UNIVERSIDAD PERUANA LOS ANDES

FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TESIS

"IMPLEMENTACION Y GESTION DE ZONAS WIFI EN LAS FACULTADES DEL CAMPUS CHORRILLOS DE LA UPLA"

PRESENTADO POR:

BACH. JHON NAVARRO CONTRERAS

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS Y COMPUTACIÓN

HUANCAYO - PERÚ

2014

_____
Mg. Ing. RUBEN TAPIA SILGUERA
PRESIDENTE

_____

……
JURADO

_____

……
JURADO

_____

……
JURADO

_____
MG. MIGUEL ANGEL, CARLOS CANALES
SECRETARIO DOCENTE

ING. JORGE VLADIMIR PACHAS HUAYTAN
ASESOR

DEDICATORIA

Este trabajo está dedicado:

A mis adorados padres Rolando y Celia que hoy gozan la dicha del señor.

A mis hermanas Nalda y Giovanna que gracias a su apoyo incondicional hicieron posible la realización de este trabajo.

Jhon Navarro Contreras.

AGRADECIMIENTOS

A los Asesores Metodológicos y Temáticos por brindarnos sus valiosos aportes para el desarrollo de la presente tesis.

ÍNDICE DE CONTENIDOS

ÍNDICE

ÍNDICE DE GRÁFICOS

ÍNDICE DE CUADROS

RESUMEN

En la presente investigación de tesis en el caso de las típicas redes de datos con cables (siendo la tecnología Ethernet la más utilizada para estos casos), tiene que asegurarse que los usuarios de una red inalámbrica se encuentren conectados a ésta de una manera segura, teniendo en cuenta que ahora el medio de transmisión ya no se restringe a un cable, sino que se encuentra en todo el ambiente que lo rodea. Debe de comprobarse que el usuario sea quien dice ser (autenticación), que solo tenga acceso a los recursos que le corresponda (autorización) y también llevar a cabo un registro de las actividades que haga dentro de la red (contabilidad); realizando todo esto de una manera segura y sin que sujetos ajenos a la red puedan estar leyendo información confidencial ni mucho menos tratar de modificarla.

En esta tesis se explica el diseño e implementación de una red inalámbrica segura que contemple la administración de sus usuarios por medio de una plataforma de gestión Web basada en PHP, integrada a un servidor de directorios LDAP con compatibilidad hacia implementaciones libres y cerradas de dicho protocolo, un servidor de autenticación RADIUS y un servidor de base de datos MySQL. Se pondrá especial énfasis en la seguridad de la red y de sus usuarios con mecanismos tales como: WPA2 (IEEE 802.11i), 802.1X, EAP, RADIUS, entre otros.

PALABRAS CLAVES: Wifi, Radius, Seguridad de redes.

ABSTRACT

In the present thesis research in the case of typical data networks cables (being the most used for these cases Ethernet technology) , you must ensure that users of a wireless network are connected to it in a safe manner , now considering that the transmission medium is no longer restricted to a cable, but is found throughout the environment that surrounds it . It must be checked that the user is who he says (authentication), which only has access to the resources that will be (released) and also hold a record of the activities done within the network (accounting); doing this safely and without parties outside the network may be reading confidential information much less try to change it.

In this thesis the design and implementation of a secure wireless network that includes the administration of its users through a Web -based management platform in PHP, integrated to an LDAP directory server with support and closed to free implementations of this protocol is explained a RADIUS authentication server and a database server MySQL. WPA2 (IEEE 802.11i) 802.1X , EAP , RADIUS , including: special emphasis on the security of the network and its users with mechanisms such as becoming .

KEYWORDS : Wifi , Radius , Network Security .

INTRODUCCION

Cabe mencionar que toda la implementación se realizó teniendo en cuenta un análisis de costo-beneficio para la empresa u organización; llegando a estudiar distintas posibilidades de implementación de acuerdo a varias marcas de equipos de access points (las funciones que soportaría cada uno) con los que se pueda probar y el costo que cada tipo de solución implicaría.

Se buscó establecer de la mejora en el intercambio de información educativa a través de la implementación de zonas wifi en la ciudad universitaria de la upla, para ello en el Capítulo I se establece los aspectos Generales conjuntamente con el planteamiento del problema, la definición del problema, los objetivos tanto general como específicos así mismo tenemos la limitación de la investigación, la factibilidad y la justificación de la investigación con las hipótesis planteadas para la investigación con sus respectivas variables.

En el Capítulo II se establece el Marco teórico, los antecedentes de la investigación, seguidamente de las bases teóricas, seguridad de las redes, posturas teóricas, que también forman parte de esta investigación.

En el Capítulo III se establece el análisis de requerimiento, el estado de la red existente, conectividad externa, requerimiento de usuarios, requerimiento de usuarios, rendimiento de aplicaciones, requerimiento de dispositivos, la metodología a usarse, requerimiento de la red, y las especificaciones de los requerimientos de la investigación.

En el Capítulo IV se desarrolla el diseño de la red, arquitectura de los datos reales a través de las entrevistas, cuestionarios, se de la red, el direccionamiento y el enrutamiento, la gestión de la red, seguridad de la red, las políticas y procedimientos, el modelo de la arquitectura de la red, el diseño de la red, la distribución de la red y el diagrama lógico.

En el capítulo V se desarrolla las pruebas e implementaciones del sistema de red finales para su perfecto funcionamiento y aprobación.

Finalmente se presenta las conclusiones y sugerencias de la investigación.

El uso de redes inalámbricas para la distribución de Internet reduce los tiempos de instalación para el cliente final, permite una solución rápida y directa para los problemas que se puedan presentar, facilita la actualización de equipo y resulta ser un método barato para la distribución de este servicio. Sin embargo, el diseño correcto de estas redes es crucial para lograr que trabajen de modo eficiente.

El presente documento se empeña en desarrollar las técnicas y conocimientos necesarios para diseñar una red inalámbrica en el campus chorrillos de la UPLA, que permita distribuir Internet a un número determinado de usuarios de un modo eficiente, práctico y rápido.

Jhon Navarro Contreras.

GENERALIDADES

CAPITULO I
ASPECTOS GENERALES

1.1. DESCRIPCION DE LA ORGANIZACIÓN

La Universidad Peruana Los Andes, nace como la primera universidad privada del centro del Perú el 30 de diciembre de 1983 por mandato de la Ley N° 23757; iniciándose con las carreras de Contabilidad, Administración de Empresas, Ingeniería Industrial, Ingeniería Agrícola, Derecho y Educación con sus especialidades de Educación Técnica, Ingeniería Agrícola y otras ramas.

La Ley de creación de la UPLA, estipula como sede central, a la ciudad de Huancayo, capital del Departamento de Junín. Hoy Región Junín acorde la nueva demarcación política en nuestro país. Asimismo, precisa que no recibirá subvención alguna del estado y, su organización y funcionamiento estará sujeto a la Ley Universitaria N° 23733.

La norma de creación 23757, fue aprobada por el Congreso de la República, en Lima, el 22 de diciembre de 1983, siendo por entonces presidente de la Cámara de Diputados, el Dr. Dagoberto Lainez Vodanovic, presidente de la Cámara de Senadores, el Dr. Ricardo Monteagudo Monteagudo. Y promulgada por el Presidente Constitucional de la República, Arq. Fernando Belaúnde Terry, un 30 de diciembre de 1983.

Desde entonces, la UPLA se ha convertido en una institución universitaria sin fines de lucro a beneficio de sus mismos estudiantes, docentes, graduados y trabajadores, guiados y conducidos por sus autoridades universitarias elegidas cada cinco años de acuerdo a su estatuto y ley universitaria vigente.

Más adelante, el 23 de Junio de 1987 se promulga la Ley Complementaria N° 24697 que oficializa el funcionamiento de la carrera profesional de Ingeniería Civil, convirtiéndose en la pionera en esta parte del país, posteriormente se crea nuevas facultades; así como nuevas carreras profesionales y se modifica la denominación de algunas ya existentes de acuerdo al avance de la ciencia, tecnología y requerimientos sociales e institucionales.

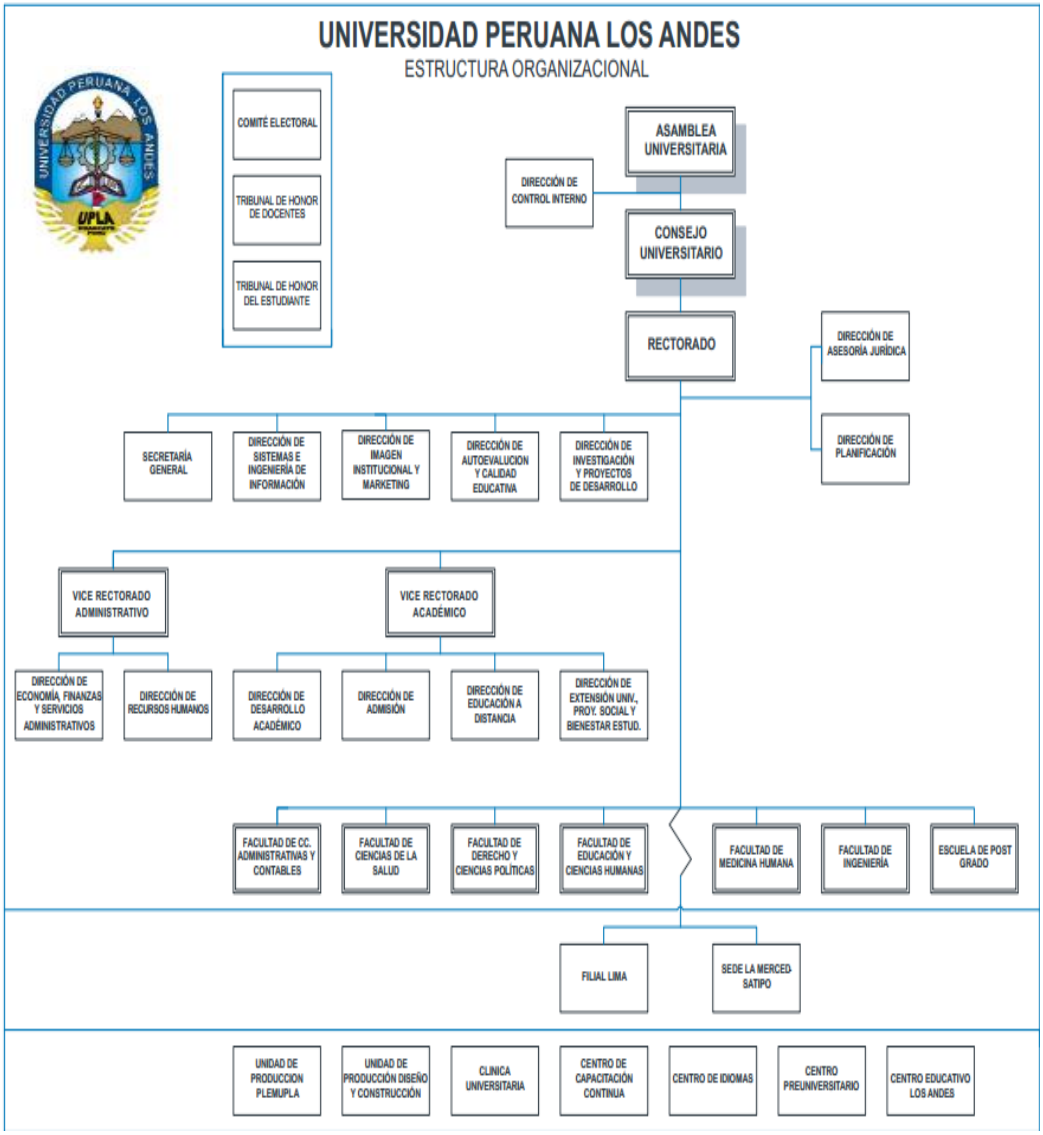


Grafico1. Estructura Organizacional de la UPLA con datos tomados de la dirección web www.upla.edu.pe

1.2. PLANTEAMIENTO DEL PROBLEMA

1.2.1. SITUCION PROBLEMÁTICA

La Universidad Peruana Los Andes (Ciudad Universitaria), dentro de su ámbito tecnológico cuenta con un parque informático considerable, instalados en las diferentes facultades, esta organización cuenta con toda su red LAN cableada.

Este problema radica en el deficiente servicio para sus usuarios móviles que cuentan con computadoras portátiles (notebooks), equipos móviles, celulares, etc. y se encuentran en constante movimiento dentro del ámbito de la infraestructura; ya que requieren ubicar una señal de red cercano donde se encuentren para poder descargar sus correos o buscar alguna información en la Internet, lo que trae consigo incomodidad y una disminución en el desempeño de dicha persona al perder tiempo realizando este proceso; tiempo que se traduce en una disminución de su aprendizaje, información y productividad.

Como segundo problema se tiene que el estado actual de la red no es el óptimo. Debido a un simple pero inadecuado direccionamiento IP de la red, así como una mala distribución del equipamiento de red, ha ocasionado que se presenten síntomas de lentitud y una respuesta tardía ante los requerimientos de sus usuarios, incluso para simples usos como descargar correos, búsqueda de información académica, desarrollo de tareas o navegar por la Internet.

Por lo tanto se recurrió a realizar la mejora en el intercambio de información educativa a través de la implementación de zonas Wifi en la ciudad universitaria de la UPLA, con el propósito de que todos los usuarios puedan acceder a Internet desde cualquier lugar o punto de la universidad; el cual permitirá en un principio, la optimización de las operaciones y el incremento de la productividad.

1.2.2. DEFINICION DEL PROBLEMA

La Universidad Peruana los Andes (ciudad universitaria) tiene como propósito prestar un eficiente y completo servicio de internet y dar un adecuado uso a todas las actividades académico y administrativas de la universidad; es por esta

razón que existe una administración y soporte de red encargada de brindar apoyo a los usuarios, con el objetivo de lograr el máximo nivel de operatividad de sus equipos, sistemas, datos, redes y software de aplicaciones disponibles en la plataforma tecnológica.

1.3. OBJETIVOS:

1.3.1. Objetivo General

Implementar la gestión de zonas WiFi en las Facultades del campus chorrillos de la Universidad Peruana Los Andes.

1.3.2. Objetivos Específicos

a) Determinar los requerimientos para la implementación y gestión de zonas WIFI en las Facultades del campus chorrillos de la UPLA.

b) Realizar el diseño de gestión de zonas Wifi en las Facultades del campus universitario chorrillos UPLA.

c) Implementar la gestión de zonas Wifi y la instalación de los equipos pertinentes en las Facultades del campus chorrillos UPLA.

1.4. LIMITACIÓN DE LA INVESTIGACIÓN

a) Limitación de Tiempo. El periodo de análisis de la investigación está comprendido en el periodo Octubre 2013 hasta Enero 2014.

b) Limitación Espacial. La investigación se desarrolló en ciudad universitaria de la UPLA, (específicamente en las diferentes facultades que existe en la universidad) la cual se encuentra ubicada en la provincia de Huancayo departamento de Junín.

c) Limitación de Recursos. La investigación está limitada en su aplicación a la toma de decisiones del Concejo Universitario.

1.5. FACTIBILIDAD

1.5.1. FACTIBILIDAD TECNICA

Este proyecto se considera factible debido a que la Universidad Peruana Los Andes cuenta con los equipos y software para poder implementar la mejora en el intercambio de información educativa a través de la implementación de zonas Wifi en la ciudad universitaria de la UPLA, para el desarrollo Web basada en PHP, integrada a un servidor de directorios LDAP con compatibilidad hacia implementaciones libres y cerradas de dicho protocolo, un servidor de autenticación RADIUS y un servidor de base de datos MySQL.

Con la fusión de estas herramientas se logró crear un sistema confiable, seguro, rápido de manejar y con respuestas oportunas a las consultas realizadas por los usuarios finales.

Con esta implementación se comprobara que el usuario sea quien dice ser (autenticación), que solo tenga acceso a los recursos que le corresponda (autorización) y también llevar a cabo un registro de las actividades que haga dentro de la red (contabilidad); realizando todo esto de una manera segura y sin que sujetos ajenos a la red puedan estar leyendo información confidencial ni mucho menos tratar de modificarla.

.

1.5.2. FACTIBILIDAD ECONOMICA

La Universidad Peruana Los Andes la inversión que tiene es poca, para todos los beneficios que este ofrece.

La finalidad de este sistema es el utilizar un software libre.

El diseño, desarrollo e implementación no generó inversión alguna a la institución, ya que por ser un proyecto elaborado como trabajo de grado (tesis), pero cabe destacar que sintetiza las cargas laborales del administrador de la red que normalmente se dedicaba a administrar toda la red, y por ende puede emplear el tiempo que se ahorran con la

implementación propuesto en otras actividades dentro de la Universidad.

1.5.3. FACTIBILIDAD SOCIAL

La implementación de zonas Wifi en la ciudad universitaria de la UPLA mejorará la administración de las redes y recursos informáticos para ofrecer servicios de calidad a toda la población educativa y administrativa; en consecuencia esto mejorará el proceso de enseñanza y aprendizaje de la Universidad Peruana Los Andes.

1.5.4. FACTIBILIDAD OPERATIVA

Cabe destacar que el personal administrativo, docentes y estudiantes de la Universidad están totalmente de acuerdo con esta implementación de este nuevo sistema de red, el cual es llevado actualmente de forma ineficiente, siendo posteriormente un sistema totalmente automatizado y eficaz. Todas las personas que integran el equipo de trabajo están dispuestos a adaptarse a nuevas tecnologías de red, pues consideran que cada día será más eficiente, rápido y seguro logrando así una mejor eficiencia organizacional.

En todo momento el personal administrativo colaboró a lo largo de la investigación, pues nos facilitaron datos que ellos creyeron importantes para la realización de la implementación de zonas Wifi, expusieron sus puntos de vista con respecto al manejo actual y los problemas que este presentaba, y por otro lado exponían la forma en que se debían llevar a cabo los diferentes procesos de distribución, compartimiento y accesos.

1.5.5. ALTERNATIVAS O PLANTEAMIENTO DE LA SOLUCION

Para la mejora en el intercambio de información educativa a través de la implementación de zonas Wifi en la ciudad universitaria de la UPLA; se plantea las siguientes alternativas de solución:

- Se implementará 5 zonas Wifi a través de antenas en los diferentes edificios (facultades) de la ciudad universitaria de chorrillos de la UPLA para que la transmisión de información, datos, etc sea más óptima, confiable y asequible para todo el personal docente, administrativo y estudiantes en general se conecten desde cualquier punto del campus.
- Con esta implementación se desea obtener resultados académicos más favorables en bien del estudiante y personal académico-administrativo.
- Se contara con un sistema de seguridad para que intrusos fuera de la universidad no puedan hackear la información confidencial que existe dentro de la universidad a la vez no permitir el uso del internet apersonas ajenas y maliciosas.
- Se asignara un usuario y contraseña a los estudiantes con un respectivo tiempo para la utilización de la red, a la vez se asignara paginas estrictamente pedagógicas, páginas de la UPLA, asuntos académicos, tramites, y buscadores de trabajos monográficos, tesis, etc. Específicamente de investigación.
- De esta manera se pretende solucionar las grandes expectativas que tienen los estudiantes, docentes y la parte administrativa; mejorando localidad de enseñanza, educando un orden informático para la buena utilización de la internet dándole el valor necesario que realmente contiene la tecnología de hoy en día.

1.6. JUSTIFICACIÓN DE LA INVESTIGACION:

1.6.1. Justificación Práctica

La presente investigación plantea realizar la mejora en el intercambio de información educativa a través de la implementación de zonas Wifi en la ciudad universitaria de la UPLA, lo cual nos permitirá mejorar el servicio de red que será de mucho beneficio principalmente para los estudiantes, docentes y personal administrativo a tener una mejor metodología

pedagógica y tecnológica en tiempo real a los beneficiados de esta casa superior de estudios, también dicha implementación de esta red contemplará altos mecanismos de seguridad; para los cuales no permitirá que un posible intruso pueda ser capaz de leer la información confidencial de los usuarios (que estén registrados) ni de permitirle si quiera acceso a la red.

1.6.2. Justificación Metodológica

Al desarrollar la mejora en el intercambio de información educativa a través de la implementación de zonas Wifi en la ciudad universitaria de la UPLA, como el que plantea la investigación, estableceremos un procedimiento que servirá de guía para futuros trabajos que se realicen en el área.

CAPITULO II

MARCO TEORICO

2.1. ANTECEDENTES

2.1.1. INVESTIGACIONES PREVIAS

En la tesis titulada “Diseño de una red inalámbrica para una empresa de Lima” Barrenechea Zavala, Taylor Iván (2011-10-03) en el cual se concluye de la siguiente manera: “Las redes inalámbricas diseñadas permitirán brindar acceso a la información de manera oportuna. Los usuarios autorizados pueden conectarse de forma inmediata desde cualquier ubicación física en la empresa”.

