ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

FACULTAD DE INFOMATICA Y ELECTRONICA

ESCUELA DE INGENIERIA EN SISTEMAS

"ESTUDIO COMPARATIVO DE APLICACIONES PARA LA IMPLEMENTACIÓN DE PORTALES CAUTIVOS EMPLEANDO INTERCONECTIVIDAD ENTRE LOS LOCALES DE BONNY RESTAURANT"

TESIS DE GRADO

Previa a la obtención del título de

INGENIERO EN SISTEMAS INFORMATICOS

Presentado por:

MÉLIDA MARIANA FIERRO FIERRO

FABIÁN ALEJANDRO GONZÁLEZ BONIFAZ

RIOBAMBA – ECUADOR

2011

AGRADECIMIENTO

Agradezco a Dios a mis padres y a mis abuelitos por su infinito amor, por su apoyo incondicional para que siga adelante, sin decaer ante los fracasos y adversidades, por siempre estar a mi lado inculcándome el valor de la verdad, de la vida, el respeto y la fortaleza para siempre luchar por mis propósitos; a mis hermanos por su motivación, a mis amigos por estar siempre apoyándonos e impulsándonos juntos y a Faby por ser mi apoyo y fortaleza durante este proyecto que hoy se convierte en un gran logro para ambos.

Mélida Fierro Fierro

Mi agradecimiento a Dios, a mi familia y amigos que con su granito de arena me supieron dar un gran apoyo para la culminación de este gran paso, a Dios por ponerme el camino y los obstáculos que permitieron lograr fortalecer mi mente y mi espíritu, a mi familia, por haber confiado en las capacidades y bondades que puedo ofrecer, el cariño, el apoyo, y la guía para lograr cumplir sueños y metas planteadas, a mis amigos, que durante toda mi vida supieron valorar el tipo de persona que siempre fui, y en especial a ti Meli, por brindarme tu tiempo, tu amor, tu compañía y las fuerzas necesarias para alcanzar metas que día a día nos proponemos.

Fabián González Bonifaz

DEDICATORIA

A mis padres, a mis abuelos, hermanos y amigos por estar en las buenas y malas, brindándome siempre su apoyo incondicional y a los profesores que con esmero y dedicación a su profesión guían a los estudiantes hacia una meta profesional.

Mélida Fierro Fierro

Dedico este trabajo a Dios, ya que el tiene un único propósito en la vida para cada uno de nosotros, y esta oportunidad me la está dando a mi, por la salud, y la sabiduría, a mis padres porque gracias a sus valores, aprendí que si las cosas se hacen bien, solo Dios se encargará de todo, a mis amigos que siempre estuvieron ahí con su apoyo.

Fabián González Bonifaz

“Nosotros, Fabián Alejandro González Bonifaz y Mélida Mariana Fierro Fierro, somos los responsables del contenido, ideas y resultados planteados en el presente proyecto de tesis, y el patrimonio intelectual del mismo pertenece a la Escuela Superior Politécnica Chimborazo”.

Fabián Alejandro González Bonifaz	**Mélida Mariana Fierro Fierro**

INDICE ABREVIATURAS

AAA: Authentication, Authorization and Accounting

ALTQ: Alternate Queueing

AP: Access Point

ARP: Address Resolution Protocol

CGI: Common Gateway Interface

CHAP: Challenge Handshake Authentication Protocol

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

EAP: Protocolo Extensible de Autenticación

EAPOL: EAP sobre LAN

HTTP: Protocolo de transferencia de Hipertexto

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos

LAN: Red de Área Local

IP: Internet Protocol

MAC: Medium Access Control

MD5: Message-Digest Algorithm 5

MIC: Message Integrity Code

NAS: Network Attached Storage

OSI: Open System Interconnection

PAM: Pluggable Authentication Module

PAP: Password Authentication Protocol

PDA: Asistente Digital Personal

PGP: Pretty Good Privacy

PHP: Hypertext Preprocessor

PPP: Protocolo punto a punto

RADDB: Directorio de Configuración de Radius

RADIUS: Remote Authentication Dial IN

RSN: Red de Seguridad Sólida

SSID: Service Set Identifier

SSL: Secure Socket Layer

TCP: Protocolo de Control de Transmisión

TLS: Seguridad de la Capa de Transporte

TTLS: Tunneled Transport Layer Security

TKIP: Protocolo de Integridad de Clave Temporal

TUN: Dispositivo Virtual Punto Punto

UDP: Protocolo de Datagrama de Usuario

VLAN: Red de área local virtual

VPN: Red Virtual Privada

VSA: Atributos Específicos del proveedor

WEP: Wired Equivalent Privacy

WPA: Wi-Fi Protected Access

INDICE GENERAL

INDICE GENERAL

CAPITULO I

CAPITULO II

CAPITULO IV

CAPITULO V

INDICE DE FIGURAS

INDICE DE TABLAS

CAPITULO I

1. MARCO REFERENCIAL

1.1. Antecedentes

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. Estas redes facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas todo esto con la finalidad de mejorar la funcionalidad y disponibilidad de usar la red.

Actualmente se está usando la tecnología Hotspot por todo el mundo, varios hoteles, aeropuertos, restaurantes, parques y otros lugares públicos han puesto en píe dicha tecnología, pero algunos de estos Hotspots son inseguros por lo que puede ser utilizado de forma maliciosa, por personas que solo deseen hacer daño a la empresa que la provee.

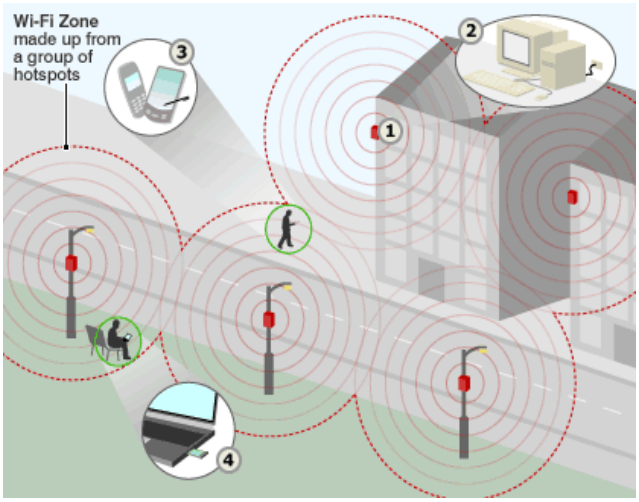


Figura I.1 Uso de los hotspots

Bonny Restaurant por ser un lugar al que acuden extranjeros, empresarios y público en general que buscan conectarse con una red ya sea para cerrar negocios, enviar correos, descargar información, etc, ha implementado el servicio de WI-FI en sus instalaciones, teniendo así una red que es usada para conectar las máquinas de la empresa y para brindar el acceso público a la red. Gracias al ancho de banda de un 3 MB que Bonny Restaurant ha adquirido en los últimos meses ha proporcionado un servicio adicional de videoconferencias garantizando así la calidad en la transmisión.

Uno de los principales problemas que afronta el Restaurant es que mientras existe una videoconferencia se deben desconectar los puntos de acceso que se encuentran en el Restaurant para que la transmisión sea la correcta, provocando así que los clientes del restaurant no puedan acceder al Internet mientras esto sucede.

La infraestructura de red que actualmente posee Bonny Restaurant es:

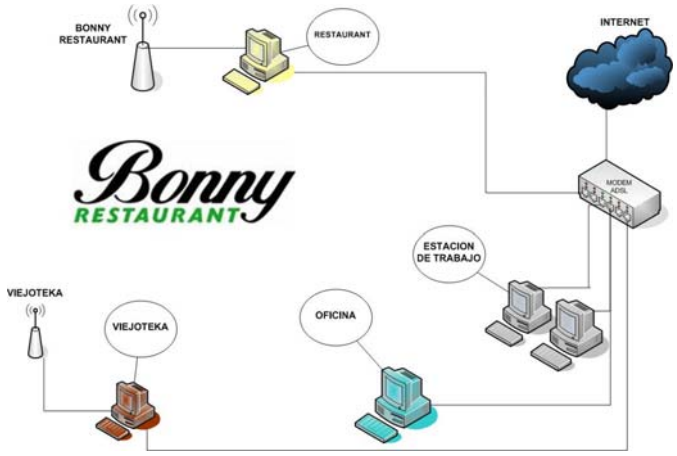


Figura I.2 Infraestructura Actual de la Empresa

Cabe recalcar que la infraestructura antes mencionada pertenece a uno de los 2 locales de Bonny, puesto que el otro local no cuenta en la actualidad con ningún tipo de infraestructura, sería factible que existiera alguna para que pueda brindar el mismo servicio en el otro local.

Bonny Restaurant posee un Hotspot vulnerable ya que no cuenta con ningún tipo de seguridad, por lo cual está expuesto a varios ataques de usuarios malintencionados que pueden provocar que la información pueda ser usada de forma negativa, causando así daños y alteración de la misma.

Sabemos que en el mercado existen varias aplicaciones de Portales cautivos que ofrecen varios servicios, tales como:

- Zero Shell
- Pfsense
- Chillispot
- AirMarshal
- WifiDog
- NoCatauth

De los cuales analizaremos Zero Shell, Chillispot, WifiDog y NoCatauth.

1.2. Justificación

En toda empresa la tecnología inalámbrica ofrece beneficios para todos los empleados ya que mejora la movilidad, los procesos de negocios, mantienen la ventaja competitiva e incrementan los ingresos.

Existen algunas ventajas de usar la tecnología WLAN ventajas tanto empresarial como operativas; donde la parte empresarial se ve reflejada en el aspecto laboral como en los servicios que ésta brinda permitiendo así mejorar productividad de la empresa o Institución, en el aspecto operativo éste provoca menores gastos administrativos y de capital.

En la actualidad muchas empresas se han ido expandiendo teniendo así una matriz y varias sucursales alrededor del país, las mismas que necesitan dar capacitaciones, charlas, conferencias a sus empleados de forma rápida y global para lo cual el servicio de videoconferencias es el más optado en esta situación, viendo esta necesidad Bonny Restaurant empieza brindando el servicio gratuito de WI-FI a sus clientes como también el servicio de Videoconferencias a empresas públicas, privadas y personas naturales, para lo cual se requiere que la calidad de servicio sea la adecuada. Lo que significa, implementar una seguridad que permita obtener dicha calidad y así satisfacer las necesidades a los usuarios de la red.

Mediante las aplicaciones para implementar portales cautivos corporativos se pretende lograr que la red de Bonny Restaurant brinde un servicio óptimo a sus clientes, mediante un control de acceso de usuarios, que permita asegurar que el servicio que se brinde tenga la calidad necesaria para la actividad que el cliente este desarrollando,

asimismo llevar un control sobre el ancho de banda destinado a cada uno de ellos y el uso que se le está dando.

Aprovechando el uso de Zona Wifi Gratuita en la matriz de Bonny, se pretende proyectarla hacia la primera sucursal ubicada en las calles Villarroel y Almagro, mediante antenas, permitiendo así que la aplicación funcione para los dos locales de esta manera:

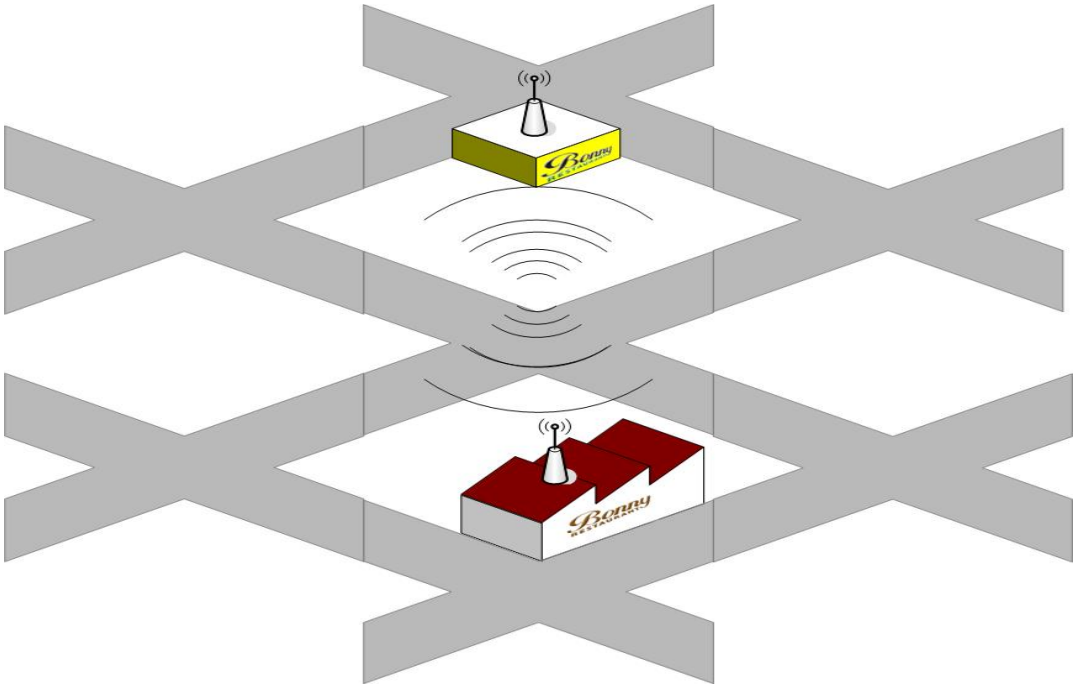


Figura I.3 Interconectividad entre los 2 locales

Con la selección de una aplicación para implementar portales cautivos en Bonny Restaurant se logrará:

- Controlar el acceso al Internet mediante autenticación y validación de cada usuario con un portal cautivo en un servidor GNU/Linux
- Conocer que equipos están conectados a la red y que están haciendo.
- Distribuir el ancho de banda para brindar un mejor servicio a los usuarios conectados en la red

- Proteger la información de la empresa de usuarios malintencionados tanto internos como externos.
- Mantener la integridad de la información
- Verificar que el ancho de banda sea usado adecuadamente por usuarios de la empresa.
- Garantizar que la velocidad del Internet sea optima para los servicios que Bonny Restaurant ofrece a sus clientes.

1.3. Objetivos

1.3.1. Objetivo General

Realizar un estudio comparativo de las aplicaciones para implementar portales cautivos empleando interconectividad entre los locales de Bonny Restaurant, y seleccionar la aplicación que mejor se ajuste a las necesidades del Restaurant.

1.3.2. Objetivo Especifico

- Realizar un estudio comparativo de las aplicaciones para implementar portales cautivos corporativos en un servidor GNU/LINUX.

- Analizar los aplicaciones para la implementación de portales cautivos en una red inalámbrica

- Realizar un enlace punto a punto entre los dos locales de Bonny Restaurant ubicados en las calles Villarroel y Almagro y en la Primera Constituyente y Darquea.

- Implementar y administrar un portal Cautivo usando una de las aplicaciones que se ajuste a las necesidades de la empresa todo esto en un servidor GNU/Linux.

- Analizar las vulnerabilidades que llegan a presentarse en una red inalámbrica.

- Evaluar la seguridad de la red mediante software libre

1.4. Hipótesis

La selección de una aplicación para la implementación de un portal cautivo, empleando interconectividad entre los locales del Restaurant Bonny, permitirá administrar la seguridad de acceso de los usuarios a la red inalámbrica corporativa del Restaurant.

CAPITULO II

2. MARCO TEORICO

ESTUDIO DE LAS TECNOLOGIAS Y SEGURIDADES INALAMBRICAS

2.1. Que son las redes inalámbricas WIFI

Las redes inalámbricas son aquellas que logran una comunicación por un medio de transmisión no guiado (sin cables) mediante ondas electromagnéticas, tanto la transmisión como en la recepción se lo hace por medio de antenas, algunas de las ventajas que encontramos en la utilización de este tipo de tecnología es la rápida instalación ya que no se necesita de cableado, así mismo la movilidad que los usuarios poseen al circular de forma libre y el costo es mucho menor que el de la red normal.

En los últimos años las redes inalámbricas han ganado mucha popularidad, debido a las prestaciones que estas tienen, y cada día se van descubriendo nuevas aplicaciones para ellas.

Las redes WLAN permiten a sus usuarios conectarse a una red, acceder a información específica y recursos de la red, todo esto sin la necesidad de permanecer físicamente conectado a un determinado lugar.

Generalmente las redes inalámbricas se aplicaban solamente en empresas, pero con la demanda de dispositivos WLAN, estas redes se las están aplicando también en ambientes públicos, áreas metropolitanas, como medio para acceder al servicio de Internet gratuito, donde existen zonas de alta densidad de usuarios (Hotspots).

2.2. Características de las redes inalámbricas WIFI

Las redes inalámbricas tienen varias características que impulsan tanto a las empresas como a la sociedad, por lo que en la actualidad las WLAN a más de ser consideradas como un medio de comunicación son consideradas como una necesidad, algunas de las características más notables y beneficiosas para las empresas que tienen redes inalámbricas son:

Movilidad: Las redes inalámbricas permiten transmitir información en tiempo real en cualquier lugar de la organización o empresa a cualquier usuario, permitiendo que exista mayor productividad y posibilidades de servicio.

Simplicidad y facilidad de instalación: La instalación de una red inalámbrica elimina la necesidad de tirar cables a través de paredes y techos, ahorrando espacio, evitando dañar la estética del lugar y permitiendo así reducir los tiempos de instalación.

Flexibilidad de la instalación: Las redes inalámbricas permiten llegar a lugares donde el cable no puede llegar.

Costos reducidos: La inversión inicial requerida para una red inalámbrica puede ser costosa que la de una red LAN, pero los beneficios a largo plazo son superiores en ambientes dinámicos que requieran acciones y movimientos frecuentes.

Escalabilidad: Las redes inalámbricas pueden ser configuradas en una gran variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones utilizadas dentro de una empresa o institución. Las configuraciones son muy fáciles de cambiar y además resulta muy fácil la incorporación de nuevos usuarios de la red.

2.3. Portales Cautivos

INTRODUCCIÓN

Un portal cautivo es un servicio Web para el acceso a Internet. Un portal cautivo recoge todo el tráfico http y redirecciona estas peticiones a un conjunto de páginas especiales, previamente definidas, como paso previo para permitir al usuario la navegación normal.

Es decir, antes de que el usuario pueda salir a Internet, está obligado a pasar por determinadas páginas en donde, normalmente, deberá autenticarse y se le muestra información importante de diversa índole, como puede ser instrucciones de uso, propaganda, ofertas, recomendaciones o acuerdos de utilización del servicio de acceso a Internet. Una vez que el usuario cumple con los requisitos exigidos en estas páginas iníciales, se permite se navegación a Internet con toda normalidad, siempre y cuando los sitios que quiera visitar estén permitidos.

A primera vista este servicio se asemeja bastante al trabajo que realiza un cortafuegos, firewall, y a las que realiza un proxy, pero en la práctica un portal cautivo no sustituye a ninguno de ellos. Pensado para gestionar el acceso a Internet, su ámbito de actuación está limitado al tráfico http, peticiones que atiende en función de la autenticación válida del usuario que las solicita y de reglas que permiten o prohíben alcanzar los sitios solicitados, todo ello en un entorno dirigido a través de páginas Web predefinida. Los

portales cautivos operan detrás del firewall, cuando estos están presentes y pueden combinare con el trabajo del proxy.

Por otra parte, la facilidad de configuración de este servicio permite crear y personalizar las páginas que se muestran al usuario y Administrador, sin que sea imprescindible contar con programadores.

La idea de un portal cautivo surge y se desarrolla en Linux, plataforma en la que encuentra el más amplio catálogo de este servicio. Aunque en menor medida, es también fácil encontrar desarrollos en entorno Windows.

Un portal cautivo además, puede adicionar programación que limita el uso excesivo de la conexión gratuita, por ejemplo el tamaño de los archivos a descargar o la velocidad a la cual se descargan los mismos, tiempo de uso, programas o páginas de acceso, etc.

Para montar este servicio se requiere de un equipo dimensionado al número de conexiones que se esperan, con al menos dos tarjetas de red, sistema operativo y un programa de portal cautivo, Para el equipo, no es imprescindible presupuestar un ordenador tipo servidor, ya que no es un servicio que tenga un elevado consumo de recursos de proceso.

Un portal cautivo proporciona un servicio de control de acceso web que si bien está orientado a redes abiertas, normalmente asociadas a enlaces inalámbricos, como aeropuertos, hoteles, restaurantes, centros de negocios, cafeterías, café Internet, etc.

Pueden aplicarse en multitud de situaciones: eventos, aulas, puntos de acceso tipo Kiosco, puntos de venta-expositores, oficinas remotas.

Un portal cautivo resuelve de manera sencilla y limpia el acceso a Internet, facilitando la conexión de usuarios externos y brinda la oportunidad de ofrecer nuevas aplicaciones de conexión que en entornos con pocos recursos técnicos, no resultan viables. La facilidad de instalación, configuración y uso, está propiciando su rápida difusión.

TIPOS DE PORTALES CAUTIVOS

Se pueden diferenciar dos grandes tipos de portales cautivos y un subtipo. El que es necesario tener una cuenta es decir debe tener un nombre de usuario y contraseña (una cuenta) y en el que simplemente debe aceptar las condiciones de la red para ser parte de ella, el subtipo de portal cautivo llamado también “walled garden” combina los dos tipos de portales, este tipo de portal ofrece acceso libre a determinados sitios o contenidos sin tener que realizar autenticación login del usuario. Un ejemplo complejo de todo esto sería un WIFI Access Point en un restaurant que permite ver información de los platos que ofrece, costos, servicios que presta y sitios de anunciantes, sin tener que ingresar un usuario y contraseña. Pero, con una cuenta se puede ingresar a la web en general, inclusive usar algún mensajero instantáneo y bajas correo con Outlook Express.

MODELOS DE PORTALES CAUTIVOS

De a cuerdo con el modo de acceso y fin que tenga un portal cautivo se pueden diferenciar los siguientes modelos de Portales Cautivos:

- Abiertos sin usuarios, mostrando un splash con condiciones de uso, información de la red, etc.
- Abiertos con usuarios, que se pueden registrar.
- Cerrado, con usuarios que gestiona el administrador
- De pago previa suscripción.

FUNCIONES DE LOS PORTALES CAUTIVOS

Una herramienta común de autenticación utilizada en las redes inalámbricas es el portal cautivo. Este utiliza un navegador web estándar para darle al usuario la posibilidad de presentar sus credenciales de registro. También puede utilizarse para presentar información (como Política de uso Aceptable) a los usuarios antes de permitir el acceso. Mediante el uso de un navegador web en lugar de un programa personalizado de autenticación, los portales cautivos funcionan en prácticamente todas las computadoras portátiles y sistemas operativos. Generalmente se utilizan en redes abiertas que no tienen otro método de autenticación (como WEP o filtros MAC).

