cada nodo sea mayor de dos.
- Los costes de cableado son superiores, y la estación requiere al menos dos tarjetas de interfaces.

5.2. Por su tamaño.

Por su tamaño pueden dividirse en:

a) Redes de área local (LAN: Local area network).

Son redes privadas con un medio físico de comunicación propio. Se consideran restringidas a un área geográfica determinada: centro docente, empresa, etc. aunque puedan extenderse en varios edificios empleando distintos mecanismos y medios de interconexión. En las redes de área local, la longitud máxima de los cables, que unen los diferentes ordenadores, puede ir desde 100 metros, con cable de par trenzado, hasta algunos kilómetros en segmentos unidos por fibra óptica. La velocidad de transmisión típica va desde los 10 Megabit/s hasta 1 Gigabit/s en la actualidad.

b) Redes metropolitanas (MAN: Metropolitan area network).

Este tipo de redes es similar en su estructura y funcionamiento a las LAN, si bien ocupan una mayor extensión geográfica y pueden ser públicas o privadas. Disponen de una serie de estándares específicos que las diferencian de las redes LAN y WAN. Uno de estos estándares es conocido como DQDB (Bus Dual de Cola Distribuida) y está adaptado a las características de las redes MAN, que no necesitan elementos de conmutación y dirigen la información empleando dos cables unidireccionales, es decir, un bus doble en el que cada uno de los cables opera en direcciones opuestas. En este tipo de redes no se pueden producir colisiones ya que no es un medio Ethernet, sino que se procuran métodos para el control de acceso al medio, los generadores de tramas emiten de forma regular una estructura de trama que permite la sincronización de los equipos a la hora de transmitir, ya que podrán acceder al medio cuando un contador interno (sincronizado por la trama enviada por el generador) se ponga a cero. Cada nodo recibe la información por un bus de los nodos posteriores y envía por el otro, de manera que puede estar emitiendo y recibiendo información de forma simultánea.

c) Redes de área extensa (WAN: wide area network).

Consisten en ordenadores y redes de área local y metropolitanas, unidas a través de grandes distancias, conectando equipos y redes a escala nacional o internacional. La comunicación se consigue mediante routers (encaminadores) y en algunos casos gateways (llamados también convertidores de protocolos o pasarelas).

Sus características son:

- Velocidades de transmisión lentas comparadas con redes de área local.

- Alta tasa de errores, necesitando sistemas de detección y recuperación de errores.
- Posibilidad de reconfiguración de las redes debido a su menor fiabilidad.
- Técnicas de almacenamiento y reenvío (Store and Fordward) en los nodos de comunicación. Están compuestas por un conjunto de nodos interconectados donde los datos son encaminados a través de los mismos desde un emisor hasta el receptor.

La comunicación entre los nodos se puede establecer mediante tres sistemas de conmutación:

Conmutación de circuitos: Se establece una comunicación dedicada entre los nodos. El camino queda fijado durante toda la llamada se transmitan o no datos. El circuito de llamada se establece de manera similar a una llamada telefónica y se comporta como un circuito dedicado, aunque solo mientras dura la conexión.

La conmutación de circuitos es la técnica que emplean las líneas telefónicas. Cada teléfono está conectado a una central, que al recibir la solicitud de llamada hacia un número de teléfono, abre una línea hacia ese número o hacia otra central, hasta que se consigue que exista un circuito real de comunicación entre ambos teléfonos. Es decir, la petición de llamada y la conversación ocupan una línea que puede circular por todo el globo, conectando una a una las líneas que unen ambos teléfonos. De ahí que, cuando llame alguien a nuestro teléfono y estemos hablando, no puede acceder a la línea, ya que está ocupada.

Conmutación de mensajes: El emisor añade al mensaje la dirección de destino pasando de un nodo al siguiente sin establecer un circuito físico entre los nodos que se comunican.

Conmutación de paquetes: Consigue mejor rendimiento que las anteriores. La información se divide en paquetes grupos de bits que tienen una parte destinada a los datos propiamente dichos y otra a las señales de control como son el origen y el destino, los mecanismos de recuperación de errores, etc. Tienen una longitud máxima permitida y si se excede pueden ser divididos en paquetes más pequeños. Se retransmiten nodo a nodo y se certifica sin están libres de errores antes de reenviarlos al nodo siguiente.

En una red WAN pueden darse distintos tipos de tecnologías, lo que supone que, en algunos casos, una trama de datos deba dividirse todavía más, en función del paso de una red a otra. Una vez que se ha producido esta división, los paquetes no se vuelven a unir hasta el host de destino.)

d) Internet.

Internet es una red de redes. Ya que Conecta multitud de redes, de distinta índole, tamaño, características, etc., distribuidas por todo el mundo. Las redes

pueden ser públicas: institucionales, educativas, o privadas: empresariales, de ocio, etc. La conexión es posible entre redes de distintas plataformas y ambientes. Esta conexión, entre redes tan distintas, es posible porque todas utilizan el mismo protocolo de comunicación, el TCP/IP. En realidad son dos protocolos, TCP (Transmisión Control Protocol) e IP (Internet Protocol).

Los ordenadores se suelen comunicar usando la tecnología punto a punto, por medio de paquetes, que contienen, por un lado, la dirección del origen y el destino, y por otro, los datos a transmitir. Todo este proceso, está regido por una serie de normas incluidas en los protocolos TCP/IP. Cada ordenador está identificado inequívocamente por su dirección IP. Está constituida por cuatro números separados por puntos, de la forma 172.244.232.16 (cuatro octetos binarios). Las tramas de datos circulan por las distintas redes dirigidas por los enrutadores, hasta que llegan a la dirección de destino. Además de la dirección IP, también puede identificarse un ordenador por su nombre de dominio. Estos tienen una estructura jerárquica. Son una serie de letras separadas por puntos, de la forma cnice.mecd.es Esta forma es más fácil de recordar, ya que cada palabra entre puntos puede tener un significado. Entre la dirección IP y el nombre de dominio hay una relación biunívoca. De esta forma siempre que se da el nombre de un ordenador, en realidad se da su dirección IP.

WIFI

Wifi es una tecnología inalámbrica utilizada para conectar e intercambiar información entre dispositivos electrónicos sin necesidad de conectarlos mediante el uso de cables físicos. Wifi pertenece al conjunto de tecnologías conocidas como Wireless (sin cables) con mayor aceptación y uso en la mayoría de dispositivos electrónicos como smartphones, tablets, ordenadores de sobremesa y portátiles, cámaras digitales o consolas de videojuegos gracias al cual podemos disponer de una red de comunicación entre varios dispositivos y con acceso a Internet.

Tal y como hemos indicado anteriormente wifi es una tecnología inalámbrica la cual envía paquetes de información y establece la comunicación entre diferentes dispositivos mediante la emisión y recepción de ondas de radio, la ondas o señales de radio corresponden a una banda específica del espectro electromagnético las cuales pueden propagarse a través del espacio al igual que lo hacen las ondas del radar, de la televisión o de la telefonía móvil. Comprenderemos mejor el funcionamiento del wifi con el siguiente ejemplo, cuando conectamos nuestro smartphone a una red wifi para poder navegar por Internet realmente nos conectamos a un router que está físicamente conectado a internet mediante un cable, este router se ocupa de transformar la información digital binaria (unos y ceros) en ondas de radio que son transmitidas a lo largo de un área y que son captadas por decodificadores que tienen nuestro smartphone, dichos decodificadores vuelven a transformar las ondas de radio en

información la digital inicial la cual es interpretada por el microprocesador y el software alojado en nuestro smartphone.

Una de las principales ventajas del wifi es la posibilidad de conectar múltiples dispositivos electrónicos a internet con un solo Router, así por ejemplo podemos estar leyendo esta web mientras nuestro ordenador de sobremesa está descargándose la última actualización del sistema operativo y nuestra smart tv está emitiendo una película en streaming, en este ejemplo 3 dispositivos electrónicos están conectados a Internet a través de un único router.

Estrictamente la palabra wi-fi hace referencia a todos los dispositivos electrónicos diseñados para establecer una comunicación inalámbrica y que han sido certificados por la organización Wi-Fi Alliance. Wi-Fi Alliance es una asociación compuesta por diversas empresas tecnológicas cuyo objetivo principal es fomentar, mejorar y garantizar la calidad de todos los dispositivos que utilizan esta tecnología como medio de comunicación inalámbrica, wifi es una marca registrada por la Wi-Fi Alliance que es concedida a todos aquellos dispositivos que han sido certificados por esta organización bajo el estándar IEEE 802.11.

APLICACIONES WIFI

Tal y como hemos citado anteriormente esta tecnología es utilizada para establecer una comunicación inalámbrica entre dispositivos electrónicos eliminando el cableado físico y mejorando la movilidad y uso de los diferentes dispositivos.

Principalmente la tecnología wifi se aplica como medio para conectar a Internet diversos dispositivos electrónicos como smartphones, tablets u ordenadores, permitiendo compartir una sola conexión con múltiples dispositivos, millones de hogares, cafeterías, hoteles, aeropuertos y universidades de todo el mundo utilizan esta tecnología como medio de acceso a la Red.

Otras de las aplicaciones es la creación de una red local de ordenadores conectados inalámbricamente, este tipo de aplicación wifi se utiliza por ejemplo en centros comerciales donde los terminales de venta están conectados entre sí o en los almacenes donde se registra todos movimientos de mercancías en un ordenador central conectado a diversos terminales. Cada vez diversos sectores industriales aplican esta tecnología en cada una de sus etapas productivas, eliminando los obstáculos del cableado y aumentando la flexibilidad y movilidad a través de las diferentes estaciones de trabajo.

Ventajas

- Flexibilidad

  Dentro de la zona de cobertura de la red inalámbrica los nodos se podrán comunicar y no estarán atados a un cable para poder estar comunicados por el mundo Por ejemplo, para hacer esta presentación se podría haber colgado la presentación de la web y haber traído simplemente el portátil y abrirla desde Internet incluso aunque la oficina en la que estuviésemos no tuviese rosetas de acceso a la red cableada.

- Poca planificación

Con respecto a las redes cableadas. Antes de cablear un edificio o unas oficinas se debe pensar mucho sobre la distribución física de las máquinas, mientras que con una red inalámbrica sólo nos tenemos que preocupar de que el edificio o las oficinas queden dentro del ámbito de cobertura de la red.

- Diseño

Los receptores son bastante pequeños y pueden integrarse dentro de un dispositivo y llevarlo en un bolsillo, etc.

- Robustez

Ante eventos inesperados que pueden ir desde un usuario que se tropieza con un cable Y lo desenchufa, hasta un pequeño terremoto o algo similar. Una red cableada podría llegar a quedar completamente inutilizada, mientras que una red inalámbrica puede aguantar bastante mejor este tipo de percances inesperados

Otra de las aplicaciones es la conexión inalámbrica directa entre diferentes aparatos electrónicos como cámaras fotográficas, impresoras, mandos o gamepads, etc. conocido como wifi direct esta tecnología permite compartir y transferir información y archivos de un dispositivo a otro directamente sin necesidad de disponer de un acceso a Internet ganando terreno a otras tecnologías inalámbricas como el bluetooth. Gracias al wifi direct podemos hacer una fotografía con nuestra cámara de fotos y enviarla a nuestro smartphone o a nuestro tablet, podemos mandar a imprimir documentos en nuestra impresora wifi sin necesidad de estar conectada a un cable o podemos sincronizar nuestra agenda del portátil con nuestro smartphone todo ello sin utilizar un acceso a Internet.