Así mismo tenemos la tesis titulada “Diseño e implementación de un sistema de gestión de accesos a una red wi-fi utilizando software libre” López Mori, Jorge Alonso (2008-11-11) en el cual se concluye de la siguiente manera “Es posible la integración de todas las herramientas de software libre utilizadas en la presente tesis (FreeRADIUS, OpenLDAP, SAMBA, MySQL) con un dominio

desarrollado con Microsoft Windows. Es decir, en el caso de que se le desee implementar en una red ya existente y que utilice herramientas comerciales (tales como MS Windows 2003 Server y/o MS Active Directory) bastaría con modificar algunos parámetros en los archivos de configuración de las herramientas de software libre utilizadas para poder lograr la integración y trabajo entre todos estos".

También se tiene la tesis titulada "Diseño de una red de acceso inalámbrico utilizando tecnología CDMA 450 Mhz para el distrito de Ahuac, provincia de Chupaca, departamento de Junín" Llamoca Chahua, Yessenia Kioko (2012-03-12) concluyendo de la siguiente manera: "Utilizando el programa informático ICS Telecom, se realizó un estudio teórico para simular la instalación de la tecnología de acceso múltiple por división de código en la banda 450 MHz; CDMA 450".

También tenemos la tesis titulada "Implementación de un sistema red inalámbrico para compartir recursos informáticos en el instituto superior tecnológico público huaycán" Quispe Manco, Manuel Enrique (2010-06-20) concluyendo de la siguiente manera: "La seguridad es un factor muy importante en el diseño e implementación de redes inalámbricas, ya que por su forma de transmisión (el aire) son vulnerables al ataque de intrusos. Es por esto que se debe tomar las medidas necesarias para evitar que personas mal intencionadas ingresen a la red".

También tenemos la tesis titulada "Diseño de una PBX inalámbrica para la prestación de servicios de tipo fijo y móvil utilizando wi-fi y telefonía IP" Mendoza Cámac, José Luis (2007-09-10) concluyendo de la siguiente manera: "Al contar con una red de acceso inalámbrica se atenderán los requerimientos de la demanda móvil de los usuarios de la empresa, facilitando sus

operaciones, potenciando su desempeño y aumentando su disponibilidad de manera significativa".

Roure, Antoni (Lima – 2009), "Seguridad Informática y Redes Wireless" La seguridad es un factor muy importante en el diseño e implementación de redes inalámbricas, ya que por su forma de transmisión (el aire) son vulnerables al ataque de intrusos. Es por esto que se debe tomar las medidas necesarias para evitar que personas mal intencionadas ingresen a la red.Este trabajo nos da una visión de cómo funciona la seguridad en redes inalámbricas que pretendemos utilizar en el proyecto.

Relación: Esta tesis se toma en consideración porque a través de esta implementación de zonas Wifi permitirá tener un mejor control en la administración de recursos de hardware/software y la seguridad de la red a través del administrador.

Gonzales, Luis (Lima - 2008) "Tecnologías de redes inalámbricas" que abordan las WLAN ofrecen muchos beneficios, aumentando la productividad y rentabilidad de la empresa, permitiendo ir a la par con el desarrollo de la tecnología, También, se revisa los estándares en que se basa y la tendencia de los requerimientos en el mercado tanto a corto como a mediano plazo.

Relación: Esta tesis se toma en consideración porque a través de esta implementación de zonas Wifi se enfoca a brindar una mejora en la búsqueda de información para el aprendizaje, desarrollo de actividades, ahorrando tiempo y dinero a toda la población estudiantil, docente y administrativo.

2.2. BASES TEORICAS

A. RED INALÁMBRICA

Fidel García (Abril 2003) “Redes Inalámbricas WI-FI” Una red inalámbrica de área local (Wireless LAN) es un sistema flexible de transmisión de datos implementados como una extensión, o como alternativa, de una red cableada. Utiliza tecnología de radio frecuencia, transmite y recibe datos utilizando como medio el aire, minimizando la necesidad de una conexión de cable, permitiendo la combinación conectividad y movilidad.

B. RED DE COMPUTADORAS LOCAL INALÁMBRICA

Editan Coit Aeit (Revista BIT N°138 – 2010) “Especial Redes Inalámbricas” Es un sistema de comunicación de datos que utiliza tecnología de radiofrecuencia. En esta red se transmite y recibe datos sobre aire, minimizando la necesidad de conexiones alámbricas.

C. WIFI

Ruiz Padilla José (Libera Networks para mundo internet 2004) “Redes WIFI” Es el nombre comercial del estándar IEEE 802.11. Es una tecnología novedosa y práctica que se está difundiendo muy rápidamente por todo el planeta. Por estos mismos motivos, WiFi es una tecnología inmadura, que va requiriendo nuevos estándares o modificaciones en los estándares existentes, a medida que van apareciendo inconvenientes.

D. ZONA WI-FI

Gilbertt Ateros, (Agosto 2001 España) “Zones Wireless” Es el área donde puedes encontrar señal inalámbrica con la que te conectas a internet desde tu portátil. Es común en los centros comerciales, escuelas y universidades.

E. PUNTO DE ACCESO

Javier Gabiola Francisco (Agosto - 2004) “Mundo Internet” Es solo el equipo electrónico que permite la conexión inalámbrica.

F. RADIUS

Julio Alba, David Roldán Martínez. (2010, Junio). “Aplicaciones de WiFi” RADIUS (acrónimo en inglés de Remote Authentication Dial-In User Server).Es un protocolo de autentificación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza los puertos 1812 y 1813 UDP para establecer sus conexiones (para autenticar/autorizar y contabilizar, respectivamente).

G. LDAP

Jes Nyhus. (2010) Redes y Redes Inalámbricas Sociedad Editora KnowWare LDAP (Light weight Directory Access Protocol) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) al que pueden realizarse consultas. Habitualmente, almacena la información de login o acceso a un sistema (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc).

H. WPA/WPA2 (IEEE 802.11i)

Julio Alba, David Roldán Martínez. (2010, Junio). “Aplicaciones de WiFi” WPA (Wi-Fi Protected Access - 1995 - Acceso Protegido Wi-Fi) es un sistema para proteger las redes

inalámbricas Wi-Fi; creado para corregir las deficiencias del sistema previo WEP. Los investigadores han encontrado varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros).

I. 802.1X

Profesionales, G. N. (2010). La situación de las Tecnologías WLAN basadas en el estándar IEEE 802.11 y sus variantes ("WiFi") El IEEE 802.1X (Port-based Network Access Control) es un estándar de la IEEE para Control de Admisión de Red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Con la aparición de las redes inalámbricas Wi-Fi, también es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en protocolo de autenticación extensible (EAP– RFC 2284).

J. LIMITES DE LA RED

Javier Gabiola Francisco (Agosto - 2004) "Mundo Internet" Los límites de la red 802.11. son difusos ya que pueden solaparse diferentes BSS.

K. ONDA DE RADIO

Javier Gabiola Francisco (Agosto - 2004) "Mundo Internet" En general estamos familiarizados con las vibraciones u oscilaciones de varias formas.

L. FIREWALL

Rodríguez-Ovejero, L. (2010). El futuro de las comunicaciones móviles Literalmente "Muro de Fuego o cortafuegos" se trata de cualquier programa que protege a una red de otra red.

LL.TCP/IP

Rodríguez-Ovejero, L. (2010). El futuro de las comunicaciones móviles (Transmission control protocol/internet protocol) familia de protocolos definidos en RFC793, en los que se basa internet, el primero se encarga de dividir la información en paquetes en origen, para luego recomponerla en destino, mientras que el segundo se responsabiliza de dirigirla adecuadamente a través de la red.

M. DIRECCION IP

Rodríguez-Ovejero, L. (2010). El futuro de las comunicaciones móviles Dirección de 32 bits definida por el protocolo internet en STD 5, RFC93, en los que se basa internet. El primero se encarga de dividir la información en paquetes en origen, para luego recomponerla en destino, mientras que el segundo se responsabiliza de dirigirla adecuadamente a través de la red.

N. BANDA ANCHA

Rodríguez-Ovejero, L. (2010). El futuro de las comunicaciones móviles Se denomina así a los canales de comunicación cuya velocidad de transmisión es muy superior a la de un canal de banda local, aunque el límite no está claramente determinado, se suele aplicar a velocidades superiores a los 250kbit/s.

2.2.1. DEFINICIÓN DE REDES

El término Network. Es un conjunto de hardware y software de gestión necesario para la conexión de múltiples ordenadores con el fin de que puedan intercambiar información entre ellos y compartir recursos. La Red puede ser de área local (LAN) o de área amplia (WAN).

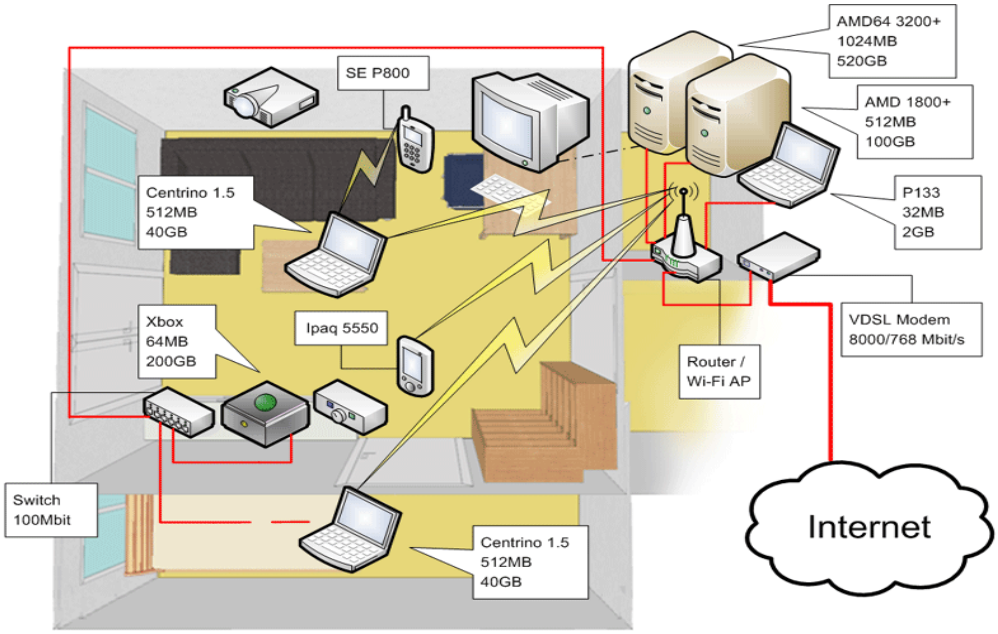


Grafico 2. Diagrama de una Red Corporativa con datos tomados de la dirección web www.coppernic.blogspot.com

En la figura se muestra el diagrama de una red corporativa de mediano porte. En ella se muestran los dispositivos de uso frecuente en las redes. De manera general los objetivos de diseño de una red son:

- Funcionalidad
- Performance
- Seguridad
- Gestión
- Escalabilidad
- Compatibilidad

A. MODELOS DE REFERENCIA

Los Modelos de referencia proveen la ventaja de dividir la complejidad de las operaciones de la red en un conjunto manejable de niveles o capas. El diseño de protocolos en base a los modelos de referencia posibilita la introducción de cambios en una capa, sin que las otras se vean afectadas. Es un instrumento eficaz para analizar todo tipo de redes.

B. MODELO DE REFERENCIA OSI

El modelo de referencia OSI es un modelo de trabajo desarrollado por la ISO para promover la estandarización de los protocolos utilizados en la interconexión de sistemas heterogéneos (abiertos).

Grafico 3. Modelo OSI con datos tomados de la dirección www.pesmec5aeq1.weebly.com

Cuadro 1
Descripción de Capas Modelo OSI

CAPA OSI	DESCRIPCIÓN FUNCIONAL	EJEMPLOS
(7) APLICACIÓN	Semántica. Interface con las aplicaciones/usuarios.	Telnet, http, FTP, www, NFS, SMTP, SNMP, X400.
(6) PRESENTACIÓN	Formato de los datos. Sintaxis. Procesamientos especiales	JPEG, ASCII, EBCDIC, TIFF, GIF, PICT, encryption, MPEG, MIDI.
(5) SESIÓN	Flujo ordenado de los datos entre las partes intervinientes (transacciones).	RPC, SQL, NFS, nombres NetBios, AppleTalk, ASP, DECnet SCP.
(4) TRANSPORTE	Calidad de servicio. División entre res y capas sup. Mux.	TCP, UDP, SPX.
(3) RED	Direccionamiento lógico.	IP, IPX, APPLETALK, ICMP
(2) ENLACE DE DATOS	Acceso al medio. Enlace entre estaciones vecinas. Manejo de errores.	IEEE 802.3/802.2, HDLC, Frame Relay, PPP, FDDI, ATM, IEEE 802.5/802.2.
(1) FÍSICA	Señales físicas, conectores, temporización.	EIA/TIA-232, V35, EIA/TIA-449, V.24, RJ-45, Ethernet, 802.3, 802.5, FDDI, NRZI, NRZ, B8ZS[1]

Nota. Información obtenida de la dirección www.monografias.com/trabajos29/modelo- osi/modelo-osi.shtml

C. MODELO DE REFERENCIA TCP/IP

En el modelo TCP/IP no existen las capas de presentación y sesión. Directamente sobre la capa de transporte se encuentra la capa de aplicación, la cual contiene todos los protocolos de alto nivel.

Un gran vacío (y por ende gran flexibilidad) existe por debajo de la capa internet en el modelo TCP/IP, dado que no define ningún

protocolo (solamente menciona que el host debe conectarse a la red utilizando algún protocolo para enviar los paquetes).

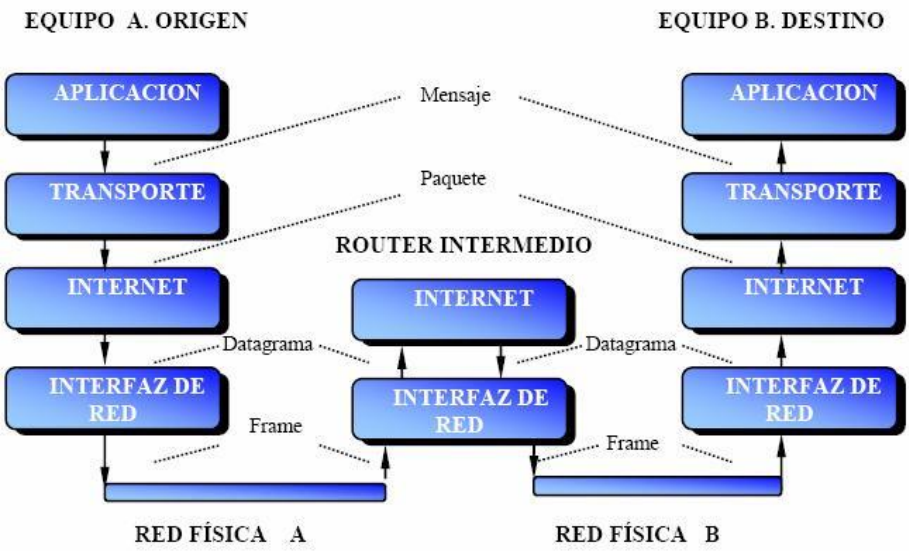


Grafico 4. Modelo TCP/IP datos tomados de la dirección www.inglopezpaez.wordpress.com

D. COMPARACIÓN ENTRE EL MODELO OSI y TCP/IP

Las diferencias entre la arquitectura OSI y la del TCP/IP se relacionan con las capas encima del nivel de transporte y aquellas del nivel de red. OSI tiene una capa de sesión y una de presentación en tanto que TCP/IP combina ambas en una capa de aplicación. El requerimiento de un protocolo sin conexión, también requirió que el TCP/IP incluyera además, las capas de sesión y presentación del modelo OSI en la capa de aplicación del TCP/IP.

En la capa Acceso a la red, la suite de protocolos TCP/IP no especifica cuáles protocolos utilizar cuando se transmite por un medio físico; sólo describe la transferencia desde la capa de Internet a los protocolos de red física. Las Capas OSI 1 y 2 analizan los procedimientos necesarios para tener acceso a los medios y los medios físicos para enviar datos por una red.

Los paralelos clave entre dos modelos de red se producen en las Capas 3 y 4 del modelo OSI. La Capa 3 del modelo OSI, la capa Red, se utiliza casi universalmente para analizar y documentar el rango de los procesos que se producen en todas las redes de datos para direccionar y enrutar mensajes a través de una internetwork.

La Capa 4, la capa Transporte del modelo OSI, con frecuencia se utiliza para describir servicios o funciones generales que administran conversaciones individuales entre los hosts de origen y de destino. Estas funciones incluyen acuse de recibo, recuperación de errores y secuenciamiento.

La capa de aplicación TCP/IP incluye una cantidad de protocolos que proporcionan funcionalidad específica para una variedad de aplicaciones de usuario final. Las Capas 5, 6 y 7 del modelo OSI se utilizan como referencias para proveedores y programadores de software de aplicación para fabricar productos que necesitan acceder a las redes para establecer comunicaciones.

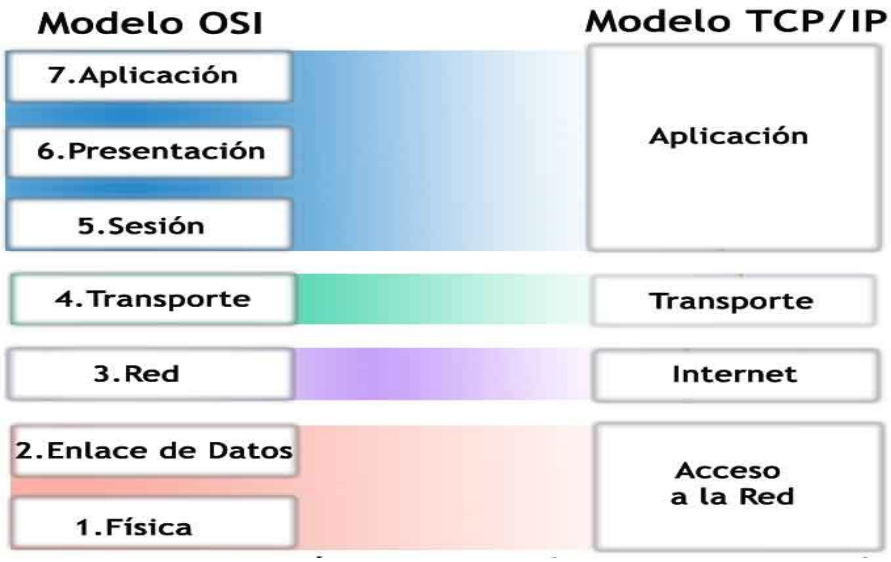


Grafico 5. Comparación Modelo OSI / TCP/IP las semejanzas más importantes las encontramos en la capa de red y de transporte

2.2.2. TIPOS DE RED.

Las redes se clasifican por su alcance, porque de acuerdo a la extensión geográfica se clasifican de la siguiente manera:

A. RED DE ÁREA LOCAL (*LAN Local Area Network*).

Una LAN permite la transferencia rápida y eficaz de información en el seno de un grupo de usuarios reduciendo los costos de explotación. Una LAN suele estar formada por un grupo de computadoras, impresoras o dispositivos de almacenamiento de datos como unidades de disco duro.

Otra característica de dicha red es que cada dispositivo está conectado a un repetidor, un equipo especializado que transmite de forma selectiva la información desde un dispositivo hasta uno o varios destinos en la red Las conexiones que unen las LAN con otras LAN o una base de datos remota utilizando recursos externos se denominan puentes, ruteadores y puertas de redes (gateways).

Los avances en la forma en que una red encamina o rutea la información permitirán que los datos circulen directamente desde la computadora origen hasta la del destino sin interferencia de otras computadoras, esto provoca un mejoramiento en la transmisión de flujos continuos de datos, como señales de audio o de vídeo.

El uso generalizado de computadoras portátiles ha llevado a importantes avances en las redes inalámbricas. Las redes inalámbricas utilizan transmisiones de infrarrojos o de radiofrecuencia para conectar computadoras portátiles a una red.

Las LAN inalámbricas de infrarrojos conectan entre sí computadoras situadas en una misma habitación, mientras que las LAN inalámbricas de radiofrecuencia pueden conectar computadoras separadas por paredes.