Para comenzar, el usuario abre su computadora portátil y selecciona la red. Su computadora solicita una dirección mediante DHCP y le es otorgado. Luego usa su navegador web para ir a cualquier sitio en Internet.

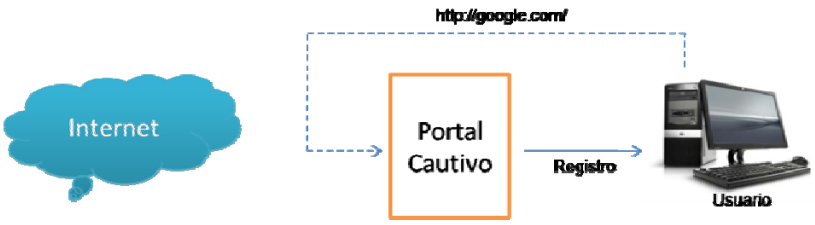


Figura II.4: El usuario solicita una página web y es redireccionado.

En lugar de recibir la página solicitada, al usuario se le presenta una pantalla de registro. Esta página puede solicitarle al usuario que ingrese su nombre de usuario y una contraseña, simplemente oprime el botón de “registro” (login). El punto de acceso u otro servidor en la red verifica los datos. Cualquier otro tipo de acceso a la red se bloquea hasta que se verifiquen las credenciales.

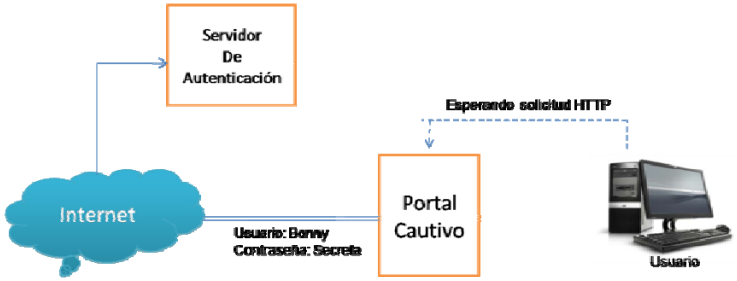
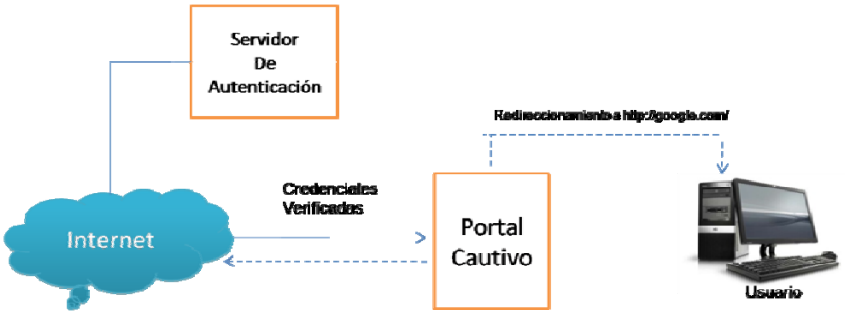


Figura II.5: Verificación de credenciales

Una vez que el usuario ha sido autenticado, se le permite el acceso a los recursos de la red y en general es redireccionado al sitio web que solicito originalmente.



FiguraII.6: Después de que el usuario es autenticado, se le permite el acceso a la red

Los portales cautivos no proveen encriptación para los usuarios de redes inalámbricas, en su lugar confían en las direcciones MAC e IP del cliente como identificadores únicas.

Si bien esto no es necesariamente muy seguro muchas implementaciones van a solicitar que el usuario se re-autentique periódicamente. Esto puede hacerse automáticamente minimizando una ventana emergente (pop-up) del navegador, cuando el usuario se registra por primera vez.

VENTAJAS Y DESVENTAJAS DE LOS PORTALES CAUTIVOS

Encontramos algunas de las ventajas al usar Portales Cautivos como método de Seguridad en nuestra red inalámbrica de las cuales podemos destacar las siguientes:

- Seguridad Basada en Identidades
- Configuración sencilla.
- Estadísticas de Uso por usuario.
- Mejor despliegue que VPN: no necesita cliente, solo es necesario un navegador.
- Más rápidos: No existe latencia por cifrado.
- Pueden utilizar Autenticación Centralizada.
- Permite aplicar políticas por usuario.
- No se compromete todo el Sistema
- Ofrece muchas soluciones comerciales y libres.

Entre las desventajas que los portales Cautivos podemos enumerar las siguientes:

- Menos seguros que otras soluciones (se puede combinar con WEP/WPA).
- Vulnerables a Spoofing de MAC e IP.
- No se cifra el tráfico (depende de los protocolos de aplicación: https, ssh, etc.)

- Si el dispositivo no tiene navegador no es posible autenticarse
- Los clientes asociados al AP tienen visibilidad entre ellos aunque no estén autenticados.

APLICACIONES

En la actualidad los portales cautivos son aplicados especialmente en redes inalámbricas abiertas, donde se interesa mostrar un mensaje de bienvenida a los usuarios, propagandas, servicios que brinda la empresa o institución, y para informar de las condiciones del acceso es decir se informa al usuario de los puertos permitidos, responsabilidad legal, etc. Los administradores suelen usar un portal cautivo para que los usuarios se responsabilicen de sus acciones, además permite distribuir mejor el ancho de banda de la red dándole un uso adecuado a las necesidades del usuario. Entre los principales lugares donde se aplican los portales cautivos están:

- Restaurantes
- Aeropuertos
- Museos
- Bares
- Hoteles
- Hosterías
- Mall
- Parques, etc

Los portales cautivos a más de ser una herramienta que permite administrar la red y a los usuarios de la misma, permite que las empresas o lugares donde se los use proyecten sus productos, den información acerca de la empresa, guíen a los usuarios, utilicen propaganda ya sea en beneficio de la empresa o de otros lugares, etc.

ARQUITECTURA DE LOS PORTALES CAUTIVOS

Los portales cautivos están conformados por varios protocolos de autenticación y seguridad los mismos que interactúan de tal forma que permiten obtener la funcionalidad del portal cautivo de la siguiente manera:

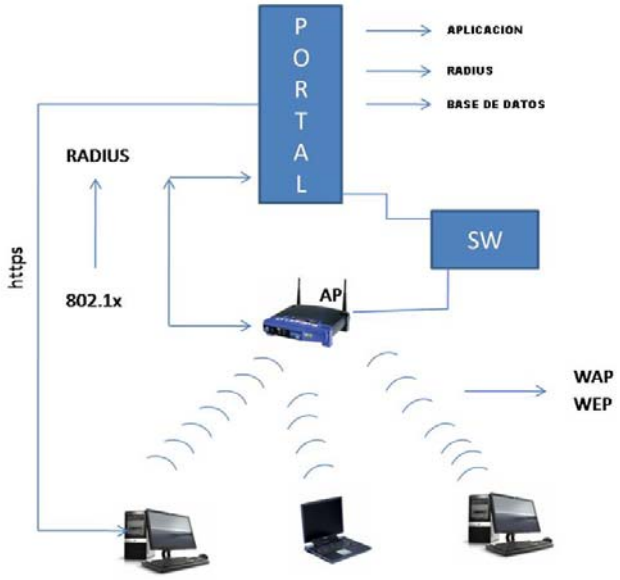


Figura II.7: Arquitectura del Portal Cautivo

2.4. Protocolos de Autenticación

2.4.1. Estándar 802.1x

QUE ES EL ESTÁNDAR 802.1X

802.1x es un estándar creado por la IEEE, para realizar control de acceso a nivel de la capa 2 del modelo OSI o “capa de enlace”, mediante un proceso de autenticación que habilita o no el acceso de los dispositivos que se conectan a una red estos pueden ser: dispositivos inalámbricos, clientes, puntos de acceso y servidores.

El estándar 802.1x puede ser implementado tanto en redes cableadas como en redes inalámbricas y puede ser utilizado para la administración de claves utilizadas para proteger la información que transmiten los dispositivos autenticados.

El estándar 802.1x hace referencia al uso del protocolo de autenticación extensible EAP entre el usuario que desea conectarse a la red o suplicante, el autenticador (switchs o points) y los servidores de autenticación que pueden ser RADIUS.

POR QUE USAR 802.1X

Muchas recomendaciones se han dado para minimizar los riesgos asociados al acceso indebido en redes inalámbricas. Entre las principales están:

- Evitar la difusión del identificador de red o SSID.
- Establecer listas de control de acceso por directorios, físicas o de MAC de los dispositivos que acceden a la red.
- Utilizar cifrado en las conexiones inalámbricas.
- Segmentar los puntos de acceso inalámbricos en zonas de seguridad administradas por un firewall.
- Establecer redes privadas virtuales o VPNs en las conexiones inalámbricas.
- Combinar mecanismos de autenticación a la red y cifrado de datos
- No implementar infraestructura inalámbrica.

Viendo estas necesidades se creó el protocolo WEP el cual utiliza una clave secreta estática (es decir no hay renovación de la clave de manera automática ni frecuente) que es compartida por el punto de acceso a todos los clientes que

accedan a la red y con la cual se realiza la autenticación y la protección de los datos, sin embargo no paso mucho tiempo para empezar a detectar y difundir las falles de la WEP, debido al manejo estático de su llave y al uso de un vector de inicialización VI; que se puede identificar en los paquetes transmitidos, de manera periódica, lo que hace que el protocolo sea susceptible a ataques mediante un tráfico capturado con el mismo vector de inicialización VI, más aún cuando hoy en día no se requiere de una gran cantidad de datos capturados ni de conocimientos para llevar a cabo este tipo de procesos, puesto que se han desarrollado una gran variedad herramientas que automatizan y facilitan este proceso, tales como Kismet, Aircrak, WepLab, etc.

La IEEE consciente de estas fallas desarrolla el estándar de seguridad 802.11i para redes inalámbricas al cual también se le conoce como “red de seguridad sólida” (RSN), por otro lado el consorcio de proveedores de tecnología inalámbrica con mejor fidelidad “Wi-Fi”, genera el estándar WPA para la protección de los datos y el control del acceso inalámbrico a las redes, el cual se basa en el estándar 802.11i y puede implementarse en las tecnologías inalámbricas de tipo Wi-Fi, el mismo que incluye mecanismos más adecuados para realizar el control de acceso y protección de datos en redes inalámbricas ya que integra mecanismos fuertes de autenticación, control de acceso, integridad y confidencialidad.

WPA utiliza 802.1x como mecanismo de control de acceso, autenticación a la red y para generar y entregar las llaves de sesión WPA a los usuarios autenticados. WPA utiliza el protocolo TKIP que aumenta el tamaño de las claves, las refresca periódicamente utilizando un contador de secuencia VI y realiza una función de mezcla por paquete, adicionalmente WPA utiliza una función de encriptación llamado MIC mediante el cual verifica la integridad de los mensajes transmitidos y previene que atacantes capturen paquetes, los modifiquen y los reenvíen.

El problema de la WPA radica en que es un estándar que aun se encuentra en proceso de adopción, puesto que muchas tecnologías inalámbricas no se encuentran habilitadas para implementarlo. Adicionalmente el estándar 802.11i o WPA2 aún se está ratificando y posteriormente se requerida una actualización de Hardware y Software de acceso inalámbrico para su implementación.

Como alternativa realmente viable para quienes tiene dispositivos inalámbricos que no soportan WPA, surgió la integración del mecanismo de control de acceso y autenticación a la red 802.1x con el uso de cifrado WEP con manejo dinámico de claves (WEP dinámico).

La implementación de 802.1x para redes inalámbricas utiliza un servidor de autenticación que puede ser RADIUS o IAS, el cual no solo es quien valida la identidad de quien accede a la red (a través de un método EAP) si no que es quien fuerza, con cierta frecuencia, la generación de una nueva clave de cifrado para la conexión establecida, haciendo que la probabilidad de que un ataque identifique de la clave de cifrado sea mínima, además el 802.1x posee ciertos métodos de autenticación EAP como TLS y TTLS que permiten elevar aún más la seguridad mediante el uso de certificaciones digitales de autenticación de usuarios o estaciones.

Finalmente, este tipo de implementación es fácilmente adaptable a los cambios o crecimientos de las infraestructuras tecnológicas y también se pueden utilizar modelos de autenticación distribuidos para organizaciones con varias sedes o varias redes LAN.

ELEMENTOS QUE INTERVIENEN EN 802.1 X

802.1 x define los siguientes elementos:

- Autenticador
- Cliente/Suplicante
- Servidor de Autenticación

Autenticador

El Autenticador es el elemento que se encarga de la seguridad del puerto y controla el acceso a la red. El Autenticador es el que recibe la información del usuario (nombre, contraseña) para pasarla al Servidor de Autenticación quien habilita o impide el ingreso a la red. La comunicación entre el Servidor y el Autenticador se realiza mediante RADIUS.

Cliente o Suplicante

El cliente o también llamado suplicante es el dispositivo que intenta acceder a la red, es quien proporciona la información (nombre, contraseña) al Autenticador a través del Protocolo de Autenticación Extensible (EAP).

Servidor de Autenticación

El Servidor de Autenticación es quien negocia y valida la identidad del suplicante, y le informa el éxito o fracaso del proceso para que ejecute la acción indicada.

FUNCIONAMIENTO DE 802.1X

Como conocimos el estándar 802.1x emplea tres actores principales en la autenticación: El suplicante, el Autenticador, y el Servidor Autenticación, mismos que se comunican de la siguiente manera:

1) Para empezar el proceso autenticación el puerto de acceso donde el cliente se conecta se va a encontrar en un estado de No Autorizado, se debe tomar en cuenta que el puerto de acceso que se configura para usar 802.1x tenga dos canales disponibles para el tráfico de datos:

- El primer canal para que los datos trafiquen entre el cliente y la red
- El segundo canal para el trafico 802.1x de la autenticación.

2) La comunicación empieza con un cliente o suplicante no autenticado que intenta conectarse a la red.

3) El punto de acceso responde permitiendo pasar solamente paquetes EAP desde el cliente al Servidor de Autenticación. Puesto que el puerto está en estado No Autorizado.

4) El punto de acceso bloquea cualquier otro tipo de tráfico como paquetes HTTP, DHCP, POP3, hasta que el punto de acceso verifique la identidad del cliente mediante el Servidor de Autenticación.

5) El cliente envía un mensaje EAP-start.

6) El punto de acceso responde con EAP-request identity para obtener la identidad del cliente.

7) El cliente contesta con su identidad y el Autenticador reenvía este mensaje al Servidor de Autenticación.

8) La autenticación se realiza de acuerdo con el algoritmo de autenticación seleccionado y el resultado (Aceptación o Negación) lo envía el Servidor de autenticación al punto de acceso.

9) Si la autenticación es correcta, el estado del puerto pasa ha Autorizado para otros tipos de tráfico del cliente.

10) Para desconectar el acceso el cliente enviara un mensaje EAP-logoff con lo que el punto de acceso pone al puerto en estado No Autorizado.

A continuación se muestra el proceso de autenticación que realiza 802.1x:

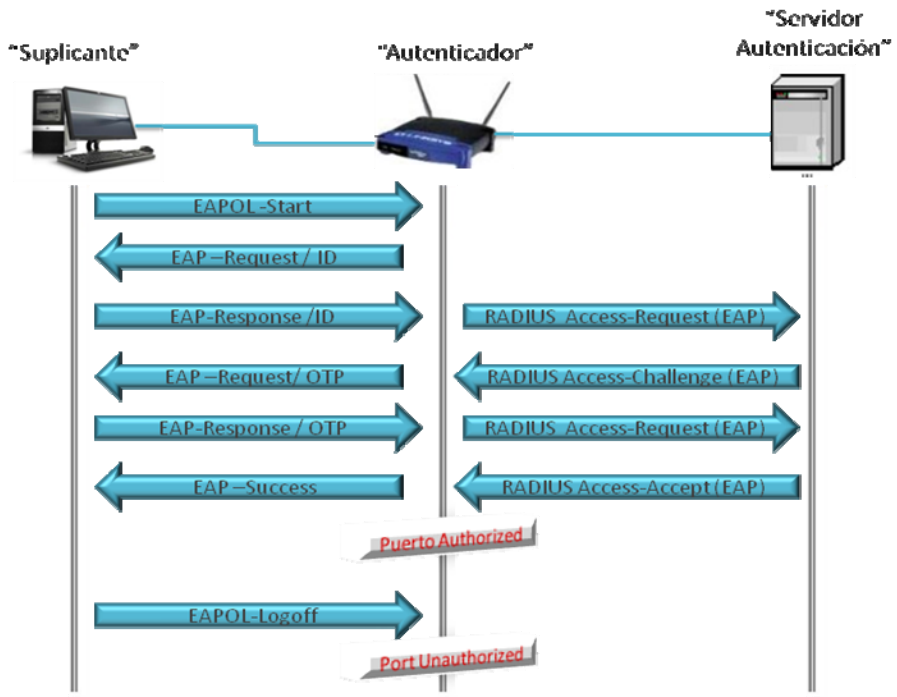


Figura II.8: Proceso de Autenticación 802.1x

2.4.2. Protocolo EAP

INTRODUCCIÓN

EAP (Protocolo de Autenticación Extensible) fue desarrollado para mitigar la proliferación de soluciones de autenticación propietarias que podían causar problemas en la inter-operabilidad entre equipos de diferentes proveedores, generalmente funciona directamente sobre capas de enlace de datos como un protocolo punto a punto, como el PPP o el IEEE 802.1X, sin requerir IP. Este protocolo puede ser utilizado en circuitos conmutados, enlaces dedicados y enlaces cableados o no cableados.

Lleva el nombre de “extensible” porque soporta múltiples mecanismos de autenticación, el dialogo entre el usuario y el servidor de autenticación se lleva a cabo mediante tramas EAP. La forma encapsulada del EAP, conocida como EAP sobre LAN o EAPOL, es usada para todo tipo de comunicación entre el usuario y el Autenticador.

En una red WLAN el punto de acceso actúa como un Proxy EAP entre el terminal y el servidor de autenticación, aceptando paquetes EAPOL del terminal y diseccionándolos al servidor de autenticación con un protocolo como RADIUS. A su vez el punto de acceso direcciona todos los paquetes EAP del Servidor de Autenticación sobre EAPOL al terminal inalámbrico.

Debido a que el EAP fue originalmente diseñado para redes cableadas este asume que la capa física es segura. En el caso de una WLAN esta premisa no es cierta porque un adversario puede fácilmente escuchar el aire para obtener tráfico EAP.

Por lo tanto, debe haber algún método de proteger criptográficamente al EAP de cualquier ataque adversario.

EAP incorpora un sistema dinámico para asignar claves WEP, generando una nueva para cada sesión. Básicamente su uso dentro de una WLAN es la autenticación por lo que generalmente se combina con el estándar 802.1X para el control de acceso. El proceso de autenticación está conformado por tres elementos principales que son:

1. Supplicant (client software) Suplicante (software cliente) que quiere ser validado mediante unas credenciales.
2. Authenticator (access point) Autenticador (punto de acceso)
3. Authentication Server (a RADIUS/AAA server) Servidor de autenticación (un radio / servidor AAA)

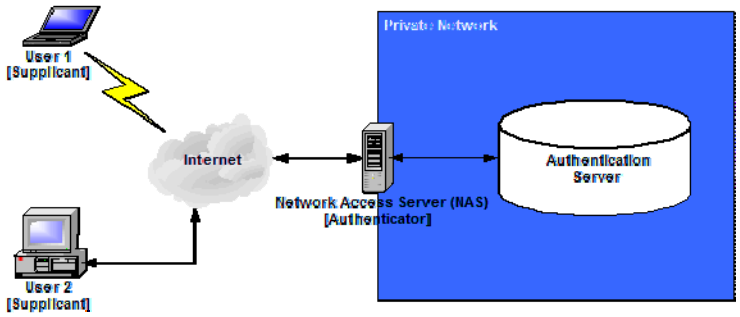


Figura II.9: Arquitectura EAP

TIPOS MÁS COMUNES DE EAP

Puesto que EAP es un protocolo flexible y soporta varias opciones de autenticación existen múltiples tipos de EAP, algunos son estándares y otros son soluciones propietarias de empresas. Entre los tipos de EAP podemos mencionar los siguientes:

EAP –TLS

EAP-TLS (Seguridad de Capa de Transporte) es un sistema de autenticación fuerte basado en certificados digitales, tanto el cliente como el servidor RADIUS necesitan de certificaciones X.509 es decir requiere de una clave de infraestructura pública (PKI) en ambos extremos. TLS es el nuevo estándar que sustituye a SSL.

EAP-TTLS

TLS Tunneled es un sistema de autenticación basado en una identificación de usuarios y contraseñas que se transmiten cifrados mediante TLS, para evitar su transmisión en texto limpio. Es decir se crea un túnel mediante TLS para transmitir el nombre de usuario y la contraseña. A diferencia de EAP-TLS solo requiere un certificado de servidor.

PEAP

EAP Protegido consiste en un mecanismo de validación similar a EAP-TTLS, basado en usuario y contraseña también protegidos. Es un método de autenticación de dos fases. En la primera fase un túnel de TLS se crea entre el cliente y el servidor RADIUS. El túnel de TLS solo es creado por el uso de un certificado en el servidor RADIUS. La segunda fase el cliente se autentica usando el protocolo MS-CHAPv2 O Token Cards. El uso de MS-CHAPv2 o las Token Cards le permite al cliente autenticarse usando credenciales de las bases de datos, existiendo directorios o sistemas de contraseña one-time.

LEAP

EAP Lightweight es un método de autenticación desarrollado por Cisco. Es una autenticación 802.1x de servidor a cliente que utiliza una contraseña de inicio de

sesión proporcionada por el usuario. Cuando el punto de acceso inalámbrico se comunica con un RADIUS habilitado para LEAP de Cisco (servidor de control de acceso seguro de Cisco (ACS)), LEAP ofrece el control del acceso a través de la autenticación mutua entre los adaptadores inalámbricos de los clientes y la red inalámbrica y brinda claves de codificación de usuario individuales y dinámicas para ayudar a proteger la privacidad de los datos transmitidos.

MD5

Message Digest EAP son considerados la forma más simple de EAP. Transfiere un hash con el nombre de usuario, su contraseña y una cadena arbitraria. El servidor utiliza la clave en texto claro y la cadena arbitraria para generar su propio hash, el mismo que es comparado con el hash entrante. EAP-MD5 no es un método seguro contra ataques tipo diccionario. Además, en una Wireless LAN, es imposible crear claves WEP dinámicas utilizando EAP/MD5. Por tanto, este método sólo está indicado para las pequeñas redes cableadas.