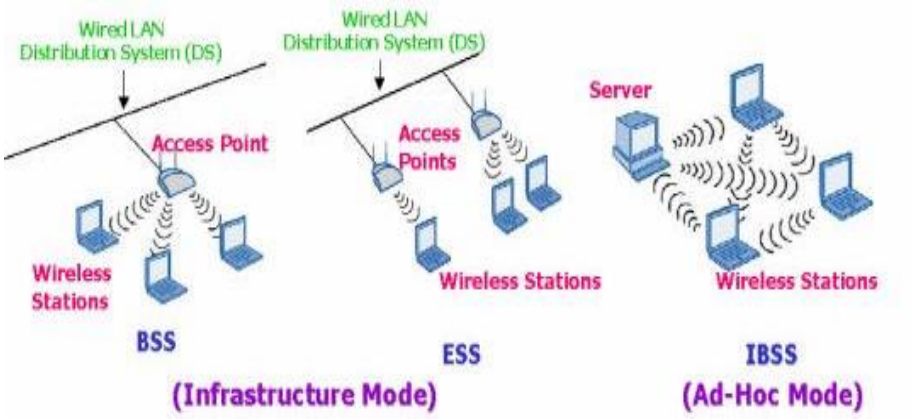
TECNOLOGÍAS DE REDES IEEE 802.11x

IEEE 802.11 comprende varios estándares:

- Definen la subcapa MAC y la física
- No son compatibles entre sí, algunos ni siquiera con ellos mismos
- Los hay de transmisión: 802.11 original (1997), 802.11b, 802.11a y 802.11g
- Extensiones al estándar 802.11a: 802.11h y 802.11i
- 802.11e, extensión para Calidad de Servicio (QoS)

Modos de operación

Hay dos modos de operación, uno ad-hoc, en el que las estaciones se comunican entre sí directamente, y otro de Infraestructura, en el que las estaciones acceden a la red a través de uno o varios puntos de acceso.



802.11

Estándar de la IEEE, 1997

- Hasta 2Mbit/s.
- 3 Especificaciones de capas físicas: 2 para radio, en la banda de los 2,4GHz y una para infrarrojos. De éstas, la de infrarrojos nunca fue implementada, y una de las de radio fue el embrión de 802.11b.
- Obsoleto, pero todavía compatible con 802.11b.

802.11b

- Es el estándar más utilizado
- Se supone que alcanza 11Mbit/s, pero una tasa de transferencia más real es de unos 4Mbit/s, incluso menos, dependiendo del entorno y la distancia al punto de acceso CSMA/CA (Sense Multiple Access with Collision Avoidance) o RTS/CTS (Request to Send/Clear to Send), 4-Way Handshake
- Alcance de 30m en interiores

802.11a

- Estándar, pero no necesariamente interoperable
- La Wireless Ethernet Compatibility Alliance (WECA) es la organización encargada de la normalización de los diferentes dispositivos que salen al mercado, de acuerdo con la especificación Wi-Fi5.
- No cumple la normativa europea, al respecto de control de potencia y gestión del espectro de frecuencias.
- Utiliza CSMA –CA.
- Alcance a 54Mbit/s: 10 metros.
- Corrección de Errores: Forward Error Correction (FEC).

802.11g

- Estándar todavía en desarrollo
- Supuestamente compatible hacia atrás con 802.11b, pero esto todavía no está garantizado.
- Alto consumo.

Seguridad

- Encriptación WEP (Wired Equivalence Privacy), basado en RC4.
- Inseguro: periódicamente genera paquetes “débiles”, que pueden ser aprovechados para reconstruir la clave, y acceder a la red.
- Más de la mitad de las redes no lo usan.
- A veces se trata como red segura (interna), cuando por definición es insegura y debería ponerse delante del firewall, y no detrás con el resto de la LAN.

Seguridad - 802.11i

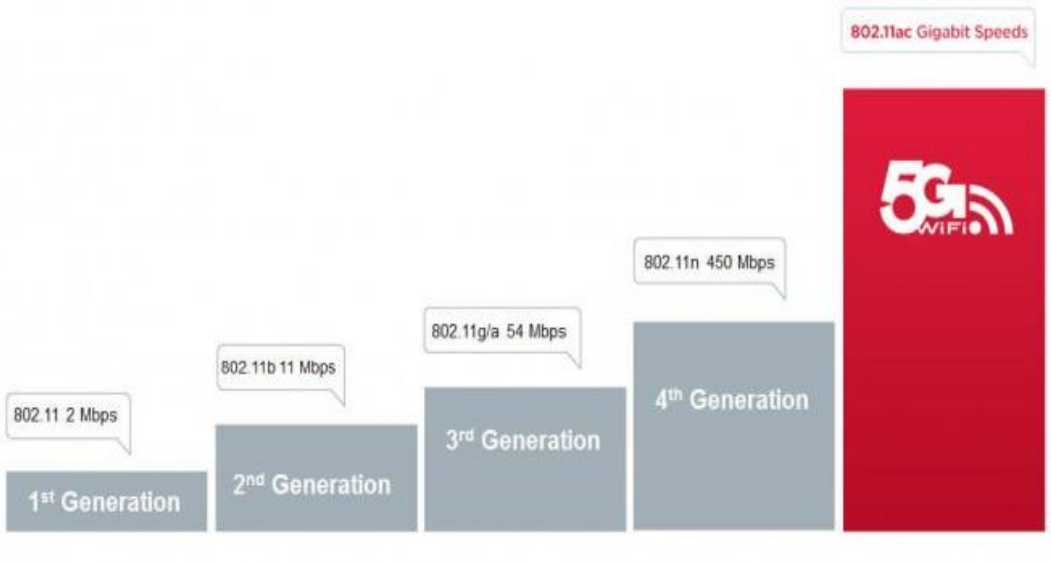
Estándar adicional, todavía en desarrollo, con dos vertientes:

- Temporal Key Integrity Protocol
- Es un RC4 reparado
- Genera claves nuevas cada 10 Kbytes
- Aplicable a equipamiento actual
- AES
- Más robusto
- No aplicable a equipamiento actual

802.11h - Para la UE

- Desarrollado por exigencia de la Unión Europea para la autorización de operación del estándar 802.11.
- Dynamic Frequency Selection, para gestión del espectro.
- Transmit Power Control, para control de potencia de transmisión.

Desarrollado para desbancar a HiperLAN2, estándar impulsado por la UE.



ACCES POINT

Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación alámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos. Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming".

Por otro lado, una red donde los dispositivos cliente se administran a sí mismos sin la necesidad de un punto de acceso se convierten en una red ad-hoc.

Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados. Los puntos de acceso (AP) son dispositivos que permiten la conexión inalámbrica de un equipo móvil de cómputo (ordenador, tableta, smartphone) con una red. Generalmente los puntos de acceso tienen como función principal permitir la conectividad con la red, delegando la tarea de ruteo y direccionamiento a servidores, ruteadores y switches. La mayoría de los AP siguen el estándar de comunicación 802.11 de la IEEE lo que permite una compatibilidad con una gran variedad de equipos inalámbricos. Algunos equipos incluyen tareas como la configuración de la función de ruteo, de direccionamiento de puertos, seguridad y administración de usuarios. Estas funciones responden ante una configuración establecida previamente. Al fortalecer la interoperabilidad entre los servidores y los puntos de acceso, se puede lograr mejoras en el servicio que ofrecen, por ejemplo, la respuesta dinámica ante cambios en la red y ajustes de la configuración de los dispositivos. Los AP son el enlace entre las redes cableadas y las inalámbricas. El uso de varios puntos de acceso permite el servicio de roaming. El surgimiento de estos dispositivos ha permitido el ahorro de nuevos cableados de red. Un AP con el estándar IEEE 802.11b tiene un radio de 100 m aproximadamente.

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada.

Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. Este o su antena normalmente se colocan en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red WLAN a través de adaptadores situados en sus equipos (ordenador, tableta, smartphone, Smart TV, radio por Internet). Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena inalámbrica.

SWITCH

Un switch es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. El switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir

tiempo de espera y bajar el costo por puerto. Opera en la capa 2 del modelo OSI y reenvía los paquetes en base a la dirección MAC.

El switch segmenta económicamente la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final. No están diseñados con el propósito principal de un control íntimo sobre la red o como la fuente última de seguridad, redundancia o manejo.

Al segmentar la red en pequeños dominios de colisión, reduce o casi elimina que cada estación compita por el medio, dando a cada una de ellas un ancho de banda comparativamente mayor.

Los Switch se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Área Network- Red de Área Local).

ROUTER

Router o ruteador lo que podemos interpretar como simplemente una guía. Se trata de un dispositivo utilizado en redes de área local (LAN – Local Area Network), una red local es aquella que cuenta con una interconexión de computadoras relativamente cercanas, por medio de cables. El Router permite la interconexión de redes LAN y su función es la de guiar los paquetes de datos para que fluyen hacia la red correcta e ir determinando que caminos debe seguir para llegar a su destino, básicamente para los servicios de Internet, los cuáles recibe de otro dispositivo como un módem del proveedor de Internet de banda ancha.

DIRECCION IP

Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del Modelo OSI. Dicho número no se ha de confundir con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red. La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP decida asignar otra IP (por ejemplo, con el protocolo DHCP). A esta forma de asignación de dirección IP se denomina también dirección IP dinámica (normalmente abreviado como IP dinámica).

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados generalmente tienen una dirección IP fija (comúnmente, IP fija o IP estática). Esta no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red.

Las computadoras se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, a los seres humanos nos es más cómodo utilizar otra notación más fácil de recordar, como los nombres de dominio; la traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS, que a su vez facilita el trabajo en caso de cambio de dirección IP, ya que basta con actualizar la información en el servidor DNS y el resto de las personas no se enterarán, ya que seguirán accediendo por el nombre de dominio.

Dirección Ip v4

Las direcciones IPv4 se expresan por un número binario de 32 bits, permitiendo un espacio de direcciones de hasta 4.294.967.296 (2^{32}) direcciones posibles. Las *direcciones IP* se pueden expresar como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal de cada octeto está comprendido en el rango de 0 a 255 [el número binario de 8 bits más alto es 11111111 y esos bits, de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 255].

En la expresión de direcciones IPv4 en decimal se separa cada octeto por un carácter único, un “punto”. Cada uno de estos octetos puede estar comprendido entre 0 y 255.

- Ejemplo de representación de dirección IPv4: 10.128.1.255

En las primeras etapas del desarrollo del Protocolo de Internet, los administradores de Internet interpretaban las direcciones IP en dos partes, los primeros 8 bits para designar la dirección de red y el resto para individualizar la computadora dentro de la red.

Este método pronto probó ser inadecuado, cuando se comenzaron a agregar nuevas redes a las ya asignadas. En 1981 el direccionamiento internet fue revisado y se introdujo la arquitectura de clases. (Classful network architecture).

En esta arquitectura hay tres clases de direcciones IP que una organización puede recibir de parte de la Internet Corporation for Assigned Names and Numbers (ICANN): clase A, clase B y clase C.