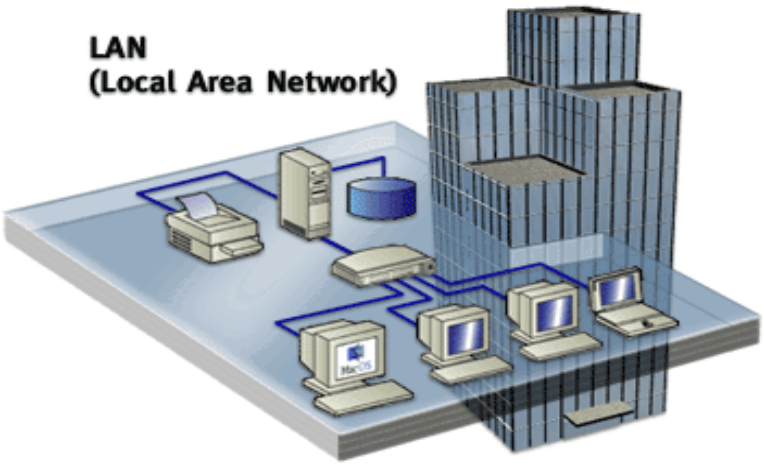


Grafico 6. Red de Área Local tomado de la dirección www.taringa.net

B. RED DE ÁREA METROPOLITANA (MAN Wide Área Network).

La MAN es una red que abarca un área metropolitana, como, por ejemplo, una ciudad o una zona suburbana. Una MAN generalmente consta de una o más LAN dentro de un área geográfica común. Por ejemplo, un banco con varias sucursales puede utilizar una MAN. Normalmente, se utiliza un proveedor de servicios para conectar dos o más sitios LAN utilizando líneas privadas de comunicación o servicios ópticos. También se puede crear una MAN usando tecnologías de puente inalámbrico enviando haces de luz a través de áreas públicas.

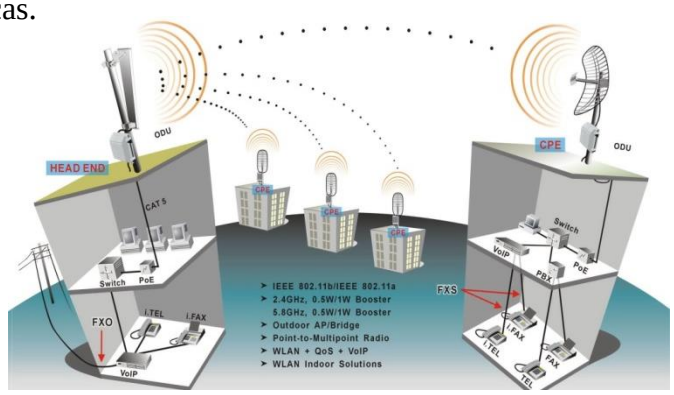


Grafico 7. Red de Área metropolitana tomado de la dirección www.redes.20.galeon.com

C. REDES DE ÁREA AMPLIA (WAN).

Las WAN interconectan las LAN, que a su vez proporcionan acceso a los computadores o a los servidores de archivos ubicados en otros lugares. Como las WAN conectan redes de usuarios dentro de un

área geográfica extensa, permiten que las empresas se comuniquen entre sí a través de grandes distancias. Las WAN permiten que los computadores, impresoras y otros dispositivos de una LAN compartan y sean compartidas por redes en sitios distantes. Las WAN proporcionan comunicaciones instantáneas a través de zonas geográficas extensas. El software de colaboración brinda acceso a información en tiempo real y recursos que permiten realizar reuniones entre personas separadas por largas distancias, en lugar de hacerlas en persona. Networking de área amplia también dio lugar a una nueva clase de trabajadores, los empleados a distancia, que no tienen que salir de sus hogares para ir a trabajar.

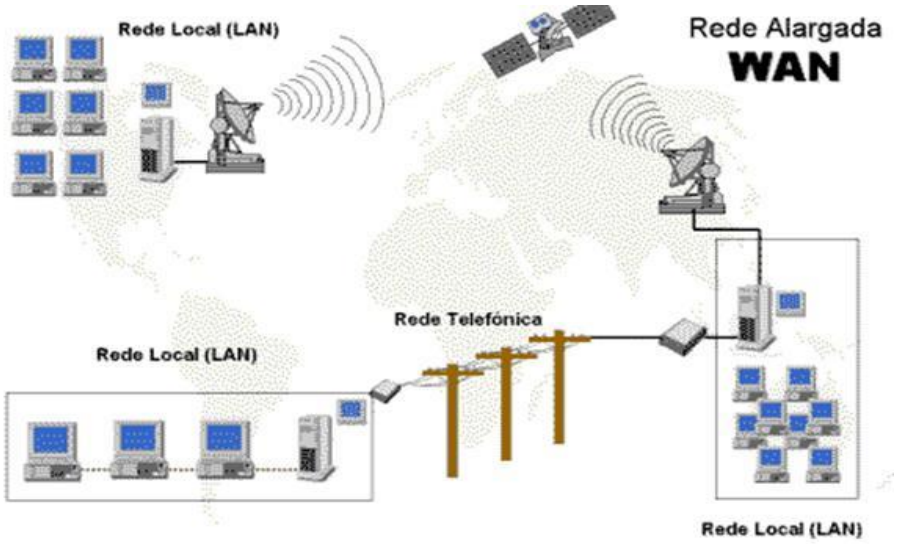


Grafico 8. Red de Área extensa tomado de la dirección www.redesdedatosinfo.galeon.com

2.2.3. TOPOLOGÍAS DE RED

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

- Una topología de bus usa un solo cable backbone que debe terminarse en ambos extremos. En esta topología se permite que todas las estaciones de trabajo (hosts) reciban la información de manera secuencial. Existen algunas desventajas que hacen que esta topología esté dejándose de utilizar, la principal es que si el cable resulta dañado, la información llegará hasta ahí, ya que la información o datos viajan de manera secuencial por el cable.
- La topología de anillo conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable. Los datos o la información viaja de un sólo lado, de la misma manera que en la topología Bus, si un nodo (estación de trabajo o computadora) se rompe la red deja de funcionar.
- La topología en estrella conecta todos los cables con un punto central de concentración. Ésta topología es la más utilizadas ya que los datos viajan desde el concentrador o host hacia el destino. Las ventajas más notables de esta topología es que si un host o estación de trabajo falla, el fallo no afecta el desempeño de la red
- Una topología en estrella extendida conecta estrellas individuales entre sí mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red.
- Una topología jerárquica es similar a una estrella extendida. Pero en lugar de conectar los hubs o switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.
- La topología de malla se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio.

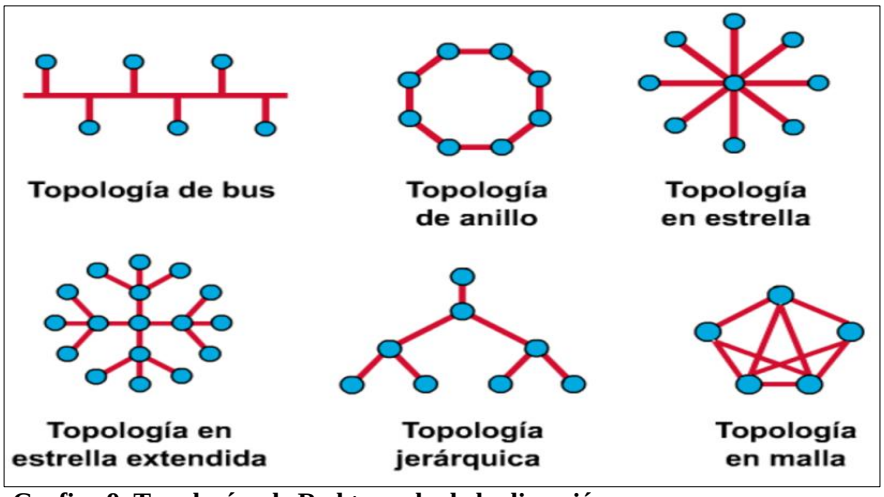


Grafico 9. Topologías de Red tomado de la dirección www.toopologiias1.blogspot.com

2.2.4. TECNOLOGÍAS DE RED

Las Redes Convergentes incrementan la productividad del mercado empresarial, y requieren para su correcta operación una Infraestructura de Red Inteligente, Confiable, Segura y de Alta Disponibilidad.

A. TECNOLOGÍAS Ethernet

Ethernet ha sobrevivido, en su batalla inicial, como una tecnología de medio físico esencial a causa de su tremenda flexibilidad y relativa simplicidad de implementación y comprensión.

Ethernet es el nombre que se le ha dado a una popular tecnología LAN de conmutación de paquetes inventada por Xerox PARC a principios de los años setenta. Xerox Corporation, Intel Corporation y Digital Equipment Corporation estandarizaron Ethernet en 1978; IEEE liberó una versión compatible del estándar utilizando el número 802.3. Ethernet se ha vuelto una tecnología LAN popular; muchas compañías, medianas o grandes, utilizan Ethernet. Dado que Ethernet es muy popular existen muchas variantes. Cada cable Ethernet tiene aproximadamente ½ pulgada de diámetro y mide hasta 500 m de largo. Se añade una resistencia entre el centro del cable y el blindaje en cada extremo del cable para prevenir la reflexión de señales eléctricas.

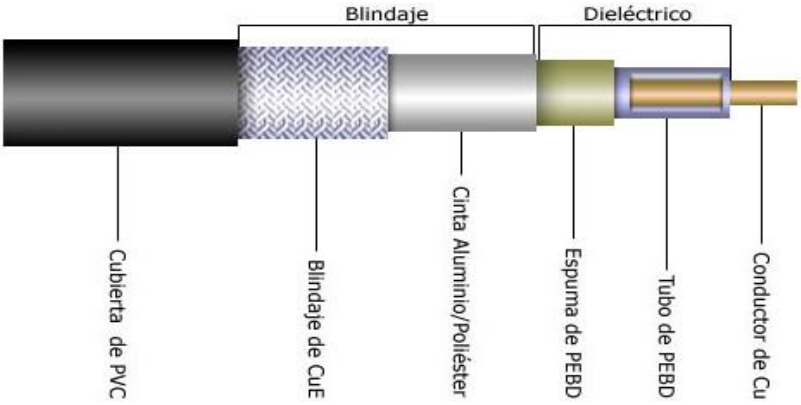


Grafico 10. Medio físico de tecnología Ethernet tomado de la dirección www.uhu.es

El término Ethernet se aplica a la familia de implementaciones LAN, las cuales incluyen:

	IMPLEMENTACIÓN	ESTANDAR IEEE	AÑO	VELOCIDAD	TIPO DE CABLE	FULL DUPLEX
ETHERNET	10base-T	802.3i	1990	10Mbps	UTP CAT 3	Si
	10base-5	802.3	1983	10 Mbits/s	RG8 o RG11	No
	10base-2	802.3a	1985	10Mbps	RG-58	No
FAST ETHERNET	100base-TX	802.3u	1995	100Mbps	UTP CAT5	Si
	100base-FX	802.3.	1995	100 Mbit/s	fibra óptica multi-modo	si (2km)
	100base-T4	802.3u	1995	100Mbps	UTP CAT5	No
GIGABIT ETHERNET	1000base-T	802.3ab	1999	1000Mbps	UTP cat-5e	Si
	1000base-X	802.3z y 802.3ab	1998	1000 Mbit/s	Fibra Optica	Si
	1000base-SX	802.3z	1998	1000 Mbps	Fibra Optica Multi Modo	Si
	1000base-LX	802.3ab y 802.3z	1998	1000 mbps	fibra mono modo(SMF)	SI
10 GIGABIT ETHERNET	10Gbase-SR	802.3ae	2002	10 Gbit/s	fibra óptica multi-modo	
	10Gbase-LR	802.3ae	2002	10.3 Gbit/s	fibra óptica (mono-modo)	NO
	10Gbase-LX4	802.3ae	2002	10.3 Gbit/s	fibra óptica (multimodo y monomodo)	
	10GBase-ER	802.3	2002	10.3125 Gbit/s.	fibra optica(mono modo)	
	10GBase-LRM	802.3aq	2002	103125 Gbit/s	fibra optica multi-modo	
	10Gbase-CX4	802.3ak	2002	3.125 GHz	cable de cobre infiniband	si
	10Gbase-T	802.3ae	2002	10.000Gb`s	fibra óptica multi-modo	Si

Grafico 11. Tecnología Ethernet tomado de la dirección www.acacha.org

B. 100-Mbps Ethernet (IEEE 802.3u)

Esta tecnología de LAN de alta velocidad ofrece una actualización importante en ancho de banda disponible. 100BaseT es la especificación de implementación 100 Mbps Ethernet sobre UTP y STP.

La subcapa MAC es compatible con IEEE 802.3, se mantiene el formato, tamaño y mecanismos de detección de errores, a la vez que soporta todas las aplicaciones y software de red de las redes 802.3.

C. 100BaseT

Soporta ambas velocidades 10 y 100 Mbps, pero el diámetro máximo de la red queda reducido aproximadamente 10 veces respecto a 10BaseT (de 2000 a 205 metros), debido a la necesidad de detectar las colisiones dentro del tiempo necesario para transmitir un frame de longitud mínima de 64 bytes, aunque las estaciones se encuentren en los extremos de la red.

D. **1 Gigabit Ethernet**

GE es una extensión del estándar IEEE 802.3, la cual ofrece 1 Gbit/s de ancho de banda, manteniendo la compatibilidad con los dispositivos de red Ethernet y Fast Ethernet.

1GE provee un nuevo modo operativo full-dúplex para conexiones switch-to-switch y switch-to-station. Sin embargo, utiliza el mismo formato y tamaño de trama, y objetos de gestión de las redes IEEE 802.3.

Esta red ha sido diseñada para operar sobre fibra óptica, pero podrá ser implementada sobre UTP 5 y cable coaxil. El Grupo de Trabajo IEEE 802.3 formó a la Fuerza de Tareas 802.3z Gigabit Ethernet para desarrollar los estándares. El objetivo fue permitir operaciones full y half dúplex a 1 Gbps., de conformidad con el formato de frame tradicional y el método CSMA/CD de acceso al medio. También se prevé compatibilidad retroactiva con 10BaseT y 100BaseT.

Además el estándar especifica el soporte de enlaces de fibra multimodo con una longitud máxima de 500 metros, enlaces de fibra monomodo de hasta 2 Km, y enlaces de cobre de 25 metros como mínimo.

E. Gigabit Ethernet

La especificación de Ethernet a 10 Gigabit (10GE) es significativamente diferente en varios aspectos, a los primeros estándares Ethernet, principalmente en que solamente provee soporte para fibra óptica y opera en modo full-duplex. Lo cual significa que los protocolos de detección de colisiones no son necesarios.

Pero a pesar de escalar a 10 Gigabits por segundo, Ethernet conserva el formato de la trama y las capacidades actuales, de forma tal que no torna obsoletas a las inversiones en infraestructura de redes. 10GE es interoperable con otras tecnologías de networking, tales como SDH, haciéndose posible el tránsito de tramas Ethernet sobre trayectos SDH con muy alta eficiencia.

La expansión de Ethernet para su uso en redes de área metropolitana impulsa aún más el avance que la tecnología había experimentado con las redes a 1 Gbps., haciendo posible las conexiones Ethernet de extremo a extremo. Ethernet a 1 Gigabit ya ha sido desarrollada como tecnología de backbone para las redes metropolitanas con fibra oscura. Con las interfaces 10GE, transceptores ópticos y fibra monomodo, los proveedores de servicios podrán construir enlaces con un alcance mayor a los 40 Km.

2.2.5. EQUIPOS DE COMUNICACIÓN DE REDES

Los dispositivos de red más utilizados son:

Repeaters (Repetidores).- Un repetidor es un dispositivo de capa física utilizado para interconectar los segmentos de una red extendida. El repetidor esencialmente se comporta posibilitando que varios segmentos de cable sean tratados como uno solo. Reciben señales de un segmento de red, las amplifican, re temporizan y las retransmiten hacia los demás segmentos. Estas acciones previenen el deterioro de las señales causadas por la longitud del cable y la cantidad de los dispositivos conectados.

Grafico 12. Repetidor tomado de la dirección www.ciudadwireless.com

Hubs.- Un Hub es un dispositivo de capa física que conecta múltiples estaciones de usuario a través de un cable dedicado. Las conexiones eléctricas se establecen en el interior del Hub. Los Hubs crean una red física estrella, al mismo tiempo que mantienen la configuración lógica en bus o ring de la LAN. Podría decirse que el Hub funciona como un repeater multipuerto.

Grafico 13. Hub tomado de la dirección www.ictlisfun.blogspot.com

Bridges y Switches.- Los bridges y switches son dispositivos que funcionan principalmente en la capa 2 del Modelo de Referencia OSI. (Dispositivos de capa de enlace de datos). Varios tipos de operaciones de bridging han tenido lugar en los escenarios de internetworking. Los bridges transparentes han sido principalmente aplicados en los entornos Ethernet, mientras que los bridges source-route se utilizaron en las redes Token Ring. Los bridges de capa MAC, están diseñados para operan entre redes homogéneas, mientras que otros pueden traducir diferentes protocolos de capa de enlace (por ejemplo IEEE 802.3 e IEEE 802.5).

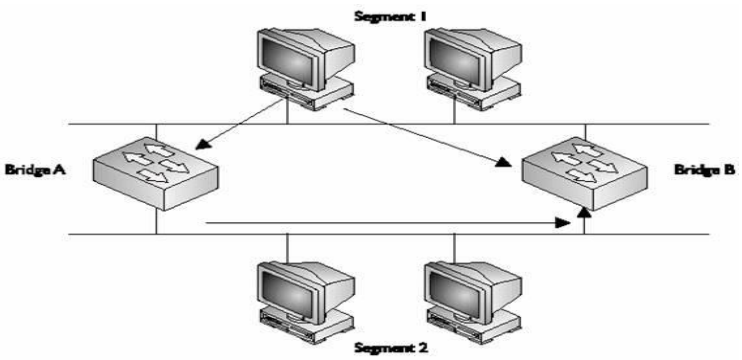


Grafico 14. Funcionamiento de un Bridge

Actualmente la tecnología de conmutación (switching) ha emergido como sucesor evolucionario en las soluciones de red. Superior performance, throughput, mayor densidad de puertos, menor costo por port y mayor flexibilidad son las características que contribuyeron al éxito de los switches para reemplazar a los bridges y complementar a los routers.

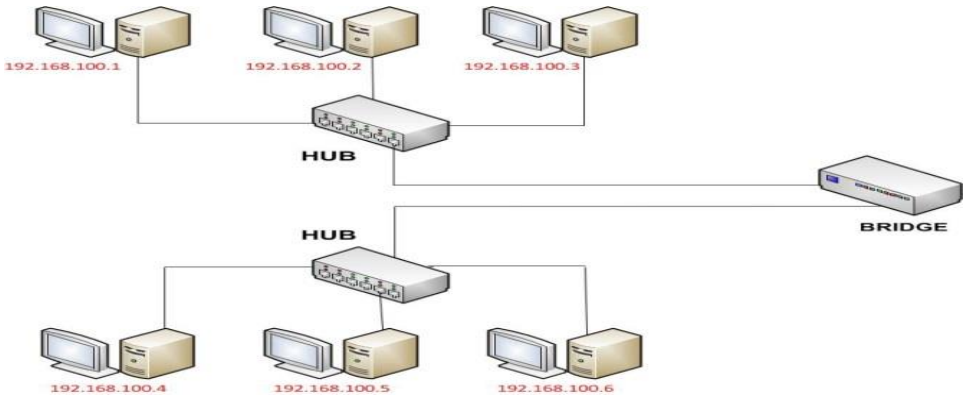


Grafico 15. Distribución de un Bridge

Los switches son significativamente más rápidos que los bridges porque la conmutación se implementa en hardware (existen switches store&**forward**, cut-through y fragment-free). Pueden interconectar redes Ethernet a 10, 100 y 1000 Mbps.

Routers.- Una de las formas más usuales de interconectar LAN´s y subredes en la actualidad es a través del uso de routers. Los routers se instalan en los puntos límites entre dos subredes físicas y/o lógicas. El routing es un método más sofisticado que el bridging para implementar el internetworking. En teoría, un router (o un conmutador de capa de red) puede oficiar de traductor entre una subred con un protocolo de capa física P1, un protocolo de capa de enlace de datos DL1, y un protocolo de capa de red N1, y otra subred con protocolo de capa física P2, un protocolo de capa de enlace de datos DL2, y un protocolo de capa de red N2. En general, un router se utiliza para interconectar redes que utilizan la misma capa de red, pero diferentes protocolos de capa de enlace.