A continuación se detallan las principales características y vulnerabilidades de cada uno de ellos:

TABLA II.I: Características y vulnerabilidades de los Tipos de EAP

TIPO	CARACTERÍSTICAS	PROPIETARIO	VULNERABILIDADES
LEAP	• Soporta redes con varios sistemas operativos	CISCO	• Su capacidad depende del tamaño de su clave • Usa MV-Chap conocido por su vulnerabilidad en la autenticación.
MD5	• Simple • Requiere poca memoria y es fácil de implementar	RSA Security	• Susceptible a ataques man-in-the-middle • No provee métodos de autenticación de AP
PEAP	• Combina la autenticación especificada por el administrador y EAP	CISCO Microsoft, RSA	• No se encuentra
TLS	• Autenticación en doble sentido. • Descendiente directo de SSL	Microsoft	• Requiere PKL
TTLS	• Utiliza un túnel • Autentica en un solo sentido	Funk Software Certicom	• Certificados menos seguros que los utilizados en TLS

FORMATO DE LOS PAQUETES EAP

El proceso de validación está conformado por tres elementos, un solicitante que quiere ser validado mediante unas credenciales, un punto de acceso y un Servidor

de Autenticación los mismos que se comunican mediante paquetes que contienen información vital para este proceso. El formato de dichos paquetes es la siguiente:

TABLA II.II: Formato de los paquetes EAP

Código	Identificador	Longitud	Datos
1 byte	1 byte	2 bytes	De longitud variable

Cada uno de los campos del paquete contiene la siguiente información:

Código: Tiene un byte de longitud y se utiliza para interpretar el campo de datos, identificando el tipo de paquete EAP.

TABLA II.III: Códigos del paquete EAP

CÓDIGO	DESCRIPCIÓN	REFERENCIA
0	--	--
1	Solicitar	RFC 3748
2	Respuesta	RFC 3748
3	Éxito	RFC 3748
4	Error	RFC 3748
5	Iniciar	RFC 5296
6	Finalizar	RFC 5296
7-255	--	--

Identificador: Es un byte de largo y contiene un entero sin signo utilizado para satisfacer las peticiones con las respuestas. Cada nueva transmisión utiliza un número de identificador nuevo.

Longitud: Está formado por 2 bytes de longitud y contiene el número de bytes en el paquete entero. EAP supone algo más de la longitud es de relleno que puede ser ignorado.

Datos: Este campo tiene una longitud variable (incluyendo el cero bytes). El valor del campo Código define la forma en que el campo de datos debe ser interpretado.

FORMATO DEL PAQUETE EAP DE RESPUESTA Y SOLICITUD:

El formato del paquete EAP de respuesta y solicitud incrementa el campo tipo y Tipo de Datos, este tipo de paquetes son utilizados por el Autenticador para enviar solicitudes al sistema de búsqueda de acceso y las respuestas de conceder o denegar el acceso.

TABLA II.IV: Formato EAP de solicitud y respuesta

Código	Identificador	Longitud	Tipo	Tipo de Datos
1 byte	1 byte	2 bytes	1 byte	De longitud variable

Los paquetes EAP de respuesta y solicitud son identificados en el campo Código, que representa una solicitud con el valor 1 y una respuesta con el valor 2 en el campo, el campo identificador y Longitud son utilizados como se mencionó anterior mente.

Tipo: Este campo tiene una longitud de un byte y define el tipo de petición o respuesta. Sólo un tipo se utiliza en cada paquete y el tipo de respuesta coincide

con el tipo de solicitud, excepto si la solicitud es inaceptable, en este caso se sugiere una alternativa.

Tipo de Datos: Este campo tiene una longitud variable y el valor del campo Tipo, define la forma en que interpreta el Autenticador el tipo de datos.

A continuación se muestra la secuencia de las tramas EAP:

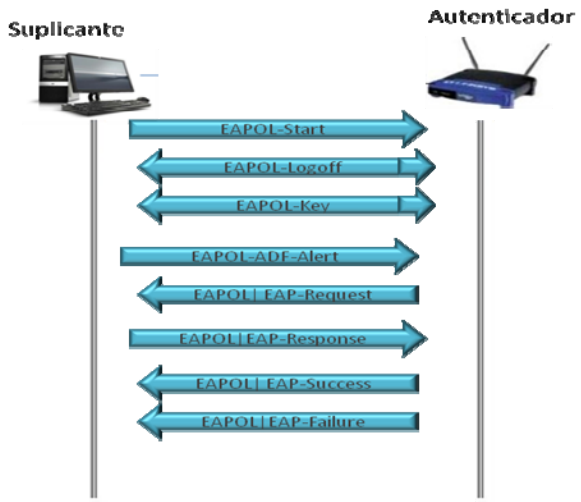


Figura II.10: Secuencia EAP

2.4.3. Protocolo RADIUS

QUE ES EL PROTOCOLO RADIUS

Radius es un protocolo cliente-servidor y un software que es utilizado por NAS (o aplicaciones), para autenticar usuarios remotos y autorizarlos a acceder a los recursos de una red. Un Servidor corriendo en servicio Radius es comúnmente llamado servidor RADIUS. RADIUS es típicamente usado como un sistema central de Autenticación que provee la autenticación, autorización y administración de usuarios remotos.

RADIUS además facilita una administración centralizada de usuarios. Si se maneja una enorme cantidad de usuarios, continuamente cientos de ellos son agregados o eliminados a lo largo del día y la información de autenticación cambia continuamente. En este sentido, la administración centralizada de usuarios es un requerimiento operacional.

Los clientes RADIUS envían credenciales de usuario e información de parámetros de conexión en forma de un mensaje RADIUS al servidor. Éste autentica y autoriza la solicitud del cliente y envía de regreso un mensaje de respuesta. Los mensajes RADIUS son enviados como mensajes UDP utilizando el puerto UDP 1812 para mensaje de autenticación RADIUS y, el puerto UDP 1813, es usado para mensajes de cuentas RADIUS.

Algunos servidores usan el puerto UDP 1645 para mensajes de autenticación y, el puerto 1646, para mensajes de cuentas, debido a que son los puertos que se usaron inicialmente para este tipo de servicio.

ESTRUCTURA DE PAQUETES RADIUS

El intercambio de datos entre el cliente y el servidor se hacen a través de paquetes RADIUS estos paquetes contienen la siguiente información:

TABLA II.V: Formato de los paquetes RADIUS

CÓDIGO	IDENTIFICADOR	LONGITUD
AUTENTICADOR		
ATRIBUTOS		

Cada uno de estos campos contiene la siguiente información:

Campo Code (Código): Está formado por un octeto, indica el tipo de paquete RADIUS, puede tomar los siguientes valores:

TABLA II.VI: Valores del campo código del paquete RADIUS

VALOR TRANSMITIDO	DESCRIPCIÓN
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server
13	Status-Client
255	Reserved

De donde:

Access-Request: Es enviado por un cliente RADIUS al servidor RADIUS para solicitar autenticación y autorización para conectarse a la red. Debe contener el usuario y contraseña (ya sea de usuario o CHAP); además del puerto NAS, si es necesario, si este paquete es enviado el campo código tendrá el valor de 1.

Access-Accept: Es un paquete enviado por el servidor RADIUS en respuesta a un paquete “Access-Request” y contienen la información de la configuración para que el usuario pueda hacer uso del servicio, informa que la conexión está autenticada y autorizada, si este paquete es enviado el valor del campo código será 2.

Access-Reject: Es un paquete enviado por el servidor RADIUS en respuesta a un paquete “Access-Request”, en caso de que uno de los atributos no sea aceptado. Un servidor RADIUS envía este mensaje ya sea porque las credenciales no son

auténticas o por que el intento de conexión no está autorizado, el valor del campo código será 3.

Accounting-Request: Es un paquete enviado por el cliente RADIUS para especificar información de la cuenta para la conexión que fue aceptado. El valor del campo código en el paquete será de 4.

Accounting-Response: Es un paquete enviado por un servidor RADIUS en respuesta a un mensaje Accounting-Request. Este mensaje reconoce el procesamiento y recepción exitosa de un mensaje de Accouting-Response. El valor del campo código en el paquete será de 5.

Access-Challenge: Es un paquete enviado por un servidor RADIUS en respuesta a un mensaje “Access-Request”. Este mensaje es enviado cuando se desea que el usuario conteste a un reto. Si este tipo de paquete es soportado, el servidor pide al cliente que vuelva a enviar un paquete Access-Request para hacer la autenticación. En caso de que no sea soportado, se toma como un Access-Reject, el valor del campo código es 11.

Otros de los valores que puede tomar el campo código son:

- Status-Server (experimental), el valor del campo código será 12.
- Status-Client (experimental), el valor del campo código será 13.
- Reserved, el valor del campo código será 255.

Campo Identifier (Identificador): Está formado por un octeto, y es usado para emparejar las peticiones y las respuestas.

Campo Length (Longitud): Está formado por 2 octetos, e indica la longitud del paquete incluyendo los campos código, identificador, longitud, Autenticador y

campos de atributos. Los octetos adicionales al límite indicado por el campo longitud son considerados como relleno y son ignorados al momento de ser recibidos, en caso que el paquete sea menor a la longitud que indica el campo longitud este es descartado, siendo la longitud mínima de 20 y la máxima de 4096 bytes.

Authenticator (Verificador): Está formado por 16 octetos, es utilizado para autenticar la respuesta del servidor RADIUS y es empleado en el algoritmo para ocultar las contraseñas. El autenticado puede ser:

- Autenticador de requerimiento: El NAS y el servidor RADIUS comparten un secreto, esa clave compartida seguida por el autenticador de requerimiento, los mismos que son pasados por una función hash MD5 de una vía, generando un valor, el cual se hace la función XOR con la contraseña ingresada por el usuario, siendo este resultado colocado en el atributo “User-Password” del paquete “Access-Request”.

- Autenticador de respuesta: El valor del campo autenticador en los paquetes “Access-Accept”, “Access-Reject” y “Access-Challenge” es considerado como respuesta, el mismo que es generada al aplicar una función hash MD5 sobre los campos código, identificador, longitud, autenticador del paquete “Access-Request”, atributos y el secreto compartido.

Campo Attributes(Atributos): Es un campo que contiene información acerca de la información del paquete como el tipo de autenticación a emplearse, autorización, detalles de información y configuración en respuestas o requerimientos.

FUNCIONAMIENTO RADIUS

El proceso de RADIUS empieza cuando un usuario intenta acceder al AccessServer usando RADIUS, de la siguiente manera:

1) Primero se le solicita al usuario que envié su username y password.

2) El username y el password del usuario son encriptados con una llave secreta y enviada a un Access-Request al servidor RADIUS.

3) El cliente ahora envía un mensaje de Accounting-Request (Start) con la información correspondiente a su cuenta y para indicar que el usuario está reconocido dentro de la red.

4) El Servidor responderá con un Accounting-Response, cuando la información de la cuenta es almacenada.

5) El usuario recibirá una de las siguientes respuestas por parte del servidor RADIUS.

    - Aceptado: Si el usuario es autenticado.
    - Rechazado: El usuario no es autenticado por el servidor RADIUS y se le solicita que reingrese sus datos para acceder o denegar el ingreso.
    - Cambios de Password: El servidor RADIUS solicita al usuario que seleccione una nueva contraseña.

6) Una vez que el usuario ha sido identificado puede hacer uso de los servicios proporcionados por la red.

7) Finalmente, cuando el usuario desee desconectarse enviara un mensaje Accounting-Request (Stop) con la siguiente información:

- Delay Time. Tiempo que el cliente lleva tratando de enviar el mensaje.
- Input Octets. Número de octetos recibido por el usuario.
- Output Octets. Número de octetos enviados por el usuario.
- Session Time. Número de segundos que el usuario ha estado conectado.
- Input Packets. Cantidad de paquetes recibidos por el usuario.
- Output Packets. Cantidad de paquetes enviados por el usuario.
- Reason. Razón por la que el usuario se desconecta de la red.

8) El servidor RADIUS responde con un mensaje Accounting-Response cuando la información de la cuenta es almacenada.

A continuación se muestra la secuencia que sigue el protocolo RADIUS:

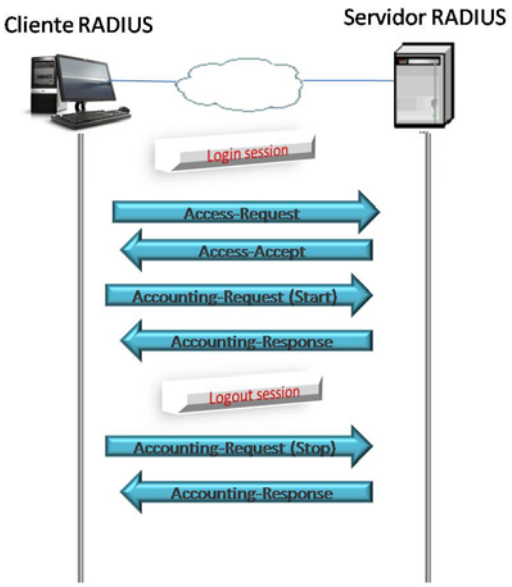


Figura II.11: Secuencia Protocolo RADIUS

2.4.4. FREERADIUS

INTRODUCCIÓN

FreeRadius es un servidor RADIUS de código abierto, rápido, flexible, configurable y con soporte de protocolos de autenticación. Este servidor fue liberado bajo GNU General Public License (GPL), lo que quiere decir que este software es libre de ser descargado e instalado por cualquier persona.

Comenzó como una variante del servidor Cistron RADIUS server, no tienen mucho en común hoy en día tiene muchas más características que Cistron o Livingston y es mucho mas configurable.

FreeRadius es un demonio de autenticación de Internet, el cual implementa el protocolo RADIUS según los RFCs 2865 y 2866. Este servidor permite a los Servidores de Acceso Remoto (NAS) realizar la autenticación para usuarios dial-up. También existen clientes RADIUS para servidores web, firewalls, UNIX logins, por mencionar algunos.

El empleo de un servidor RADIUS permite que la autenticación y autorización para una red sean centralizadas y minimiza la cantidad de reconfiguraciones que deben ser hechas cuando se añaden o eliminan usuarios.

FreeRadius es más que un servidor RADIUS, pues incluye módulos de autenticación PAM y un módulo de autenticación para Apache 1.3 y 2.0. El servidor viene con una herramienta de administración de usuarios llamada Dial-up Admin escrita en PHP. FreeRadius tiene todas las características de un servidor RADIUS distribuido de forma comercial, sin la asociación de costos involucrada.

En la actualidad FreeRADIUS es considerado como la primera fuente abierta del servidor RADIUS y aunque las estadísticas detalladas no están disponibles, se cree que FreeRADIUS está dentro de los cinco servidores RADIUS más usados en el mundo entero. Puesto que es rápido, flexible, configurable, y soporta los protocolos de autenticación más que muchos servidores comerciales.

CARACTERÍSTICAS DEL SERVIDOR FREERADIUS

FreeRadius viene con soporte para bases de datos LDAP, MySQL, PostgreSQL y Oracle. Y soporte de protocolos de autenticación como EAP, EAP-MD5, EAP-SIM, EAP-TLS, EAP-TTLS, EAP-PEAP, y Cisco LEAP.

FreeRadius dispone de muchas características de los servidores de autenticación RADIUS, a continuación se redactan las más relevantes.

1) Características de Plataforma

FreeRadius ha sido compilado y se ha probado su funcionalidad en las siguientes plataformas:

- Linux (todas las versiones)
- FreeBSD
- NetBSD
- Solaris

Plataformas en las que es soportado pero no ha sido completamente probado:

- HP/UX
- AIX
- MINGW32, CygWin (Unix-style environment under Windows NT)
- SFU (or Interix, for Windows XP)

2) Soporte de RFCs y Atributos VSA(Vendor Specific Attibutes)

El Servidor viene con soporte completo para los RFCs 2866 y con VSA para alrededor de cincuenta vendedores incluyendo Ascend, Microsoft, Shiva, USR/3Com, Cisco, Livingston, Versanet, Acc/Newbridge por mencionar algunos.

3) Atributos de Configuración Adicionales del Servidor FreeRADIUS

El servidor RADIUS tiene un número de atributos de configuración, los mismos que permiten controlar casi cualquiera de los requerimientos RADIUS entrantes. Se puede emplear estos atributos de la siguiente manera:

- Ligar atributos a requerimientos
- Reescribir algún atributo del requerimiento
- Replicación de requerimientos a otro servidor RADIUS
- Poder escoger el método de autenticación a ser usado con cada uno de los clientes.
- Administrar a los usuarios por grupos
- Implementar restricciones de acceso por hora del día
- Ejecutar un programa local
- Limitar el número de sesiones simultáneas por usuario.

Todos estos atributos pueden ser usados en solicitudes de autenticación (Authenticate-Request) o solicitudes de auditoría RADIUS (Accounting-Request). Siendo esta una de las ventajas del servidor FreeRADIUS frente a otros que generalmente permiten manejar estos atributos solo en el requerimiento de autenticación.

2.5. Protocolos de Seguridad de la WIFI

2.5.1. SEGURIDAD DE LAS REDES INALÁMBRICAS

Hoy en día las redes inalámbricas se están convirtiendo poco a poco en parte esencial de las redes LAN tradicionales, como se conoce la implantación se está realizando a mayor velocidad en entornos domésticos, así mismo en PYMES como también en las grandes empresas donde requieren amplia movilidad para su trabajo, pero este mercado está menos concienciado de los problemas de seguridad, donde un punto de acceso a la red inseguro podría acarrear graves problemas en estos lugares.

Se puede decir que cualquier equipo que se encuentre a 100 metros o menos de un punto de acceso, podrá tener acceso a la red inalámbrica.

Se puede destacar algunos métodos para lograr una configuración segura de la red inalámbrica donde cada uno de estos métodos logra un distinto nivel de seguridad presentando las ventajas y desventajas de cada una de ellas.

Filtrado de Direcciones MAC

Esta es una de las opciones de autentificación adicional, que brindan muchos puntos de acceso en la cual solo se permite la conexión de las tarjetas de red identificadas a partir de su dirección MAC. Este tipo de seguridad es fiable para entornos pequeños debido a que en cada uno de los puntos de acceso se crea una tabla con cada una de las direcciones MAC de las máquinas asociadas a la red, pero la desventaja vendría si estas tablas habrían de configurarse en un nivel mayor de puntos de acceso ya que:

- No sería escalable ya que al momento de tener configurada una dirección MAC en cada uno de los puntos de acceso, al dar de baja a esta dirección,

habría que acceder a cada una de las tablas para eliminarla, lo cual se tornaría tedioso si existieran numerosos puntos.

- Debido a que las redes inalámbricas se propagan de manera libre sin cifrado por el aire, cualquier persona que conozca de la rama podría atacar a la red capturando una de las tantas direcciones empleando software como Airjack 6 o Wellenreiter, de esta manera asignarle una de ellas a su computador por medio de software específico, de este modo el atacante puede hacerse pasar por un cliente válido.

Se debe tomar en cuenta que este tipo de seguridad no garantiza la confidencialidad de la información transmitida por lo que no provee ningún mecanismo de cifrado.

Wired Equivalent Privacy (WEP)

Siempre en una red inalámbrica cabe la necesidad de transmitir información por radio de forma segura frente a la pérdida de confidencialidad, viendo que existen muchos intrusos en la red que pueden capturar dicha información, es por ello que hay que hacer uso de encriptación en este caso el método más conocido es el sistema de encriptación WEP, pero aquí se analizará por qué este protocolo provee de un mecanismo de encriptación débil, siendo considerablemente sencillo descubrir la clave de encriptación

Características

- Forma parte de la especificación del estándar 802.11.
- Opera en el nivel 2 del modelo OSI (Subcapa MAC).
- Soportado por una amplia mayoría de fabricantes de soluciones inalámbricas.

- Utiliza el algoritmo de Encriptación RC4.

Funcionamiento

- Existe una clave secreta compartida entre emisor y receptor que puede tener un valor de 40 o 128 bits.
- A la trama que se quiere enviar, se le aplica un código de integridad denominado “Integrity Check Value” (ICV), mediante el algoritmo CRC-32. Este código va a actuar como “checksum”, para asegurarse que lo recibido corresponde exactamente con lo que envió el emisor, es decir, la trama no ha sido modificada durante su trayecto.
- Luego de esto, se concatena la clave secreta con un número aleatorio llamado vector de Inicialización (IV), que tendrá una longitud de 24 bits. Si utilizáramos siempre una misma clave para cifrar las tramas, dos tramas iguales darían lugar a tramas cifradas similares. Esto ayudaría a cualquier intruso, a descifrar los datos sin conocer la clave secreta, por ello, este vector irá cambiando en el envío de cada trama.
- El algoritmo de encriptación RC4 dispondrá de dos entradas; por una parte la clave secreta + IV (semilla) y por otra parte los datos modificados con el código de integridad (cola CRC-32). Dicho algoritmo, basándose en un proceso de XOR bit por bit generará la trama cifrada.
- Se enviará al receptor la trama cifrada (datos + CRC) junto con IV e ICV sin encriptar.
- El receptor utilizará la clave secreta que tiene compartida con el emisor, junto con el IV enviado para generar la semilla. Por medio de la semilla calculada y el algoritmo RC4 se generará la trama en claro junto con el ICV.

- Por último, el receptor calculará el ICV de los datos recibidos, y lo comparará con el ICV recibido, y si no concuerdan, descartará tanto a la trama como al emisor de la misma.

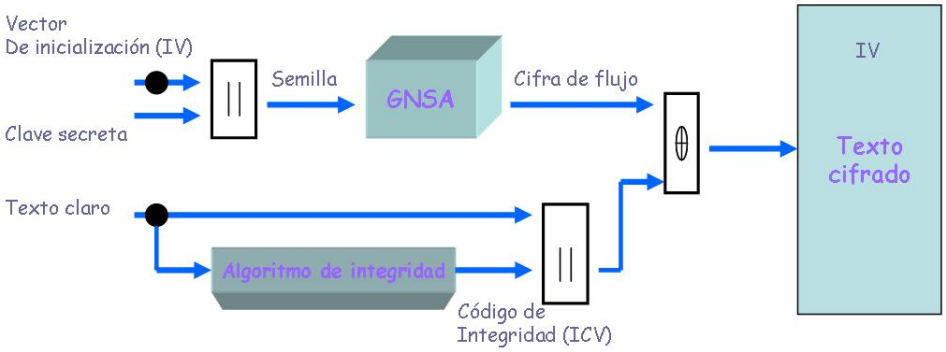


Figura II.12: Muestra el funcionamiento del algoritmo WEP

Problemas

- La clave secreta compartida entre las estaciones que intercambian tráfico posee varios problemas:
  - Utilización de clave estática no modificada.
  - La modificación de esta clave estática debe hacerse de forma manual.
  - El password del administrador es directamente la clave por ello ésta puede ser fácilmente descubierta por ataques de diccionario.
  - Todas las estaciones que comparten el AP utilizan la misma clave.
  - De esta manera resulta bastante sencillo romper la clave ya que existe varias cantidades de tráfico cifradas con la misma clave.
- El IV utilizado es de longitud insuficiente (24 bits). El número total de vectores de inicialización será entonces 2^{24}. Esto quiere decir, que en una red con alto tráfico (recordando que se utiliza un IV distinto por cada trama enviada) el espacio de IV distintos se agotará en un plazo

relativamente corto de tiempo, de modo que la captura de dos tramas con un mismo IV no será demasiado improbable, esto hace que con métodos estadísticos se pueda obtener el texto en claro de una trama, aplicando el algoritmo RC4, se pueda llegar a descubrir la clave secreta entre las dos estaciones.