- En una red de clase A, se asigna el primer octeto para identificar la red, reservando los tres últimos octetos (24 bits) para que sean asignados a los *hosts*, de modo que la cantidad máxima de *hosts* es 2^{24} - 2 (se excluyen la dirección reservada para *broadcast* (últimos octetos en 255) y de red (últimos octetos en 0)), es decir, 16 777 214 *hosts*.
- En una red de clase B, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que sean asignados a los *hosts*, de modo que la cantidad máxima de *hosts* por cada red es 2^{16} - 2, o 65 534 *hosts*.

En una red de clase C, se asignan los tres primeros octetos para identificar la red, reservando el octeto final (8 bits) para que sea asignado a los *hosts*, de modo que la cantidad máxima de hosts por cada red es 2^8 - 2, o 254 *hosts*.

Clase	Rango	N° de Redes	N° de Host Por Red	Máscara de red	Broadcast ID
A	0.0.0.0 - 127.255.255.255	128	16 777 214	255.0.0.0	x.255.255.255
B	128.0.0.0 - 191.255.255.255	16 384	65 534	255.255.0.0	x.x.255.255
C	192.0.0.0 - 223.255.255.255	2 097 152	254	255.255.255.0	x.x.x.255
D	224.0.0.0 - 239.255.255.255	histórico			
E	240.0.0.0 - 255.255.255.255	histórico			

- La dirección 0.0.0.0 es reservada por la IANA para identificación local.
- La dirección que tiene los bits de host iguales a cero sirve para definir la red en la que se ubica. Se denomina dirección de red.
- La dirección que tiene los bits correspondientes a *host* iguales a 255, sirve para enviar paquetes a todos los *hosts* de la red en la que se ubica. Se denomina dirección de *broadcast*.
- Las direcciones 127.x.x.x se reservan para designar la propia máquina. Se denomina dirección de bucle local o *loopback*.

El diseño de redes de clases (*classful*) sirvió durante la expansión de internet, sin embargo este diseño no era escalable y frente a una gran expansión de las redes en la década de los noventa, el sistema de espacio de direcciones de clases fue reemplazado por una arquitectura de redes sin clases Classless Inter-Domain Routing (CIDR) en el año 1993. CIDR está basada en redes de longitud de máscara de subred variable (variable-length subnet masking VLSM) que permite asignar redes de longitud de prefijo arbitrario. Permitiendo una distribución de direcciones más fina y granulada, calculando las direcciones necesarias y "desperdiciando" las mínimas posibles.

Creación de subredes

El espacio de direcciones de una red puede ser subdividido a su vez creando subredes autónomas separadas. Un ejemplo de uso es cuando necesitamos agrupar todos los empleados pertenecientes a un departamento de una empresa. En este caso crearíamos una subred que englobara las direcciones IP de éstos. Para conseguirlo hay que reservar bits del campo host para identificar la subred estableciendo a uno los bits de red-subred en la máscara. Por ejemplo la dirección 172.16.1.1 con máscara 255.255.255.0 nos indica que los dos primeros octetos identifican la red (por ser una dirección de clase B), el tercer octeto identifica la subred (a 1 los bits en la máscara) y el cuarto identifica el host (a 0 los bits correspondientes dentro de la máscara). Hay dos direcciones de cada subred que quedan reservadas: aquella que identifica la subred

(campo host a 0) y la dirección para realizar broadcast en la subred (todos los bits del campo host en 1).

IP dinámica

Una dirección IP dinámica es una IP asignada mediante un servidor DHCP (Dynamic Host Configuration Protocol) al usuario. La IP que se obtiene tiene una duración máxima determinada. El servidor DHCP provee parámetros de configuración específicos para cada cliente que desee participar en la red IP. Entre estos parámetros se encuentra la dirección IP del cliente.

DHCP apareció como protocolo estándar en octubre de 1993. El estándar RFC 2131 especifica la última definición de DHCP (marzo de 1997). DHCP sustituye al protocolo BOOTP, que es más antiguo. Debido a la compatibilidad retroactiva de DHCP, muy pocas redes continúan usando BOOTP puro.

Las IP dinámicas son las que actualmente ofrecen la mayoría de operadores. El servidor del servicio DHCP puede ser configurado para que renueve las direcciones asignadas cada tiempo determinado.

Ventajas

- Reduce los costos de operación a los proveedores de servicios de Internet (ISP).
- Reduce la cantidad de IP asignadas (de forma fija) inactivas.
- El usuario puede reiniciar el router para que le sea asignada otra IP y así evitar las restricciones que muchas webs ponen a sus servicios gratuitos de descarga o visionado multimedia online.

Desventajas

- Obliga a depender de servicios que redirigen un host a una IP.

Asignación de direcciones IP

Dependiendo de la implementación concreta, el servidor DHCP tiene tres métodos para asignar las direcciones IP:

Manualmente: cuando el servidor tiene a su disposición una tabla que empareja direcciones MAC con direcciones IP, creada manualmente por el administrador de la red. Sólo clientes con una dirección MAC válida recibirán una dirección IP del servidor.

Automáticamente: donde el servidor DHCP asigna por un tiempo pre-establecido ya por el administrador una dirección IP libre, tomada de un rango prefijado también por el administrador, a cualquier cliente que solicite una.

Dinámicamente: el único método que permite la re-utilización de direcciones IP. El administrador de la red asigna un rango de direcciones IP para el DHCP y cada ordenador cliente de la LAN tiene su software de comunicación TCP/IP configurado para solicitar una dirección IP del servidor DHCP cuando su tarjeta de interfaz de red se inicie. El proceso es transparente para el usuario y tiene un periodo de validez limitado.

IP fija

Una dirección IP fija es una dirección IP asignada por el usuario de manera manual (Que en algunos casos el ISP o servidor de la red no lo permite), o por el servidor de la red (ISP en el caso de internet, router o switch en caso de LAN) con base en la Dirección MAC del cliente. Mucha gente confunde IP Fija con IP Pública e IP Dinámica con IP Privada.

Una IP puede ser Privada ya sea dinámica o fija como puede ser IP Pública Dinámica o Fija.

Una IP pública se utiliza generalmente para montar servidores en internet y necesariamente se desea que la IP no cambie por eso siempre la IP Pública se la configura de manera Fija y no Dinámica, aunque si se podría.

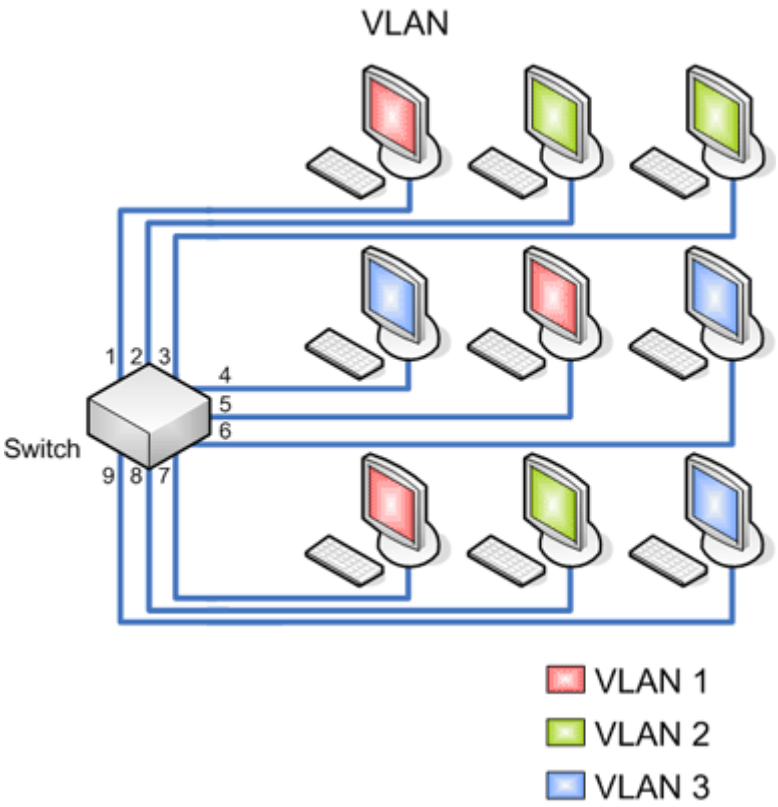
En el caso de la IP Privada generalmente es dinámica asignada por un servidor DHCP, pero en algunos casos se configura IP Privada Fija para poder controlar el acceso a internet o a la red local, otorgando ciertos privilegios dependiendo del número de IP que tenemos, si esta cambiara (fuera dinámica) sería más complicado controlar estos privilegios (pero no imposible).

VLANS

Una red de área local (LAN) está definida como una red de computadoras dentro de un área geográficamente acotada como puede ser una empresa o una corporación. Uno de los problemas que nos encontramos es el de no poder tener una confidencialidad entre usuarios de la LAN como pueden ser los directivos de la misma, también estando todas las estaciones de trabajo en un mismo dominio de colisión el ancho de banda de la misma no era aprovechado correctamente. La solución a este problema era la división de la LAN en segmentos físicos los cuales fueran independientes entre sí, dando como desventaja la imposibilidad de comunicación entre las LANs para algunos de los usuarios de la misma.

La necesidad de confidencialidad como así el mejor aprovechamiento del ancho de banda disponible dentro de la corporación ha llevado a la creación y crecimiento de las VLANs.

Una VLAN se encuentra conformada por un conjunto de dispositivos de red interconectados.



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

Segmentación

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

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

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

Tipos de VLAN

VLAN de puerto central

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

VLAN Estáticas

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

Por puerto

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

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

Ventajas:

- Facilidad de movimientos y cambios.
- Micro segmentación y reducción del dominio de Broadcast.
- Multiprotocolo: La definición de la VLAN es independiente del o los protocolos utilizados, no existen limitaciones en cuanto a los protocolos utilizados, incluso permitiendo el uso de protocolos dinámicos.

Desventajas:

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

Por dirección MAC

Los miembros de la VLAN están especificados en una tabla por su dirección MAC.

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

Ventajas:

- Facilidad de movimientos: No es necesario en caso de que una terminal de trabajo cambie de lugar la reconfiguración del switch.
- Multiprotocolo.
- Se pueden tener miembros en múltiples VLANs.

Desventajas:

- Problemas de rendimiento y control de Broadcast: el tráfico de paquetes de tipo Multicast y Broadcast se propagan por todas las VLANs.
- Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo. También se puede emplear soluciones de DVLAN.

Por protocolo

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

Protocolo	VLAN
IP	1
IPX	2
IPX	2
IPX	2
IP	1

Ventajas:

- Segmentación por protocolo.
- Asignación dinámica.

Desventajas

- Problemas de rendimiento y control de Broadcast: Por las búsquedas en tablas de pertenencia se pierde rendimiento en la VLAN.
- No soporta protocolos de nivel 2 ni dinámicos.

Por direcciones IP

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

Ventajas:

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

Desventajas:

- El tamaño de los paquetes enviados es menor que en el caso de utilizar direcciones MAC.
- Pérdida de tiempo en la lectura de las tablas.

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

Por nombre de usuario

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

Ventajas:

- Facilidad de movimiento de los integrantes de la VLAN.
- Multiprotocolo.