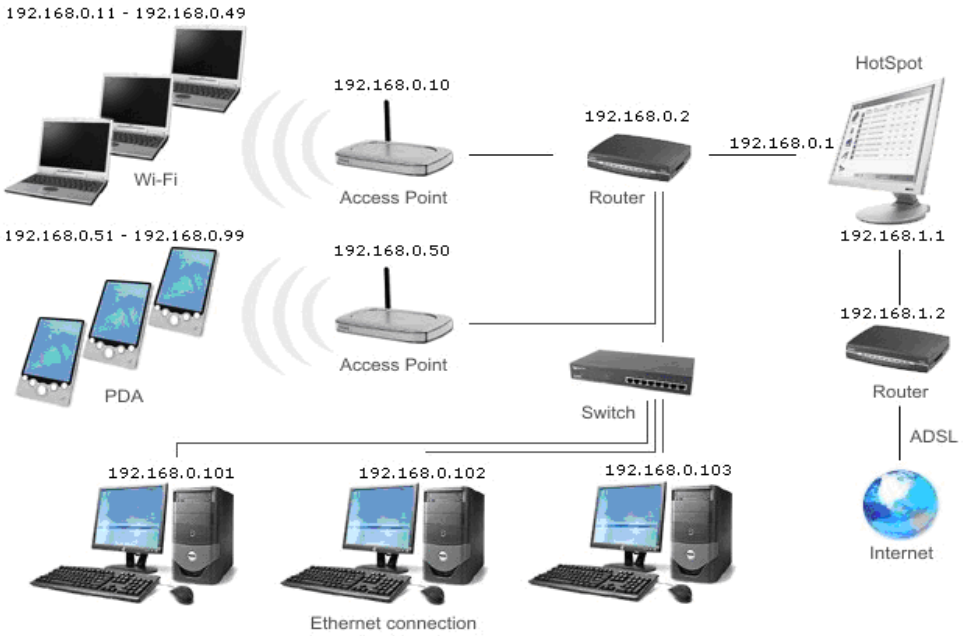


Grafico 16. Funcionamiento de un Router extraído de www.uhu.es

Los routers permiten interconectar LAN´s a través de WAN´s, utilizando los servicios tradicionales (Líneas punto a punto, Frame Relay y ATM), y los nuevos servicios de redes IP/MPLS.

Algunos routers operan directamente sobre SDH, y también pueden interconectar LAN´s diferentes, tales como Token Ring, y Ethernet.

La utilización de los routers permite el establecimiento de redes diferentes, tanto física como lógicamente, cada una con su propio espacio de direcciones. Los métodos de enrutamiento se vuelven crecientemente sofisticados, a medida que las topologías crecen en tamaño y complejidad. Los protocolos capa de red más comunes son IP, IPX, y AppleTalk, aunque la tendencia general está a favor de IP.

2.2. SEGURIDAD EN REDES.

La seguridad informática es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios. Técnicamente es imposible lograr un sistema informático ciento por ciento seguro, pero buenas medidas de seguridad evitan daños y

problemas que pueden ocasionar intrusos. Existen dos tipos de seguridad con respecto a la naturaleza de la amenaza:

- **Seguridad lógica:** aplicaciones para seguridad, herramientas informáticas, etc.
- **Seguridad física:** mantenimiento eléctrico, anti-incendio, humedad, etc.

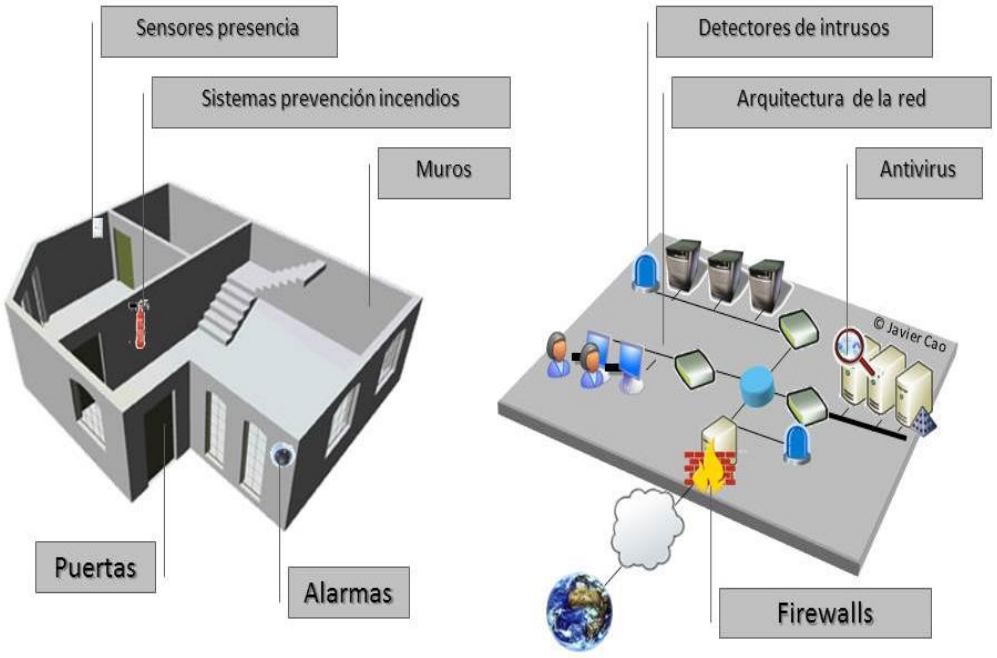


Grafico 17. Seguridad Lógica y Física de la red

2.2.1. FIREWALL O CORTAFUEGO.

Un cortafuego o firewall, es un elemento de software o hardware utilizado en una red para prevenir algunos tipos de comunicaciones prohibidos según las políticas de red que se hayan definido en función de las necesidades de la organización responsable de la red.

La idea principal de un firewall es crear un punto de control de la entrada y salida de tráfico de una red. Un firewall correctamente configurado es un sistema adecuado para tener una protección a una instalación informática, pero en ningún caso debe considerarse como suficiente. La Seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

Ventajas de un firewall

- **Protege de intrusiones:** El acceso a los servidores en la red sólo se hace desde máquinas autorizadas.
- **Protección de información privada:** Permite definir niveles de acceso a la información de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios.

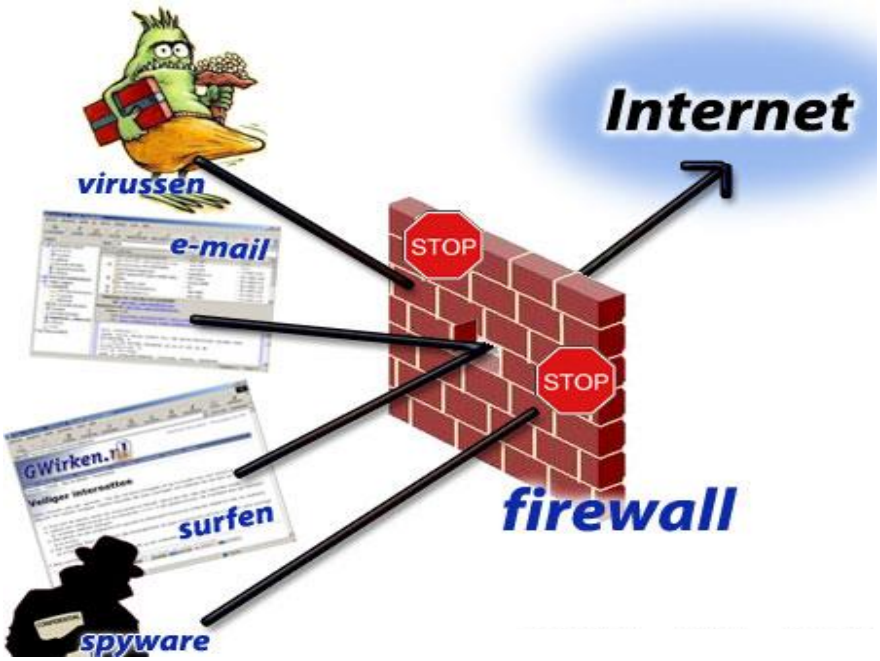


Grafico 18. Firewall o Cortafuegos extraído de www.blogs.com

2.3. POSTURAS TEORICAS

a. Uso de las redes informáticas en el trabajo en equipo

A medida en que las empresas e instituciones ampliaban su número de computadoras fue necesario unirlas entre si surgiendo el concepto de redes de cómputo y de trabajo el red (networking) para poder, de esta forma compartir archivos y periféricos entre las diferentes computadoras, pero cada una confiaba la implementación de sus redes a empresas diferentes cada una de ellas con modelos de red propietarios (modelos de hardware y software propios con elementos protegidos y cerrados) que usaban protocolos y arquitecturas diferentes.

Si esta situación era difícil peor fue cuando se quiso unir entre si a estas diferentes redes, desde entonces las empresas se dieron cuenta que necesitaban salir de los sistemas de networking propietarios optando por una arquitectura de red con un modelo común que hiciera posible interconectar varias redes sin problemas.

b. Redes y Telecomunicaciones

Una red: "es el conjunto de equipos informáticos conectados entre si por medio de dispositivos físicos que técnica utilizada para transmitir un mensaje desde un punto a otro, normalmente con el atributo típico de ser bidireccional HUIBODRO MOYA 2007".

c. Redes de comunicaciones de datos

La comunicación de datos es el movimiento de información de computadora de un punto a otro por medio de sistemas de transmisión eléctricos u ópticos tale sistemas también se denominan redes de comunicación de datos, esto contrasta con el termino más amplio de telecomunicaciones que incluye la transmisión de voz y video (imágenes y gráficos) así como datos generalmente implica mayores distancias (FITZGERALD 2009).

d. Ventajas del trabajo en red (Millán Tejedor y otros 2005) disminución del costo de hardware

Esto es posible debido que se comparten recursos de hardware, en consecuencia no es necesario por ejemplo instalar una impresora en cada computadora sino que alcanza con conectarla a una sola de las maquinas que conforman la red.

e. Disminución del costo de software

Esto se debe gracias a que es más económico adquirir un conjunto de licencias para cada máquina de la red que comprar el programa para cada Pc en particular.

f. Intercambio de información

Con la implementación de una red se evita el intercambio de información ente computadoras mediante cd, usb, u otros soportes de almacenamiento

que pueden dañarse o perderse. De esta manera el intercambio se produce en forma rápida y segura.

g. Backups o copias de seguridad

Se puede realizar una sola copia de seguridad de todo el contenido de la red, con el cual se logra una mayor velocidad en su armado y se evitan los backups fragmentados de cada máquina.

h. Administración y comunicación de los empleados

Con una red podemos administrar controlar y auditar a todos los empleados que trabajan con una computadora además todos los empleados interconectados pueden comunicarse ente si gracias al chat, correo electrónico y videoconferencias.

i. Seguridad

Mediante una red es posible verificar y controlar los accesos no autorizados instrucciones e internacionalidad de destruir información. Es posible centralizar la seguridad mediante el empleo de usuarios y contraseñas.

2.4. COMPONENTES DE UNA RED INALÁMBRICA

Una red Wi-Fi está compuesta de uno o más puntos de acceso, que son el "punto" donde los usuarios de computadora portátil o de bolsillo se conectan a la red inalámbrica. El término "Wi-Fi" proviene de una asociación internacional sin fines de lucro formada en 1999, para certificar la interoperabilidad de productos para LAN inalámbrica basados en la especificación internacional 802.11. La certificación Wi-Fi es garantía que los productos de varios fabricantes de sistemas de redes inalámbricas trabajarán en conjunto.

La figura de la siguiente página, es un ejemplo de una instalación de una red Wi-Fi. La integran un Módem que es utilizado para accesar a Internet, un Access Point (Punto de Acceso), cuatro terminales portátiles

con sus respectivas tarjetas PCMCIA, cinco terminales de escritorio con tarjetas PCI, una agenda electrónica (PDA) y un impresor con acceso compartido.

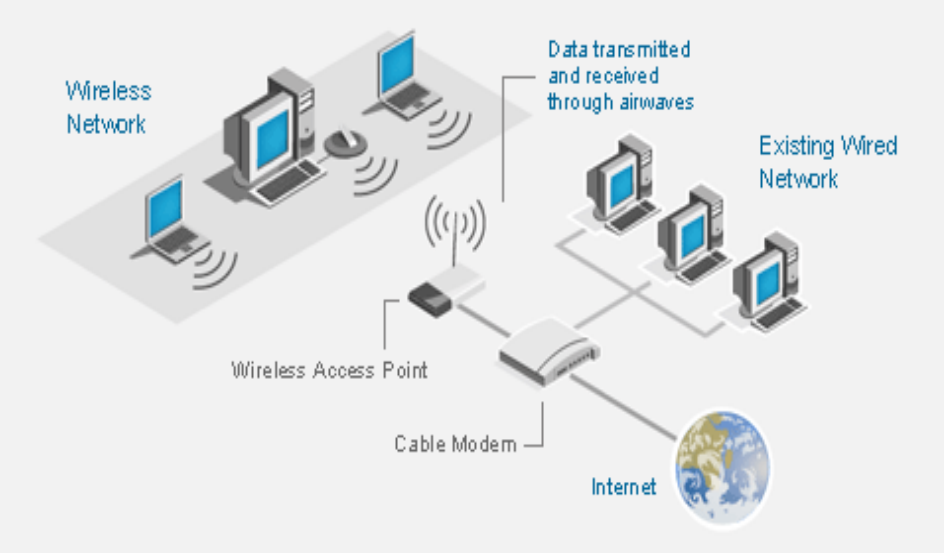


Grafico 19. Componentes de Red Inalámbrica extraído de www.redescap1.blogspot.com

Entre los componentes más utilizados para la integración de una red inalámbricos, están:

a. **Punto de acceso:**

Un punto de acceso es esencialmente un transmisor de radio compacto con antena que se conecta a un enlace por cable como por ejemplo una red Ethernet o una línea de servicio DSL o por cable provista por un Proveedor de Servicio de Internet (ISP). Existen algunos Access Point que soportan hasta 250 usuarios inalámbricos a velocidades de hasta 54 Mbps a distancias de hasta 100 metros (328 pies). Con varios puntos de acceso se puede proveer una cobertura más amplia en alguna ubicación en particular. Los puntos de acceso se pueden instalar en casi cualquier sitio porque la corriente y los

datos viajan a través de un mismo cable y sus diferentes opciones de antena ofrecen varias configuraciones de cobertura.

b. **Switch de red**:

Un switch de red provee flexibilidad de instalación al distribuir la corriente y los datos a través del mismo cable de red, por medio de su capacidad integrada de Potencia sobre Ethernet (PoE). El switch soporta entre 8 y 24 puntos de acceso inalámbricos. El switch además separa el tráfico de usuarios en la red inalámbrica; por ejemplo, separa el tráfico de usuarios públicos del tráfico de operaciones de negocios, para permitir así que las comunicaciones comerciales permanezcan privadas y seguras. El switch además establece prioridades de tráfico en el uso, brindando así un acceso ininterrumpido al Internet.

c. **Enrutador seguro**:

El enrutador seguro detecta y protege a la red inalámbrica y a sus usuarios de los ataques de *hackers* en el Internet. El enrutador seguro soporta dos canales de comunicaciones privados, o túneles de red privada virtual (VPN), para ofrecer intercambios seguros de datos y correo electrónico de localidad a localidad, o de un usuario remoto a alguna localidad.

d. **Puente para LAN inalámbrica (Bridge) Opcional**:

Un puente para grupo de trabajo de LAN inalámbrica expande el potencial de ingresos de un hotspot Wi-Fi al permitir que los usuarios de computadoras portátiles o de bolsillo sin capacidades inalámbricas

integradas se conecten a la red a través de este tipo de tecnología. Los negocios con usuarios de ocio pueden rentar un puente a/b/g Wireless LAN Workgroup Bridge y un cable LAN a sus clientes o huéspedes que deseen la conveniencia adicional del acceso a Internet durante sus estadías.

e. **Gateway de autentificación y facturación inalámbrica:**

Este gateway le permite a los negocios de hotelería y ocio controlar el acceso a la red con un hotspot Wi-Fi, llevando a cabo verificaciones de autentificación similares a las de las tarjetas de crédito o autentificación de identificación de miembros. El gateway también mantiene récord del uso inalámbrico para fines de facturación y provee servicios de transacción de pagos. Asimismo, el gateway interopera con sistemas de reservaciones de hoteles, aeropuertos y otros centros de ocio para verificar el uso apropiado de los clientes o huéspedes.

f. **Tarjetas Inalámbricas PCI**:

Dispositivo electrónico para computadoras personales, ensambladas en la ranura PCI (Peripheral Component Interface), cuya función es establecer transmisión de datos a través de medios inalámbricos.

g. **Tarjetas Inalámbricas PCMCIA**

(Asociación Internacional de Tarjetas de Memoria para Ordenadores Personales):

Es un dispositivo electrónico en forma de tarjeta de crédito que se emplea en nuestra computadora. Una de sus principales funciones es la transmisión de datos, faxes, etc. utilizando teléfonos portátiles y

laptops, mediante el estándar 802.11x conexiones desde 11Mbps hasta 54Mbps.

h. **Tarjetas Inalámbricas USB**:
   Son adaptadores de red inalámbricos que se conectan en el puerto USB para establecer la conexión a la red Wireless.

i. **Antenas Unidireccionales:**
   Transferencia o transmisión de datos en un canal en una sola dirección.

j. **Antenas Omnidireccionales:**
   Son lo contrario a las anteriores. Se utilizan para la transmisión de señales en un canal en múltiples direcciones. Generalmente, son las que integran los Access Point, y tarjetas inalámbricas.

2.5. PUBLICACIONES

En la revista PC WORLD, pagina 6 editado por Jas Acevedo se publica lo siguiente: "***Cómo evitar que los vecinos roben nuestro Wi-Fi***" para la cual dice que: Cada técnica que he visto para el craqueo de redes Wi-Fi se debe ya sea un diccionario o un ataque de fuerza bruta. Hay una herramienta muy simple para protegerse contra estos ataques: una contraseña segura. Utilice una cadena larga, aleatoria de números, letras mayúsculas y minúsculas, y puntuacion, y evite todo lo que se encuentra en el diccionario.
Pon a prueba la fortaleza de la contraseña con ¿Qué tan segura es mi contraseña, que estima cuánto tiempo se necesitaría un PC estándar para descifrar la contraseña. Si se tardaría más de un millón de años en hacerlo, considere la contraseña segura.

La queja habitual contra fuertes contraseñas es que son muy difíciles de recordar no aplica. Sólo tienes que escribir esta contraseña cuando instale un nuevo dispositivo con Wi-Fi capaz, o al ayudar a un huésped que trajo su propio dispositivo para su hogar. Usted puede simplemente mantener la contraseña en un trozo de papel o en tu gestor de contraseñas .

Por supuesto, si usted está preocupado de que un vecino ya ha entrado a su red Wi-Fi, el cambio de la contraseña lo sacará inmediatamente.

Además de la contraseña, asegúrese de que su seguridad Wi-Fi está configurado correctamente. Ve a la pantalla de ajuste de su router y comprobar las opciones. Idealmente, usted debe utilizar el cifrado WPA2. Si su módem no es compatible con WPA2, utilice WPA-Personal - o mejor aún, comprar un nuevo router. Para más información sobre estas cuestiones, véase 5 mitos de seguridad Wi-Fi debe abandonar ahora.

PRESENTACION DE RESULTADOS

CAPITULO III

ANALISIS DE REQUERIMIENTO

3.1. REQUERIMIENTOS TECNICOS

El servicio de acceso inalámbrico de la universidad (Red Wi-Fi UPLA) se basa en tecnología compatible con 802.11g, 802.11b, operando a velocidades de 1 a 54 Mbps . Soporta encriptación WEP de 64, 128 y 256 bits.

Las diferentes computadoras (Notebooks o PDAs) que deseen acceder a este servicio deberán contar con dicha tecnología integrada o adicional (tarjeta de red inalámbrica). Por el momento no se está ofreciendo el servicio a computadoras que cuenten con tecnología Bluetooth.

Presentamos a continuación una lista de algunos modelos compatibles con dicha tecnología:

Cuadro 2
iPod

Marca	**Modelo**
Apple	iPod touch

Nota: información obtenida técnicamente propia.

Cuadro 3
Laptop o Notebook

Marca	Modelo
Acer	FERRARI
Acer	TRAVELMATE
Alienware	Aurora
Apple	iBOOK
Apple	POWERBOOK
AVERATEC	3200 SERIES
Compaq	PRESARIO
Dell	INSPIRON
Dell	LATITUDE
HP	PAVILION
IBM/Lenovo	THINKPAD G, R, T, X SERIES
PACKARD BELL	EasyNote
Sony	VAIO
Toshiba	PORTEGE
Toshiba	QOSMIO
Toshiba	SATELLITE
Toshiba	TECRA

Nota: información obtenida técnicamente propia.

Cuadro 4
PDA o Pocket PCs

Marca	Modelo
ASUS	Asus MyPal a620 Pocket PC
ASUS	Asus MyPal a716 Pocket PC
ASUS	Asus MyPal a730W Pocket PC
Dell	Axim X50 520MH
Dell	Axim X50v
Dell	Axim X51 520MH
Dell	Axim X51v
HP	HX4705
HP	iPAQ h4155 Pocket PC
HP	iPAQ h4355 Pocket PC
HP	IPAQ H4550
HP	iPAQ h6315 Pocket PC - Phone Edition
HP	iPAQ h6320 Pocket PC - Phone Edition
HP	iPAQ h6325 Pocket PC - Phone Edition
HP	iPAQ hx2415 Pocket PC
HP	iPAQ hx2755 Pocket PC

HP	iPAQ hx4705 Pocket PC
HP	iPAQ rx3115 Mobile Media Companion
HP	iPAQ rx3715 Mobile Media Companion
PALM	LifeDrive
PALM	TUNGSTEN C
PALM	Tungsten T5 (*)
PALM	Zire 31 (*)
Sony	Clié PEG-TH55
Sony	Clié PEG-TJ37
Toshiba	e800 400MHz Pocket PC
Toshiba	e805 128MB Pocket PC

Nota: información obtenida técnicamente propia.