- También existen problemas con el código de integridad (ICV). Dicho código sirve para solucionar algunos de los problemas del medio de transmisión, pero no permiten evitar modificaciones maliciosas, cambiando ciertos bits de datos y calculando los cambios del CRC-32 para mantenerlo coherente.

WIFI Protected Access (WPA)

Se puede ver que el protocolo WEP tiene más puntos en su contra que a favor, ya que constituye un mecanismo muy débil de cifrado y puede servir tan solo en redes domésticas o en pequeñas oficinas, pretendiendo así usar un mecanismo más robusto para proteger la transmisión de manera profesional, por ello nace el Estándar WPA, mejorando el cifrado de los datos y ofreciendo adicionalmente un mecanismo de autentificación.

Características

- Propuesto por los miembros de la Wi-Fi Alliance en colaboración con la IEEE.
- Basado en el protocolo para cifrado TKIP.
- La longitud de las claves pasa de 40 a 128 bits y el vector de inicialización, de 24 a 48 bits.

- La clave es generada de forma dinámica para cada usuario, para cada sesión, y para cada paquete enviado, así como la distribución de claves que también es realizada de forma automática.
- El mecanismo de autentificación basado en WPA emplea 802.1x/EAP.

Funcionamiento

Antes de empezar a detallar el funcionamiento del protocolo WEP, se analizara el funcionamiento del protocolo TKIP.

- Basado en el algoritmo “Michael” para garantizar la integridad.
- Genera un bloque de 4 bytes (MIC) a partir de la dirección MAC de origen, de destino, y de los datos.
- Añade el MIC calculado a la unidad de datos a enviar.
- Posteriormente los datos se fragmentan y se asigna un número de secuencia.
- La mezcla del número de secuencia con la clave temporal, genera la clave que será utilizada para cada fragmento.

Después de detallar el TKIP se va a definir el mecanismo de autentificación que incorpora WPA y que supone una mejora con respecto a WEP.

Como se ha señalado anteriormente el mecanismo de autentificación emplea el estándar 802.1x y EAP.

Se tendrá 2 modos de autentificación basados en estas especificaciones, dependiendo de la modalidad en la que opere el punto de acceso.

- MODALIDAD RED EMPRESARIAL : En este caso se emplean los métodos soportados por EAP y se precisa de la existencia de un servidor

RADIUS, esta modalidad se la utiliza en redes considerablemente grandes, donde se precisa de una cierta infraestructura, esta modalidad se basa en la existencia de 3 componentes:

- Solicitante -> Se encuentra en la estación inalámbrica.
- Autenticador -> Se encuentra en el punto de acceso.
- Servidor de autenticación o servidor RADIUS.

El autenticador, va a crear un puerto lógico por cliente, y una vez el solicitante entra dentro del radio de cobertura del Punto de acceso, dicho punto de acceso creará un puerto para el solicitante y mientras el cliente no se haya autenticado solo se permitirá trafico 802.1x/EAP hacia el servidor de autenticación bloqueando el resto del tráfico. La autenticación del cliente pasa por varias fases:

- El cliente envía un mensaje “EAP Start”.
- El autenticador responde con un mensaje “EAP Request Identity” para obtener la identidad del cliente.
- El solicitante responde con “EAP Response” donde indica su identificador.
- El Autenticador reenviará la petición al servidor de autentificación (RADIUS).
- El cliente y servidor RADIUS pasarán a comunicarse directamente a partir de este momento, utilizando cierto algoritmo de autenticación negociado entre los dos.
- Una vez aceptada la autentificación del cliente por el servidor de autenticación, el PA (Autenticador) pasará el puerto asignado inicialmente al cliente, a un estado autorizado donde no se impondrán las restricciones de tráfico existentes inicialmente.

Los métodos de autenticación definidos en WPA (EAPTLS, EAP-TTLS y PEAP) se basan todos en la infraestructura de clave pública PKI tanto para autenticar al usuario, como al servidor de autentificación empleándose certificados digitales sujetos a la existencia de una autoridad de certificación (CA) de confianza que emita certificados para usuarios y para servidores de autentificación.

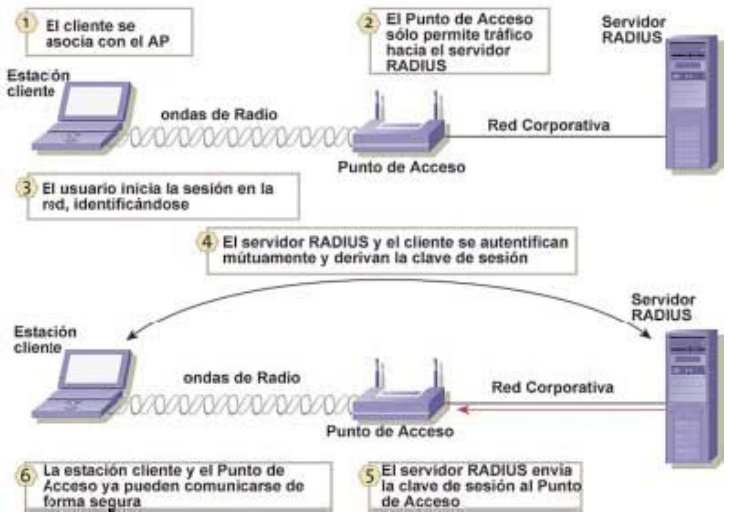


Figura II.13: Proceso de Autenticación WEP

- MODALIDAD DE RED CASERA: También llamada PSK (Pre- Shared Key) utilizada cuando no se dispone de servidor RADIUS. La solución adoptada entonces, es introducir una contraseña compartida entre los clientes y el PA. De este modo solo podrán acceder al punto de acceso, las terminales cuya contraseña coincida con la del punto de acceso. Una vez realizada la autenticación TKIP, entra en funcionamiento para garantizar la seguridad de acceso.

2.6. Vulnerabilidades de la Red Inalámbrica

Tanto las redes cableadas como las inalámbricas sufren de distintos tipos de vulnerabilidades, las redes cableadas son comúnmente atacadas por usuarios internos propios de la red pero las redes inalámbricas son aún más vulnerables debido a la

propagación de la señal por todas las direcciones, es ahí donde no se sabe que dicha señal llegó a un usuario malintencionado que desea acceder a nuestra red sea como sea, por esta razón se va a analizar los tipos de ataque más conocidas a las redes inalámbricas.

Principalmente la vulnerabilidad más conocida por todos es el spoofing que hacer referencia a al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o simplemente de investigación.

Como se ha visto anteriormente, el spoofing es el más conocido de los ataques a las redes inalámbricas, ahora se verá cómo pueden actuar otros tipos de ataques

2.6.1. Access Point Spoofing.

Access Point Spoofing o comúnmente llamado Asociación Maliciosa, el atacante se hace pasar por un access point y el cliente piensa estar conectándose a una red WLAN verdadera. Ataque común en redes ad-hoc.

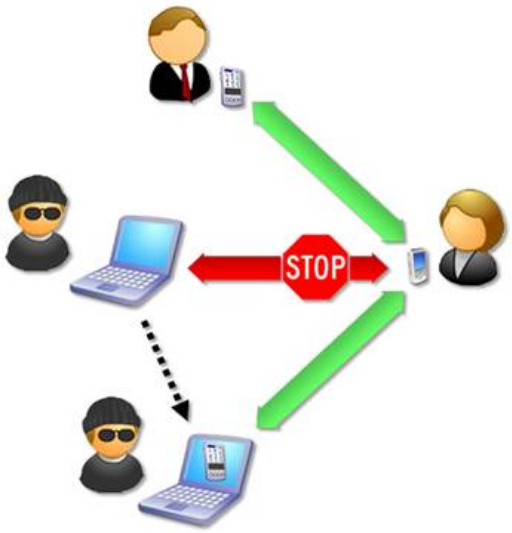


Figura II.14: Access Point Spoofing

2.6.2. ARP Poisoning

ARP Poisoning o "Envenenamiento ARP", ataque al protocolo ARP (Address Resolution Protocol) como el caso de ataque denominado "Man in the Middle" o "hombre en medio". Una computadora invasora X envía un paquete de ARP reply para Y diciendo que la dirección IP de la computadora Z apunta hacia la dirección MAC de la computadora X, y de la misma forma envía un paquete de ARP reply para la computadora Z diciendo que la dirección IP de la computadora Y apunta hacia la dirección MAC de X. Como el protocolo ARP no guarda los estados, las computadoras Y y Z asumen que enviaron un paquete de ARP request solicitando esta información, y asumen los paquetes como verdaderos. A partir de este punto, todos los paquetes enviados y recibidos entre las computadoras Y y Z pasan por X (hombre en medio).

2.6.3. MAC Spoofing

MAC Spoofing o "enmascarar el MAC", ocurre cuando alguien roba una dirección MAC de una red haciéndose pasar por un cliente autorizado. En general, las placas de redes permiten el cambio de lo numero MAC por otro, lo que posibilita este tipo de ataque.

2.6.4. Denial of Service

Denial of Service o "Negativa de Servicio", también conocido por D.O.S. Consiste en negar algún tipo de recurso o servicio. Puede ser utilizado para "inundar" la red con pedidos de disociación, imposibilitando así el acceso de los usuarios, pues los componentes de la red se asocian y desasocian una y otra vez. Al rechazar algún servicio, también puede dar origen a interferencias por equipamientos de Bluetooth, hornos de microondas y teléfonos inalámbricos, debido a que estos equipamientos trabajan en la misma franja de frecuencia que las redes inalámbricas .

2.6.5. WLAN escanners

WLAN Escáners o "Ataque de Vigilancia", consiste en recorrer un local que se desea invadir para descubrir redes WLAN activas en dicho local, así como equipamientos físicos, para un posterior ataque o robo.

2.6.6. Wardriving y Warchalking

Se llama de "Wardriving" a la actividad de encontrar puntos de acceso a redes inalámbricas, mientras uno se desplaza por la ciudad en un automóvil y haciendo uso de una notebook con una placa de red wireless para detectar señales. Después de localizar un punto de acceso a una determinada red inalámbrica, algunos individuos marcan el área con un símbolo hecho con tiza en la vereda o la pared, e informan a otros invasores actividad que se denomina "warchalking".

CAPITULO III

3. ESTUDIO DE LAS APLICACIONES PARA IMPLEMENTAR PORTALES CAUTIVOS

3.1. Análisis de Aplicaciones

3.1.1. WIFIDOG

DEFINICIÓN

Figura III.15: Identificación Wifidog

Wifidog fue diseñado como un reemplazo de otras soluciones de portales cautivos que no se ajustaban a las necesidades de los grupos de la próxima generación, una solución que sea amigable para cada persona que lo use, y que sea lo más práctico al usarlo, que no use pop-ups, ningún software cliente y que use una gestión centralizada, con el objetivo de ser uno de los portales cautivos que sea base para las soluciones de cada empresa donde se lo aplique.

WifiDog es un portal cautivo de código abierto integrable, es utilizado para crear puntos de acceso inalámbrico, fue creado y concebido por el equipo técnico de Ile Sans Fil.

Wifi Dog posee un paquete muy completo de autenticación vía portal cautivo, en muy poco espacio esto es generalmente 30Kb, no requiere de una ventana emergente ni de soporte javascript lo que le permite trabajar en una amplia variedad de dispositivos inalámbricos.

CARACTERÍSTICAS

Entre las principales características de WifiDog están:

- Es un portal que permite a los propietarios de hotspots comunicarse con sus usuarios mediante un sistema de distribución de contenido.

- Funciona en GNU / Linux y dispositivos embebidos Linux, como por ejemplo, Linksys WRT54G con OpenWRT

- Multilingüe de apoyo (a través de la detección del navegador y la selección del usuario) con la posibilidad de añadir más idiomas.

- Soporte para diferentes tipos de puntos de acceso:

  - Splash monomodo: los usuarios son redirigidos a la puerta, pero no tienen que iniciar sesión para utilizar los servicios

- Modo normal: Los usuarios son únicos y deben tener una dirección válida de correo electrónico con el fin de abrir una cuenta.

- Los usuarios pueden crear una cuenta de trabajo directamente desde cualquier hotspot. Los nuevos usuarios se inscriben en cualquier punto de acceso, crean su cuenta y se concede el acceso durante 15 minutos para confirmar un correo electrónico, si no lo hacen serán desconectados y tendrán que inscribirse nuevamente.

- La creación automática de nodo (si la persona que crea el nodo dispone de los permisos pertinentes y la función está activada).

- Informes y estadísticas, incluyendo:
  - 10 consumidores de mayor ancho de banda
  - 10 usuarios más frecuentes
  - 10 usuarios más móviles
  - Desglose de cuántos usuarios utilizan realmente la red
  - Registro de conexión
  - Visualización de contenido con un informe completo
  - Gráfico sobre el uso de la red (por hora, semana y mes)
  - Los informes de usuarios individuales, los nodos más populares (por visita)
  - Información de estado de red
  - Información sobre el estado del nodo
  - Informe de registro de inscripción
  - Informe de registro de usuario.
- Define clases de usuario
- Limitación de ancho de banda por clase
- Limitación de ancho de banda por router

- El bloqueo de puertos por clase
- Aplicar las políticas basadas en la hora del día

Además de todo esto se puede mencionar que WifiDog sobresale entre los demás portales cautivos por aspectos como la ubicación del usuario (georeferencia vía API) a través de google maps, la Autenticación puede ser a través de localuseraccount, LDAP ó RADIUS; lo cual nos indica que su nivel de seguridad es muy sobresaliente.

VENTAJAS

- Estadísticas de uso por usuario
- Soporte de multilenguaje
- La puerta de enlace no ve nunca la contraseñas
- Soporte de Contenido
- Es gratuito
- Trabaja en una amplia variedad de dispositivos inalámbricos.
- Mantiene la conexión comprobando la actividad de la red.
- Monitoreo de la red en tiempo real
- Permite a los usuarios crear cuentas de acceso inalámbrico a Internet usando el acceso para correo electrónico

INCONVENIENTES

- Escasa información
- Vulnerable a la suplantación de dirección MAC

ENTORNO DE TRABAJO

Hay tres componentes involucrados en el protocolo WifiDog, dos de los cuales son parte de la distribución WifiDog estos son: La puerta de enlace, un servidor de autenticación y el tercer componente es el cliente Web.

La puerta de enlace de Wifi-Dog: Está escrita en lenguaje C, sin dependencias más allá del núcleo de Linux, lo que permite incorporarlo en dispositivos tales como WRT54G router que ejecuta OpenWrt, FreeWRT o DD-WRT o más PCs con Linux. La puerta de enlace se instala en menos de 15 Kb en una plataforma i386.

El Servidor de Autenticación: El Servidor de Autenticación de WifiDog está escrito en lenguaje php y utiliza un motor de base de datos PostgreSQL, solución que permite autenticar a los clientes. WiFiDog proporciona autenticación específica de gestión de contenidos del portal, además permite a los usuarios crear cuentas de acceso inalámbrico a Internet usando el acceso para correo electrónico, el tiempo de actividad proporciona estadísticas de puerta de enlace y específicos de la conexión y el registro de estadísticas de usuarios.

Como trabaja WifiDog: La idea básica es que cuando un nuevo usuario se conecta a la red inalámbrica, se abrirá el navegador web para acceder a un sitio Web, la puerta de enlace lo captura y lo redirecciona al servidor de autenticación, el servidor de autenticación de alguna manera autentica al usuario y envía un Token, el servidor de autenticación se redirige de nuevo a la puerta de enlace con un nuevo Token, la puerta de enlace independientemente validará el Token de autenticación que envía el servidor y si es bueno envía al usuario a una página de bienvenida o al sitio Web al que el cliente este tratando de acceder.

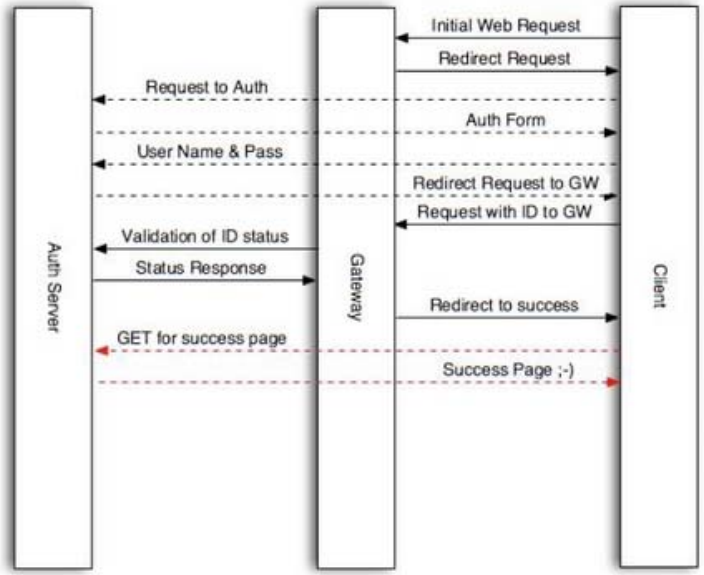


Figura III.16: Componentes de WifiDog

WifiDog posee tres escenarios de administración los mismos que se especifican a continuación:

El primer Escenario es un usuario conectado, cada cierto tiempo la puerta de entrada recorre en interacción con todos los usuarios conectados asegurándose de que ellos siguen activos, recuperando estadísticas y volviendo su Token de autenticación al servidor.

Si el usuario ya no está activo la conexión se cierra y el servidor de autenticación es informado junto con las estadísticas de su uso final, el servidor de autenticación puede también encargar a la puerta de enlace para terminar la conexión de un usuario.

El segundo escenario es un nuevo usuario, es cuando un nuevo usuario ha creado una cuenta pero aún no ha validado su dirección de correo electrónico, este tiene un

número limitado de gracia, toda la transacción se realiza en un escenario por defecto hasta que la validación se realice.

El tercer escenario es el mecanismo Ping en el cual el Gateway envía pings de información periódicamente al servidor de autenticación, el servidor registra la información y devuelve un mensaje, si existe una falta de conexión en la puerta de entrada el servidor lo marca como malo.

REQUERIMIENTOS

Para la instalación del portal cautivo WifiDog se requiere los siguientes elementos:

- GNU/Linux Server
- Linksys WRT54G con OpenWRT

3.1.2. CHILLISPOT

DEFINICION

Figura III.17: Identificación de Chillispot

Es una aplicación para portal cautivo de código abierto y de LAN inalámbrico controlada y escrito en lenguaje C, que funciona con autenticación Web, es decir, garantiza que solo naveguen por Internet usuarios autorizados registrados.

Chillispot está diseñado para autenticar verificando los datos contra una base de datos de credenciales de usuarios tal como RADIUS.

El sistema de autenticación chillispot consta de dos partes principales, una es el demonio Chillispot que se encarga de gestionar los clientes de la subred y pedirles autenticación, la otra consta del servidor radius, freeradius que es quien realiza la autenticación en este caso con la base de datos mysql.

Chillispot crea una interfaz de red virtual que se vale de la interfaz de red física por el cual está conectada a la red inalámbrica mediante la cual habilita su propio servidor DHCP.

Además esta aplicación soporta Wi-Fi Protected Access (WPA y WPA2), autenticación, autorización y contabilidad (AAA), que está a cargo de su servidor Radius.

Chillispot requiere de dos servidores adicionales externamente proporcionados para su funcionamiento los mismos que estarán integrados, estos son:

- Un portal Web donde los usuarios son redireccionados
- Un servidor Radius para autenticación.

Chillispot posee dos componentes principales:

- Una aplicación en el espacio del usuario denominada chilli que es el Portal Cautivo en sí y cumple las siguientes funciones: servidor DHCP, cliente RADIUS, Proxy-RADIUS y Redirector. Maneja ARP y DHCP peticiones de los clientes inalámbricos, las solicitudes de radio de los puntos de acceso, así como redireccionamiento de las peticiones HTTP de usuarios no autorizados.

- Un archivo cgi en el servidor web llamado hotspotlogin.cgi, que no es más que un script programado en lenguaje perl que se encarga de enviar los datos de autenticación a nuestro portal cautivo. Este script genera un protocolo de autenticación llamado desafío-CHAP para validar el usuario y la clave de acceso del cliente, a través del servidor web cifrado con el protocolo de seguridad HTTPS y es el enviado al chilli.

MÉTODOS DE AUTENTICACIÓN

Chillispot soporta dos métodos de autenticación estos son:

UAM (Método de Acceso Universal): Con este método el cliente solicita una dirección IP al punto de acceso inalámbrico, y el software chillispot se encarga de otorgar una dirección IP, al momento que el usuario inicia una búsqueda en un navegador web, Chillispot redirige el navegador a un servidor web de autenticación, donde el usuario debe ingresar sus credenciales las mismas que serán encriptados y enviadas a Chillispot, si son correctas podrá acceder a la red.

WPA (Wireless Protected Access): En este método, el punto de acceso inalámbrico realiza la autenticación del usuario, la misma que es enviada a Chillispot, si es correcta accede a la red, con el método de autenticación WPA/RSN, Chillispot soporta la asignación de IP a través de atributos RADIUS, funcionando como proxy.

Tanto UAM Y WPA remiten la solicitud de autenticación a un servidor RADIUS, el mismo que envía la confirmación o denegación del acceso a la red.

CARACTERÍSTICAS

- Chillispot soporta (AAA) Autenticación, Autorización y Registro contra un servidor Radius.

- Es compatible con dos métodos de autenticación UAM (Universal Access Method) y WPA/RSN (Wireless Protected Access)

- Posee un servicio DHCP propio para ambos métodos de autenticación.

- La autenticación con UAM soporta SSL

- Soporta cualquier AP.

- Puede utilizarse para la autenticación de usuarios en redes cableadas

- Puede actuar como Proxy-RADIUS para otros métodos de autenticación.

- Soporta scripts de inicio y final de conexión para cada cliente.

- Funciona utilizando NAT o Routing

- Permite el uso de atributos RADIUS WISPr definidos por la WIFI Aliance

- Realiza diferentes controles a través de los valores de los atributos RADIUS de los diccionarios wispr y chillispot, lo que permite controlar los volúmenes de tráfico entrante/saliente de un usuario en particular, realizar controles de ancho de banda, etc.