Desventajas:

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

VLAN Dinámicas (DVLAN)

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

Capa de Red: ELAN o Redes LAN Emuladas

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

Ventajas:

- Facilidad de administración.
- Facilidad de movimientos y cambios.
- Multiprotocolo.
-

Desventajas:

- Aplicable solo a Ethernet y Token Ring.

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

CABLE UTP PAR TRENZADO

UTP es una abreviatura de par trenzado sin blindaje (por sus siglas en inglés). Los cables UTP son rentables y son lo suficientemente flexibles para usarse con la mayoría de las aplicaciones. Hay muchos grados o niveles de cables UTP y la mayoría de ellos son técnicamente avanzados en comparación con sus predecesores.

CATEGORIAS:

Categoría 1

El cable CAT 1 o categoría 1, es el más adecuado para las comunicaciones telefónicas. No es adecuado para transmitir datos o para trabajarlos en una red. Se utiliza sobre todo en instalaciones de cableado.

Categoría 2

El cable categoría 2, o CAT 2, es capaz de transmitir datos de hasta 4 Mbps. Se trata de cable nivel 2 y se usó en las redes ARCnet (arco de red) y Token Ring (configuración de anillo) hace algún tiempo. El CAT 2 al igual que el CAT 1, no es adecuado para la transmisión de datos en una red.

Categoría 3

El cable categoría 3, o CAT 3, es un par trenzado, sin blindar, capaz de llevar a la creación de redes 100BASE-T y puede ayudar a la transmisión de datos de hasta 16MHz con una velocidad de hasta 10 Mbps. No se recomienda su uso con las instalaciones nuevas de redes.

Categoría 4

El cable categoría 4, o CAT 4, es un par trenzado sin blindar que soporta transmisiones de hasta 20MHz. Es confiable para la transmisión de datos por encima del CAT 3 y puede transmitir datos a una velocidad de 16 Mbps. Se utiliza sobre todo en las redes Token Ring.

Categoría 5

El cable categoría 5, o CAT 5, ayuda a la transmisión de hasta 100 MHz con velocidades de hasta 1000 Mbps. Es un cable UTP muy común y adecuado para el rendimiento 100BASE T. Se puede utilizar para redes ATM, 1000BASE T, 10BASE T, 100BASE T y token ring. Estos cables se utilizan para la conexión de computadoras conectadas a redes de área local.

Categoría 5e

El cable categoría 5e o CAT 5e, es una versión mejorada sobre el de nivel 5. Sus características son similares al CAT 5 y es compatible con transmisión de hasta 10MHz. Es más adecuado para operaciones con Gigabit Ethernet y es una excelente opción para red 1000BASE T.

Categoría 6

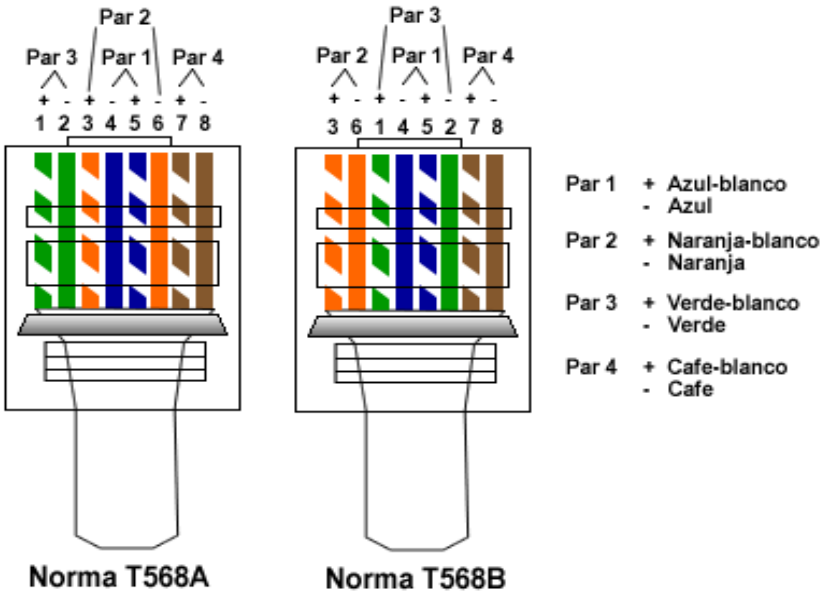
El cable Categoría 6, o CAT 6, es una propuesta de par trenzado sin blindar que puede soportar hasta 250 MHz de transmisión. Se trata de la sexta generación del cable Ethernet. Este cable con alambres de cobre puede soportar velocidades de 1 GB. CAT 6 es compatible con el CAT 5e, CAT 6 y CAT 3. Es adecuado para redes 1000BASE T, 100BASE T y 10BASE T y posee estrictas reglas acerca del ruido del sistema y la diafonía.

Categoría 7

El cable categoría 7, CAT 7, es otro proyecto de norma que admite la transmisión de hasta 600MHz. CAT 7 es un estándar Ethernet de cable de cobre 10G que mide más de 100 metros. Es compatible con CAT 5 y CAT 6 y tiene reglas más estrictas que CAT 6 sobre el ruido del sistema y la diafonía.

CONFIGURACION CABLE DE RED

El cableado estructurado para redes de computadores nombran dos tipos de normas o configuraciones a seguir, estas son: La EIA/TIA-568A (T568A) y la EIA/TIA-568B (T568B) que comúnmente le llamamos norma A y norma B. La diferencia entre ellas es el orden de los colores de los pares a seguir para el conector RJ45. A continuación se muestra el orden de cada norma:



Un cable cruzado es aquel donde en los extremos la configuración es diferente. El cable cruzado, como su nombre lo dice, cruza las terminales de transmisión de un lado para que llegue a recepción del otro, y la recepción del origen a transmisión del final.

Para crear el cable de red cruzado, lo único que deberá hacer es armar un extremo del cable con la norma T568A y el otro extremo con la norma T568B.

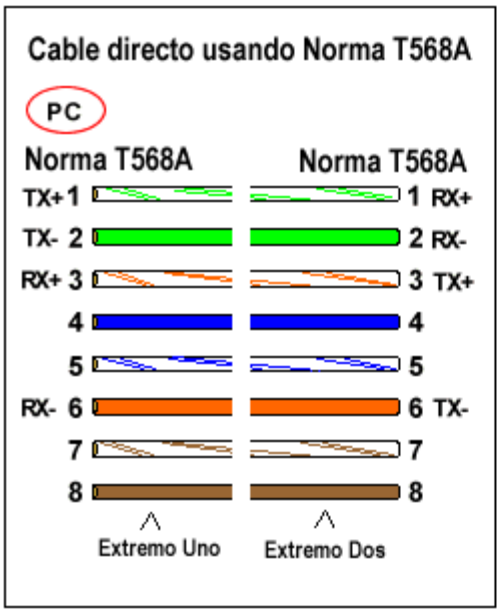
Como armar un cable de red directo para conectar a un SWITCH?

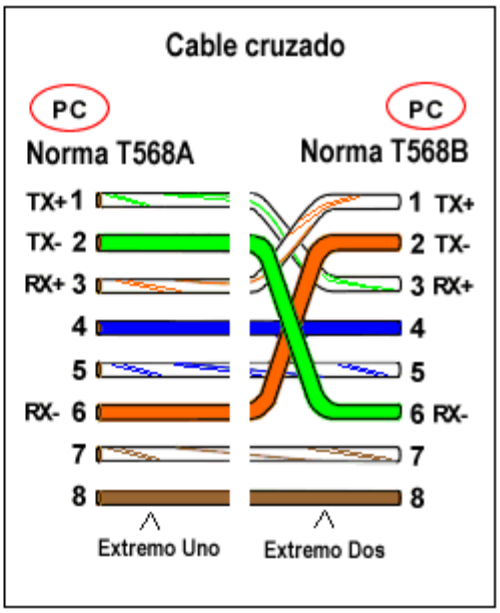
El cable recto es sencillo de construir, solo hay que tener la misma norma en ambos extremos del cable. Esto quiere decir, que si utilizaste la norma T568A en un extremo del cable, en el otro extremo también debes aplicar la misma norma T568A.

Este tipo de cables es utilizado para conectar computadores a equipos activos de red

Como Switchers, Routers. Terminales de Transmisión y Recepción.

Las redes de computadores no utilizan los 4 pares (8 cables) en su totalidad, utilizan solamente 4 cables: 2 para transmitir y 2 para recibir





Cables de Fibra Óptica

Transmiten señales luminosas por un núcleo de dióxido de silicio, tan puro que una ventana de cinco kilómetros de gruesa construida con este material no distorsionaría la vista. Las transmisiones fotónicas no producen emisiones fuera del cable y no se ven afectadas por la radiación externa.

Se recomienda el cable de fibra cuando la seguridad es clave. Las señales de las computadoras se transmiten por el cable de fibra óptica convirtiendo los 1 y los 0 electrónicos en pulsos de luz. Un diodo emisor de luz en un extremo emite pulsos de luz por un cable que recogen en el otro extremo con un sencillo fotodetector y se vuelven a convertir en señales eléctricas. Como las señales prácticamente no encuentran resistencia y no hay emisiones, las tasas de transmisión por cable de fibra sólo están limitadas por la pureza del núcleo de cristal, la calidad de los equipos y la velocidad de la luz.

Sus principales características son:

- Una baja atenuación por Km cuando se transmite por las llamadas ventanas de transmisión, que están ubicadas en torno a los valores siguientes de longitud de onda: 0.8 mm, 1.3 mm y 1.55 mm. Esta última ventana es la que presenta menor atenuación.
- Total inmunidad al ruido y a las interferencias electromagnéticas, lo que constituye un medio especialmente útil en ambientes con alto ruido.
- Uso de potencias del orden de los mW, en comparación con otros medios de comunicaciones que requieren potencias mayores.
- Su pequeño tamaño y poco peso, hacen de ellas medios de comunicaciones fáciles de instalar, especialmente cuando se trata de completar sistemas sobre ductos preexistentes, sobrecargados por otro tipo de medios que no es posible eliminar.

Teniendo en cuenta el modo de propagación, las fibras ópticas se clasifican en:

- Monomodo

Las dimensiones del nucleo son comparables a la longitud de onda de luz, por lo cual hay un solo modo de propagación y no existe dispersión.

- Multimodo

Contiene varios modos de propagación y ocurre en consecuencia al efecto de dispersión.

A su vez estas últimas se subdividen en:

<u>Índice escalón</u>

Tiene dispersión, reducido ancho de banda y son de bajo costo, dado que resultan tecnológicamente sencillas de producir.

Índice gradual

Más costosas pero de grán ancho de banda. Se puede disminuir la dispersión haciendo variar lentamente el índice de refracción entre el nucleo y el recubrimiento.