Cuadro 5
Smartphone

Marca	**Modelo**
Apple	iPhone
BlackBerry	BlackBerry 8100
BlackBerry	BlackBerry 8800
Nokia	E65
Nokia	N90
Sony Ericson	Xperia

Nota: información obtenida técnicamente propia.

(*) Requiere tarjeta de expansión modelo: PalmOne Wi-Fi Card

En el caso que su notebook no cuente con la tarjeta integrada puede adquirir una tarjeta de red inalámbrica:

Cuadro 6
Especificaciones técnicas de tarjeta de red

Marca	**Modelo**
D-Link	DWL-650 Air Wireless 2.4GHz CardBus Adapter
D-Link	DWL-650+ AirPlus Enhanced 2.4GHz Wireless CardBus Adapter
D-Link	DWL-650H Air Wireless 2.4GHz CardBus Adapter
NetGear	MA521 802.11b Wireless PC Card
NetGear	WG511 54 Mbps Wireless PC Card 32-bit CardBus
Trendnet	TEW-226PC 11Mbps Wireless LAN CardBus PC Card
Trendnet	TEW-401PC 54Mbps 802.11g Wireless PC Card
Trendnet	TEW-421PC 54Mbps 802.11g Wireless PC Card

Nota: información obtenida técnicamente propia.

3.2. ESTADO DE LA RED EXISTENTE

La Universidad Peruana los Andes desarrolla sus actividades académicas y administrativas, que está ubicado en la Av. San Carlos – Huancayo donde se encuentran concentradas oficinas administrativas y la mayoría de los laboratorios, y las facultades como Derecho, Ingeniería, Ciencias Administrativas y Contable, Medicina Humana, Enfermería, Obstetricia y demás facultades en la Ciudad Universitaria de Chorrillos, la mayoría de la infraestructura de redes ha sido instalada en las diferentes facultades que existe.

Los ambientes que está ubicado en la Av. San Carlos – Huancayo son de material noble, cada facultad son de varios pisos y rodeado de varios ambientes que han sido acondicionados como aulas y laboratorios, en el cual también sus ambientes son utilizados para oficinas, laboratorios y la biblioteca principal, todos estos ambientes se han acondicionado según las necesidades que surgían por el crecimiento de la universidad año tras año.

La implementación y crecimiento de la red no ha sido planificado, actualmente cuenta con muchos dispositivos Ethernet y FastEthernet, e incluso con algunos dispositivos GigaEthernet, el cableado está hecho con UTP CAT 5e y algunos 6e, el cableado está estructurado, cuentan con dos switchs principales que han sobrevivido al paso del tiempo, ambos switchs están conectados al router que brinda el servicio de Internet y otro router que brinda el servicio de VPN, a estos switchs se conectan otros que alimentan a las oficinas administrativas y laboratorios de cómputo de las diferentes facultades en el primer y segundo nivel de los ambientes que se encuentran en el primer piso hay switchs que están defectuosos con puertos quemados o que no funcionan apropiadamente.

El uso principal que se le da a la red es para conectarse al sistema académico de la universidad, sistemas de control administrativo de la universidad y al Internet, y en algunos casos se utiliza para compartir impresoras de una misma oficina, asimismo durante su crecimiento se han instalado equipos para brindar acceso inalámbrico a equipos de usuarios administrativos, y que también es utilizado por docentes y alumnos.

3.2.1. CONECTIVIDAD EXTERNA

- Una línea ADSL Speedy Negocios de 3Mb al 25%, para el acceso a Internet, y los usuarios pueden conectarse sin mayor control tanto desde las computadoras de la universidad como desde sus equipos personales.
- Una línea VPN que brinda conexión punto a punto a una velocidad de 900 Kbps para garantizar la conectividad.

3.3. PROBLEMAS CON LA RED EXISTENTE Y EL SISTEMA

La red de la universidad presenta algunos problemas, que diariamente se han venido observando diferentes inconvenientes que afectan el normal funcionamiento de las actividades y la consiguiente imagen de deficiente servicio.

A continuación describimos algunos de los principales problemas encontrados:

- Todos los días, en una frecuencia de hasta 2 a 4 veces por hora, se pierde conexión con el servicio del Internet, o en el mejor de los casos el servicio es inutilizable ya que se encuentra saturado, siendo necesario reiniciar el router para poder volver a recuperar el servicio.
- Al realizarse el análisis respectivo de la falla se puede identificar que los servicios ICMP se encuentra activo mientras que todos los demás presentan saturación.
- Muy a menudo se presenta conflicto de direcciones IP, la red de la universidad está configurado con direccionamiento IPv4 en todos sus equipos, por lo que éste problema genera desconexión de las computadoras siendo necesario modificar sus direcciones manualmente para que retome el acceso a Internet.
- Los docentes y alumnos conectan sus equipos personales, como laptops, a la red de la universidad y configuran manualmente sus propias direcciones, generando conflicto de direcciones IP y al incrementar el número de equipos generan colisiones de broadcast del dominio.
- Se tenía habilitado dos Access point para la conexión inalámbrica a través de éste medio, éstos equipos han sido utilizados por los docentes y alumnos para obtener acceso a la red de la universidad y conectarse a Internet incrementando el número de equipos dentro de la red.

- Los usuarios que logran conectarse al Internet no tienen ningún control, y cuando implementaban algún control los usuarios utilizaban otros métodos para saltar estos mecanismos y seguían utilizando el Internet sin restricción alguna.
- Los usuarios de las oficinas administrativas utiliza el Internet para acceder al sistema académico de la Universidad, pero también lo utilizan, y en mayor medida, para ingresar a páginas de ocio (Video, Audio, Chat's, imágenes, radios, juegos, etc, etc, etc.) que no son útiles para el trabajo diario que realizan, incluso utilizan programas que les permiten realizar descargas de programas, vídeos y música que saturan completamente el servicio del Internet.
- El cableado del backbone de la red de la universidad es bastante antiguo y no cuenta con ningún mecanismo de protección, los cables están a la intemperie y a vista y alcance de cualquier usuario, se presentan muchos problemas debido a que los cables son desconectados muy a menudo por los propios usuarios en actos involuntarios.
- Los dispositivos de conectividad, como los switchs, en su mayoría no son apropiados para soportar la carga en la transmisión de datos de la red, en un gran número de ellos están defectuosos por estar colocados en lugares inapropiados para estos equipos.

3.4. REQUERIMIENTOS DE USUARIOS, APLICACIONES, DISPOSITIVOS Y DE LA RED

Durante los meses de Noviembre y Diciembre del 2013 se realizó el levantamiento de información a través de entrevistas y conversaciones informales con los usuarios sobre el estado actual de la red, así como el análisis a los reportes de averías de los usuarios que no se registran formalmente pero que dan una visión clara sobre los requerimientos.

La prioridad asignada a los requerimientos se basa en la siguiente tabla:

Cuadro 7
Prioridades de especificaciones de requisitos

Prioridad	Descripción
1	Misión Crítica
2	Muy Importante
3	Importante

4	Normal
5	No Importante

Nota. Información obtenida por fuente propia

.

3.4.1. REQUERIMIENTOS DE USUARIOS

La universidad cuenta con diferentes facultades – administrativas, los requerimientos de los usuarios que a continuación detallamos han sido obtenidos a través de conversaciones con cada uno de ellos durante la atención de sus averías, asimismo realicé el levantamiento de información correspondiente, por lo que considero que son los requerimientos más importantes.

Cuadro 8
Especificaciones de requerimientos de usuarios

ESPECIFICACIONES DE REQUERIMIENTOS DE USUARIOS			
ID	**Fecha**	**Descripción**	**Obtenido/ Derivado**
1	28-29 Nov 2013	57 usuarios de oficinas administrativas (13 del 1er piso de la universidad, 25 del 2do piso de la casa, 19 usuarios del 1er piso en los exteriores de la universidad).	Obtenido de personal de Laboratorio
2	28-29 Nov 2013	Los usuarios de algunas oficinas administrativas requieren puntos de red adicionales para otros equipos que no están de forma permanente.	Obtenido de los Usuarios
3	30 Nov 2013	114 usuarios de los laboratorios de cómputo (52 usuarios del 1er piso de la universidad, 62 usuarios en el 1er piso de los exteriores de la universidad).	Obtenido de personal de Laboratorio
4	20 Dic 2013	Conexión inalámbrica para el acceso a Internet de docentes y alumnos	Obtenido de docentes y alumnos
5	22 Dic 2013	Acceso rápido a las aplicaciones web de la universidad	Obtenido de los Usuarios

Nota. Información obtenida mediante encuesta

3.4.2. REQUERIMIENTOS DE APLICACIONES

Las aplicaciones están desarrolladas para cumplir con los objetivos de la universidad por lo que tienen requerimientos muy importantes para su normal funcionamiento.

A. PRINCIPALES APLICACIONES

La lista de las principales aplicaciones facilita su identificación y asignación de importancia, para ello se ha tenido en cuenta 2 factores: su importancia y el número de usuarios que hacen uso del mismo. Todas las aplicaciones están íntegramente relacionadas con el cumplimiento de los objetivos de la organización:

Cuadro 9
Identificación de Principales Aplicaciones

Aplicación	Descripción	Importancia	N° Usuarios
Ap1	Academic Web: Sistema Académico de la Universidad	Crítico	125
Ap2	Sistema de Control de Asistencia de personal administrativo	Crítico	1
Ap3	Plataforma virtual de Educación a Distancia	Muy Importante	97
Ap4	Páginas webs de la universidad	Importante	169
Ap5	Correos Electrónicos	Importante	169
Ap6	Servidor de archivos de la universidad	Importante	169
Ap7	Bibliotecas virtuales en Internet	Importante	116

Nota. Información obtenida mediante fuente de la universidad

.

B. RENDIMIENTO DE APLICACIONES

El rendimiento que requieren las aplicaciones están basadas en

capacidad, retardo y fiabilidad, para ello se pueden utilizar un conjunto de métricas. En este caso teniendo en cuenta que las aplicaciones críticas están basadas en el flujo basado en el modelo Cliente-Servidor y teniendo a disposición una línea ADSL, el rendimiento se calculará en función a las características que la línea ADSL nos otorga, esto es medir la velocidad upstream y downstream; la Ap6 obtiene un rendimiento mayor debido a que es transmisión dentro de la propia red local.

Cuadro 10
Requerimiento de Rendimiento de Aplicaciones

REQUERIMIENTOS DE RENDIMIENTO DE APLICACIONES			
Aplicación	**Donde se realiza la medición**	**Método Medición**	**Capacidad Upstream Downstream**
Ap1	Entre estación de trabajo de asuntos académicos y el Switch de la LAN	Ping Wireshack	25 Kbps 70 Kbps
Ap2	Por estimaciones de la aplicación	Ping Wireshack	70 Kbps 180 Kbps
Ap3	Entre estación de trabajo de educación a distancia y el Switch de la LAN	Ping Wireshack	30 Kbps 250 Kbps
Ap4	Entre cualquier estación de trabajo y el Switch de la LAN	Ping Wireshack	15 Kbps 70 Kbps
Ap5	Entre cualquier estación de trabajo y el Switch de la LAN	Ping Wireshack	60 Kbps 200 Kbps
Ap6	Entre estación de trabajo del laboratorio y el Switch de la LAN	Ping Wireshack	5 Mbps Up/Down
Ap7	Entre estación de trabajo del laboratorio y el Switch de la LAN	Ping Wireshack	15 Kbps 70 Kbps

Nota. Información obtenida mediante el laboratorio de computación de la universidad

C. REQUERIMIENTOS DE DISPOSITIVOS

Debido a que el crecimiento de la red ha sido gradual a través del tiempo y según las necesidades se han acumulado una variedad de dispositivos tanto en rendimiento y fiabilidad.

Cuadro 11
Descripción de Dispositivos según computadoras

Tipo Dispositivo	Tipo NIC	Procesador	Sistema Operativo	Aplicaciones
PC gama baja	10M Ethernet	Pentium I	Windows 98	Word, Excel
PC gama alta	10/100M Ethernet	Core2Duo Core i3-i5-i7	Windows 7	Office, Database, Diseño Gráfico, CAD
PC genérica	10/100M Ethernet	Pentium IV	Windows XP	Word, Excel
Laptop	10/100M Ethernet	DualCore Core2Duo Core i3-i5-i7	Windows 7	Office, CAD, Database, Desarrollo

Nota. Información obtenida mediante el laboratorio de computación UPLA

Cuadro 12
Descripción de Dispositivos según computadoras

Tipo Dispositivo	Tipo NIC	Puertos	Estado
HUB	10M Ethernet	24 puertos	Defectuoso
Switch	10/100M FastEthernet	5 puertos	Defectuoso
Switch	10/100M FastEthernet	8 puertos	Defectuoso
Switch	10/100M FastEthernet	24 puertos	Defectuoso
Switch	10/100M FastEthernet	48 puertos	Defectuoso

Switch Administrable	10/100/1000M GigaE	24 puertos	Bueno
Router ADSL	10M Ethernet	4 puertos	Operativo con fallas

Nota. Información obtenida mediante el laboratorio de computación UPLA

Según los dispositivos de red disponibles se ha podido elaborar la siguiente tabla de especificaciones de requerimientos de dispositivos:

Cuadro 13
Especificaciones de Requerimientos de Dispositivos

ESPECIFICACIONES DE REQUERIMIENTOS DE DISPOSITIVOS			
ID	Fecha	Descripción	Obtenido/ Derivado
01	18 Nov 2013	Los dispositivos de red de los usuarios tienen diferentes tipos de tarjetas de red, tecnologías Ethernet, Fast Ethernet y GigaE	Obtenido de personal de Laboratorio
02	18 Nov 2013	Los switch se encuentra distribuidos a lo largo de todo el local y son de diferentes tecnologías	Obtenido de personal de Laboratorio

Nota. Información obtenida mediante el laboratorio de computación UPLA

D. REQUERIMIENTOS DE LA RED

Los requerimientos de la red permiten que se pueda atender los requerimientos de los usuarios de manera confiable. En la siguiente tabla detallamos las especificaciones de requerimientos de la red:

Cuadro 14
Especificaciones de Requerimientos de la Red

ESPECIFICACIONES DE REQUERIMIENTOS DE LA RED			
ID	**Fecha**	**Descripción**	**Obtenido/ Derivado**
01	25 Nov 2013	Los dispositivos de red de las áreas son compatibles con conexiones Ethernet y Fast Ethernet a la red troncal.	Obtenido de personal de Laboratorio
02	11 Nov 2013	La red de la universidad debe estar protegida de los ataques desde Internet	Obtenido de personal de Laboratorio
03	27 Nov	La facultad sólo cuenta con un acceso a Internet ADSL Speedy Negocios de 3Mb al 35%.	Obtenido de personal de Laboratorio

	2013		
04	28 Dic 2013	El cableado de la red actual será reemplazado, sin embargo se conservarán varios switchs	Obtenido de personal de Laboratorio
05	22 Dic 2013	Se deben contar con políticas para la gestión de los equipos que se conectan a la red	Obtenido de personal de Laboratorio
06	22 Dic 2013	El monitoreo de la red para garantizar su funcionamiento y optimizar su configuración	Obtenido de personal de Laboratorio

Nota. Información obtenida mediante el laboratorio de computación UPLA

3.5. ESPECIFICACIONES DE LOS REQUERIMIENTOS Y MAPA

La especificación de requerimientos es un documento que recoge y les da prioridad, siendo la base para la arquitectura y diseño de la red.

Los siguientes requisitos han sido obtenidos de levantamiento de información del personal encargado de laboratorio de cómputo, de entrevistas con los usuarios y otros han sido estimados, a continuación detallamos las especificaciones de requerimientos:

Cuadro 15
Especificaciones de Requerimientos

ESPECIFICACIONES DE REQUERIMIENTOS							
ID	**Fecha**	**Tipo**	**Descripción**	**Obtenido/ Derivado**	**Ubicación**	**Estado**	**Prioridad**
1	28-29 Nov 2013	Usuario	57 usuarios de oficinas administrativas (13 del 1er piso, 25 del 2do piso, 19 usuarios del 1er piso).	Obtenido de personal de Laboratorio	Ver Mapa	Info	1
2	28-29 Nov 2013	Usuario	Los usuarios de algunas oficinas administrativas requieren puntos de red adicionales para otros equipos que no están de forma permanente.	Obtenido de los Usuarios	Ver Mapa	Info	3
3	30 Nov 2013	Usuario	114 usuarios de los laboratorios de cómputo (52 usuarios del 1er piso, 62 usuarios en el 1er piso).	Obtenido de personal de Laboratorio	Ver Mapa	Info	2
4	20	Usuario	Conexión	Obtenido	Ver Mapa	Info	3

	Nov 2013		inalámbrica para el acceso a Internet de docentes y alumnos	de docentes y alumnos			
5	22 Nov 2013	Usuario	Acceso rápido a las aplicaciones web de la universidad	Obtenido de los Usuarios	Ver Mapa	Info	1
6	10 Nov 2013	Aplicación	Las páginas webs de la universidad y servicios virtuales son de acceso prioritario para todos los usuarios	Obtenido de personal de Laboratorio	Ver Mapa	Info	1
7	4 Nov 2013	Aplicación	El acceso a páginas web que no contribuyan a las actividades académicas no son prioritarias y deben ser bloqueadas	Derivado de Coord. de Sistemas	Ver Mapa	Info	2
8	4 Dic 2013	Aplicación	Control del acceso a Internet por usuarios y contenidos generales y específicos	Derivado de Coord. de Sistemas	Ver Mapa	Info	1
9	25 Nov 2013	Aplicación	Los servidores de la universidad deben ser accesibles sólo desde la red de la universidad	Obtenido de Personal de Laboratorio	Ver Mapa	Info	1
10	18 Dic 2013	Dispositivo	Los dispositivos de red de los usuarios tienen diferentes tipos de tarjetas de red, tecnologías Ethernet, Fast Ethernet y GigaE	Obtenido de personal de Laboratorio	Ver Mapa	Info	1
11	18 Nov 2013	Dispositivo	Los switchs se encuentra distribuidos a lo largo de todo las facultades y son de diferentes tecnologías	Obtenido de personal de Laboratorio	Ver Mapa	Info	1
12	25 Dic 2013	Red	Los dispositivos de red de las áreas son compatibles con conexiones Ethernet y Fast Ethernet a la red troncal.	Obtenido de personal de Laboratorio	Ver Mapa	Info	2
13	11 Dic 2013	Red	La red de la universidad debe estar protegida de los ataques desde	Obtenido de personal de Laboratorio	Ver Mapa	Info	1

			Internet				
14	27 Nov 2013	Red	La universidad sólo cuenta con un acceso a Internet ADSL Speedy Negocios de 3Mb al 35%.	Obtenido de personal de Laboratorio	Ver Mapa	Info	1
15	22 Nov 2013	Red	Se deben contar con políticas para la gestión de los equipos que se conectan a la red	Obtenido de personal de Laboratorio	Ver Mapa	Info	1
16	22 Nov 2013	Red	El monitoreo de la red para garantizar su funcionamiento y optimizar su configuración	Obtenido de personal de Laboratorio	Ver Mapa	Info	1

Nota. Información obtenida mediante el laboratorio de computación UPLA

El mapa de requisitos nos muestra de forma más gráfica la ubicación de los requerimientos de la universidad:

- En el 1er piso se ubican oficinas administrativas, laboratorios y la biblioteca, el área que administra que la conectividad se encuentra ubicado en éste nivel en un ambiente acondicionado para su funcionamiento.

  Aquí podemos ver como la diversidad de las ubicaciones de las áreas fomenta la complejidad de la distribución.

CAPITULO IV

DISEÑO DE LA RED

4.1. ARQUITECTURA DE LA RED

La arquitectura de la red es de alto nivel, a través del modelo respectivo se muestran las relaciones entre los principales componentes de la red y los mismos con la red para el logro de sus objetivos.

La arquitectura planteada pretende mejorar el rendimiento de la red y garantizar el uso de las aplicaciones según sus propios requerimientos, de ésta se garantiza estabilidad y confiabilidad en la red.

4.1.1. DIRECCIONAMIENTO / ENRUTAMIENTO

El direccionamiento planteado se basa en IPv4 en direcciones de la Clase C, también llamadas privadas, esto es debido a que sólo se cuenta con una salida al servicio de Internet y que debe ser realizada a través de un mecanismo llamado NAT.