VENTAJAS

- Es Open Source: Software Libre es decir puede ser modificado o adaptado a sus necesidades.
- Fácil Instalación
- Fácil Administración de usuarios
- Fácil Control ancho de banda y recursos
- Es gratuito
- Administración sencilla.
- Facilidad de Información
- Plan Tarifario para locales comerciales
- Control de tiempo del servicio

INCONVENIENTES

- Uso de pop-up
- Dependencia del Administrador para creación de usuarios
- No es compatible con todos los navegadores ya que requiere de soporte HTTPS.

FORMA DE TRABAJO

Chillispot toma el control de la interfaz interna utilizando un módulo vtun del kernel para mostrar una interfaz virtual (tun0). De hecho el módulo vtun del kernel se utiliza para mover paquetes IP desde el núcleo al modo usuario, de tal manera que chillispot puede funcionar sin ningún tipo de módulos no estándar del núcleo (kernel).

Chillispot entonces crea un servidor DHCP (esto se puede desactivar desde el archivo conf de chillispot) en la interfaz tun0. Cuando un cliente no autenticado

intenta conectarse a una página web por el puerto 80 o 443, la petición es interceptada por chilli y desviado hacia un perl-script llamado hotspotlogin.cgi.

Hotspotlogin.cgi ofrece una página para el usuario final con un nombre de usuario y contraseña, estos son los datos de autenticación para el servidor FreeRADIUS, que coincide con la información del "backend" (utilizando ya sea PAP o CHAP). El radius podría ser cualquier servicio tal como LDAP, Kerberos, Radius con mysql, unix passwd o incluso archivos de Active Directory.

Un usuario es rechazado o autenticado al FreeRADIUS, y entonces el hotspotlogin.cgi nos presenta ya sea un mensaje de rechazo o una página con un mensaje de éxito y un enlace para cerrar la sesión del usuario.

REQUERIMIENTOS

Los requerimientos para la instalación y correcto funcionamiento de Chillispot son:

- PC con Linux + 2 tarjetas de red (eth0 y eth1).
- Chillispot
- FreeRADIUS
- Servidor Web, Apache
- MySQL
- Soporte ssl para el servidor web
- Access point inalámbrico o Router Inalámbrico.

3.1.3. NOCAT

DEFINICION

Figura III.18: Identificación de Nocat

NoCat fue desarrollado por la comunidad Wireless de Sonoma Country- Schuyler Erle- California (EEUU), captura las peticiones de los usuarios a una web, comprueba las credenciales del usuario y máquina contra una base de datos, y mantiene la sesión mientras el usuario este autenticado.

También es un portal cautivo que provee a los usuarios de una red abierta con información y la política de uso aceptable. NoCat provee una página de ingreso modificable, donde se solicita a sus usuarios presionar el botón de “registro” antes de utilizar la red para identificar los operadores de la red y mostrar las reglas de acceso a la misma, está escrito en lenguaje PERL y correr en casi cualquier sistema operativo tipo Unix incluidos Linux, BSD.

NoCat puede funcionar de la siguiente manera:

- Portal Pasivo (Passive Portal): Como un portal cautivo pero se usa cuando hay un Firewall entre el AP y el Gateway de NoCat, se le solicita al usuario que ingrese el nombre y contraseña, es decir, el usuario tiene que estar autenticado para obtener determinados derechos de acceso.

- Portal Abierto (Open Portal): Simplemente muestra una web con las condiciones de uso, no requiere de credenciales, un usuario está obligado a aceptar las políticas establecidas de uso antes de tener acceso.

Componentes de NoCat:

- NoCat Auth: Servicio de autenticación.
- NoCat Gateway: Servicio de redirección y firewall.
- Auth DataBase: Posee un fichero propio (MD5), Base de Datos, Ldap, Radius, PAM, Samba, IMAP.
- Access Point

NoCat posee los siguientes tipos de usuario:

- Usuario Público: Puede ser cualquier usuario que quiera conectarse a Internet. Los usuarios de este tipo tienen servicios restringidos, y pueden tener acceso incluso sin tener acceso y contraseña.

- Usuario Co-op: Es un usuario de la Wireless Community Network, que ha predispuesto credenciales y recibe una velocidad de conexión más que una clase de usuario público, las normas para la adhesión se definen por grupos de la comunidad local y es configurado en el sistema de autenticación. Esta clase de usuarios se concede por más ancho de banda y el acceso a los servicios, ya que se consideran responsables de sus propias acciones.

- Usuario Propietario: se reserva para el propietario de un determinado AP y cualquier otra persona a quien desea conceder acceso, un usuario de este

tipo tiene derechos de acceso completo, utiliza todo el ancho de banda disponible y tiene un uso libre de todos los recursos de red.

CARACTERÍSTICAS

- Autenticación segura basada en SSL (navegador)
- Autoriza mediante usuario contraseña
- Informa de la entrada y salida del usuario en la red
- Añade la implementación e QoS por usuarios y grupos

VENTAJAS

- Es Open Source: Software Libre es decir puede ser modificado o adaptado a sus necesidades.
- Es simple de Configurar
- Es gratuito
- Autenticación (en modo Captive)
- Administración sencilla.
- Traffic Shaping (QoS con CBQ)
- User Friendly: aprendizaje rápido y fácil para los usuarios
- Bajo Costo

INCONVENIENTES

- Comunicación no cifrada (por defecto)
- Implementar VPN: el cliente necesita software específico.
- Vulnerable a la suplantación de dirección MAC
- El cliente requiere de un navegador especifico (Mozilla, Netscape, Opera, Galeon, Konqueror o MSIE) con soporte SSL.

- Spoofing y hi-jacking mientras dura el token temporal
- No existe Perl en sistemas empotrados.
- Se basa en varios paquetes pesados
- Demasiado grande para funcionar en la mayoría de hardware
- Carece de características de monitorización de la red
- No dispone de mecanismos para servir a diferentes contenidos de distintos puntos de acceso.
- Utiliza JavaScript para hacer ping a la puerta de entrada cada cinco minutos.

FORMA DE TRABAJO

El proceso de autenticación que realiza NoCat es el siguiente:

1) El cliente se asocia con un AP y se le asigna un IP

2) El AP reenvía las peticiones al Gateway

3) El Gateway redirige a la página de login del Auth Server

4) La conexión es autenticada vía SSL

5) El Auth Server pide usuario y contraseña al cliente (vía SSL) y la comprueba con Auth Database.

6) Los mensajes de autorización van firmados con PGP/GnuPG, el Gateway utiliza la clave publica del Auth Server

7) Si la autenticación ha sido satisfactoria el Gateway redirige el tráfico a la LAN y/o Internet.

REQUERIMIENTOS

Las necesidades del cliente:

- El cliente requiere de un navegador que puede ser (Mozilla, Netscape, Opera, Galeon, Konqueror o MSIE) con soporte SSL. Esto es independiente del SO no necesita de plugins.
- Tarjeta Wireless
- Cuenta de acceso (para Captive Mode)

Las necesidades del servidor son las siguientes:

- Servidor Web Apache
- Open SSL
- GnuPG
- Perl y módulos de perl correspondiente
- Servidor DNS
- Servidor DHCP (en el AP o en el gateway)
- Servidor para centralizar cuentas de usuarios

3.1.4. ZEROSHELL

DEFINICION

Figura III.19: Identificación ZeroShell

Zeroshell es una distribución de Linux para servidores y dispositivos embebidos que provee de servicios de red, entre ellos su propio portal cautivo. Es un Firewall gratuito que tiene características de equipos complejos de seguridad.

Zeroshell es una distribución ¨Live CD¨, lo que significa que no es necesario instalarlo en el disco duro para que funcione, ya que es capaz de funcionar desde el CD-ROM. En cuanto a su base de datos que contiene información de la red puede ser almacenada en discos ATA, SATA, SCSI y USB, dispone de un sistema de actualización on-line y puede ser descargado para formatos en tarjetas Compact Flash para ser instalados en equipos embebidos.

CARACTERÍSTICAS

Las principales características de ZeroShell son:

- Balanceo de líneas y tolerancia a fallos con conexiones múltiples de Internet.
- Conexiones UMTS y HSDPA utilizando módems 3G
- Servidor de autenticación radius
- Portal Cautivo que permite la validación web para redes, es decir el usuario debe validarse antes de poder navegar libremente por la red, con login y password.
- QoS (Calidad de servicio), permite configurar el tráfico de la red para garantizar un ancho de banda mínimo.
- HTTP Proxy transparente
- Punto de acceso wireless
- Host to LAN VPN. VPN cliente
- Lan to Lan VPN. VPN entre servidores
- Router con rutas dinámicas y estáticas

- Soporte de Lan Virtual
- Filtro de paquetes, incluido el tráfico P2P
- Traducción de direcciones (NAT)
- TCP/UDP Port Forwarding para la publicación de servidores internos
- Servidores DNS multizona
- Cliente PPPoE para la conexión Xdsl
- Cliente DNS dinámico
- Autenticación Kerberos 5
- Autenticación LDAP, NIS y RADIUS
- Sincronización con Active Directory
- Entidad certificadora X509

VENTAJAS

Unas de las principales ventajas de ZeroShell son:

- Soporta balanceo entre varias puertas de enlace con una sola interfaz
- Realiza filtros según protocolo, horas, cantidad de datos y ancho de banda
- Permite guardar distintas configuraciones para realizar pruebas
- Permite pedir autenticación antes de dar acceso
- Soporte DHCP, DNS, Web Proxy, Antivirus
- Implementa Captive Portal para proveer servicios de autentificación web para redes Ethernet e inalámbricas.
- Soporta para NAT
- Incluye servidor de DHCP
- Encapsulado de datagramas Ethernet en túneles SSL/TLS
- Fácil configuración a través de interfaz Web
- Herramientas de diagnóstico

- No requiere instalación en disco duro, ya que se puede correr como LiveCD o desde memoria USB

INCONVENIENTES

Entre los inconvenientes del portal cautivo ZeroShell se pueden mencionar los siguientes:

- No se auto instala en disco duro es necesario seguir un sencillo procedimiento.
- No muestra gráficos en tiempo real por IP conectada
- Para el acceso a algunas funcionalidades es necesario o bien una donación por Paypal o bien realizar una contribución al proyecto.
- Suplantación de la MAC
- Uso de ventanas emergentes

FORMA DE TRABAJO

Una vez instalado Zeroshell se deben realizar algunas configuraciones entre ellas, definir cuál será el lugar de almacenamiento donde se guardarán las configuraciones, estos pueden ser discos o memorias que utilicen como archivos ext3, reiserfs o fat32, entre otros sin necesidad de reformatear a las particiones.

Una vez definido el lugar de almacenamiento se crea la base de datos y se llena un formulario sencillo con información de la base, se establece la interfaz a la que van a ser redireccionados los clientes y se ingresaran manualmente los usuarios a los que se van a permitir hacer uso del servicio.

Esto obligará a los clientes a registrarse antes de poder acceder a la red, es decir, el cliente intenta conectarse a la red pero es redireccionado a una página donde debe ingresar sus datos si desea utilizar el servicio, una vez que sus datos son ingresados y validados correctamente, se mostrará un pop-up con el tiempo que tendrá el servicio el ancho de banda y el costo de la utilización del servicio, este pop-up no debe ser cerrado puesto que este mantendrá la conexión.

REQUERIMIENTOS

Requerimientos Hardware:

- Un procesador a partir de Pentium II o compatible
- 128 Mb de Ram, si se implementan más servicios se requiere más memoria
- Un disco duro de al menos 2 Gb. Puede ser IDE o SCSI
- Una tarjeta de red como mínimo y otra de interfaz, ya sea cable modem, ADSL u otra tarjeta de red.
- Teclado, una tarjeta de video, un monitor y un CDROM estos son necesarios durante el proceso de instalación.

Requerimientos Software:

- Una versión de Zeroshell
- Clientes con sistema operativo Linux o Microsoft Windows XP

CAPITULO IV

4. ANÁLISIS COMPARATIVO DE LAS APLICACIONES PARA IMPLEMENTAR PORTALES CAUTIVOS

4.1. Introducción

Cuando se habla de WIFI se refiere a una de las tecnologías de comunicación inalámbrica más utilizada hoy en día, tanto para grandes empresas como para el público en general, por lo cual se ha visto la necesidad de implementarla en varios lugares públicos tales como aeropuertos, restaurantes, parques, centros comerciales, centros de diversión , museos, etc.

Pero en el uso de las redes inalámbricas corporativas se debe tomar muy en cuenta el tipo de seguridad que se va a usar para proteger la información y rendimiento de la red en la empresa, para la cual se han creado varios tipos de seguridad para redes inalámbricas, una de ellas es el uso de portales cautivos.

En este capítulo se analizarán las características de algunos de ellos, tales como NoCat, WifiDog, ZeroShell y Chillispot para determinar el que mejor se acople a las necesidades de Bonny Restaurant y sus clientes.

4.2. Determinación de Parámetros de Comparación

Los parámetros han sido determinados tomando en cuenta las principales características de cada uno de los portales cautivos anteriormente expuestos, con el objetivo de acoplarlos a las necesidades de Bonny Restaurant, buscando mejorar la administración y seguridad de la red de la manera más fácil, simple y rápida.

En este estudio se realizara un análisis cuanti-cualitativo de las principales características que presentan cada uno de los portales que se van a ser estudiados, los parámetros a evaluar son los siguientes:

OPEN SOURCE

Open source o código abierto en español, es el término con el que se denomina al software distribuido y desarrollado de forma libre, este tipo de código tiene un punto de vista más orientado a los beneficios prácticos de compartir el código que a la parte formal como es el software libre.

Ya que este tipo de código es abierto, de muy buena calidad y a disposición de todo tipo de usuario hay ciertas pautas que debe cumplir como son:

- **Redistribución libre:** La licencia del código abierto no debe de ninguna forma cobrar royalties o cualquier otro tipo de costo.

- **Código Fuente:** El software debe agregar el código fuente y permitir la distribución en la forma de código fuente y compilada.
- La licencia no debe discriminar cualquier tipo de persona o toma de iniciativas específicas.

El gobierno actual apoya el uso de software libre, la liberación de los códigos de los programas desarrollados por órganos oficiales es considerada un bien para la sociedad, realmente la liberación del código fuente de muchos programas genera grandes beneficios a la población, entre los que se destacan, por ejemplo, los programas de educación a distancia.

Los programas mundiales más utilizados que poseen código abierto son:

- Mozilla Firefox
- Linux
- OpenOffice
- Gimp
- Emule

LENGUAJE

EL Lenguaje de programación es un tipo de comunicación diseñado para ejecutar un conjunto de acciones consecutivas en un computador.

Los lenguajes que los equipos usan para comunicarse entre ellos son distintos con los lenguajes de programación; se los conoce como protocolos de comunicación. Se trata de dos conceptos totalmente diferentes. Un lenguaje de programación es muy estricto.

El lenguaje utilizado por el procesador se denomina lenguaje máquina. Se trata de datos tal como llegan al procesador, que consisten en una serie de 0 y 1 (datos binarios).

El lenguaje máquina, por lo tanto, no es comprensible para los seres humanos, razón por la cual se han desarrollado lenguajes intermediarios comprensibles para el hombre. El código escrito en este tipo de lenguaje se transforma en código máquina para que el procesador pueda procesarlo.

Cabe destacar que el primer lenguaje de programación es el ensamblador, siendo muy similar al lenguaje máquina, pero los desarrolladores pueden comprenderlo, este lenguaje depende estrictamente del tipo de procesador utilizado, (cada tipo de procesador puede tener su propio lenguaje máquina), así, un programa desarrollado para un equipo no puede ser portado a otro tipo de equipos, por tanto no tiene la capacidad de usar un programa de software en diferentes tipos de equipos.

En este caso se analizarán los lenguajes de programación en los que fueron desarrollados los portales cautivos, para de esta forma poder estudiarlos y facilitar la configuración y adaptación de la aplicación a la red donde será implantado.

CONECTIVIDAD

La Conectividad a nivel de red es la transmisión electrónica de información ya sea entre computadoras u otros dispositivos de comunicación.

La conectividad que un usuario va a tener con una aplicación, se lo hará mediante algún método de reconocimiento por dicho sistema, en este caso podrá ser mediante un proceso de autenticación de usuario, que no es más que el ingreso de un nombre de usuario y una contraseña, la cual se verificará con el registro del usuario en la base de

datos, si la autenticación fue la correcta, el usuario obtendrá una conectividad directa con las funciones de dicha aplicación.

AUTENTICACIÓN

La autenticación no es más que un proceso de verificar la identidad digital ya sea de un equipo o de un usuario por medio de una petición para conectarse, en la web, la autenticación es un modo de asegurar que el usuario que intenta realizar las funciones de un sistema es de hecho el usuario que tiene la autorización para hacerlo.

La mayor parte de sistemas informáticos y aplicaciones web, mantienen de uno u otro modo una relación de identidades personales (usuarios) asociados comúnmente con un perfil de seguridad, roles y permisos, la autenticación de usuarios permiten a estos sistemas tener la seguridad que los usuarios que se están autenticando, son los encargados de hacer las acciones que cada uno de estos debería realizar, como parámetro principal de este tipo de autenticación es el denominado login.

El mecanismo general de autenticación consta de estos pasos.

1. El usuario solicita acceso a un sistema.
2. El sistema solicita al usuario que se autentique.
3. El usuario aporta las credenciales que le identifican y permiten verificar la autenticidad de la identificación.
4. El sistema valida según sus reglas si las credenciales aportadas son suficientes para dar o no acceso al usuario.

Existen varios métodos de autenticación que están en función de lo que utiliza para la verificación, estos se dividen en 3 categorías.

- Sistemas basados en algo conocido por ejemplo una contraseña.
- Sistemas basados en algo poseído como por ejemplo una tarjeta de identidad.
- Sistemas basados en una característica física como por ejemplo huellas digitales, verificación de voz o escritura, etc.

REQUERIMIENTOS DE INSTALACIÓN

Los requerimientos de instalación son las características que debe poseer tanto el hardware como software para poder soportar y/o ejecutar una aplicación o un dispositivo específico, los requisitos necesarios que deben estar instalados en el equipo servirán para el correcto funcionamiento del sistema como por ejemplo, velocidad de Procesador, versión del Sistema operativo, etc.

CONFIGURACIÓN

La configuración en un sistema es un conjunto de datos que determina el valor de algunas variables de un programa.
En las aplicaciones estudiadas, se definen 2 tipos de configuraciones:

Configuración Predeterminada Es la que no se ha definido aún, no es la más recomendada ya que por ese motivo se da la posibilidad que el usuario pueda modificarla, este tipo de configuración fue realizada para que usuarios de todas las edades y ambos sexos puedan usar la aplicación.

Configuración Personalizada Es la que se define especialmente por el usuario, guardada especialmente en una base de datos o en texto plano para que solamente el usuario pueda modificarla al momento de instalar o usar el sistema.

PORTABILIDAD

La portabilidad se define como la característica que posee un software para ejecutarse en diferentes plataformas, el código fuente del software es capaz de reutilizarse en vez de crearse un nuevo código, cuando el software pasa de una plataforma a otra, a mayor portabilidad menor es la dependencia del software con respecto a la plataforma lo cual reduce costos y tiempo.

Se habla de una aplicación portátil o más conocido como "portable" es una aplicación informática que puede ser utilizada en cualquier ordenador que posea el sistema operativo para el que fue programado sin instalación previa; esto significa que no es necesaria la instalación de bibliotecas adicionales en el sistema para su funcionamiento.

SEGURIDAD EN LA COMUNICACIÓN

Se puede hablar de seguridad en la ausencia de riesgo o la confianza en algo, en informática consiste en asegurar que los recursos de un sistema ya sean datos o información personal sean utilizados de la manera que se decidió, que el acceso así como su modificación, solo se lo haga a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Todas las aplicaciones trabajan en Internet, por lo que es necesario indicar los tipos de seguridad que se utiliza en la red.

- **Gestión de Claves (**Incluyendo negociación de claves y su almacenamiento**)** Antes de que el tráfico sea enviado o recibido, cada elemento activo de la red como un router, un firewall o un servidor debe ser capaz de verificar la identidad de su interlocutor.

- **Confidencialidad** La información debe ser manipulada de tal forma que ninguna persona que intente ver o atacar la red lo pueda leer, este servicio se lo puede hacer gracias al cifrado de la información mediante claves conocidas.

- **Imposibilidad de Repudio** Esto garantiza que el emisor de un mensaje, no podrá negar haberlo enviado, y el receptor no podrá negar haberlo recibido.

- **Integridad** Esta garantiza que la información no ha sido modificado en el tránsito emisor-receptor.

- **Autenticación** Confirma que tanto el emisor como el receptor son quienes dicen ser.

- **Autorización** Se trata de un mecanismo que permite que un usuario pueda acceder a servicios o realizar actividades conforme a su identidad.

Las aplicaciones de portales cautivos fijan su seguridad en la autenticación y en el cifrado, en este caso tratan de mejorar la seguridad de comunicación de la aplicación, uno de los más usados es el **SSL** (Secure socket Layer), que implementa un protocolo de negociación para establecer una comunicación segura a nivel de socket (nombre de máquina más puerto), de forma transparente al usuario y a las aplicaciones que lo usan.

MONITOREO DE LA RED

El monitoreo de Red describe el uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos que puedan hacer o causar daño a la red para luego informar sobre estas fallas a los administradores.

El monitoreo de red es muy diferente a un sistema de detección de intrusos ya que mientras éste monitorea la red por amenazas del exterior, un sistema de monitoreo de

red busca problemas causados por la sobrecarga y/o fallas en los servidores como también problemas en la infraestructura de red.

Existen muchas ventajas de monitorear la red en una aplicación de portal cautivo ya que obtiene varios beneficios para el usuario, como resultados estadísticos, puntos conectados a la red, informes, y hasta ubicación geográfica de los usuarios conectados al sistema.

MULTILENGUAJE

Un sistema es multilenguaje cuando su interfaz puede ser mostrada a elección del usuario en cualquiera de diferentes idiomas.

El Internet posee varias aplicaciones que muestran el idioma dependiendo del lugar donde lo estén visualizando, un ejemplo muy claro es GOOGLE, que posee un motor de búsqueda multilenguaje, y que muestra su página y los resultados con el idioma del lugar donde se realice dicha búsqueda.

CALIDAD

Cuando los usuarios están interesados en qué tan bien el sistema puede trabajar, es decir, facilidad de uso, la rapidez con el sistema reacciona a los usuarios, peticiones, el número de faltas y el manejo de situaciones excepcionales.

Todos estos requisitos se denominan los atributos de calidad, características que posee el diseño del sistema.

Se dice también que la calidad de servicio (QoS) son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado, permitiendo así brindar un

servicio óptimo para el usuario final, en este caso, verificando que el funcionamiento del sistema sea el indicado.