CAPITULO 3

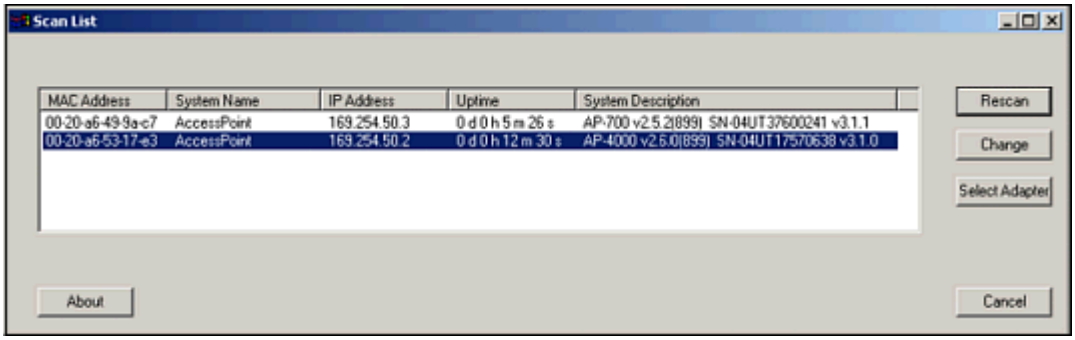
Procedimiento y descripción de las actividades realizadas

- **Revisión de equipos de comunicación.**

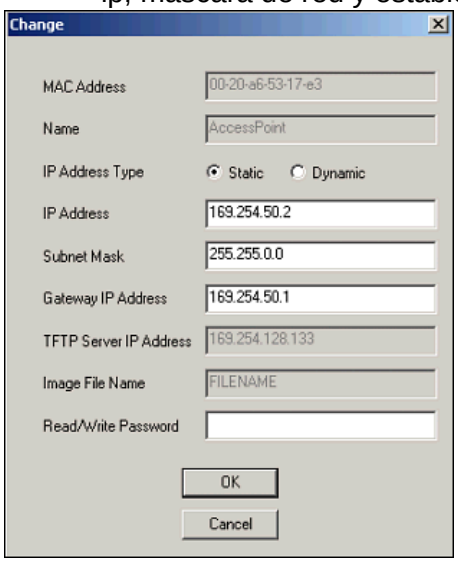
Se hace la revisión de equipos de comunicación, equipos proxim ap 4000, proxim ap 8000, AP enterasys 3640, que son equipos que se presentan en esta institución, los equipos nuevos próximos a instalar de estos modelos y de los equipos ya instalados en las áreas y facultades de la unach, como son rectoría, biblioteca central, contaduría y administración, salón de usos múltiples, facultad de medicina, facultad de pedagogía, edificio Maciel, edificio de lenguas, postgrado, área de finanzas, secretaria académica, secretaria administrativa y otras áreas donde se hizo unas pruebas diagnósticos a los equipos donde presentaban fallos o intermitencia a la hora de operar, analizando configuración, conectividad, velocidad de transmisión, dirección ip o problemas de ubicación, problemas físicos de los equipos como cables, inyectores y ranuras Revisando también si las antenas daban el alcance necesario para poder abarcar y que llegara la señal a cada usuario de las áreas.

El cual se procede con los siguientes pasos para analizar su revisión:

1. conectar el patch cord del ap al PoE y con el otro patch cord en el puerto lan, que va a la pc para poder entrar a su configuración
2. escanear la ip con el programa scanTools para poder ver la dirección ip que tiene en ese momento el equipo.

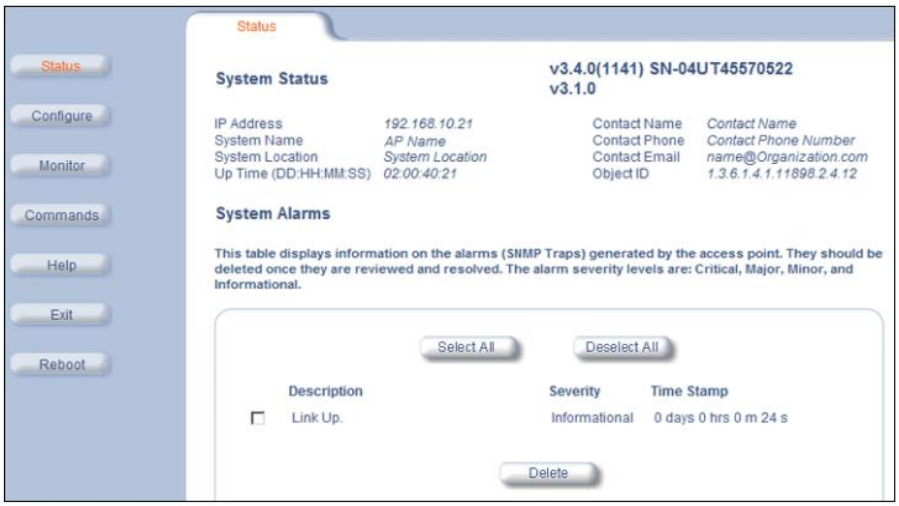


3. Para poder cambiar la dirección ip, si se requiere, podemos entrar en la pestaña “change” para poder modificar según sea el caso. permitiendo cambiar direccion ip, mascara de red y establecer si es ip dinamica o estatica.



4. Entrar a la configuración web del ap con usuario y password el cual por default es usuario “admin” y password “public”.

5. Aquí en configuración web podemos configurar nombre de la red ssid, frecuencias, dirección ip, msacara de subred, Gateway de salida y otras configuraciones de seguridad, una vez configurado el equipo tenemos que resetear el equipo para que se apliquen los cambios.



-
-

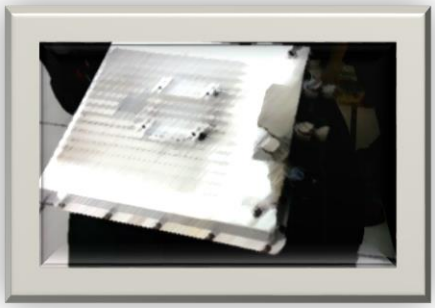
-
- **Inspección de equipos dañados.**

Supervisión de las áreas del plantel de la UNACH para ver problemas existentes de conectividad al igual la atención de problemas de los solicitantes de las distintas áreas de las facultades y oficinas para su próxima revisión y solución.

Acción tomada:

1.-Se le realizaron pruebas de conectividad para atender las solicitudes en los departamentos donde presentaban fallas, llevando el equipo a las oficinas para poder realizarle pruebas de enlace en caso de los radios proxim orinocco 8000, revisión de la frecuencia con la que trabaja, o si presentaba algún daño eléctrico Y en caso de los Access point, se conecta el patch cord para entrar a su configuración accesando a su configuración web y resetear a fabrica para que se guarde el equipo.

2.- instalación de equipo de reemplazo.

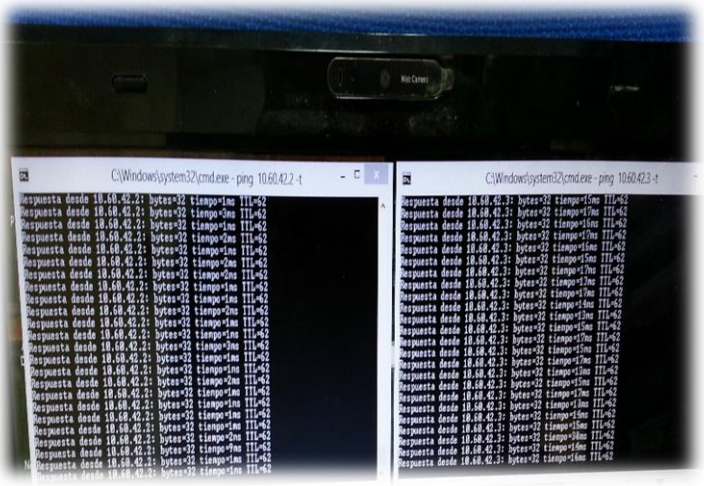


- **Soporte técnico a la red.**

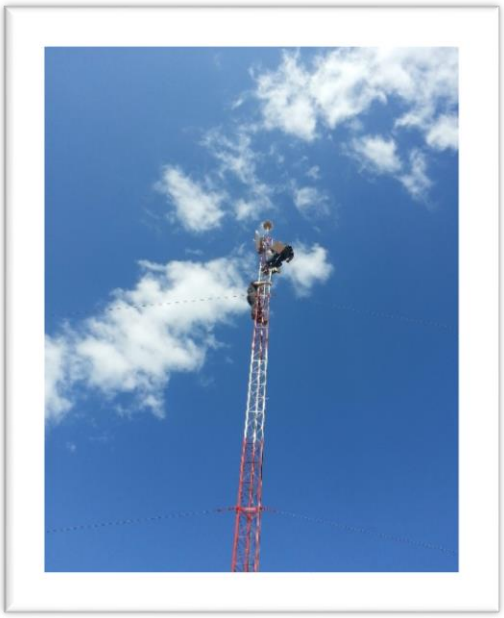
Una vez teniendo las áreas donde se presentan los problemas, acudir con el equipo necesario para Corregir y prevenir errores que provoquen un mal funcionamiento en la red de comunicación de datos, revisando los radios de comunicación punto a punto, por si hay algún problema eléctrico y si llega la señal de la unidad central que es la que se encarga de transportar los paquetes de internet, Diagnosticar cual fue el origen del problema. Y configurar e instalar los equipos para que quede operando de manera óptima y sobre todo que sea a un largo plazo.

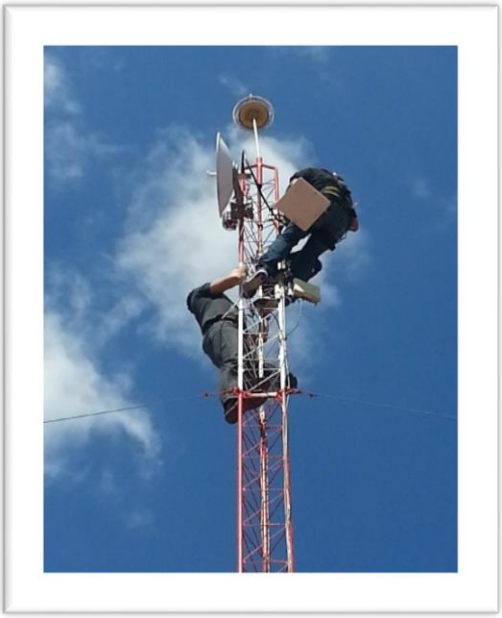
Los pasos a seguir y lo que se procedió hacer:

1. Haciendo “ping” hacia las áreas donde se ha monitoreado o donde ha habido algún reporte de falla para ver que ha sucedido con el enlace hacia esa área. Siendo de las direcciones ip clase A y manejando el ultimo octeto de dirección ip (x.x.x.2) y (x.x.x.3) El “2” para emisor y el “3” para receptor.



2. instalar y reemplazar Equipos de punto a punto a los diferentes departamentos y facultades los cuales presentaban fallas eléctricas y de intermitencia al momento de operar.





- **Instalación de nodos.**

Instalar y configurar las extensiones telefónicas de teléfonos ip, y nodos de red con la configuración del estándar según el cableado ya establecido. Se usó una configuración del estándar T-568 B para la red y Soporte de red de voz.

1.- se hizo un estudio y se tomó en cuenta un lugar estratégico para la instalación del nodo para atender la solicitud del trabajador.

2.- aplicación de comandos telnet para configuración de la extensión.