Tomando en cuenta los usuarios existentes en la universidad se plantea la creación de 3 subredes donde se administrará el tráfico de la red de la universidad, además de 1 subred necesaria para utilizar el servicio de Speedy Negocios y 1 subred adicional para el servicio de transmisión de datos vía VPN. Quedando de la siguiente manera:

Cuadro 16
Direccionamiento IPv4 de la red LAN de la UPLA

ID Red	Rango Subred	Uso	Observaciones
A	192.168.1.0/24 GW: 192.168.1.1	Speedy Negocios	Servicio de Internet
B	192.168.2.0/24 GW: 192.168.2.1	VPN	Transmisión de datos al local central
C	192.168.5.0/24 GW: 192.168.5.1	Administrativos	Red LAN, usuarios administrativos del 1er y 2do nivel.
D	192.168.6.0/24 GW: 192.168.6.1	Laboratorios	Red LAN, para los laboratorios de la universidad.
E	192.168.7.0/24 GW: 192.168.7.1	Red Inalámbrica	Red LAN, para los usuarios con dispositivos móviles de la universidad.

Nota. Información obtenida mediante el área de informática de la UPLA

Según los antecedentes de la red, ésta ha ido creciendo de forma desordenada sin una planificación adecuada y por lo que se vislumbra éste crecimiento continuará de la misma manera, por lo tanto se han separado las direcciones en grupos de 10, 20 a 30 direcciones por áreas, si bien un área tiene sólo 3 ó 6 usuarios se le han separado 10 direcciones para que los nuevos equipos que incorporen utilicen una dirección del mismo grupo, esto para garantizar la gestión adecuada de las direcciones.

En la siguiente tabla se muestra las la asignación de las direcciones IPv4 según el cuadro anterior:

Cuadro 17
Asignación de direcciones IPv4 por facultades de la UPLA

ID Red	Área	N° Usuarios	Dirección IPv4	
			Inicial	Final
A	Router Internet	1	192.168.1.1	
C	Servidores Locales	3	192.168.5.2	192.168.5.9
C	Apoyo Laboratorio Cómputo Soporte	3	192.168.5.10	192.168.5.19
C	Decano	7	192.168.5.20	192.168.5.29
	Secretaria Docente	7	192.168.5.30	192.168.5.39
C	Departamento Académico	12	192.168.5.40	192.168.5.49
C	Asuntos Académicos	20	192.168.5.50	192.168.5.59
C	Coordinaciones de Proyección Social, Grados y Títulos, Prácticas Profesionales	15	192.168.5.60	192.168.5.69
C	Coordinación Administrativa y de Planificación	2	192.168.5.70	192.168.5.79
C	Coordinación Ing.	3	192.168.5.80	192.168.5.89
C	Coordinación Derecho	1	192.168.5.90	192.168.5.99
C	Coordinación Medicina Humana	1	192.168.5.100	192.168.5.109
C	Coordinación Enfermería	1	192.168.5.110	192.168.5.119
C	Coordinación Obstetricia	1	192.168.5.120	192.168.5.129
C	Coordinación Talleres Técnicos	2	192.168.5.130	192.168.5.139
C	Biblioteca	2	192.168.5.140	192.168.5.149

ID Red	Área	N° Usuarios	Dirección IPv4	
C	Capítulos Estudiantiles	2	192.168.5.160	192.168.5.169
D	Laboratorio 1	20	192.168.6.10	192.168.6.29
D	Laboratorio 2	22	192.168.6.40	192.168.6.79
D	Laboratorio 3	20	192.168.6.70	192.168.6.99
D	Laboratorio 4	26	192.168.6.100	192.168.6.129
E	Red Inalámbrica Docentes	90	192.168.7.10	192.168.7.99
E	Red Inalámbrica Alumnos	140	192.168.7.100	192.168.7.239

Nota. Información obtenida por fuente propia

Las direcciones IPv4 serán asignadas de la siguiente manera:

- La asignación de la dirección del ID A se hará de forma manual, y sólo a equipos determinados, para este caso sólo se le asignará una dirección al equipo que se encargará de gestionar toda la red, el ruteo será gestionado por el gestor de la red.
- La asignación de la dirección ID B se hará de forma manual, y sólo a los equipos que se autoricen, el ruteo en estos equipos es de forma estática en cada equipo, así mismo sólo estará dirigido a los equipos de la oficina de Asuntos Académicos.
- La asignación de las direcciones C y D serán dinámicas a través de un servidor DHCP con identificación de MAC, para el caso de las computadoras de los usuarios administrativos y de los laboratorios se hará el levantamiento de las direcciones MAC y en función a su ubicación y función se le asignará una dirección IP dentro del rango de red que le corresponda.
- Para el caso de la red inalámbrica se creará un red WiFiUPLA, la asignación de las direcciones del ID E será de forma automática en función a lo siguiente: se registrará la dirección MAC de los docentes, previamente identificados, y en función a ello se le asignará una

dirección IP del rango que le corresponda, y para el caso de los alumnos el sistema le asignará una dirección de forma automática y para que pueda tener acceso a Internet deberá ingresar un código que tendrá validez por un determinado tiempo, luego del cual se cortará la conexión.

4.1.2. GESTIÓN DE LA RED

La arquitectura de la red está pensada en un modelo híbrido entre Cliente-Servidor y el modelo de arquitectura de computación distribuida, en la mayoría de la red estará funcionando sobre el modelo Cliente-Servidor y sólo en un área funcionará en base al modelo de computación distribuida.

La gestión de la red se divide en tres actividades: Monitoreo, Instrumentación y Gestión. Para éste caso se utilizará el sistema pfSense como sistema central para la administración de la red, el cual permitirá aplicar las configuraciones necesarias y realizar las gestiones de administración de red requeridas.

- **MECANISMOS DE MONITOREO**

  Se obtendrán los valores de extremo a extremo, por enlace, por protocolo. Se recogerán los datos que fluyen a través de la red y se mostrarán en herramientas gráficas accesibles vía un entorno web.

  Se podrá apreciar el tráfico en tiempo real identificando las direcciones origen y destino, el estado de la conexión, el tiempo, la cantidad de paquetes que se transfieren y el consumo que cada conexión acumula.

```
pfTop: Up State 1-21/21, View: default, Order: bytes
PR    D SRC                 DEST                STATE   AGE   EXP  PKTS BYTES
tcp   I 190.98.12.92:64411  192.168.1.1:80      10:10    99    79   563  502K
icmp  O 10.9.3.1:41587      10.9.3.2:0           0:0    260    10   522 33408
icmp  O 10.9.2.1:41587      10.9.2.2:0           0:0    260    10   522 33408
tcp   I 190.98.12.92:64435  192.168.1.1:80       4:4      8 86400    25 10468
tcp   I 192.168.1.150:3969  74.125.229.79:80    10:10    30    61    10  2358
tcp   O 192.168.1.150:3969  74.125.229.79:80    10:10    30    61    10  2358
udp   O 10.9.3.1:42285      200.144.121.33:123   2:2    256    37    26  1976
udp   O 10.9.3.1:25106      146.164.48.5:123     2:2    256    35    26  1976
udp   O 10.9.3.1:31268      200.160.7.193:123    2:2    256    31    24  1824
udp   I 87.251.43.124:4569  192.168.1.200:4569   2:2    256    58    35  1424
udp   O 87.251.43.124:4569  192.168.1.200:4569   2:2    256    58    35  1424
tcp   I 192.168.1.140:50097 93.94.226.59:110      9:9     87     5    21  1103
tcp   O 192.168.1.140:50097 93.94.226.59:110      9:9     87     5    21  1103
tcp   I 192.168.1.150:2267  85.214.90.202:5938   4:4    240 86381    18   806
tcp   O 192.168.1.150:2267  85.214.90.202:5938   4:4    240 86381    18   806
udp   I 190.98.12.92:4569   192.168.1.201:4569   2:2      3    57     9   662
udp   O 190.98.12.92:4569   192.168.1.201:4569   2:2      3    57     9   662
udp   I 192.168.1.150:64909 200.1.159.58:53      1:2     30     0     2   402
udp   O 192.168.1.150:64909 200.1.159.58:53      2:1     30     0     2   402
udp   I 192.168.1.150:51441 200.1.159.58:53      1:2     30     0     2   205
udp   O 192.168.1.150:51441 200.1.159.58:53      2:1     30     0     2   205
```

Grafico 21. Monitoreo de los enlaces con pftop

Acumulación del tráfico según días y frecuencia de horas:

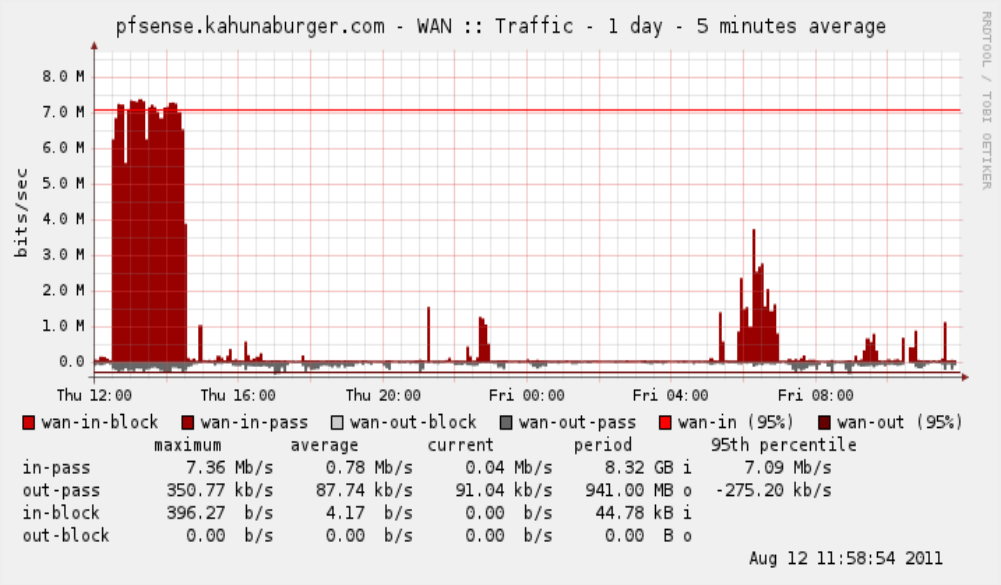


Grafico 22. Graficas de consumo acumulado

Estado del tráfico actual en tiempo real, con salidas a Internet, identificando host origen y ancho de banda utilizado:

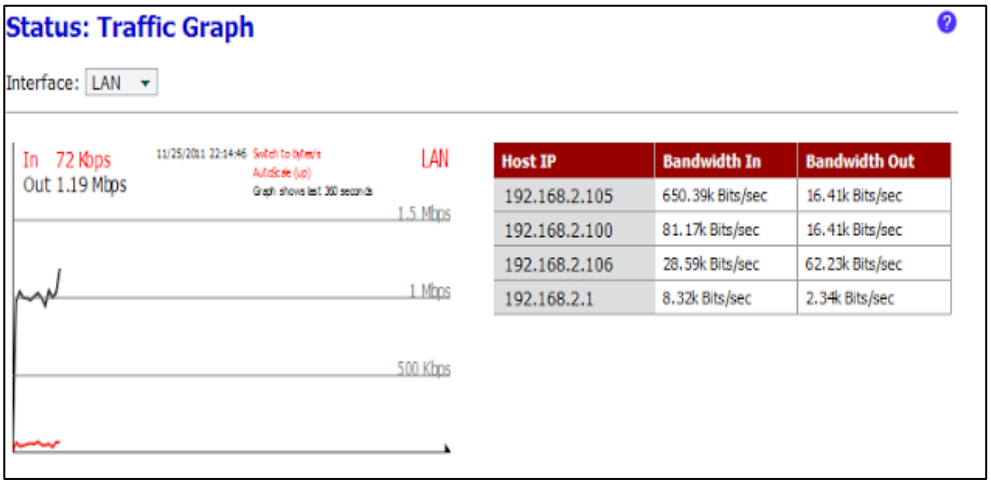


Grafico 23. Estado de Grafico actual, WAN o LAN, con identificación de host origen.

Estado de los servicios del servidor de administración de red:

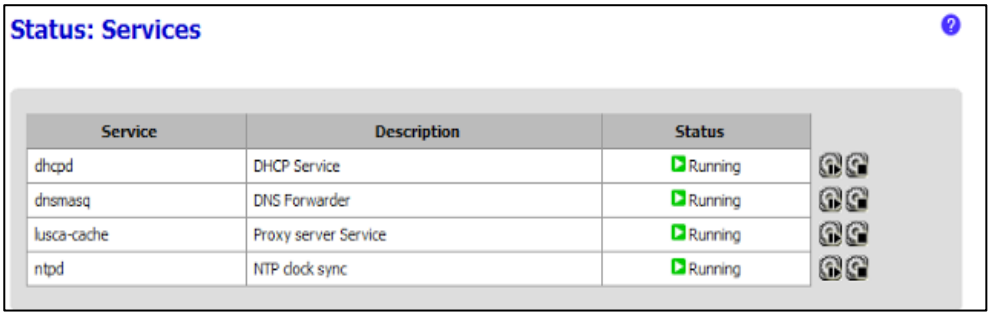


Grafico 24. Estado de los servicios del servidor de administración de red.

Monitoreo de la asignación de direcciones IPv4 a través del servidor DHCP del servidor de administración de red:

Grafico 25. Direcciones DHCP asignadas automáticamente.

- **MECANISMOS DE INSTRUMENTACIÓN**

  Los mecanismos de instrumentación son el conjunto de herramientas y utilidades necesarias para el seguimiento y la sonda de la red.

  Las herramientas de monitoreo incluyen utilidades como: ping, Traceroute y TCPdump, y también mecanismos de conexión remota como FTP, TFTP, SSH vía consola.

  Todos estos mecanismos vienen por default en el servidor de administración de red pfSense.

- **MECANISMOS DE CONFIGURACIÓN**

  El servidor de administración de red pfSense se encargará de gestionar toda la red, para ello cuenta con herramientas para la configuración remota o local.

  De forma remota tiene acceso vía Web a una interfaz desde donde se puede realizar la configuración y ajustes de toda o parte de la red. También, de forma remota, se tiene acceso vía SSH para la gestión de toda la configuración del sistema, incluso dispone del servicio SNMP para poder realizar el monitoreo y configuración de red remota.

4.2.3. SEGURIDAD DE LA RED

Para poder garantizar la seguridad en la red, en ésta sección detallamos los componentes importantes para preparar la seguridad: Análisis de las Amenazas, y Políticas y procedimientos.

- **ANÁLISIS DE AMENAZAS**

  Para realizar el análisis de las amenazas primero hemos identificado los componentes del sistema que deben ser protegidos y los tipos de riesgos de seguridad.

Cuadro 18
Análisis de amenazas para la red de la universidad

Efecto/ Probabilidad	**Usuario Hardware**	**Servidores**	**Dispositivos de Red**	**Software**	**Servicios**	**Datos**
Acceso No Autorizado	B/A	B/B	C/B	A/B	B/C	A/B
Revelación No Autorizada	B/C	B/B	C/C	A/B	B/C	A/B
Denegación de Servicio	B/B	B/B	B/B	B/B	B/B	D/D
Robo	A/D	B/D	B/D	A/B	C/C	A/B
Corrupción	A/C	B/C	C/C	A/B	D/D	A/B
Virus	B/B	B/B	B/B	B/B	B/C	D/D
Daño Físico	A/D	B/C	C/C	D/D	D/D	D/D

Efecto		**Probabilidad**	
A : Destructivo	**B** : Desactivación	**A** : Cierto	**B** : Probable
C : Disruptivo	**D** : Sin Impacto	**C** : Improbable	**D** : Imposible

Nota. Información obtenida por fuente propia

- **POLÍTICAS Y PROCEDIMIENTOS**

  Normalmente hay una confusión en confundir seguridad con control sobre los usuarios y sus acciones, esto generalmente se produce cuando las reglas y los guardianes de seguridad se colocan por encima de los objetivos que la organización está tratando de lograr. Normalmente las debilidades de seguridad en la red se encuentran en las áreas de sistema y software de aplicación, las formas en que los mecanismos de seguridad se implementan y en cómo los usuarios hacen su trabajo. En esta última tarea es más beneficioso educar a los usuarios.

  Las políticas y procedimientos de seguridad son declaraciones formales sobre las normas para el acceso al sistema, la red y la información y su uso, cuyo objetivo es el de minimizar la exposición a las amenazas de seguridad. Para ello es importante aclarar a los usuarios cuales son las amenazas de seguridad, qué se puede hacer para reducir estos riesgos y las consecuencias de no ayudar a reducirlos. Actualmente no existen políticas de seguridad en la red de la facultad, y se tiene una visión errada sobre las políticas y procedimientos de seguridad, al permitir un

acceso completo y sin control sobre el servicio de Internet, que es el principal servicio de la red.

Debido a que actualmente no se tienen áreas de desarrollo de sistemas o software no es necesario aplicar más políticas de seguridad, los mecanismos de seguridad de las aplicaciones que actualmente utiliza la facultad están fuera del alcance del presente trabajo.

Por lo tanto, siendo el servicio de Internet el principal servicio utilizado para acceder a las aplicaciones, en el presente trabajo de red se define como política general de acceso el denegar sitios específicos y aceptar todo lo demás, lo que refleja la filosofía de una red abierta, debido a la alta cantidad de usuarios que requieren utilizar el Internet como fuente de información para su formación profesional, de ésta manera será posible identificar las fuentes de amenazas y bloquearlas dejando libremente el flujo a las demás conexiones.

4.2. MODELO DE ARQUITECTURA

La arquitectura de una red viene definida por su topología, el método de acceso a la red y los protocolos de comunicación. Antes de que cualquier estación de trabajo pueda utilizar el sistema de cableado, debe definirse con cualquier otro nodo de la red.

La topología sobre la cual se propone que se implemente es la Topología Estrella, también conocida como Acceso / Distribución / Núcleo (Access / Distribution / Core), y teniendo en cuenta el flujo de datos el modelo está basada sobre Cliente-Servidor.

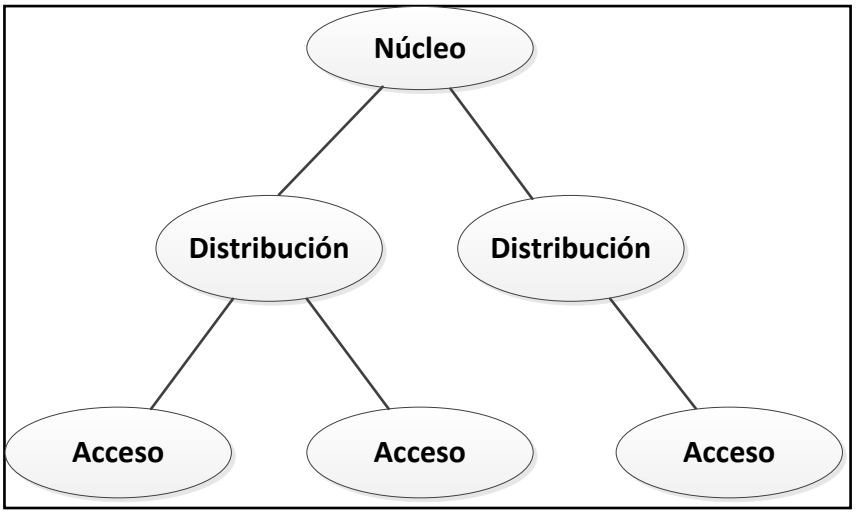


Grafico 26. Topología de la arquitectura Núcleo / Distribución / Accesos de la red.

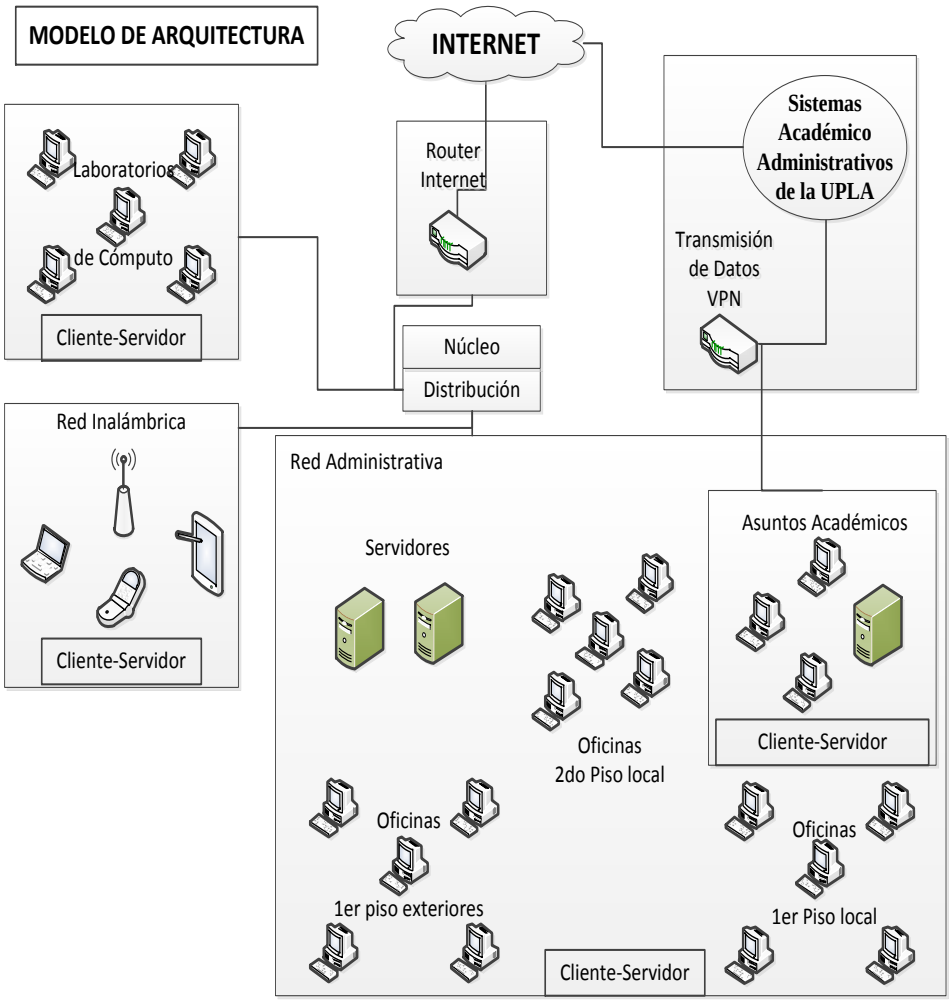


Grafico 27. Modelo de la arquitectura de la red basada en Cliente/Servidor.