En este proyecto se analizará la calidad de Servicio por medio de estos atributos tanto para el administrador

- **Mantenimiento** Indica lo fácil que el sistema puede ser corregir un defecto o hacer un cambio en el software.
- **Portabilidad** El esfuerzo necesario para migrar de un entorno operativo de otro.
- **Reutilización** La capacidad del sistema para ser parte de otro proyecto.
- **Capacidad de Prueba** El esfuerzo necesario para encontrar y solucionar un problema.

Estos son los atributos de calidad que se debe tomar en cuenta para los usuarios que usarán el sistema.

- **Disponibilidad** El sistema debe estar disponible 24 horas al día, los 7 días a la semana, es decir en cualquier momento.
- **Eficiencia** Es decir qué tan bien el sistema utiliza el ancho de banda, tiempo de respuesta, la latencia, etc.
- **Flexibilidad** La facilidad con nuevas capacidades que pueden ser agregadas.
- **Integridad** El acceso autorizado sólo a quien debe concederse.
- **Fiabilidad** Nos indica la confianza total en el servicio.
- **Robustez** La estabilidad del sistema, la potente respuesta sobre los errores de los usuarios.
- **Usabilidad** Facilidad de uso, el tiempo empleado para instalar y registrar un punto de acceso, la latencia, facilidad de aprender

FUNCIONALIDAD

Cuando un sistema empieza a trabajar, éste debe ser capaz de funcionar correctamente y permitir que los usuarios puedan utilizar el producto, como el objetivo principal de este proyecto de tesis, es de administrar la seguridad de las red en base a la autenticación y autorización de los usuarios, éste debería trabajar con un estilo amigable al usuario, con facilidades al momento de usar el sistema ya sea en dispositivos inalámbricos como PDA´s o teléfonos con acceso WIFI, permitiendo así que este sistema pueda brindar todas las bondades al momento de la conexión.

4.3. Análisis Cuanti-Cualitativo de los Portales Cautivos NoCat, WifiDog y ZeroShell

El análisis cualitativo se refiere al estudio de las principales cualidades y características de las aplicaciones, en busca de una descripción holística, es decir intenta analizar exhaustivamente, con detalle una determinada aplicación.

A diferencia de los estudios descriptivos, correlacionales o experimentales, más que determinar la relación de causa y efectos entre dos o más aplicaciones, la investigación cualitativa se interesa más en saber cómo se da la dinámica o cómo ocurre el proceso de funcionalidad de la aplicación.

Mientras que el análisis cuantitativo nos permite contabilizar y calificar cada una de las características cualitativas de las aplicaciones para portales cautivos estudiados anteriormente, para lo cual es necesario establecer una tabla de equivalencias que den valor al estudio, las equivalencias que utilizaremos será la siguiente:

TABLA IV.VII: Sistema de evaluación cuanti-cualitativo

Cuantitativa	**0**	**1**	**2**	**3**	**4**
Cualitativa	NO			Medianamente	SI
	No se conoce	Desactualizado	Poco Actual	Actual	Muy Actual
	Bajo	Regular	Buena	Medianamente Buena	Muy Buena
	Baja	Regular	Buena	Medianamente Alta	Muy Alta
	Muy Difícil	Difícil	Medianamente Fácil	Fácil	Muy Fácil
Valor Porcentual	0%	25%	50%	75%	100%

4.3.1. Open Source

WifiDog posee todas las características de un Open Source

Zeroshell es Open Source pero no en su totalidad ya que existen ciertos módulos y funcionalidades que requieren de una donación por paypal para ser adquiridos.

Chillispot es una aplicación para portal cautivo con todas las características de open source.

NoCat es una aplicación con todas las características de un Open Source

TABLA IV.VIII: Valoración del parámetro Open Source

Herramienta	Open Source	Valor
WifiDog	SI	4
ZeroShell	Medianamente	3
NoCat	SI	4
Chillispot	SI	4

Los rangos de valoración se basan tomando en cuenta como Open Source la facilidad de integrar componentes, modificar la apariencia, y adaptar a las necesidades de quien lo utilice. Obteniendo los siguientes resultados:

- WifiDog es 100% Open Source ya que permite modificar, actualizar e integrar componentes para acoplar la aplicación a las necesidades de quien lo utilice.

- ZeroShell es medianamente Open Source con un 75% ya que implementa su funcionalidad como Portal cautivo de forma nativa, y por cuestiones de organización de los creadores de Zeroshell, no se puede descargar todo el software [1], y requiere de una donación por paypal para adquirir ciertos módulos y funcionalidades.

- NoCat es 100% Open Source ya que permite modificar, actualizar e integrar componentes permitiendo mejorar y acoplar la aplicación a las necesidades de quien lo utilice.

[21] http://www.zeroshell.net/license/

- Chillispot es una aplicación para portal cautivo 100% Open Source que es administrable y adaptable a las necesidades de cualquier red, con una configuración.

4.3.2. Lenguaje

Se refiere al lenguaje en el que está desarrollada cada aplicación ya que de esto dependerá la facilidad de modificación y acoplamiento a las necesidades de Bonny Restaurant.

WifiDog está desarrollado en C, el portal principal del Servidor de Autenticación está codificado en PHP y usa una base de datos PostgresSQL.

Zeroshell es una distribución GNU/LINUX basada en Debian, que implementa su propio portal cautivo programado en C.

NoCat existen dos versiones una desarrollada en Perl (NocathAuth) que es la que más se asemeja a las necesidades de Bonny Restaurant y la versión NocatSplash que está desarrollada en C.

Chillispot está desarrollado en C y la autenticación en lenguaje Perl.

Los rangos de valoración se basan en la facilidad, dominio y familiaridad del lenguaje de la siguiente manera:

TABLA IV.IX: Valoración del parámetro Lenguaje

Herramienta	Lenguaje	Valor
WifiDog	Fácil y Actual	4
ZeroShell	Difícil	1
NoCat	Difícil y Desactualizado	1
Chillispot	Muy Fácil y Muy Actual	4

De los resultados obtenidos en la tabla de valoración del parámetro Lenguaje se puede concluir que:

- WifiDog con un 100% es la aplicación que posee un lenguaje de programación fácil de comprender y de conocer ya que es actual, agilitando su modificación y adaptabilidad a las necesidades de la red en la que va ha ser implementada y a los usuarios de la misma.

- Mientras que NoCat con un 25% es una aplicación que posee un lenguaje de programación poco común, desactualizado y difícil de comprender perjudicando su comprensión y el tiempo de modificación de la aplicación.

- ZeroShell como Portal Cautivo a pesar de ser una aplicación desarrollada en lenguaje C, su código se encuentra comprimido en tar.gz y tar.bz2 y ligado al núcleo de Linux es por ello que su clasificación es de Difícil con un 25% de facilidad de comprensión.

- Chillispot es un Portal Cautivo que posee un gran soporte de lenguajes, brindando mayor facilidad para el desarrollador. Es decir es 100% actual y

fácil de implementar, instalar y configurar, ya que los lenguajes que soporta son en su mayoría los más universales en la Web.

4.3.3. Conectividad de Usuarios

Se refiere a la forma en que el portal verifica y mantiene la conectividad de un usuario.

Wifidog mantiene la conexión con los usuarios comprobando actividad en la red.

Zeroshell utiliza la autenticación keberos 5 usa un tercero de confianza o un KDC, el cual consiste de dos partes un servidor de autenticación y un servidor de tickets, además utiliza pop-up para mantener la cuenta activa

NoCat utiliza java scripts para hacer ping a la puerta de entrada cada cinco minutos para mantener la conexión.

Chillispot utiliza una conexión en tiempo real con los usuarios.

La valoración para este parámetro se basa en la seguridad de la red y optimización de recursos:

TABLA IV.X: Valoración del parámetro Conectividad de usuarios

Herramienta	Conectividad de Usuarios	Valor
WifiDog	Bueno	2
ZeroShell	Regular	1
NoCat	Bueno	2
Chillispot	Medianamente Bueno	3

Luego de realizar un estudio del parámetro Conectividad de usuarios de las aplicaciones podemos concluir qué:

- Mediante el estudio realizado del parámetro Conectividad de Usuarios se determinó que WifiDog posee una conectividad buena con un porcentaje de 50%, ya que presenta grandes problemas en seguridad ya que permite que el usuario se cree su propia contraseña, ingrese a grupos, etc.

- Nocat posee un conectividad buena con un porcentaje de 50% es una aplicación que permite llevar un control de los usuarios de la red, sin cuadros estadísticos ni en tiempo real, lo que impide tomar decisiones en tiempo real.

- ZeroShell posee una conectividad regular con un porcentaje de 25% es una aplicación que se basa en un pop-up que debe permanecer activado para mantener la conexión, lo que es algo molestoso tanto para los usuarios como para el administrador ya que los usuarios que cierren el pop-up deben volver a conectarse obligadamente.

- Chillispot es 75% seguro en la conectividad de la red con los usuarios ya realiza un control en tiempo real de los usuarios activos, manteniendo un registro en la página de administración.

4.3.4. Autenticación

Como se menciona en el estudio de portales cautivos existen 3 tipos de portales cautivos los que requieren registrarse, los que permiten acceder aceptando las condiciones de la red y el que combina ambos, para determinar este parámetro se tomó en cuenta el tipo de servicio que se desea dar en el Restaurant Bonny que es un servicio óptimo y controlado a la vez.

WifiDog permite el acceso a la red únicamente si el usuario ha sido registrado mediante (login y password) de usuario.

ZeroShell da el acceso a los usuarios únicamente si estos están previamente creados, es decir el usuario debe tener obligatoriamente un login y password creado.

NoCat permite la conexión a la red únicamente si el usuario ha sido registrado con un login y un password.

Chillispot permite la conectividad a la red únicamente si el usuario esta registrado con un login y un password, usando la autenticación RADIUS.

La valoración de este parámetro se determinó de acuerdo al grado de seguridad de acceso a la red y al control de usuarios de la siguiente manera:

TABLA IV.XI: Valoración del parámetro Autenticación que requiere

Herramienta	Logeo que requiere	Valor
WifiDog	Medianamente Buena	3
ZeroShell	Medianamente Buena	3
NoCat	Medianamente Buena	3
Chillispot	Medianamente Buena	3

De los datos obtenidos del análisis del campo Autenticación de las aplicaciones para portales cautivos se puede concluir que:

- Las cuatro aplicaciones estudiadas WifiDog, ZeroShell, NoCat y WifiDog requieren de un proceso de autenticación similar mediante un login y password, con un porcentaje de 75%, se puede determinar que poseen un proceso de autenticación medianamente bueno, no obtuvieron un 100% debido a que las 3 aplicaciones para portales cautivos son vulnerables a sustitución de MAC.

4.3.5. Requerimientos de Instalación

WifiDog para el correcto funcionamiento de esta aplicación se requiere GNU/Linux server, un router Linksys WRT54G con Open WRT y con DHCP desactivado, el servidor de autenticación requiere también un web server Apache2 y PHP de preferencia la última versión, los requerimientos de Hardware son mínimos es decir una PC con CDROM, Procesador 486 o más avanzado, 32 MB RAM, 1 GB hard disk, 2 x 10/100 Ethernet Cards.

Zeroshell requiere para su funcionamiento una versión de zeroshell y un cliente que puede ser Linux o Microsoft Windows Xp, en cuanto a los requerimientos de Hardware son mínimos con 2 tarjetas de red, grabadora de CDROM y puerto USB.

NoCat requiere para su funcionamiento correcto los siguientes herramientas en el cliente requiere un navegador con soporte SSL, tarjetas Wireless y los requerimientos mínimos de una PC, en cuanto al servidor requiere un Servidor web Apache, Open SSL, GnuPG, servidor DNS, servidor DHCP y un servidor para centralizar cuentas de usuario.

Chillispot es una aplicación para portal cautivo muy sencilla de instalar y configurar, requiere únicamente de un PC con Linux + 2 tarjetas de red. (eth0 y eth1), Chillispot, FreeRADIUS, Servidor web, Apache, MySQL, Soporte ssl para el servidor web, Access point inalámbrico o Router Inalámbrico.

Para determinar el valor de este parámetro se tomo en cuenta la facilidad de instalación, tiempo y acceso a los requerimientos.

TABLA IV.XII: Valoración del parámetro Requerimientos de Instalación

Herramienta	**Requerimientos De Instalación**	**Valor**
WifiDog	Medianamente Fácil	2
ZeroShell	Fácil	3
NoCat	Medianamente Fácil	2
Chillispot	Muy Fácil	4

Mediante el estudio realizado al parámetro Requerimientos de Instalación de las aplicaciones podemos concluir qué:

- ZeroShell es una aplicación fácil de instalar con un valor porcentual de 75%, ya que posee requerimientos mínimos para que su funcionamiento sea adecuado.

- WifiDog con un 50% es una aplicación medianamente fácil de instalar ya que requiere ciertas condiciones como es un router Linksys WRT54G con OpenWRT, pero en cuanto al software posee librerías dispersas, y recursos separados.

- NoCat con un 50% es una aplicación medianamente fácil de instalar, que requiere de un Hardware robusto, y no justifica la inversión el desempeño de la aplicación.

- Chillispot con un 100% es la aplicación más fácil de instalar y configurar requiere de elementos mínimos y configuraciones básicas ya que es a la vez su propio DHCP.

4.3.6. Configuración

WifiDog permite configurar las plantillas html y los archivos css más no el código fuente la misma, además no dispone del archivo wifidog-auth/config.php

Zeroshell es simple de configurar y adaptarlo a nuestras necesidades en cuanto se refiere a los pop-ups, ingreso de usuarios, etc pero no es posible configurar su código fuente.

NoCat es simple de configurar las reglas de uso de la red, ingreso usuarios, diseño de los pop-ups pero no es posible modificar su código fuente.

Chillispot es una aplicación fácil de configurar ya que posee un gran soporte de lenguajes que ayuda a los desarrolladores a acoplar con mayor facilidad la aplicación a sus necesidades.

El valor de este parámetro se ha determinado por la facilidad de modificación en cuanto a la adaptación a las necesidades de la red de Bonny Restaurant más no configuraciones para cambiar la funcionalidad de la aplicación de la siguiente manera:

TABLA IV.XIII: Valoración del parámetro Configuración

Herramienta	Configuración	Valor
WifiDog	Difícil	1
ZeroShell	Fácil	3
NoCat	Fácil	3
Chillispot	Muy Fácil	4

Luego de realizar un estudio al parámetro configuración de las aplicaciones podemos determinar qué:

- WifiDog es 25% Configurable ya que existe escasez de información y procesos incompletos con librerías dispersas que causan problemas en una u otra parte del proceso.

- Tanto ZeroShell como NoCat obtuvieron un 75% puesto que es fácil de configurar ciertos parámetros, la interfaz, condiciones de uso de la red, etc pero no permiten configurar su código fuente en sí.

- Chillispot es 100% configurable ya que brinda todas las herramientas necesarias para su adaptabilidad a cualquier red.

4.3.7. Portabilidad

WifiDog funciona con cualquier plataforma con un navegador web, incluyendo PDAs y teléfonos móviles ya que no posee javascripts.

ZeroShell funciona para todo hardware existente para x86, puede usarse con un navegador Mozilla u otro navegador, Internet Explorer no es recomendable.

NoCat para que su funcionamiento sea el correcto se requiere un navegador especifico Mozilla, Netscape, Opera, Galeon, Konqueror o MSIE con soporte SSL, a demás no posee mecanismos para servir a diferentes contenidos de distintos AP.

Chillispot funciona en cualquier navegador web pero requiere que el pop-up este habilitado, funciona sobre cualquier plataforma incluido PDAs o dispositivos Inteligentes.

Para determinar el valor de este parámetro se tomó en cuenta la portabilidad de la aplicación para plataformas de uso actual como laptop, celulares y PDAs y su funcionamiento en los principales navegadores de mayor uso para los usuarios de la siguiente manera:

TABLA IV.XIV: Valoración del parámetro Portabilidad

Herramienta	Portabilidad	Valor
WifiDog	Muy Buena	4
ZeroShell	Buena	2
NoCat	Buena	2
Chillispot	Muy Buena	4

De los resultados obtenidos en la tabla de valorización del parámetro portabilidad de las aplicaciones podemos determinar qué:

- La aplicación WifiDog es una aplicación 100% portable es decir posee una portabilidad muy buena, ya que funciona y es compatible en cualquier PC, laptop, teléfonos celulares y PDA.

- ZeroShell es una aplicación 50% portable es decir posee una portabilidad buena, puesto que requiere de un determinado tipo de navegador para funcionar, y es totalmente incompatible con Internet Explorer que es uno de los navegadores más utilizados en la actualidad.

- NoCat es una aplicación con una portabilidad buena es decir es 50% portable ya que requiere de un navegador y un AP específico para que su funcionamiento sea correcto.

- Chillispot es una aplicación para portal cautivo 100% portable puesto funciona sobre cualquier navegador web y sobre cualquier plataforma incluido PDAs o dispositivo inteligente.

4.3.8. Seguridad en la Comunicación

WifiDog posee una seguridad SSL para la comunicación del portal, esta opción viene por defecto en la instalación de la aplicación, en cuanto a la contraseña nunca es vista por la puerta de enlace.

ZeroShell posee un encapsulamiento SSL/TLS para guardar la seguridad de la información, pero no posee seguridad de usuario ya que varias personas pueden usar la mismo login y password ya sea de forma simultáneamente o no, provocando así inconsistencia de la red.

NoCat esta aplicación no cifra por defecto pero si posee la opción de SSL.

Chillispot con la autenticación UAM soporta SSL, además lleva un control administrativo de los clientes.

El valor de este parámetro fue determinado tomando en cuenta la seguridad que tienen los datos que son transmitidos en la red, de la siguiente manera:

TABLA IV.XV: Valoración del parámetro Seguridad de Comunicación

Herramienta	Seguridad de Comunicación	Valor
WifiDog	Medianamente Alta	3
ZeroShell	Regular	1
NoCat	Regular	1
Chillispot	Medianamente Alta	3

Al analizar el parámetro Seguridad de comunicación de las aplicaciones se pude concluir qué:

- Wifidog es una aplicación con una Seguridad de Comunicación Alta de 75%, que posee seguridad SSL y protege en todo momento la información de los usuarios, pero da privilegios a usuarios que no deberían tener, como crear sus propias credenciales, ver estadísticas, etc.

- ZeroShell es una aplicación con una seguridad de comunicación buena del 25%, puesto que posee SSL/TLS, pero la facilidad de que los usuarios puedan usar los mismos datos de logeo simultáneamente o no, pone vulnerable a la red ya que no se conocería a ciencia cierta quién está haciendo uso de la cuenta. Además por uso de pop-up para mantener la cuenta activa los usuarios pueden ser víctimas robo o cambios en su información en caso de olvidar su cuenta activa.

- NoCat es 25% Segura en la comunicación es decir posee una seguridad de comunicación regular poco confiable, que no cifra por defecto pero si tiene la opción de activar SSL, y al no cifrar deja a la deriva la información de los usuarios.

- Chillispot es una aplicación 75% segura en la comunicación ya que posee SSL, además el registro de los usuarios es conocido solo por el administrador, es el único capaz de crear usuarios, asignarles cuentas, ver estadísticas, bloquear usuarios, y la conexión permanece abierta hasta que el usuario se desconecte o se le termine su tiempo de uso.

4.3.9. Monitoreo de la red

WifiDog es una aplicación que permite el monitoreo de la red en tiempo real, con estadísticas e informes de la red, sistema de distribución de contenido, multilenguaje y ubicación geográfica de los usuarios conectados mediante google maps.

ZeroShell como portal cautivo permite realizar un monitoreo de red mediante SNMP (es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red) pero no en tiempo real, y con estadísticas básicas.

NoCat carece de características de monitoreo de red y fue descontinuado ya que fue remplazado por WifiDog.

Chillispot permite el monitoreo de la red con cuadros estadísticos básicos, del tiempo de uso de la red por usuario y el ancho de banda utilizado.

Para determinar el valor de este parámetro se tomo en cuenta las bondades que presenta cada aplicación y la veracidad de los datos de la red, de la siguiente manera:

TABLA IV.XVI: Valoración del parámetro Monitoreo de red

Herramienta	**Monitoreo de Red**	**Valor**
WifiDog	Muy Buena	4
ZeroShell	Buena	2
NoCat	Regular	1
Chillispot	Buena	3

Del estudio realizado al parámetro Monitoreo de la red de las aplicaciones para portales cautivos se determinó que:

- WifiDog presenta características de monitoreo de la red muy buenas 100% adaptables a las necesidades de los usuarios ya que muestra estadísticas en tiempo real del uso de la red, permite adaptar el lenguaje de la pantalla de bienvenida al idioma que el usuario requiera, realizar gestión de contenido y brinda la ubicación geográfica del usuario.

- ZeroShell presenta buenas características de monitoreo de red con un porcentaje del 50%, que permiten generar estadísticas básicas pero no en tiempo real, lo que impide conocer a ciencia cierta el estado de la red.

- Nocat posee características de monitoreo de red regulares con un porcentaje del 25%, es decir realiza monitoreo de la red pero no en tiempo real ni presenta estadísticas, fue descontinuado por WifiDog.

- Chillispot con un 75% permite realizar un monitoreo de red mediante estadísticas básicas, tanto del tiempo de uso de la red como del ancho de banda utilizado.

4.3.10. Multilenguaje

WifiDog posee la opción de multilenguaje que permite adaptar el idioma de acuerdo a las necesidades de los usuarios.

ZeroShell no posee la opción de multilenguaje se crea con el lenguaje configurado por el administrador.

NoCat esta aplicación no posee multilenguaje.

Chillispot posee multilenguaje pero para el administrador de la red, los lenguajes que soporta son Inglés, Español e Indonés.

Para determinar el valor de este parámetro se tomo en cuenta la capacidad de la aplicación de permitir adaptar el idioma del portal a las necesidades de cada usuario, de la siguiente manera:

TABLA IV.XVII: Valoración del parámetro Multilenguaje

Herramienta	Multilenguaje	Valor
WifiDog	Muy Alta	4
ZeroShell	Regular	1
NoCat	Regular	1
Chillispot	Medianamente Alta	3

De los datos obtenidos en el análisis del parámetro Multilenguaje de las aplicaciones se puede resumir que:

- WifiDog es una aplicación que posee características de multilenguaje alta ya que permite adaptar el lenguaje de la página de bienvenida de la aplicación a las necesidades del usuario.

- Mientras que ZeroShell y NoCat posee características de multilenguaje regulares ya el usuario está obligando a adaptarse al lenguaje de la aplicación.

- Chillispot es una aplicación con un 75% de multilenguaje ya que incrementa esta característica para 3 idiomas y solo para el administrador no para los usuarios.

4.3.11. Calidad

WifiDog presenta varias características tanto de mantenimiento como de portabilidad, reusabilidad y capacidad de prueba, wifidog presenta gran capacidad de compatibilidad, adaptabilidad, control de usuarios, detección y solución de problemas. En cuanto al usuario brinda un servicio clave para mejorar la calidad de uso de la red.