-En esta sección se realizan comandos para la habilitación de una extensión, y el poder operar cualquier función, requiere de inicio de sesión con nombre de usuario y contraseña, datos solo administrados por la universidad.

```
login: admin2
password:

The software and data stored on this system are the property of,
or licensed to, Nortel Networks and are lawfully available only
to authorized users for approved purposes.  Unauthorized access
to any software or data on this system is strictly prohibited and
punishable under appropriate laws.  If you are not an authorized
user then logout immediately.  This system may be monitored for
operational purposes at any time.


oam> 31/03/2014 12:17:53 LOG0004 tLogin: User <admin2> has logged into the syste
m.
cslogin



SCH0101

REQ: prt     <<<-------
TYPE: dnb    <<<--------
CUST 0       <<<--------
DN   1853
DATE
PAGE
DES

DN   1853    <<<----- (EXTENSION)
     CPND
       CPND_LANG ROMAN
         NAME DEPT ADMISION DDA
         XPLN 22
         DISPLAY_FMT FIRST,LAST
TYPE SL1
TN   062 0 00 21 V  KEY 00   MARP  DES TELIP      1 JUL 2010   ++++++TELNET++++++
     (I2001 )


NACT
login:

login: admin2
password:

The software and data stored on this system are the property of,
or licensed to, Nortel Networks and are lawfully available only
to authorized users for approved purposes.  Unauthorized access
to any software or data on this system is strictly prohibited and
punishable under appropriate laws.  If you are not an authorized
user then logout immediately.  This system may be monitored for
operational purposes at any time.


oam> 31/03/2014 12:19:35 LOG0004 tLogin: User <admin2> has logged into the syste
m.
cslogin

REQ: ?      <<<<<---------------- (AYUDA)
  CDCS CDSP CHG CMIN CONV
  CPWD CPY DISC DISI DISL
  DISN DISS DISU DSCT DSPS  <<<----TOMAMOS EL COMANDO (DISU)
  DSXP ENCT END ENLC ENLG
  ENLL ENLN ENLS ENLU ENPS
  ENXP FDLC FDLF FDLI FDLS
  FDLU FSUM FWUV IDC IDCS
  IDU LBSY LDIS LIDL LMNT
  LTN LUC LUDU LUU LUVU
  MOV NEW OUT PBXT PRT
```

```
  SDLC STAT SUPL TRK XNTT
  XPCT XPEC

REQ: disu       <<<<-----(DISU)

NPR002
REQ: disu ?
NPR002
REQ: disu

NPR002
REQ: ***            <<<<-------- (4 ASTERISCOS PARA BOTARLO)  (2 PARA BORRAR COMANDO ANTERIOR)
OVL000
>ld 11
SL1000
MARP NOT ACTIVATED

MEM AVAIL: (U/P): 2336666    USED U P: 623475 87282    TOT: 3047423
DISK RECS AVAIL: 128
DIGITAL TELEPHONES     AVAIL:    28    USED:    20    TOT:    48
IP USERS               AVAIL:     0    USED:   160    TOT:   160
BASIC IP USERS         AVAIL:     0    USED:     0    TOT:     0
ACD AGENTS             AVAIL:     2    USED:     8    TOT:    10
PCA                    AVAIL:     0    USED:     0    TOT:     0
AST                    AVAIL:     0    USED:     1    TOT:     1
TNS                    AVAIL:  2159    USED:   341    TOT:  2500
DATA PORTS             AVAIL:  2500    USED:     0    TOT:  2500

REQ: disu


NPR002
REQ: ****
>
OVL000
>ld 32            <<<<------ (LD 32 )  **PENDIENTE**
NPR000
.disu 66 14       <<<<------- (DESHABILITAR)

.disu 66 15

.disu 66 13

.disu 62 21

.stat 66 14    <<<<-------- (STATUS)
DSBL UNREGISTERED 00
.enlu 66 14     <<<<--------(HABILITAR)

.stat 66 14
IDLE UNREGISTERED 00    <<<-----( YA ESTA HABILITADO)
.enlu 66 15

.enlu 66 13

.enlu 62 21

.***
OVL000
>logo            <<<---------- (SALIR)
TTY #12 LOGGED OUT ADMIN2 12:22  31/3/2014
SESSION DURATION:  00:25
```

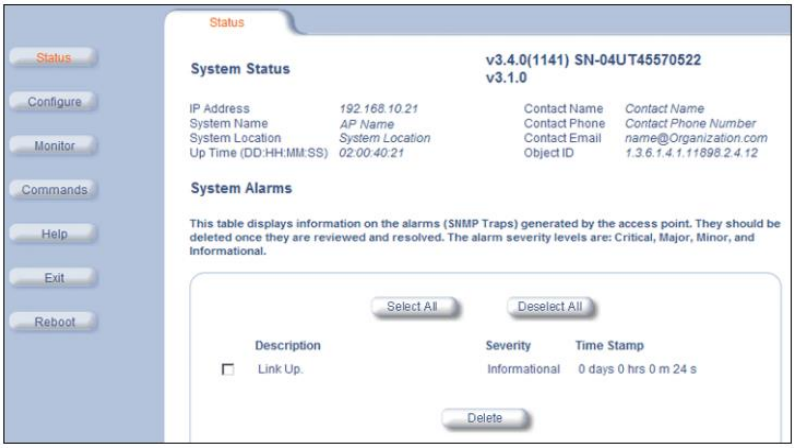
- **Mantenimiento y configuración a equipos.**

Se configuran los equipos de las diferentes áreas para que funcione en óptimas condiciones para el uso que se le pretende dar. Reseteando totalmente y volviendo a configurar con las configuraciones necesarias, Estableciendo el segmento de la ip de la clase A. También se realizó configuración de los equipos nuevos que se pretenden montar a las áreas requeridas.

1.- dar un hard reset presionando el botón del ap que tienen esa opcion, otra forma es dando reset con el PoE y asi restaurando todos los valores por deafult. Entrando a la configuración por medio de la ip 169.254.128.132 para eso hay que cambiar la ip de la pc para que se encuentre dentro del mismo segmento que la ip default y entramos a configuración de red con usuario:admin password:public

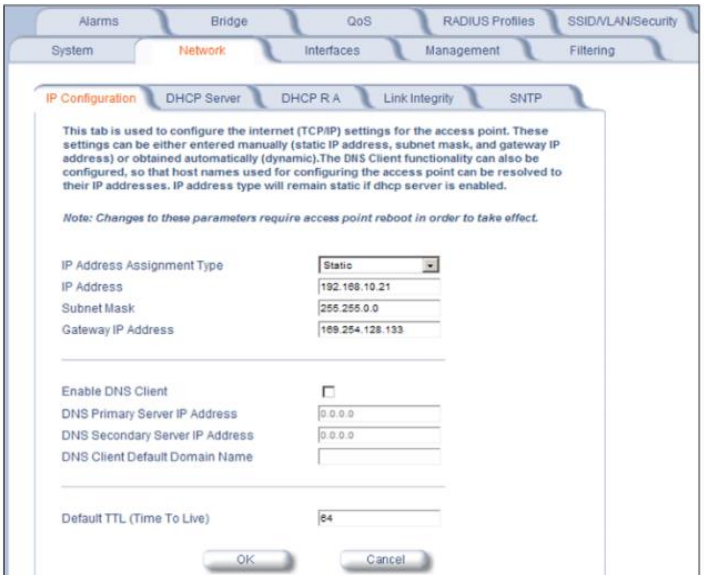
2.-volver a poner las configuraciones que son pre denominadas en esa área. Ya que volvieron a sus valores por defaults.

Entramos a la pestaña configuración para poder modificar el nombre de la red, dirección ip, mascara de red, Gateway de salida, frecuencia de las antenas.

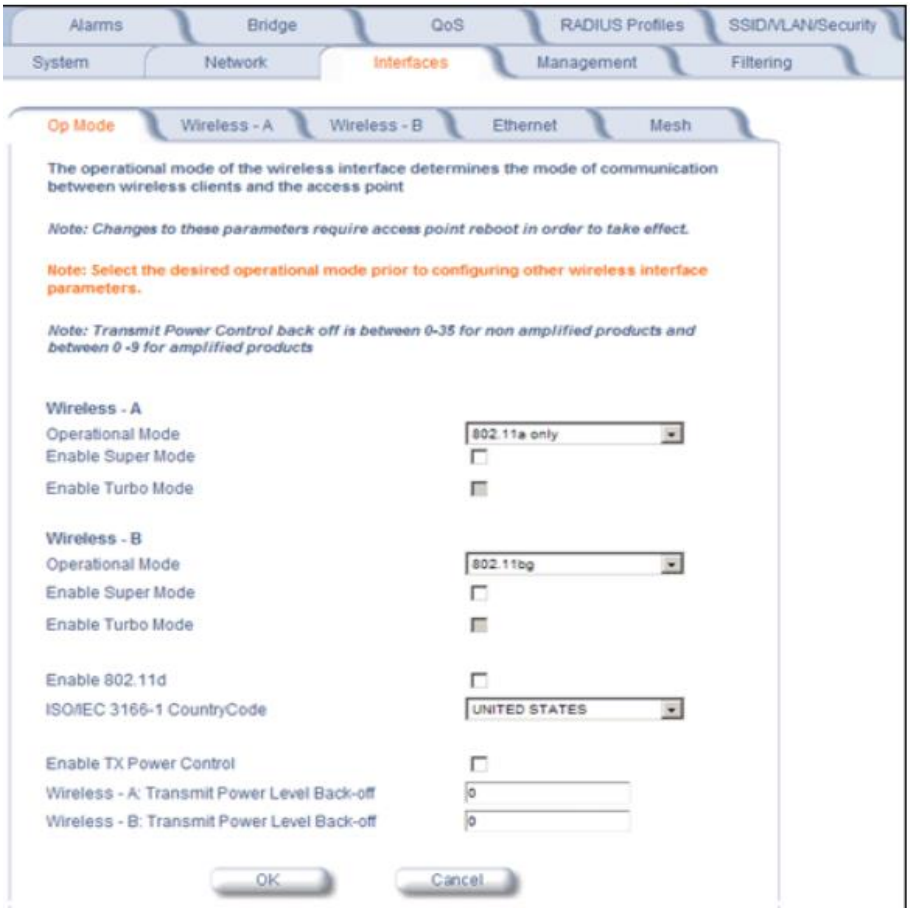


2.-aquí vemos para poder cambiar los parámetros de la red. Como:

- Tipo de ip
- Ip
- Mascara de red
- Gateway de salida



3.- en el manejo de las interfaces se define el tipo de tecnología como ya habíamos mencionado, tecnlogias de wifi, 802.11 /a/b/g/n o sea el caso combinadas.



4.-Otro método que facilita todos estos pasos, y como ya hay un respaldo de la información, es cargar el archivo con la configuración ya predeterminada de las áreas que presentaron problemas y que se atendieron de acuerdo a las quejas de los usuarios.

- Configuración de equipos de comunicación punto a punto.

Se realiza configuración de los equipos de enlace punto a punto. Viendo la frecuencia de los canales, la dirección ip que pertenecen a la clase A, y realizar pruebas si se logra un enlace entre el emisor y receptor o si presenta fallas el equipo.

1.- conectamos el equipo a un PoE y conectamos a nuestra pc.