4.3. DISEÑO DE LA RED

El diseño de la red es el objetivo final del presente informe, la culminación de los procesos de análisis y arquitectura de redes, el análisis nos proporciona la comprensión y la arquitectura de red proporciona las descripciones conceptuales (en tecnología y topología) por lo que el diseño se basa en éstos.

4.2.1. DISTRIBUCIÓN DE LA RED

A. DIAGRAMA LÓGICO

El primer diagrama lógico muestra el diseño del núcleo y los switchs de distribución, apreciamos como elemento central a un servidor Firewall, se han realizado pruebas con pfSense y cumple muy bien los requerimientos de gestión. El servicio Internet se conectará a una e al servidor Firewall, el servidor tendrá 4 tarjetas de red FastEthernet: 1 para la red Administrativa, 1 para la red de Laboratorios y 1 para la red inalámbrica. El servicio VPN conectará al switch de la oficina de asuntos académicos en el 2do nivel.

4.4. ESQUEMA DE DISEÑO DE RED

El diseño de la red inalámbrica. Se comenzará dimensionando las áreas que tendrán cobertura inalámbrica Wi-Fi. Además, se realizará el cálculo de los radioenlaces Wi-Fi para la implementación del puente inalámbrico. El puente inalámbrico, logra interconectar los distintos puntos de acceso que proporcionan las celdas de cobertura Wi-Fi. También, se mencionará la selección de la mejor opción de la tecnología a utilizarse en el radioenlace para el teleférico. Posteriormente, se escogerán los equipos que permitirán el procesamiento de los datos que estarían ubicados en el cuarto de comunicaciones. Los equipos a implementarse serán: switchs, routers, servidores, reservas de energía, entre otros. Una vez diseñada la solución inalámbrica que brindará conectividad a los usuarios, se definirán también las políticas y parámetros de QoS, para poder asignar prioridad a los paquetes especialmente a los de voz. También, se procederá a definir las políticas de

seguridad y autenticación más viables para el Teleférico. Además, segmentaremos la red haciendo uso de redes LAN virtuales (VLAN), y se propondrá una alternativa de direccionamiento IP de los hosts. A continuación, se presentarán las características que deberá tener el proveedor de servicios de Internet (ISP). Se definirá también, la tecnología de transporte de datos hacia el Internet y el tipo de servicio a contratar al ISP.

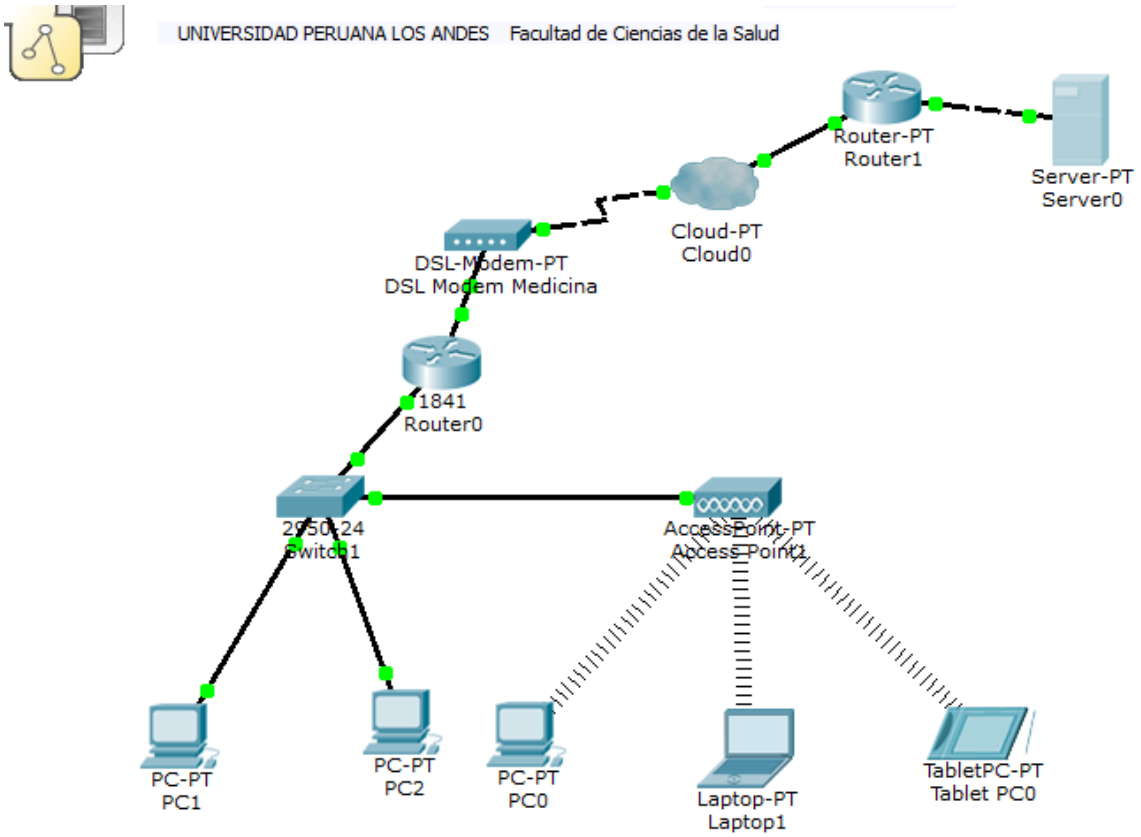


Grafico 28. Esquema de Diseño de la red simulado con el Packet Tracer.

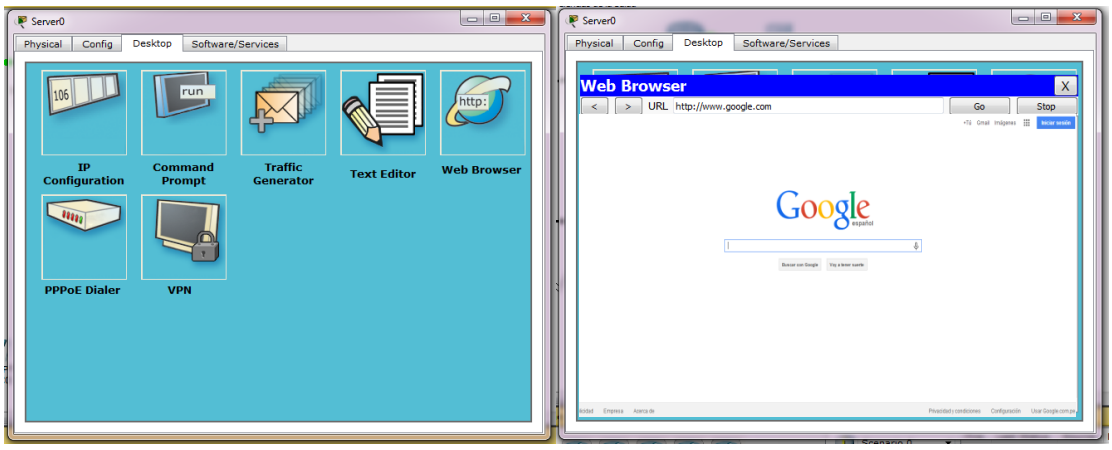


Grafico 29. Probando el internet con la simulación del Packet Tracer

DISCUSION DE RESULTADOS

CAPITULO V

PRUEBAS E IMPLEMENTACION DEL SISTEMA RED

5.1. PRUEBAS DEL SISTEMA

Una vez que el sistema estuvo debidamente implementado en su versión piloto (laptop/servidor, PDA, Celular, Emuladores), se pudieron realizar diferentes tipos de pruebas, suscitándose ciertos problemas que pudieron ser solucionados de manera inmediata. Así también, este sistema fue probado dentro de sus parámetros del Campus chorrillos de la UPLA con la presencia algunas autoridades, docentes, estudiantes, y por otros miembros de la UPLA, quienes pudieron dar sus opiniones y sugerencias para realizar ciertas correcciones del sistema. Estas correcciones incluyeron modificaciones y la creación de una segunda versión, la cual fue desarrollada e implementada como parte de otro proyecto de tesis que se desarrollara más adelante.

5.1.1. PRUEBAS DE DISPOSITIVOS

Se detallan pruebas directamente relacionadas a los dispositivos, que comprenden desde la verificación de los parámetros, especificaciones técnicas y funcionalidad para el estudio y desarrollo del presente sistema. Así como también se detallan las experiencias suscitadas durante el desarrollo del mismo.

Estas pruebas se realizaron para la verificación del alcance de dispositivos en comunicación (distancia), según sus correspondientes especificaciones técnicas. Se pudo constatar que las condiciones especificadas no siempre se cumplen. Para la comunicación del PDA y PC (Servidor) fueron necesarios distintas ubicaciones del AP hasta encontrar el lugar ideal para una buena transmisión/recepción de datos.

En el caso de utilizar celulares, habría que considerar que el ancho de banda de Bluetooth es limitado (1 Mbps) lo cual representa un problema en aplicaciones de altas tasas de transferencia. Como se muestra en la figura

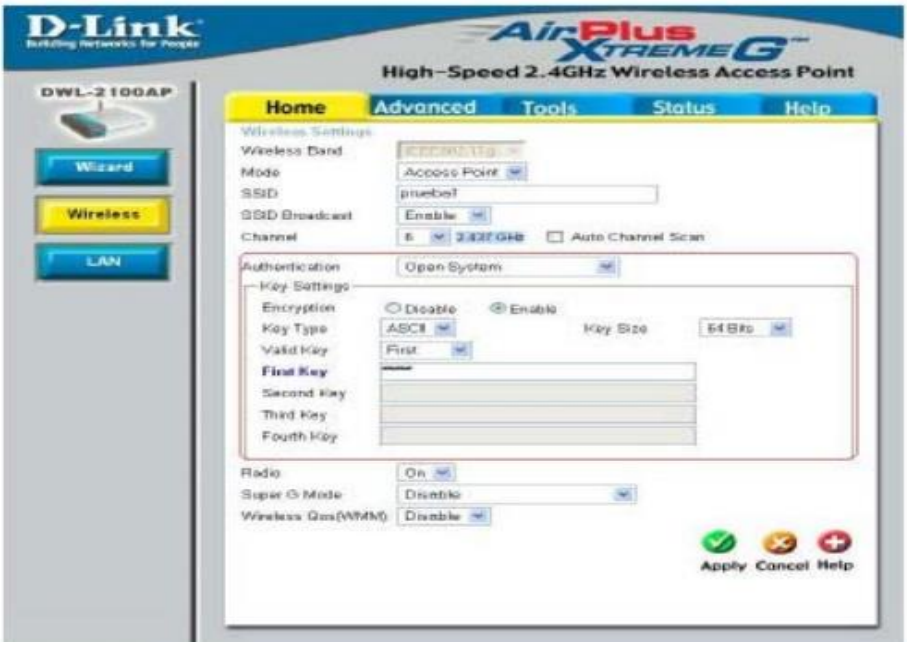


Grafico 28. Pantalla de configuración de seguridad

5.1.2. PRUEBAS DE FUNCIONABILIDAD

El requerimiento básico por parte de los alumnos para el funcionamiento del sistema denominado SEDAC es que cuenten con cualquier dispositivo móvil como un celular o una PDA, el cual debe tener operativa una máquina virtual de java (KVM) con soporte Bluetooth y Wifi. Si bien hoy no existe una masificación de estos equipos con estas características, la penetración de estos aumenta en los distintos segmentos sociales y cada vez mayor número de modelos incorporan soporte Java y Bluetooth. En el caso del computador del profesor, éste debe tener un puerto USB 2.0 y se requiere un Adaptador Bluetooth USB o equivalente para proveer conectividad Bluetooth al computador del profesor y al menos la versión 1.5 de J2SE.

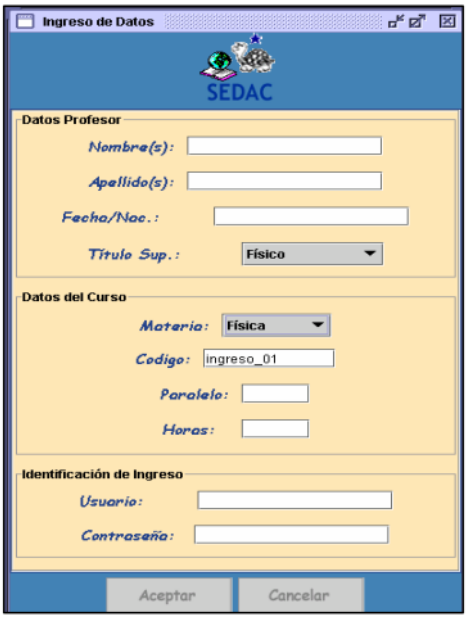


Grafico 29. Pantalla de ingreso de datos para autentificación

Se realizaron pruebas con el Software Cliente en dispositivos móviles, constatando las siguientes tareas:

- Identificación del usuario
- Responder preguntas
- Registro de los alumnos
- Detectar a los alumnos
- Captura de respuestas
- Registro de largo plazo

5.1.3. PRUEBAS DE COMUNICACIÓN

Se realizaron todas las verificaciones de las tecnologías implícitas en los dispositivos móviles. En la PDA, una vez instalado el software y hecha la sincronización, se realizó pruebas de comunicación con la creación de redes ad-hoc PDA-PC, utilizando el programa AVANTGO. Con el celular, la prueba de verificación de comunicación se realizó mediante la creación de una red ad-hoc CELULAR-PC haciendo uso de un dispositivo adaptador USB Bluetooth.

Con el AP, se realizó pruebas de reconocimiento de dispositivos móviles.

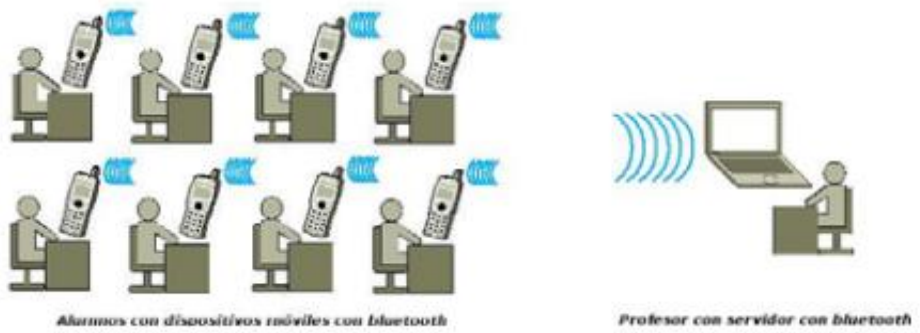


Grafico 30. Esquema general de la comunicación Bluetooth

5.1.4. PRUEBAS DE INTERACCIÓN Y COMPATIBILIDAD

Ambas tecnologías trabajan en el rango de los 2,4 GHz, más sin embargo se pudo comprobar que para la interacción de estas dos tecnologías en un mismo proyecto, eran necesarios dos Dispositivos de Comunicación que soporten estas 2 diferentes tecnologías con sus correspondientes protocolos de comunicación.

Así de esta manera la Red Celular Bluetooth funcionaría independientemente de la Red WiFi; pudiendo interactuar simultáneamente en el proceso de comunicación.

5.1.5. RESULTADO DE PRUEBAS Y PROBLEMAS SUSCITADOS

Se concluyó que las pruebas resultaron satisfactorias, puesto que el sistema funcionó como se esperaba durante la realización de estas, las mismas que fueron realizadas en presencia del Vicerrector General y de los demás altos jerárquicos de la UPLA, así como también de otros

profesores que se encontraban en el campus universitario de chorrillos de la UPLA.

5.2. APLICACIÓN DEL SISTEMA EN DIVERSAS FACULTADES

Se puede resumir que este proyecto representa una herramienta importante para su aplicación, sobretodo en el sector académico-educativo, no solamente a nivel de la UPLA sino también a nivel de Colegios y Escuelas como una nuevo método de enseñanza pedagógica para mejorar el nivel de aprendizaje conceptual de los estudiantes, así como también fomentar una relación de interactividad constante entre los estudiantes con su profesor, el cual podrá medir constantemente y de forma inmediata el avance académico de sus alumnos, entre otras razones académicas las cuales también se detallaran más adelante en este proyecto.

Además, el Sistema de Evaluación Dinámico de Aprendizaje Conceptual (SEDAC), representa a su vez un valioso proyecto en el campo científico-tecnológico, ya que en él se aplican diferentes tecnologías tanto de Hardware como de Software, así mediante su uso por parte de los estudiantes se motivará a estos a convivir con estas nuevas herramientas, ayudando así a romper las barreras tecnológicas.

Por otra parte, existe una gran variedad de dispositivos móviles, protocolos de comunicación, sistemas operativos, frameworks de desarrollo, estándares y soluciones que nos proveen los diferentes proveedores y empresas de telecomunicaciones. La elección de la solución adecuada para el desarrollo de la aplicación móvil es vital en un ambiente tan heterogéneo y en constante evolución y cambio.

Cabe recalcar las aplicaciones comerciales que de este proyecto se puedan suscitar, al igual que las de carácter académico, no solo están ligadas a su explotación en la UPLA, sino a su desarrollo e implementación a nivel de Escuelas, Colegios y otras instituciones

educativas, así como también a diferentes sectores socio-económicos de la sociedad.

5.3. IMPLEMENTACION

5.3.1. IMPLEMENTAR PUNTOS DE ACCESO INALÁMBRICO

El proceso para implementar APs inalámbricas varía dependiendo del protocolo de seguridad que se utilice.

- **Autenticación 802.1x:** El proceso y los pasos se definen en la siguiente sección
- **WPA:** Sistema para proteger las redes inalámbricas Wi-Fi; creado para corregir las deficiencias del sistema previo WEP.
- **WEP:** WEP no requiere una configuración del lado del servidor y es relativamente sencillo de configurar utilizando las instrucciones de configuración que proporciona el proveedor.

5.3.2. PRERREQUISITOS

Los servicios de red inalámbrica que se describen en *Small IT Solution* se basan en Windows Small Business Server 2003 y Microsoft Windows XP Professional. Los elementos que se necesitan implementar antes de implementar los APs inalámbricos incluyen:

- LAN física a la que se conectan los servidores.
- Windows Small Business Server 2003.
- Servicios DHCP de Windows Small Business Server 2003.
- Servicios de la Entidad emisora de certificados (CA) de Windows Small Business Server 2003, Entidad emisora de certificados (CA) y servicio de autenticación e Internet (IAS).
- Los clientes inalámbricos que se agregaron al dominio de Windows Small Business Server 2003 Active Directory.

5.3.3. CONFIGURAR UNA INFRAESTRUCTURA DE RED INALÁMBRICA SEGURA

Para que la autenticación 802.1x funcione, complete las siguientes tareas:

- **Configurar el servidor:** Es necesario configurar Windows Small Business Server 2003 antes de realizar los pasos que se presentan en la sección “Configurar el servidor”. Para configurar Windows Small Business Server 2003, siga los pasos que se proporcionan en el capítulo "Small Business Server".
- **Configurar el AP inalámbrico:** El dispositivo AP inalámbrico necesita dar soporte a la autenticación 802.1x.
- **Configurar clientes inalámbricos:** Observe que muchos dispositivos de cliente inalámbricos tales como cámaras Web y PDAs es posible que no den soporte a la autenticación 802.1x.

5.3.4. CONFIGURAR EL SERVIDOR

La norma 802.1x, que utiliza el Protocolo de autenticación extensible (EAP) para autenticación del cliente inalámbrico, cumple con los requisitos de seguridad de una LAN inalámbrica. WEP proporciona encriptación de tráfico, pero cuenta con una funcionalidad deficiente de administración de claves. Para administrar el proceso de utilizar WEP para la encriptación, Microsoft, junto con otros proveedores, ha desarrollado métodos para administrar las claves de encriptación WEP de manera más segura cuando utiliza TLS o TTLS. Estos métodos permiten que el AP inalámbrico cree claves de sesión únicas para la encriptación WEP entre el punto de acceso y el cliente.