ZeroShell posee Qos que permite medir los tiempos de respuesta, pérdida de información, calidad de transmisión, etc.

NoCat posee Qos que permite medir los tiempos de respuesta, pérdida de información, calidad de transmisión, etc.

Chillispot es una aplicación que presenta varias características de calidad tales como, reusabilidad, portabilidad, seguridad y además soporta QoS.

Para determinar el valor de este parámetro se tomo en cuenta las facilidades que presenta la aplicación para implementar QoS, de la siguiente manera:

TABLA IV.XVIII: Valoración del parámetro Calidad

Herramienta	Calidad	Valor
WifiDog	Fácil	3
ZeroShell	Fácil	3
NoCat	Fácil	3
Chillispot	Fácil	3

Con los resultados obtenidos en el análisis del parámetro de Calidad se puede determinar qué:

- Tanto WifiDog, NoCat, ZeroShell y Chillispot buscan la calidad, y brindan en un 75% facilidad para implementarla, pero existen condiciones tanto de la arquitectura de la red como de usuarios maliciosos que pueden alterar o cambiar las condiciones de la aplicación.

4.3.12. Funcionamiento

WifiDog es una aplicación amigable y adaptable al uso del usuario, no requiere de ventanas emergentes continuas que molestan y puedan alterar el normal funcionamiento de la red.

ZeroShell es una aplicación que se basa en la presentación de una o varias ventanas emergentes que son indispensables para mantener la conexión activa del usuario.

NoCat requiere de scripts y ventanas emergentes para el correcto desarrollo de la aplicación durante el proceso de conexión a la red, pero no son indispensables para mantener la conexión.

Chillispot es una aplicación para portal cautivo fácil de utilizar y de intuir, ya que muestra una interfaz amigable tanto para el administrador como para el usuario de la red, es fácil de administrar y de configurar, utiliza un pop-up de confirmación o negación de acceso.

Para determinar este parámetro se tomó en cuenta la familiaridad, comodidad y facilidad que presenta la aplicación para el usuario, de la siguiente manera:

TABLA IV.XIX: Valoración del parámetro Funcionalidad

Herramienta	Calidad	Valor
WifiDog	Muy Buena	4
ZeroShell	Regular	1
NoCat	Buena	2
Chillispot	Medianamente Buena	3

Luego del análisis del parámetro Funcionalidad de las aplicaciones se resume que:

- La familiaridad, comodidad y facilidad de uso que presenta WifiDog es muy buena ya que posee un 100% aceptable tanto para los usuarios locales, administradores y externos, ya que brinda varias herramientas y características amigables y útiles para cada uno de ellos.

- ZeroShell es una aplicación con una funcionalidad regular con un 25% de aceptabilidad ya que utiliza recursos incompatibles, e incluso molestosos para el usuario impidiendo así el uso normal de la aplicación.

- NoCat es una aplicación con un funcionamiento Bueno con un 50% de aceptabilidad por parte del usuario ya que posee incompatibilidad y no presenta características que ayuden a las necesidades de los distintos usuarios de la red.

- Chillispot en su funcionalidad es 75% aceptable ya que presenta interfaces amigables para sus usuarios, uso de lenguajes conocidos y fáciles de

comprender y adaptar a las necesidades de cualquier red, su defecto es el uso de pop-up para confirmación de acceso de los usuarios.

4.4. Similitudes y Diferencias entre las aplicaciones para Portales Cautivos Estudiadas

4.4.1. WifiDog vs. ZeroShell

SIMILITUDES

- WifiDog y ZeroShell son aplicaciones de portales cautivos, es decir permiten redireccionar el tráfico a una página especial donde el usuario debe registrarse o aceptar las condiciones de la red para acceder a la misma.

- Ambas realizan un acceso a la red mediante un login y password es decir el usuario debe estar registrado para poder acceder a los servicios de la red.

- Tanto WifiDog como ZeroShell utilizan una seguridad SSL para la comunicación del portal.

- Tanto WifiDog como ZeroShell permiten aplicar Calidad de Servicio que permite dar un mejor servicio para los usuarios.

DIFERENCIAS

- WifiDog posee todas las características de Opens Source mientras que ZeroShell es una distribución de Linux que Implementa una aplicación para portales cautivos de forma nativa.

- Wifidog ha sido desarrollado en C, con el portal principal de Autenticación esta codificado en PHP y una base de datos PostgressSQL, mientras que Zeroshell se basa en Debian pero utiliza dos tipos de programación para su desarrollo C y C++.

- Wifidog mantiene la conexión con los usuarios comprobando la actividad de la red, mientras que ZeroShell mantiene la conexión mediante el uso de keberos 5 y la activación de ventanas emergentes.

- Wifidog requiere para su instalación GNU/Linux server, un router Linksys WRT54G con Open WRT y con DHCP desactivado, el servidor de autenticación requiere también un web server Apache2 y PHP de preferencia la última versión mientras que ZeroShell es una distribución Live CD de Linux.

- WifiDog da la posibilidad a los usuarios de adaptar el portal al idioma que requiera, es decir posee multilenguaje mientras que ZeroShell no.

- WifiDog permite configurar las plantillas html y los archivos css mientras que Zeroshell no permite personalizar completamente el portal de bienvenida y toda su configuración es mediante la Web.

- Wifidog es una aplicación portable es decir funciona sobre cualquier plataforma mientras que ZeroShell requiere de una plataforma especifica esta puede ser Mozilla u otra plataforma que no sea Internet Explorer dado que en la actualidad existen una gran cantidad de dispositivos que son utilizados para acceder a Internet por lo cual se requiere una aplicación portable.

- Wifidog protege la información del usuario durante todo el proceso de comunicación mientras que ZeroShell no protege la información en la puerta de enlace y puede reutilizar la información con varios usuarios.

- WifiDog no posee Qos pero puede ser implementado mediante plugins mientras que ZeroShell posee Qos por defecto en la instalación.

- WifiDog permite un monitoreo y administración de la red en tiempo real con estadísticas y gráficas exactas, mientras que ZeroShell permite realizar un monitoreo de la red con datos almacenados que no son reales puesto que los usuarios pueden incrementar y decrementar al paso de varios minutos.

- WifiDog brinda a los usuarios un ambiente familiar y sin complicaciones mientras que ZeroShell requiere el uso de una ventana emergente para mantener la conexión es decir el usuario debe mantenerla abierta para no perder su conectividad.

4.4.2. ZeroShell vs. NoCat

SIMILITUDES

- Tanto ZeroShell como NoCat son aplicaciones de portales cautivos, es decir cuando un usuario quiere acceder a la red se ve obligado a registrarse antes de proceder al acceso.

- Ambas realizan un acceso a la red mediante un login y password es decir el usuario debe estar registrado para poder acceder a los servicios de la red.

- NoCat como Zeroshell hacen uso de javascripts y ventanas emergentes y requieren navegadores específicos para su correcto funcionamiento.

- Ambos poseen una seguridad SSL para cifrar la información que se transmite en la red.

- ZeroShell y NoCat poseen Qos que les permite controlar localidad de la transmisión y funcionamiento de la red.

DIFERENCIAS

- NoCat posee todas las características de Opens Source mientras que ZeroShell es una distribución de Linux que posee una aplicación para portales cautivos.

- ZeroShell es una distribución Live CD de Linux que permite implementar un portal cautivo de forma nativa y esta desarrollado en C y C++, mientras que

NoCat está programado en PERL que es un tipo de programación algo obsoleto.

- ZeroShell es una distribución Live CD de Linux mientras que NoCat es una aplicación que requiere que el cliente con soporte SSL, tarjetas Wireless y los requerimientos mínimos de una PC. En cuanto al servidor se requiere un Servidor Web Apache, Open SSL, GnuPG, servidor DNS, servidor DHCP y un servidor para centralizar cuentas de usuario.

- ZeroShell permite configurar de forma gráfica ciertos parámetros, condiciones, etc; pero no su código en si mientras que NoCat utiliza un lenguaje de programación posible de configurar.

- ZeroShell tiene SSL activado por defecto mientras que NoCat se instala con el SSL desactivado y debe ser activado.

- ZeroShell posee varias herramientas de monitoreo de red pero no en tiempo real mientras que NoCat carece de características de monitoreo de red.

4.4.3. WifiDog vs. NoCat

SIMILITUDES

- Wifidog y NoCat son aplicaciones para portales cautivos es decir redireccionan el tráfico para que el usuario deba interactuar con una página web antes de garantizar su acceso a las funciones normales de la red.

- Ambas aplicaciones permiten el acceso a la red únicamente si el usuario ha sido registrado con login y password.

- Tanto NoCat como WifiDog son aplicaciones con todas las características de Open Source.

- Las dos permiten configurar la web del portal, las condiciones, los usuarios, las reglas de la conexión pero no el código en sí de la aplicación.

- WifiDog y NoCat posee SSL para cifrar la comunicación.

DIFERENCIAS

- WifiDog está desarrollado en un lenguaje de programación más sencillo, actual usa C, PHP y PostgressSQL mientras que NoCat utiliza PERL que es un lenguaje de programación obsoleto.

- WifiDog mantiene la conectividad de los usuarios comprobando la actividad de la red mientras que NoCat se basa en java scripts y ventanas emergentes.

- WifiDog es totalmente portable para cualquier plataforma mientras que NoCat no y requiere un navegador específico con soporte SSL.

- WifiDog permite adaptar el idioma del portal a las necesidades de cada usuario, es decir posee multilenguaje mientras que NoCat no.

- WifiDog instala por defecto SSL mientras que NoCat se instala con el SSL desactivado.

- WifiDog posee grandes características para administración y monitoreo de la red en tiempo real mientras que NoCat carece de dichas características.

- WifiDog no posee Qos pero puede implementarse mediante plugins mientras que NoCat se instala por defecto con Qos.

- WifiDog posee un ambiente más amigable para los usuarios mientras que NoCat se basa en varias ventanas emergentes que pueden fastidiar al usuario durante el uso de la red.

4.4.4. Chillispot vs. Zeroshell

SIMILITUDES

- Tanto Chillispot como Zeroshell son aplicaciones de portales cautivos, es decir cuando un usuario quiere acceder a la red se ve obligado a registrarse antes de proceder al acceso.

- Ambas realizan un acceso a la red mediante un login y password es decir el usuario debe estar registrado para poder acceder a los servicios de la red.

- Chillispot como Zeroshell utilizan pop-up para enviar mensajes de conectividad de la red.

- Ambos soportan una seguridad SSL para cifrar la información que se transmite en la red.

- ZeroShell y Chillispot soportan Qos que les permite controlar localidad de la transmisión y funcionamiento de la red.

- Ambas realizan un monitoreo de red pero no en tiempo real.

DIFERENCIAS

- Chillispot posee todas las características de Opens Source mientras que ZeroShell es una distribución de Linux que posee una aplicación para portales cautivos.

- ZeroShell es una distribución Live CD de Linux que permite implementar un portal cautivo de forma nativa y esta desarrollado en C y C++, mientras que Chillispot está desarrollado en C y la autenticación en Perl pero soporta varios lenguajes como PHP, HTML, CGI y Javascripts.

- ZeroShell es una distribución Live CD de Linux mientras que Chillispot es una aplicación que requiere ser instalada en una distribución de Linux.

- ZeroShell permite configurar de forma gráfica ciertos parámetros, condiciones, etc; pero no su código en sí. Mientras que Chillispot presenta grandes ventajas de modificación y adaptabilidad a cualquier red.

- Chillispot es totalmente portable para cualquier plataforma mientras que Zeroshell es compatible con pocos navegadores.

- Chillispot brinda facilidades de control y administración de usuarios mientras que las características de Zeroshell son escasas.

4.4.5. Nocat vs. Chiillispot

SIMILITUDES

- Chillispot y NoCat son aplicaciones para portales cautivos es decir redireccionan el tráfico para que el usuario deba interactuar con una página web antes de garantizar su acceso a las funciones normales de la red.

- Ambas aplicaciones permiten el acceso a la red únicamente si el usuario ha sido registrado con login y password.

- Tanto NoCat como Chillispot son aplicaciones con todas las características de Open Source.

- Las dos permiten configurar la web del portal, las condiciones, los usuarios, las reglas de la conexión pero no el código en sí de la aplicación.

- Chillispot y NoCat soportan SSL para cifrar la comunicación.

DIFERENCIAS

- Chillispot es una herramienta muy versátil en cuanto al soporte de lenguajes lo que facilita su comprensión y agilitan el tiempo de adaptabilidad a cualquier red, mientras que NoCat utiliza PERL que es un lenguaje de programación obsoleto.

- Chillispot mantiene la conectividad de los usuarios por tiempos límites y mediante el uso de pop-up mientras que NoCat se basa en java scripts y ventanas emergentes.

- Chillispot es totalmente portable para cualquier plataforma mientras que NoCat no y requiere un navegador específico con soporte SSL.

- Chillispot es una aplicación portable es decir funciona sobre cualquier plataforma que tenga activo el HHTPS mientras que ZeroShell requiere de una plataforma especifica esta puede ser Mozilla u otra plataforma que no sea Internet Explorer dado que en la actualidad existen una gran cantidad de dispositivos que son utilizados para acceder a Internet por lo cual se requiere una aplicación portable.

- Chillispot permite adaptar el idioma del portal a las necesidades del usuario en tres tipos de idiomas Inglés, Español e Indonés, es decir posee multilenguaje mientras que NoCat no.

- WifiDog instala por defecto SSL mientras que NoCat se instala con el SSL desactivado.

- Chillispot posee grandes características para administración y monitoreo de la red en tiempo real mientras que NoCat carece de dichas características.

- Chillispot soporta Qos pero lo trae por defecto mientras que NoCat se instala por defecto con Qos.

- Chillispot posee un ambiente más amigable para los usuarios mientras que NoCat posee una interfaz poco amigable.

4.4.6. Chillispot vs. WifiDog

SIMILITUDES

- WifiDog y Chillispot son aplicaciones de portales cautivos, es decir permiten redireccionar el tráfico a una página especial donde el usuario debe registrarse o aceptar las condiciones de la red para acceder a la misma.

- Ambas realizan un acceso a la red mediante un login y password es decir el usuario debe estar registrado para poder acceder a los servicios de la red.

- Tanto WifiDog como Chillispot utilizan una seguridad SSL para la comunicación del portal.

- Ambos soportan Qos.

- Tanto WifiDog como Chillispot permiten aplicar Calidad de Servicio mejorando servicio para los usuarios.

- Tanto Chillispot y WifiDog le dan la posibilidad a los usuarios de adaptar el lenguaje de la aplicación.

- Tanto WifiDog como Chillispot están desarrollados en C.

- Tanto WifiDog como Chillispot poseen informes estadísticos

- Las dos aplicaciones son portables ya que funcionan para cualquier navegador que soporte HTTPS por el nivel de seguridad que posee.

- Ambos funcionan sobre cualquier dispositivo electrónico o PDAs.

- Ambos son Configurables y Adaptables.

- Ambas aplicaciones brindan a los usuarios un ambiente familiar y sin complicaciones.

DIFERENCIAS

- Chillispot es más accesible en la instalación y configuración mientras que WifiDog tiene un grado alto de dificultad al momento de instalarlo y configurarlo ya que los paquetes, librerías y archivos vienen dispersos y existe escasa información sobre esta aplicación.

- Wifidog ha sido desarrollado en C, con el portal principal de Autenticación está codificado en PHP y una base de datos PostgressSQL, mientras que Chillispot soporta varios lenguajes como PHP, HTML, Javascripts y CGI.

- Wifidog mantiene la conexión con los usuarios comprobando la actividad de la red, Chillispot mantiene la conexión mediante expiración de la cuenta o cierre de sesión de la misma.

- Chillispot posee una mejor administración de usuarios ya que controla su acceso mediante el administrador mientras que WifiDog permite que sea el

propio usuario quien se cree su cuenta, además le presenta opciones que no debería tener como ver estadísticas, etc.

- Wifidog requiere para su instalación GNU/Linux server, un router Linksys WRT54G con Open WRT y con DHCP desactivado, el servidor de autenticación requiere también un web server Apache2 y PHP de preferencia la última versión mientras que los requerimientos de instalación de Chillispot son básicos ya que puede utilizar cualquier AP.

4.5. Resumen Comparativo

Luego de realizar un análisis de las principales características de WifiDog, NoCat y ZeroShell aplicaciones utilizadas para implementar portales cautivos se obtuvo la siguiente tabla resumen donde se presenta los resultados del estudio comparativo realizado:

TABLA IV.XX: Resumen de la Evaluación

Portales Cautivos / Parámetros	WifiDog	ZeroShell	NoCat	Chillispot
Open Source	4	3	4	4
Lenguaje	4	1	1	4
Conectividad de Usuarios	2	1	2	3
Autenticación	3	3	3	3
Requerimientos de Instalación	2	3	2	4
Configuración	1	3	3	4
Portabilidad	4	2	2	4
Seguridad de Comunicación	3	1	1	3
Monitoreo de Red	4	2	1	3
Multilenguaje	4	1	1	3
Calidad	3	3	3	3
Funcionalidad	4	1	2	3
TOTAL	38	24	25	41

Dado que el número de características evaluadas en el análisis comparativo de las aplicaciones, es un total de 12, valoradas cada una con un máximo de 4, obteniendo un resultado de 48, equivalente al 100%, podemos concluir que:

- Zeroshell obtuvo un total de 24 puntos equivalente a 50%, es decir es una aplicación para implementar un Portal Cautivo de forma sencilla, pero es poco adaptable y amigable con los usuarios de la red, sus características son escasas para las necesidades de la red de Bonny Restaurant.

- Con 25 puntos se puede concluir que NoCat presta un 52% de las características necesarias para satisfacer los requerimientos de la implementación de un Portal Cautivo seguro, pero posee grandes vacíos en cuanto a adaptabilidad, portabilidad, gestión de usuarios, estadísticas poco expresivas, etc.

- WifiDog con 38 puntos, es la aplicación para implementar un Portal Cautivo 79% más segura y que brinda las mejores características que Nocat y Zeroshell tanto para los usuarios externos de la red como para los internos y el administrador.

- Chillispot obtuvo 41 punto equivalente a 85% es decir es la aplicación que brinda mejores características tanto en administración de usuarios, portabilidad, sencillez de configuración e instalación, etc.

4.6. Resultados de la Comparación

- Al realizar la comparación entre las diferentes aplicaciones que permiten implementar portales cautivos, se llega a la conclusión que, las cuatro aplicaciones son herramientas capaces de montar un portal cautivo, cada una con mejores características de la otra.

- Los costos de instalación de cualquiera de las cuatro aplicaciones estudiadas son mínimos ya que se requiere de equipos básicos y software libre.

- Las cuatro aplicaciones permiten implementar un portal cautivo con características particulares de cada una de ellas y también permiten enviar propaganda de los servicios del restaurant mientras el usuario no esté registrado lo cual es uno de los objetivos buscados.

- Poseen cifrado de claves mediante SSL y posibilidad de Qos, unas lo poseen de forma implícita y otros pueden adaptarlos mediante plugins.

- Chillispot es una aplicación sumamente completa y compatible para varias plataformas y navegadores lo que da mayor campo de usabilidad, ya que en la actualidad los clientes que usan la red de Bonny Restaurant utilizan equipos como Laptops, PDAs o celulares por tanto ZeroShell y NoCat no serían tan aceptados por sus requerimientos de funcionalidad.

- También se pudo conocer que Chillispot y WifiDog poseen grandes características de monitoreo y administración de la red, dándole al administrador gran facilidad de desarrollar sus funciones optimizando tiempo y recursos de la mejor manera, mientras que ZeroShell y NoCat realizan un monitoreo y administración pobre y no en tiempo real.

- Las prestaciones de multilenguaje que presenta WifiDog y Chillispot permiten satisfacer varias necesidades del Restaurant y facilitan el entendimiento de la aplicación a los usuarios.

- Chillispot es una herramienta que cumple con las características necesarias para satisfacer las necesidades de Bonny Restaurant ya que los usuarios deben ser controlados por el administrador.

- El estudio y el análisis comparativo entre NoCat, ZeroShell, WifiDog y Chillispot han permitido determinar que la aplicación que más se adapta a las necesidades de la red de Bonny Restaurant ,y la que brinda mejores beneficios tanto para la administración de la red como para los usuarios y de mejores características es: Chillispot

- Los resultados obtenidos se basan fundamentalmente en las prestaciones y características de las aplicaciones estudiadas, reflejadas en las necesidades de la red inalámbrica corporativa de Bonny Restaurant.

CAPÍTULO V

5. CONFIGURACIÓN DE LA APLICACIÓN SELECCIONADA PARA LA IMPLEMENTACIÓN DE UNA APLICACIÓN PARA PORTAL CAUTIVO EN LA RED DE BONNY RESTAURANT

5.1. Visión Del Sistema

El sistema que se va a implementar ofrece un servicio de autenticación centralizada y de autorización para la WIFI, es decir la implementación de una aplicación para portal cautivo ayudará a los usuarios de la red a compartir su ancho de banda con otros miembros de Bonny Restaurant, mediante una autenticación de confianza para los usuarios. El sistema está pensado para proporcionar eficiencia y confiabilidad de autorización para todos los usuarios.

Un servicio de red WiFi centralizado permitirá que los usuarios externos que desean conectarse a la red deban registrarse y que los usuarios internos sean capaces de compartir su ancho de banda utilizando un punto de acceso inalámbrico. El sistema será gestionado por un administrador de red, que actuará como soporte al mismo tiempo.

La red de Bonny Restaurant será debidamente compartida, lo que mejorará la calidad de uso de la red, ya que el ancho de banda será dado de acuerdo a las necesidades de cada usuario, dando flexibilidad y facilidad para conectarse a la red desde cualquier punto dentro de la cobertura de la misma.

Dentro del sistema se ha diferenciado dos tipos de usuarios: los usuarios finales y el administrador de la red.

El usuario administrador, tiene derecho a supervisar el sistema (estadísticas, lista de puntos de acceso), gestionar las cuentas, crear, modificar, eliminar y bloquear un usuario, limitar el tiempo, limitar de ancho de banda del usuario, gestionar la red, etc.

Un usuario Final, es un usuario tanto interno como externo que desea obtener acceso a Internet por medio de los puntos de acceso inalámbrico de la red, este tipo de usuario deberá poseer una cuenta de usuario en el sistema o requerir una para acceder a los beneficios que presta la red.