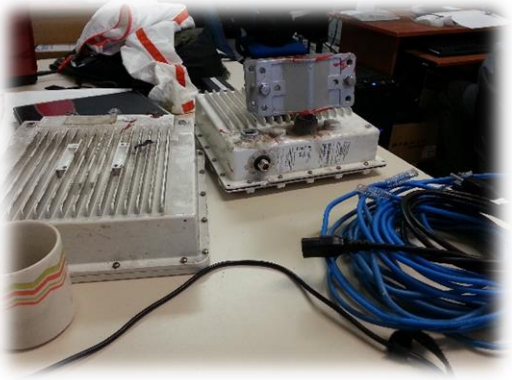
2.- esperamos a que de respuesta el equipo y comenzar a operar analizando la ip que trae el equipo con scantools.

3. una vez teniendo la ip del equipo, cambiar la ip de la pc con una de la misma clase de la que tiene el equipo.

4.-habiendo cambiado la ip del equipo, se procede a entrar a la configuración via web del equipo, colocando en los campos de seguridad, nombre de usuario y password.

5.- se procede a cambiar la direcciones ip como habíamos mencionado, y mascara de red. Se hara el mismo procedimiento con el otro equipo. Para tener nuestro emisor y ceceptor.

6.- realizar pruebas con otro equipo colocándolos a una cierta distancia para ver si se logra tener un enlace, haciendo ping desde nuestra pc, aun conectada, hacia el otro equipo que se configuro con otra dirección ip, y ver cuál ha sido el resultado para poder el funcionamiento del equipo.



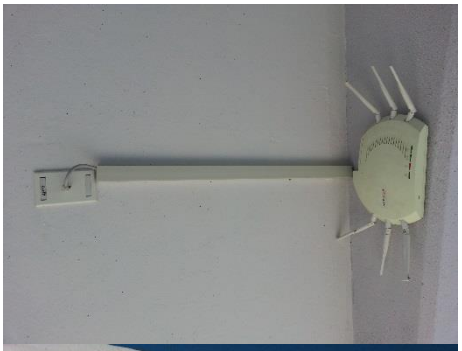
- **Reubicación de equipos de AP´S para mejor rendimiento.**

Debido a la demanda de usuarios, o mala ubicación debido a los movimientos de las oficinas, el ap no ofrece el máximo rendimiento, por lo que se fuerza a mover el equipo o colocar otro equipo AP, se colocan equipos proxim ap-4000, y equipos proxim 8000, debido a las características que estos manejan, que tienen la capacidad de modificarse extendiendo el cableado desde el site, hasta la nueva ubicación del AP o cambiar por un equipo que de mayor alcance y utilizar antenas amplificadoras para lograr la máxima cobertura y buena velocidad de conexión.

Ap proxim 8000

RADIO Y TRANSMISIÓN	
RADIO	• Dual Radio Access Point con la radio 802.11a/b/g/n • MIMO 3x3
CONFIGURACIONES DE RADIO	• 2 x 802.11b/g/n • 2 x 802.11b/g/n y 1 x 802.11a / n • 2 x 802.11a / n
Método de modulación	• MSC0 - MSC15 para 802.11n (6.5Mbps - 300 Mbps) • BPSK, QPSK, 16-QAM y 64-QAM para 802.11a y 802.11g (6Mbps-54Mbps) • DSSS para 802.11b (11Mbps-1Mbps)
BANDA DE FRECUENCIAS	5,15-5,85 GHz 2,4 a 2,483 GHz
Potencia de transmisión	
802.11n	19.5 dBm
802.11a	17 dBm
802.11bg	16.5 dBm
INTERFACES	
CONECTOR ANTENA	6 conectores RP-SMA
ANTENAS	6 de doble banda inversa conector SMA Omni Antena con ganancia 3 dBi
ETHERNET	Con detección automática 10/100/1000BASE-T Ethernet
FÍSICA	
DIMENSIONES SIN EMBALAR	11 5/16 x 7 x 1 3/4 in (287.34 x 177.8 x 44.75 mm)
PESO SIN EMBALAR	1,5 libras (0,7 kg)

AMBIENTAL	
TEMPERATURA	0 ° a 55 ° C (en funcionamiento) -20 ° a 75 ° C (almacenamiento)
HUMEDAD	Humedad relativa máxima del 95% (sin condensación)
ELÉCTRICA	
FUENTE DE ALIMENTACIÓN	110/220 VAC, 50/60 Hz (entrada), 5V 3A (salida) adaptador de corriente
POE	802.3af
LEDS	Cuatro indicadores en el panel superior indican el poder, el tráfico inalámbrico, el tráfico Ethernet, y las condiciones de error.
GESTIÓN	
LOCAL	RS-232 puerto serie; DB9 hembra
REMOTO	SNMP v1; V2c SNMP; DHCP; Telnet; HTTP; TFTP; SNTP; Escaneo y Cambio; BootP; Syslog
SEGURO	SSH, SNMPv2, HTTPS
MTBF	43.800 horas
CONTENIDO DEL PAQUETE	• (1) punto de acceso 802.11n AP-8000 • (1) 110/220V adaptador de alimentación de todo el mundo • (1) para montaje en pared / techo kit




1.- razón:

La reubicación de equipos se viene dando, Teniendo en cuenta que en algunas oficinas hay movimientos de inmuebles. A veces el ap no está ubicado en la mejor posición para poder transmitir su señal, debido a que tiene algún obstáculo por algún muro, mueble o ventanas. Y es por eso que se necesita un cableado nuevo hacia el nuevo lugar donde podrá abarcar hacia toda el área.

2.-Otra opción:

Es colocando otro ap para que no se sature un solo acces point, y así puedan conectarse a los dos para que tengan buena operatividad y no se sature la red al estar conectados a uno solo, ya que estos acces point tienen un número de usuarios aproximadamente de 150 y debido a variedad de equipos se llega a saturar la red, por eso es conveniente

tener dos o más acces point y habilitar el uso compartido gracias a los beneficios técnicos del ap ya mencionados en la hoja de datos.

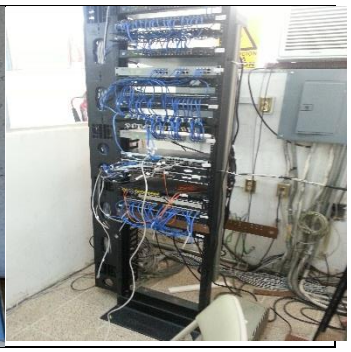
- **Cableado estructurado de los racks.**

Se realizó conexión a los diversos equipos instalados en el rack del SITE de las diferentes facultades de la UNACH, ya que como se pretende alojar un gran número de dispositivos, el cableado estructurado y etiquetado es necesario para la fácil localización del cable que se pretende buscar. Al igual ordenar los cables que ya presentaban una mala organización para que el usuario administrador pueda trabajar en el área sin ninguna dificultad.

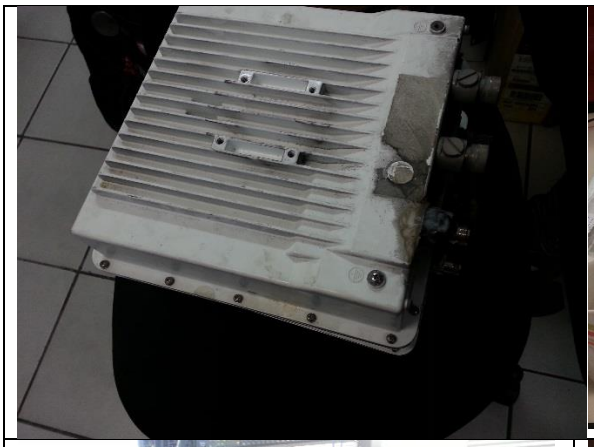
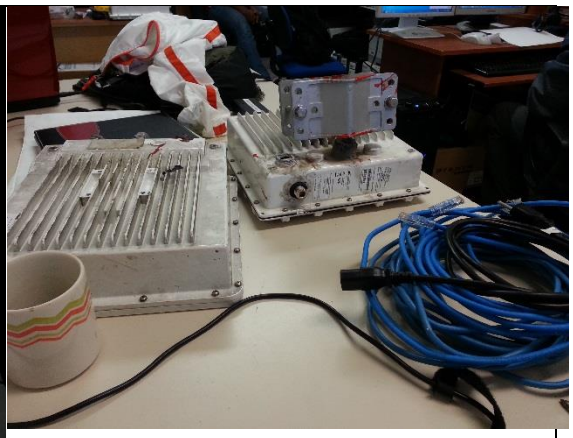
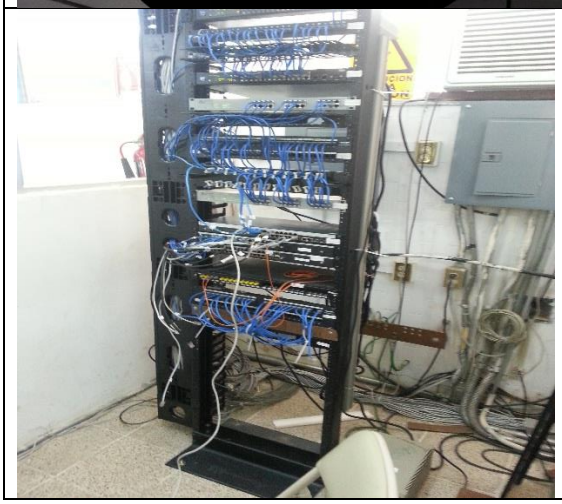
- **Cableado y comunicación edificios.**

Se realizó el cableado del edificio de rectoría el cual se pasó por el techo de falso plafón del área específica donde se requería. Se tendió cable del site hasta las oficinas donde se pretendían hacer las nuevas conexiones, llevando el cable por las canaletas de plástico para una mejor vista estética y con ello se permitió interconectar equipos activos, de diferentes o igual tecnología permitiendo la integración de los diferentes servicios que dependen del tendido de cables como datos, telefonía, etc.