La norma WPA es un conjunto de estándares basados en la industria. Incluye todas las normas y un protocolo estandarizado para la administración de claves conocido como Temporal Key Integrity Protocol (TKIP).

Nota: Ninguna de las mejoras de WPA aborda las debilidades de la Denegación de servicios (DoS) de las normas 802.11 y 802.1x. Sin embargo, las debilidades DoS no son tan graves como las otras fallas de WEP debido a que casi todas los ataques DoS demostrados provocan únicamente una interrupción temporal. Sin embargo, estas debilidades siguen siendo una preocupación importante para algunas organizaciones y es poco probable que se resuelva el problema antes del lanzamiento de la norma (IEEE) 802.11i del Institute of Electrical and Electronics Engineers.

5.3.5. CONFIGURAR COMPONENTES DEL SERVIDOR DE AUTENTICACIÓN

Se necesita configurar a dos componentes de servidor para la autenticación 802.1x:

- Servicio de autenticación de Internet (servidor RADIUS).
- Entidad emisora de certificados para autenticación cliente–servidor (Protocolo de autenticación extensible – Autenticación TLS).

Para que la autenticación 802.1x se configure como se describe en este capítulo, se supone que el ambiente se está ejecutando en Windows Small Business Server 2003. Se requiere esta base para garantizar que los servicios de Active Directory ofrecieron los servicios de autorización y autenticación.

5.3.6. INSTALAR EL SERVICIO DE AUTENTICACIÓN DE INTERNET

Instale IAS en Windows Small Business Server 2003 realizando los siguientes pasos:

- Abra Agregar o quitar programas en el Panel de control.
- Haga clic en Agregar o quitar componentes de Windows.
- En el cuadro de diálogo Asistente para los componentes Windows cuadro de diálogo Asistente para los componentes Windows Servicios de red, y después en Detalles

- En el Servicios de red cuadro de diálogo, seleccione Servicios de autenticación de Internet, haga clic en Aceptar, y después en Siguiente.
- Cuando se le pida, inserte el CD de Windows Small Business Server 2003
- Después de instalar IAS, haga clic en Finalizar , y después haga clic en Cerrar
- Abra el indicador de comando y ejecute el comando netsh ras add registeredserver. command.

El último paso garantiza que el servidor IAS se coloque dentro del grupo de seguridad Servidores RAS e IAS en el dominio de Active Directory. Esto garantiza que los servidores IAS tengan los permisos adecuados para leer las propiedades de acceso remoto de las cuentas de usuario y PC.

5.3.7. INSTALAR EL SERVICIO ENTIDAD EMISORA DE CERTIFICADOS

IAS requiere un certificado de servidor para la autenticación EAP-TLS. Usted puede adquirir un certificado de autenticación de servidor de un proveedor que no es de Microsoft, o instalar el servicio de la Entidad emisora de certificados (CA) que se incluyen con los productos de la familia Windows Server™ 2003. Esta sección describe el proceso de instalación de la CA y la cómo emitir el certificado para la autenticación inalámbrica.

Siga estos pasos, para instalar el servicio CA:

1. Inicie sesión en Windows Small Business Server como un Administrador.
2. Abra Agregar o quitar programas en el Panel de control.
3. Haga clic en el botón Agregar o quitar Componentes de Windows.
4. En el diálogo Asistente de componentes Windows, seleccione el cuadro Servicios de certificado. Un cuadro de mensaje indica que el

PC no se puede renombrar y que no puede agregar ni quitar de un dominio después de haber instalado los servicios de autenticación. Haga clic en Sí y después en el botón Siguiente.

5. Seleccione la opción CA raíz de la empresa.
6. En el campo Nombre común para este CA, ingrese el nombre común del CA, como *BusinessName CA*.
7. En el campo Periodo de Validez, especifique 10 años como el periodo de validez para el CA raíz y haga clic en el botón Siguiente.
8. Acepte las ubicaciones de almacenamiento predeterminadas y haga clic en el botón Siguiente.
9. Aparecerá un cuadro de mensaje que indica los "Los servicios de certificación deben detener temporalmente los Servicios de información de Internet". Haga clic en Sí..
10. Cuando se indique, inserte el CD de Windows Small Business Server 2003.
11. Haga clic en Terminar para completar el asistente.

De manera predeterminada, el CA emite un certificado del Controlador de dominio para todos los controladores de dominio. El servicio IAS utiliza este certificado para la autenticación EAP-TLS.

5.3.8. CONFIGURAR LA POLÍTICA DEL SERVICIO DE AUTENTICACIÓN DE INTERNET INALÁMBRICO

El Servicio de autenticación de Internet (IAS) debe estar configurado con la política de acceso remoto y las configuraciones de solicitud de conexión para la autenticación y autorización de usuarios y PCs inalámbricos en la red inalámbrica. Además, el IAS debe estar configurado para aceptar las conexiones de los clientes RADIUS (APs inalámbricos). Los APs inalámbricos se deben configurar para utilizar los servidores IAS para pasar las solicitudes de autenticación.

Nota: Debe esperar por lo menos 30 minutos después de instalar la Entidad emisora de certificados antes de crear la política de acceso remoto. De otra manera, no podrá agregar el certificado de autenticación del servidor a la política de acceso inalámbrico, como se describe en los siguientes pasos.

Realice los siguientes pasos utilizando la consola de administración del Servicio de autenticación de Internet (IAS) en el menú Herramientas administrativas.

1. Haga clic con el botón alterno en la carpeta Políticas de acceso remoto y seleccione la opción Nueva política de acceso remoto.
2. Titule la política Habilitar acceso inalámbrico y seleccione la opción Utilizar el asistente para configurar la política típica para un escenario común.
3. Seleccione Inalámbrico como el método de acceso.
4. Otorgue el acceso, con base en el grupo y agregue el grupo de seguridad Usuarios móviles a la lista de grupos que cuentan con derechos de acceso inalámbrico.
5. Seleccione EAP protegido (PEAP) para el Tipo de EAP.
6. Seleccione Configurar y después agregue el certificado de autenticación del certificado de autenticación del servidor que se instaló para IAS.
7. Haga clic en el botón Finalizar y salga del asistente.
8. Nota: La política Permitir el acceso inalámbrico que se creó durante la instalación de IAS puede coexistir con otras políticas de acceso remoto. Sin embargo, asegúrese que otras políticas de acceso remoto se incluyan en la siguiente lista de políticas Permitir acceso inalámbrico en la carpeta. Las políticas que se encuentran en la parte superior de la lista de políticas invalidan las configuraciones establecidas en las políticas con nivel de prioridad más bajo. Utilice las flechas que aparecen junto a la lista para mover la política Permitir acceso inalámbrico a la parte superior de la lista.

5.3.9. AGREGAR CLIENTES RADIUS AL SERVICIO DE AUTENTICACIÓN DE INTERNET

Debe agregar APs inalámbricos como clientes RADIUS a IAS antes de que se puedan configurar para conectarse al servidor IAS. Realice los siguientes pasos, para agregar un AP inalámbrico como un cliente

RADIUS, utilizando la consola de administración **Servicio de autenticación de Internet (IAS):**

1. Haga clic con el botón alterno en la carpeta Clientes RADIUS y seleccione Nuevo cliente RADIUS. .
2. Ingrese un nombre amigable y la dirección IP de la AP inalámbrica. Este es el mismo nombre y dirección IP que se ingresó para el AP inalámbrico. Si aún no tiene configurado el AP inalámbrico, utilice estos mismos valores cuando configure el AP inalámbrico.
3. Seleccione la Norma RADIUS como el atributo cliente-proveedor y después ingrese el secreto compartido para este AP inalámbrico en particular. Después seleccione en el cuadro la Solicitud de contener el atributo Autenticador de mensajes. Si no ha instalado aún el AP inalámbrico, utilice el mismo secreto compartido cuando configure el AP inalámbrico.

   Nota: La mayoría de los APs inalámbricos no requieren los atributos específicos del proveedor (VSA). Sin embargo, algunos clientes RADIUS pueden necesitar el configurar VSA para que funcione correctamente. Para obtener más información sobre requisitos VSA, refiérase a la documentación específica de su proveedor.

5.3.10. MODIFIQUE LAS CONFIGURACIONES DEL PERFIL DE LA POLÍTICA DE ACCESO INALÁMBRICO

Configure Active Directory para ignorar las configuraciones de marcación del usuario, para evitar problemas potenciales con algunos APs inalámbricos. Además, los atributos RADIUS se deben establecer para la reautenticación del cliente en intervalos de tiempo que garanticen que las claves de sesión WEP se actualicen.

Realice los siguientes pasos para modificar las configuraciones del perfil de la política de acceso remoto:

1. Seleccione la carpeta de Políticas de acceso remoto y la política Permitir acceso remoto que se creó para el acceso remoto.
2. Abra las propiedades de la política y después haga clic en Editar

perfil. .

3. En la pestaña Restricciones de marcación, seleccione la opción Se pueden conectar los clientes por minuto (tiempo de espera de la sesión) , y después ingrese 30 minutos por valor.
4. En la pestaña Avanzado:

a) Establezca el atributo Ignorar propiedades de marcación del usuario a Verdadero.

b) Establezca el atributo Terminación-Acción a Solicitud de RADIUS.

5. Cierre los cuadros de diálogo y salga de la consola de administración del Servicio de autenticación de Internet (IAS).

Nota: En algunos APs 802.1x de soporte inalámbrico, la condición de política "corresponde con el tipo del puerto NAS" se tendrá que eliminar.

5.3.11. AGREGAR USUARIOS

Es necesario que los usuarios agreguen el grupo Usuarios móviles para poder conectarse a la red inalámbrica.

Al agregar usuarios al grupo de Usuarios móviles, realice los siguientes pasos:

1. Abra la consola de Administración del servidor y amplié el contenedor Grupos de seguridad.
2. Agregue a los usuarios a los que se les permite acceder a la LAN inalámbrica al grupo Usuarios móviles.
3. Agregue los PCs a los que se les permite acceder a la LAN inalámbrica al grupo de Usuarios móviles.

5.3.12. CONFIGURAR LOS PCS CLIENTE INALÁMBRICOS

La configuración del cliente involucra dos elementos; la configuración del dominio del cliente y la configuración de las propiedades inalámbricas del PC.

Nota: : Las cuentas del usuario y PC deben estar en el mismo Dominio de Active Directory que el servidor IAS.

5.3.13. CONFIGURAR DOMINIOS DEL PC CLIENTE

Si el PC aún no está conectado al dominio, realice los siguientes pasos para unir el PC al dominio:

1. En Windows Small Business Server, utilice la consola de Administración del servidor y seleccione el contenedor PCs cliente.
2. Elija Configurar PCs cliente. Siga las instrucciones para crear una entrada de Active Directory para el PC cliente.
3. Mientras esté conectado a la LAN alámbrica, desplácese a http://<Small Business Server Name>/Connect Computer, seleccione el PC que se creó en los pasos anteriores y complete los pasos que se requieren para conectarse al dominio de la pequeña empresa. Esto puede requerir varios reinicios del PC cliente.

5.3.14. CONFIGURACIÓN DEL MANUAL DEL CLIENTE INALÁMBRICO

Si el GPO de "Configuración inalámbrica del PC cliente" no está configurado en Windows Small Business Server, entonces es necesario configurar los clientes inalámbricos de manera manual.
Para configurar manualmente Windows XP para la autenticación PEAP/802.1x, realice los siguientes pasos:

1. Abra el Panel de control y haga clic en Conexiones de red.
2. Haga clic con el botón alterno en el adaptador de red inalámbrica y seleccione Propiedades.
3. Haga clic en la pestaña Redes inalámbricas.
4. Haga clic en Agregar para agregar redes inalámbricas SSID y configurar la autenticación.
5. En la Red de nombre SSID, ingrese el SSID o el nombre de la red inalámbrica conforme se haya configurado en el AP inalámbrico.
6. Realice las siguientes configuraciones. Se deben conservar los

valores predeterminados para el resto de las configuraciones.

1. En el cuadro desplegable Encriptación de datos, seleccione WEP.
2. En el cuadro de la lista desplegable Autenticación de la red, seleccione Compartida.
3. Seleccione el cuadro Me proporcionaron la clave automáticamente.
6. Seleccione la pestaña Autenticación.
7. Seleccione el cuadro Habilitar la autenticación IEEE para esta red.
8. En el cuadro de la lista desplegable tipo EAP, seleccione PEAP.
9. Click OK and close the Properties dialog.

CONCLUSIONES

1. La implementación de zonas Wifi en la ciudad universitaria de la UPLA en el intercambio de información educativa, generara que la información sea transmitida y compartida de manera más fácil, rápida, sencilla, eficaz en cuanto se refiere al intercambio de información, compartimiento de archivos y almacenamiento de datos.
2. El nivel de influencia que ejerce la implementación de zonas Wifi en la ciudad universitaria de la UPLA, en la tecnología de intercambio de información educativa la red planteada facilitará la utilización de recursos informáticos desde cualquier punto de la infraestructura, los usuarios podrán transferir sus archivos vía red antes que usar los disquetes, CD, memoria flash, los periféricos de calidad y alto costo pueden ser compartidos por los integrantes de la red. Lo más importante esta trasferencia de datos es confiable, a la vez se pueden implementar políticas de seguridad según el tipo de trabajo que realizan los usuarios de la red.
3. Para la implementación de esta red inalámbrica considerando los más altos grados de seguridad a través de un sistema Firewall como pfSense permite monitorear, controlar y configurar adecuadamente los requerimientos de la red, aplicaciones y usuarios.

RECOMENDACIONES

1. Se debe contar con personal capacitado y dedicado (administrador de red) para las funciones de administración y soporte de la red para garantizar la escalabilidad de la solución de manera rápida, segura y confiable.
2. Definir e implementar formalmente la utilización de políticas de administración de red para los usuarios que harán uso de la red a través de claves o contraseñas por un tiempo limitado.
3. Implementar un sistema de procedimientos estandarizados y documentar la configuración de los Puntos de Acceso, Router, Switch y demás dispositivos instalados para su mejor administración.

BIBLIOGRAFÍA

- Alonso C., (2006), "Proteger una red Wireless", PC World Profesional Noviembre 2006, IDG, Madrid, España.

- Baghaei N., (2003), "IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients", Honours Project Report, University of Canterbury, Christchurch, New Zealand

- Chávez A.(2007), "Redes de área local inalámbricas (WLAN)", Material del curso Ingeniería Inalámbrica, PUCP, Lima, Perú

- Cisco Systems Inc., (2004), "Academia de Networking de Cisco Systems: Guía del segundo año. CCNA® 1 y 2", Ed. Pearson Educación S.A., Madrid, España

- Gast M.(2005), "802.11 Wireless Networks: The Definitive Guide", O'Reilly 2nd Edition, California, USA

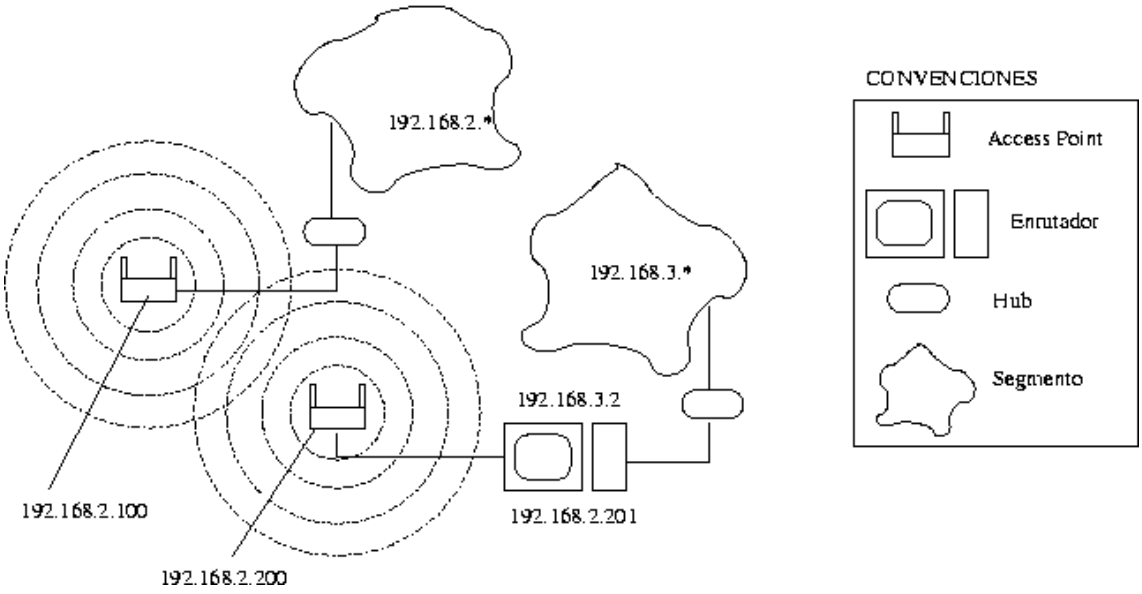
- IEEE Std. 802.11 (2003), "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", Reaffirmed, New Jersey, USA.

- Enrique de Miguel Ponce, (2008), "Redes inalámbricas", IEEE 802.11.

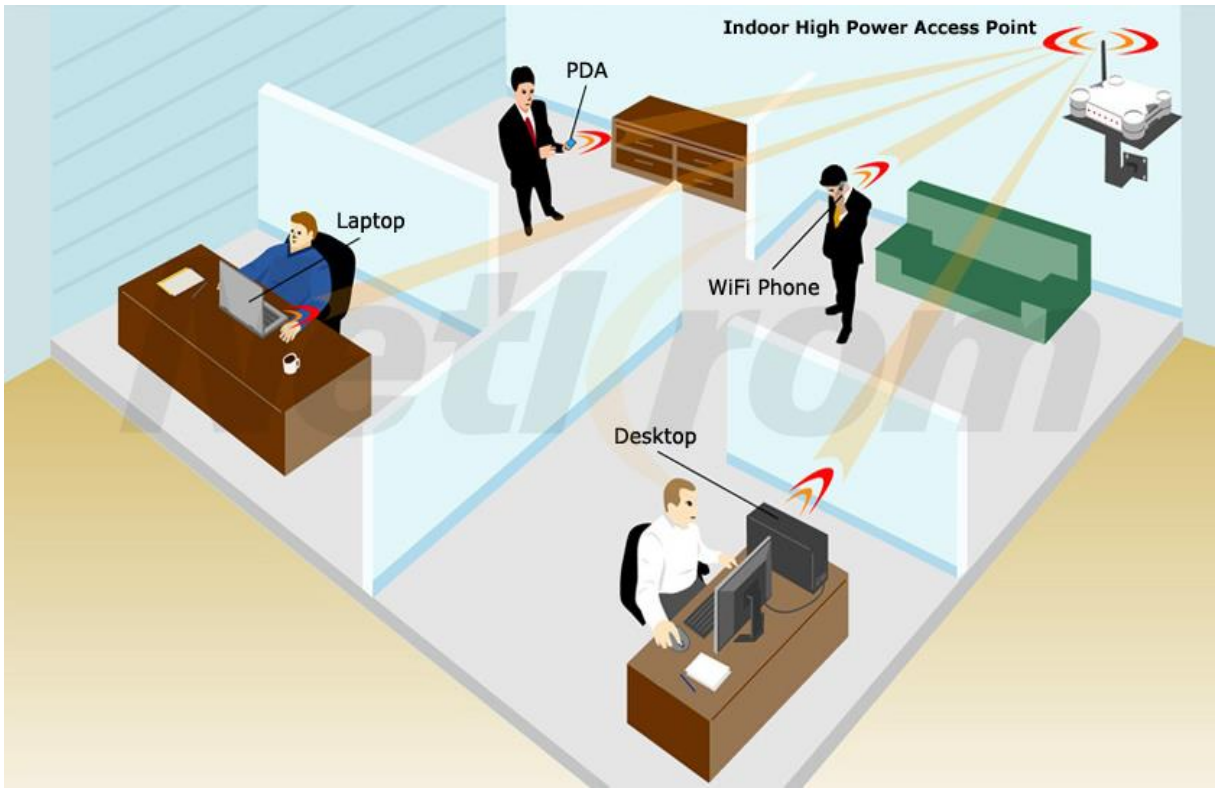
.

ANEXOS

ANEXO N° 01
ESQUEMA DE LA RED A IMPLEMENTAR



ANEXO N° 02
DISEÑO IMPLEMENTADO



ANEXO N° 03

DISPOSITIVOS PARA LA IMPLEMENTACION DE LA RED INALAMBRICA

ANEXO N° 04

TIPOS DE ANTENAS PARA USUARIOS

ANEXO N° 05
SISTEMA WPA2