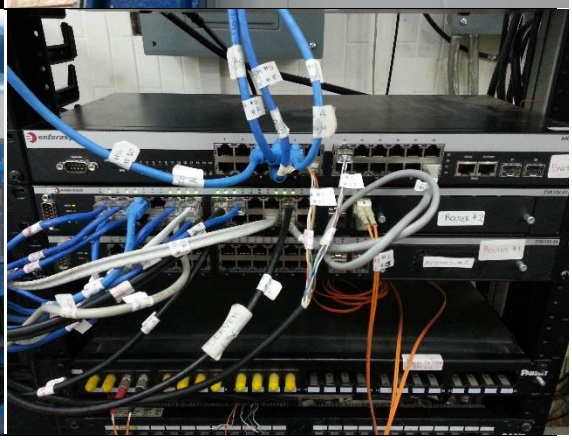
Resultados, planos, evidencias

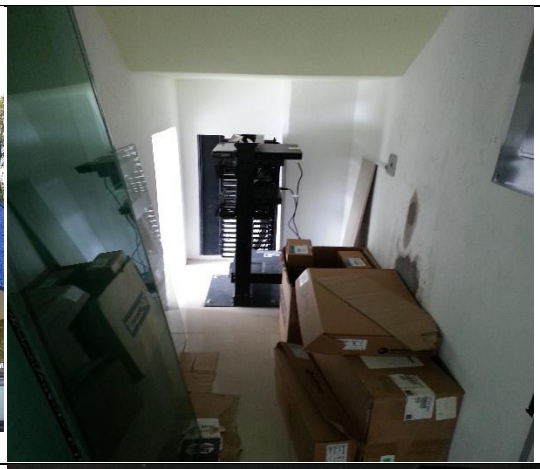






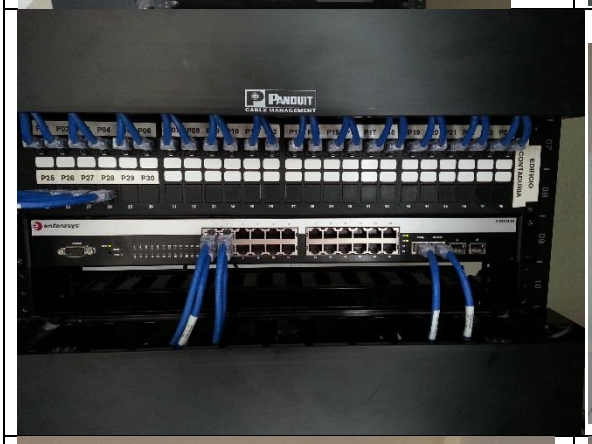
UNIVERSIDAD AUTÓNOMA CHIAPAS
METODOLOGIAS PARA DESARROLLOS AGILES

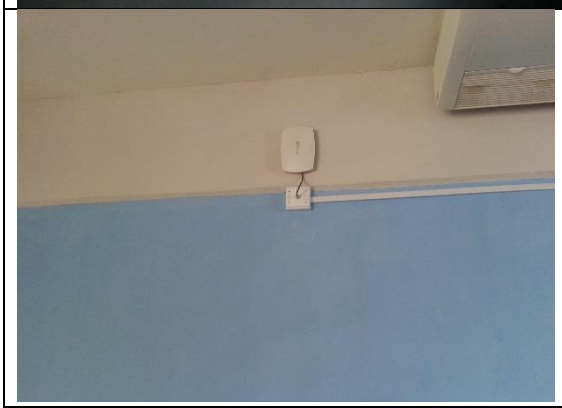

CENTRO
DE
COMPUTO

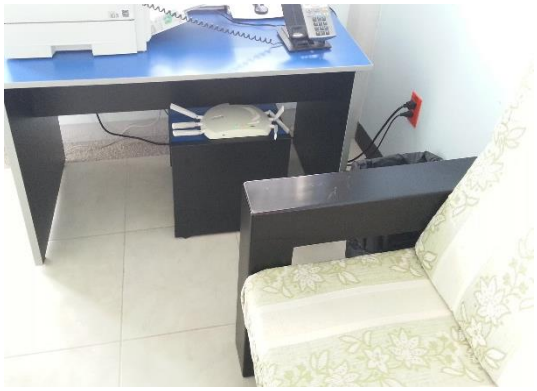


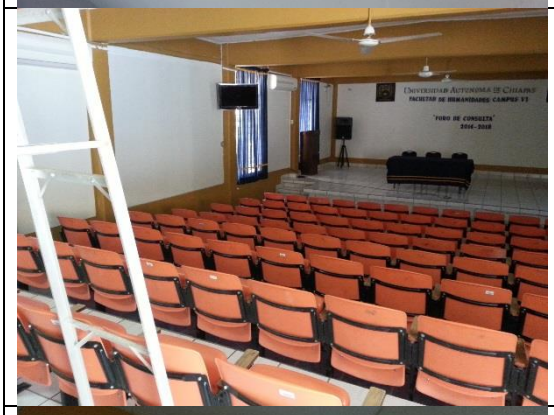



PANDUIT


PANDUIT
CABLE MANAGEMENT



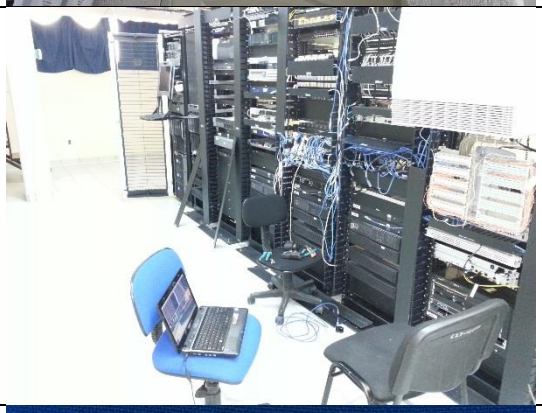


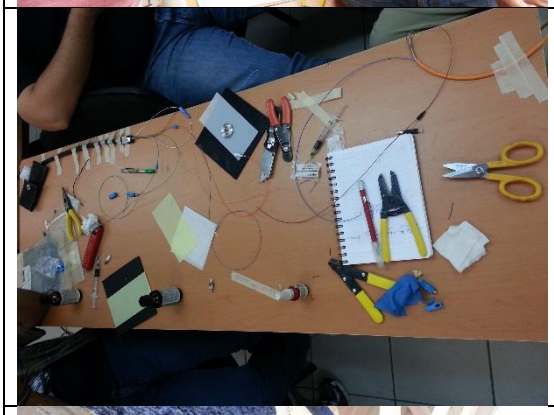

UNIVERSIDAD AUTÓNOMA DE CHIAPAS
FACULTAD DE HUMANIDADES CAMPUS VI
"POZO DE CONSULTA"
2014 - 2018

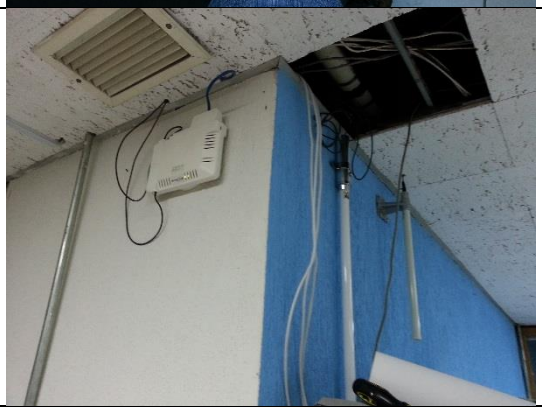

Coordinación

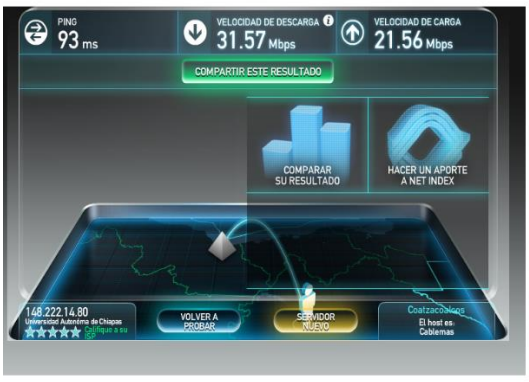









PING
93 ms
VELOCIDAD DE DESCARGA
31.57 Mbps
VELOCIDAD DE CARGA
21.56 Mbps
COMPARTIR ESTE RESULTADO
COMPARAR SU RESULTADO
HACER UN APORTE A NET INDEX
148.222.14.80
Universidad Autónoma de Chiapas
VOLVER A PROBAR
SERVIDOR NUEVO
Coatzacoalcos
El host es: Cablemas

CONCLUSIONES Y RECOMENDACIONES.

Como conclusión podremos decir que la tecnología ha evolucionado espectacularmente en los últimos años, debido especialmente a su capacidad de interconexión a través de la Red.

Esta nueva fase de desarrollo va a tener gran impacto en la organización de la enseñanza y el proceso de aprendizaje. En este caso como herramienta indispensable para todos los usuarios de la UNACH que requieran el uso del internet.

El llevar acabo la residencia con único propósito de optimizar las comunicaciones inalámbricas, teniendo en cuenta la tecnología manejada en la universidad 802.11a/b/g/n, servicios de transmisión de datos y VoIP, de cada una de las áreas de la universidad para que tengan una funcionalidad efectiva, que no sea intermitente y a largo plazo. Para una mayor calidad de servicio.

Siendo así se presentan los problemas comunes, de exigencia por la velocidad de la red, ya que esos problemas siempre se presentan y más cuando los usuarios van incrementándose, al igual los problemas cuando se presenta algún cambio en la arquitectura de las áreas y no dejando en una buena zona los puntos de acceso para que tenga mayor cobertura, resolviendo con unos equipos de mayor alcance, reubicando el equipo en una zona estratégica o comprando accesorios que hagan incrementar la potencia del equipo para el mejor servicio posible.

Otro factor es cuando los equipos son expuestos a la intemperie y cuando no son protegidos o hay errores al protegerlos, tienden a que estos equipos no trabajen bien o se dañen, provocando la caída de la red o haciéndola intermitente. Y volviendo a realizar cambios y conexiones nuevas para volver a tener las conexiones adecuadas y para que funcione con una buena calidad. Cuando no se usa el tipo de cable adecuado que si es para exterior o para interior.

Existen necesidades de seguir avanzando con esta tecnología, ya que la demanda de usuarios es cada vez mayor, y con mayor exigencia los trabajos requieren de una buena calidad de red para lo que es el servicio de internet. Así q habrá necesidad de aumentar el ancho de banda que mantiene la unach para poder soportar a todos los usuarios y facultades que tiene la universidad. Ya que ahora cuenta con 200MB y el crecimiento de la red proporcionaría grandes beneficios, velocidad y buena calidad, teniendo en cuenta los gastos que estos presentan sería una inversión a largo plazo. Al igual el mejorar y usar nuevas tecnologías en los equipos inalámbricos tendría grandes beneficios ya que ahora hay nuevos aparatos con mejores tecnologías.

Siendo así el trabajo hecho fue para poder optimizar y tomando en cuenta los factores de protección, normas, análisis, conexión, configuración y seguridad, tener el máximo rendimiento teniendo en cuenta las mejores configuraciones, diverso al uso que se le quiera dar, ya que existes distintas configuraciones y protocolos de red, que dependen del usuario administrador elegir y tener una misma configuración predeterminada para todos los equipos para que coincidan siempre, para que tenga una mayor eficacia con el cual tener un mayor plazo de funcionalidad, para la calidad de servicio en la ciudad universitaria.

Competencias desarrolladas y/o aplicadas.

Configuración de equipos de red:

Configuración para la interconexión de equipos acces point:

- Interfaz de usuario
- Nombre de la red
- Seguridad y Contraseña.
- Dirección ip
- Mascara de red
- Gateway de salida

Ponchado de cable UTP con sus respectivas categorías, y conector rj45

Comandos telnet

Tendido de cableado hacia los equipos en las áreas deseadas.

Cableado estructurado.

Realizar testeo de cables

Comandos para configurar switch

Teléfonos ip:

Configuración del teléfono

Reparación

Selección de la extensión del teléfono.

Referencias bibliográficas y virtuales.

- http://www.empretel.com.mx/wi-fi-ap/716-punto-de-acceso-inalambrico-ap-8000-320-mbps.html
- http://www.i4shop.net/cz/iobchod/2005/html/ap4000/helpfiles/Chapter2.htm
- http://es.scribd.com/doc/209518258/Wireless-AP-Ds
- http://www.textoscientificos.com/redes/redes-virtuales
- http://www.ehowenespanol.com/tipos-cables-utp-lista_85429/
- http://myhowtosandprojects.blogspot.mx/2012/03/enterasys-switches-crash-course.html
- http://cisconet.com/vendor/enterasys/234-enterasyshow-to-upgrade-firmware-html.