A continuación se muestra la infraestructura que tendrá la aplicación de portal cautivo sobre la red del Restaurant Bonny:

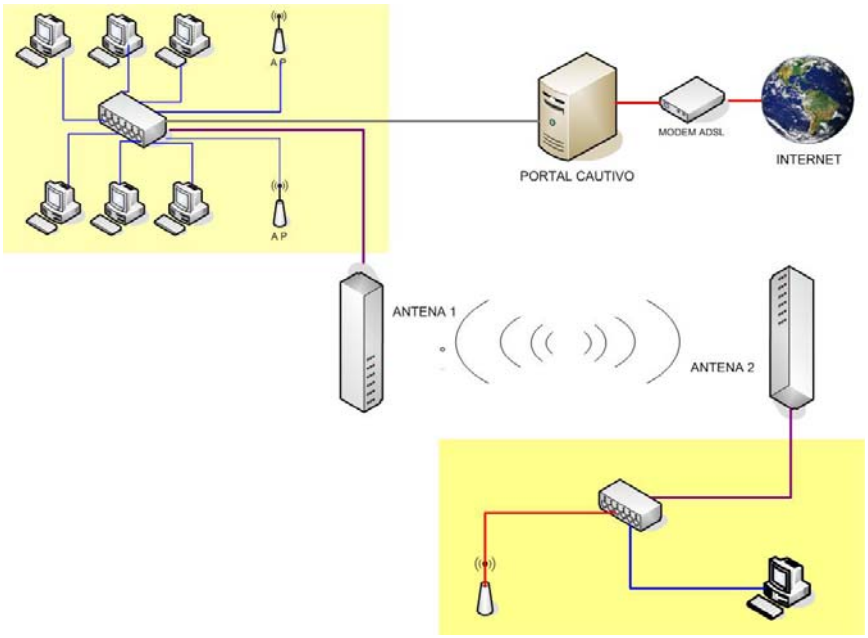


Figura V.20: Implementación de una aplicación de portal cautivo en la red Inalámbrica de Bonny Restaurant

5.2. Diseño e Implementación

DIAGRAMAS DE CASO DE USO:

Un diagrama de caso de uso, permite describir la interacción del usuario con la aplicación y la secuencia de las operaciones que realiza la aplicación en respuesta a la acción de los usuarios. Los diagramas de casos de usos se emplean durante el proceso de desarrollo de una aplicación o sistema para definir los requisitos funcionales del mismo, ya que muestran la funcionalidad de la aplicación desde el punto de vista del usuario, describiendo las acciones que el usuario desea obtener de la aplicación o sistema.

En la red de Bonny Restaurant se diferencian dos grupos de usuarios, un usuario Administrador y el usuario final, los mismos que serán representados por un agente dentro de un diagrama de caso de uso. A continuación se detalla cada uno de ellos:

a) El usuario Administrador de la red debe ser capaz de hacer gestión de usuarios, es decir podrá añadir, remover y bloquear a los mismos, adaptar la interfaz, además puede condicionar la navegación de los usuarios en la red mediante un nombre, contraseña de usuario, etc.

En el caso que se sospecha que un AP es iniciador de spam, virus, etc., el usuario administrador puede bloquear o incluso forzar a salir de la red.

Debe ser capaz de gestionar el contenido de la aplicación, página de bienvenida, publicidad y proporcionar información a los puntos de acceso. Para controlar la red y para identificar las amenazas en las primeras etapas, el administrador de la red debe realizar estadísticas de la red y hacer informes del tráfico por la red, la actividad del usuario, etc., es decir podrá obtener informes y estadísticas de diagrama.

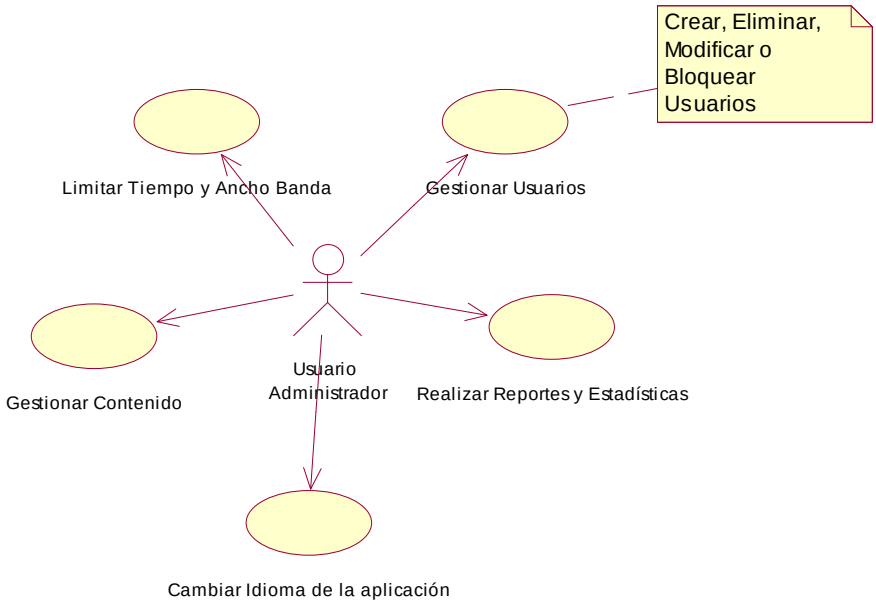


Figura V.21: Diagrama de Caso de Uso del Usuario Administrador

b) El segundo tipo de usuarios de la red de Bonny Restaurant, pueden ser personas que trabajan dentro de la empresa o clientes asiduos que buscan acceso a Internet, la interacción que tendrán con el portal será básica y sencilla ya que solamente deberán registrarse donde el administrador, ingresar sus datos (Login y Password) aceptar las condiciones de uso y podrán navegar de acuerdo a sus necesidades.

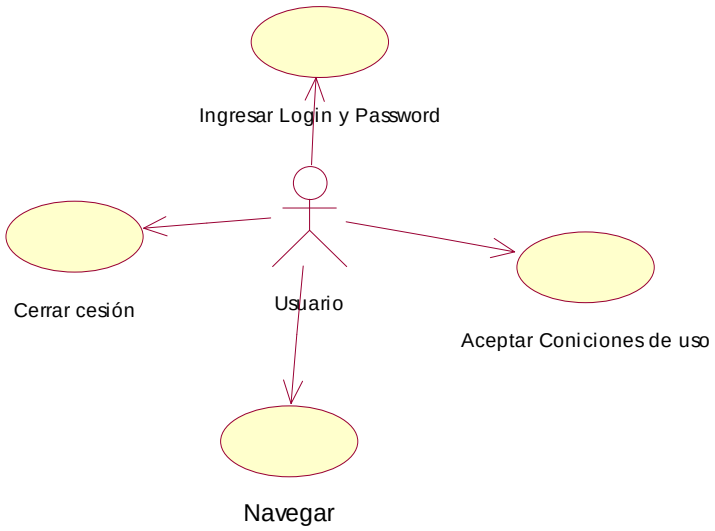


Figura V.22: Diagrama de Casos de Uso del Usuario Final

DISEÑO DEL SISTEMA

La solución para la red de Bonny Restaurant, se basa en la implementación de una aplicación para portal cautivo que permita administrar la seguridad de acceso a los usuarios y mejorar el uso de la red.

Luego de realizar un estudio de 4 diferentes tipos de aplicaciones para implementar portales cautivos, se determinó que las que brindan mejores prestaciones, para la red de Bonny Restaurant son Chillispot y WifiDog, pero por las facilidades de configuración e

instalación se ha seleccionado Chillispot, ya que es una herramienta Open Source y tiene varias características implementadas que se ajustan a los requerimientos de la empresa, tales como gestión de usuarios, realización de reportes y estadísticas de la red, gestión de contenido, adaptabilidad de lenguaje (Inglés, Español o Indonés) a las necesidades del Administrador , etc., que complementan y benefician al servicio que la brinda la red de Bonny Restaurant.

La aplicación Chillispot se compone de dos partes que son:

- Una aplicación en el espacio del usuario denominada chilli que es el Portal Cautivo en sí y cumple las siguientes funciones, servidor DHCP, cliente RADIUS, Proxy-RADIUS y Redirector.

- Un archivo cgi en el servidor Web llamado hotspotlogin.cgi, que no es más que un script programado en lenguaje perl que se encarga de enviar los datos de autenticación a nuestro portal cautivo. Este script genera un protocolo de autenticación llamado desafío-CHAP para validar el usuario y la clave de acceso del cliente, a través del servidor web cifrado con el protocolo de seguridad HTTPS y es el enviado al chilli.

INFRAESTRUCTURA DEL SISTEMA

La infraestructura necesaria para el funcionamiento del sistema consiste en ubicar un equipo con una aplicación central, con un sistema operativo Linux en este caso Ubuntu Server y con un router inalámbrico. Este equipo formará parte de la red de Bonny Restaurant, esto no implica que deba estar permanentemente dentro de la red, pero deberá estarlo a la hora de administrar los dispositivos que forman parte de ella.

El otro componente básico para nuestra infraestructura son los puntos de acceso, todos ellos deberán estar funcionando y correctamente configurados.

En resumen, la aplicación en sí se instalará en el punto de control y en los puntos de acceso será necesario el uso de un software muy reducido para comunicarse con el punto de control, además de una serie de configuraciones.

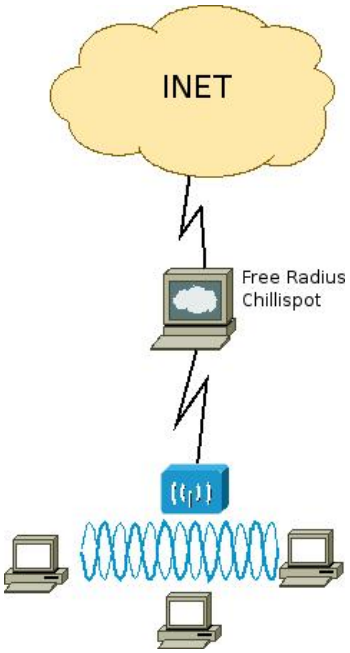


Figura: V.23: Topología Chillispot

SOTWARE UTILIZADO

La solución que se ha definido para nuestra aplicación utiliza software de código abierto y publicado bajo licencia GPL o bajo licencias que son compatibles con GP lo que significa que la solución es libre y cada uno puede utilizarlo en condiciones de GPL.

El software del servidor se compone de varios componentes que proporcionan el servicio básico para nuestra aplicación. El servidor Web es Apache HTTP de Apache Software

Foundation, es de código abierto, proporciona un servicio fiable y ha sido el servidor web más popular en el Internet desde abril de 1996.

Chillispot que es la aplicación para portal cautivo que más se adapta a las necesidades de nuestra red, una de las extensiones requeridas es PHP extensión, ya que el servidor web de Chillispot está escrito en PHP, por otra parte, Chillispot utiliza una base de datos MySql, por lo tanto, la extensión mysql PHP también debe ser instalado. A continuación se detalla cada software que será utilizado en la aplicación de Bonny Restaurant:

- MySql es un sistema de gestión de base de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones, es software libre en un esquema de licenciamiento dual. Por un lado se ofrece bajo la GNU GPL para cualquier uso compatible con esta licencia, pero para aquellas empresas que quieran incorporarlo en productos privativos deben comprar a la empresa una licencia específica que les permita este uso, está desarrollado en su mayor parte en ANSI C.

- Chillispot es el portal que más características brinda para la red de Bonny Restaurant, es el más sencillo de configurar e instalar, tiene seguridad con la información del usuario ya que solo el por defecto usa chilli CHAP-Challenge y CHAP con contraseña permiten que solo el servidor web y el servidor RADIUS conozcan las contraseñas reales, ni chilli ni los servidores proxy radio conocen la contraseña real.

- FreeRadius es el servidor RADIUS más popular es compatible con todos los protocolos comunes de autenticación y el servidor viene con un PHP de administración de usuarios basada en web, llamado dial up admin, es la base para muchos productos RADIUS y servicios comerciales, como los sistemas integrados, además sirve de apoyo en redes de control de acceso y WiMAX.

- Servicio DNS es una base de datos distribuida y jerárquica que contiene información que es usada para traducir los nombres de dominio, La traducción entre nombres de dominio y direcciones IP es realizada mediante la biblioteca de resolución DNS al igual que los destinos a ser conectados con la aplicación que requieren servicio de nombres.

- En cuanto a DHCP es un protocolo de servicio TCP/IP que ofrece configuración dinámica de terminales, con concesión de direcciones IP de host y otros parámetros de configuración para clientes de red el mismo que es proporcionado por el chilli de Chillispot

- ARP será proporcionado por chilli de Chillispot y es el protocolo de resolución de direcciones, es el responsable de encontrar la dirección de hardware que corresponde a una determinada dirección IP.

- Los servicios de cortafuegos y NAT son proporcionados por iptables, un paquete de software que permite configurar las tablas que contienen cadenas de normas para el tratamiento de los paquetes.

5.3. Diseño de la red Inalámbrica de Bonny Restaurant

INTRODUCCION

El Restaurant Bonny es una empresa que quiere brindar a sus clientes un servicio de calidad tanto en el uso de sus instalaciones, gastronomía y uso de internet, es por esto que se ha visto en la necesidad de implementar una red LAN para los usuarios internos y una red WLAN para los clientes del Restaurant.

El Restaurant posee en la actualidad 6 máquinas físicas conectadas mediante un switch D-LINK a Internet, también cuenta con dos AP para brindar el servicio de red Inalámbrica a los clientes del restaurant, una PC que actúa como DHCP asignando direcciones dinámicas a las PC la misma que está conectada al Modem ADSL y al switch D-Link, pero no cuenta al momento con algún sistema o aplicación que le permita controlar el uso del ancho de banda y el tiempo de uso de los usuarios peor aun controlar o defender a la red de usuarios maliciosos lo que provoca el continuo formateo de las máquinas por virus, etc.

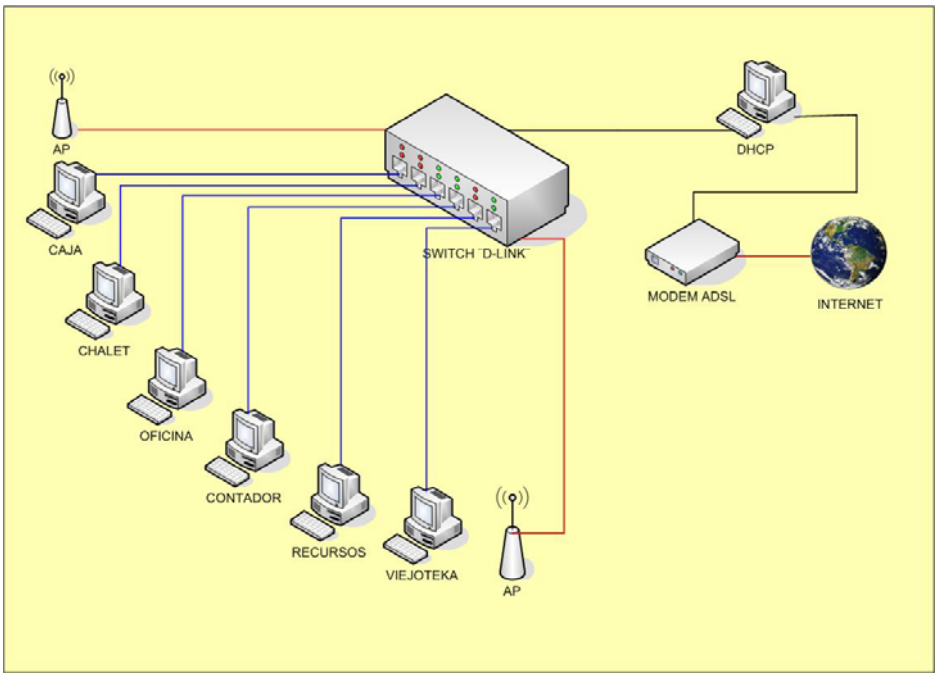


Figura: V.24: Red Inalámbrica que posee Bonny Restaurant

Bonny además desea implementar el servicio de Internet en su primera sucursal ubicada en las calles Villarroel y Almagro para lo cual se ha realizado una solución en la que el Internet será distribuido desde la sucursal de la Primera Constituyente y Darquea mediante el uso de antenas y con un administración de usuarios de la red mediante el uso de una aplicación para portal cautivo en este caso Chillispot.

En la implementación de esta red se utilizaron herramientas tales como ponchadoras para construir los cables de red, dos tarjetas de red adicional instalada en el equipo que distribuirá el servicio de Internet, un Router que soporte FreeRadius en este caso Router TP-LINK modelo TL-WR 941 ND.

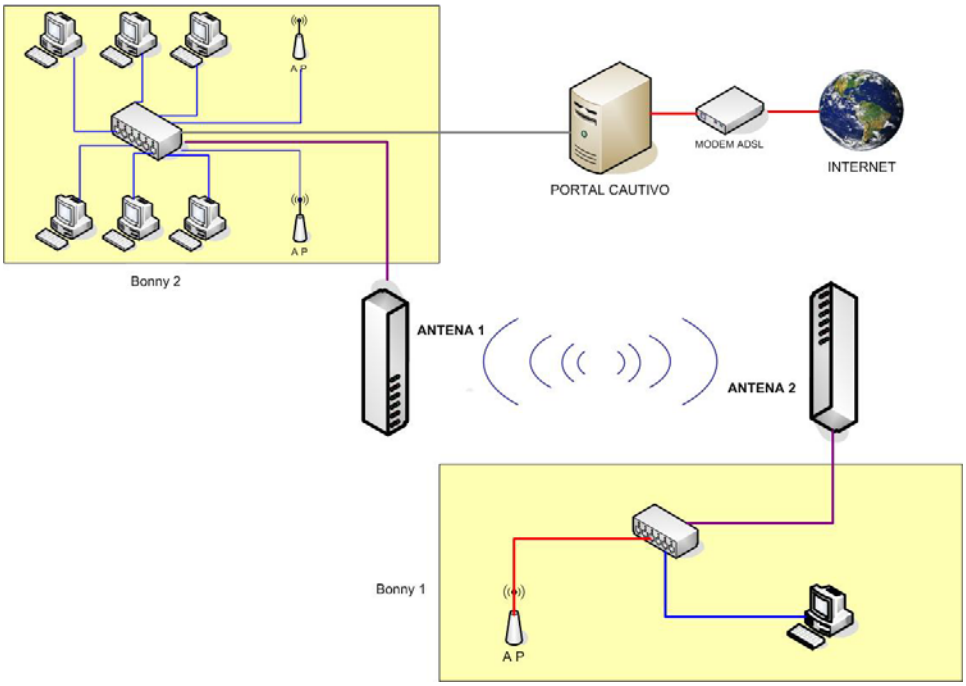


Figura: V.25: Red Inalámbrica de Bonny Restaurant usando Portal Cautivo

MATERIALES UTILIZADOS

Los materiales que fueron usados para la implementación de la red son las siguientes:

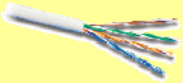
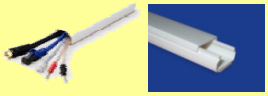
IMAGEN	NOMBRE
	Dos switch D-LINK o concentrador de 8 puertos
	Conectores hembra de base RJ45 (este es el tipo de clavija) para pared
	Cable UTP Categoría 5-e
	Conectores aéreos macho RJ-45 y boots de cubrimiento
	Tres Router TP-LINK modelo TL-WR 941 ND
	Canaletas para cubrir Los cables de instalación
	Taladro y tornillos para realizar los huecos y asegurar la canaleta a la pared
	Ponchadora con ranura RJ – 45
	2 Tarjeta de Red Adicional
	Dos Antenas Nano Station 5 cpe 2.4ghz 400mv

Figura: V.26: Materiales de Red

HERRAMIENTAS UTILIZADAS

Las herramientas que fueron usadas para la implementación y pruebas de la extensión de red son las siguientes:

IMAGEN	NOMBRE
	Ponchadora
	Tester
	Pelador de Cables
	Clipadora

Figura: V.27: Norma TIA/568B

PROCESO DE INSTALACION

1.- Primero se implementa la red cableado del Bonny 1 ubicado en las calles Villarroel y Almagró ya que no posee ningún tipo de red mediante los siguientes pasos:

a) Se realizó un estudio de factibilidad de la instalación de las canaletas que llevará lo cables de Datos.

b) Se poncharon los cables de tipo TIA/EIA 568B para la red LAN.

PIN	COLOR	PAR	FUNCION
1	Blanco Naranja	3	TD+
2	Naranja	3	TD -
3	Blanco Verde	2	RD +
4	Azul	1	Ninguna
5	Blanco Azul	1	Ninguna
6	Verde	2	RD -
7	Blanco Marrón	4	Ninguna
8	Marrón	4	Ninguna

TD: Transmisión de Datos.
RD: Recepción de Datos.

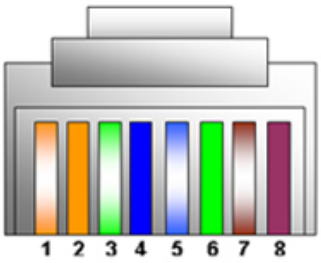


Figura: V.28: Norma TIA/568B

Debemos calcular la cantidad de metros que debe poseer los cables para cada uno de los puntos de red, en cada uno de ellos debe haber un conector macho RJ-45, esto se lo hace con una herramienta llamada ponchadora.

Figura: V.29: Ponchadora

Esta herramienta tiene una serie de zócalos para fijar el cable con el conector RJ-45, para ello se realiza el siguiente proceso:

- Se debe cortar 2cm de la envoltura de plástico que se encuentra cubriendo a los cables, esto se lo hace para poder insertar los cables en el conector RJ-45, para insertarlos, debemos ver que los 8 hilos tengan la misma dimensión, sino, ocupamos una cuchilla que viene en la ponchadota y cortamos los 8 hilos de la misma dimensión.

- En este momento se inserta los hilos en el conector, verificando que las puntas entren completamente y hagan contacto con los dientes del conector.
- Una vez comprobados estos pasos, se coloca el conector RJ-45 en el zócalo de la ponchadora y procedemos a presionar con fuerza para que la ponchadora pueda presionar a los dientes del conector y pueda hacer contacto con los hilos del cable, como muestra:

Figura: V.30: Cable ponchado

Estos mismo pasos se siguen con cada uno de los cables que lleva desde el ordenador hasta su adaptador RJ-45 de la pared así como las del Switch o de las Impresoras, en todas va igual y conforme ponga los colores de los cables de una manera determinada, ponga todos los cables igualmente en todas las conexiones.

Una vez montados los cables, es aconsejable pasar un escáner o comprobador para asegurarse de que todas las conexiones de los cables, tanto los aéreos como los de la regleta, están correctamente.

Estas herramientas de comprobación nos dirá si alguno de los cables no está correctamente instalado o falla la conexión, debe tener en cuenta que un

solo cable que no funcione puede hacer que el ordenador de esa conexión no funcione en red.

c) Se debe Instalar las tarjetas de red en las máquinas que no venían integradas, en la figura que se muestra posteriormente, se puede comprobar cuando el ordenador cuenta con la tarjeta de red, dado que todos los ordenadores que se vayan a montar necesitan una tarjeta de red para su conexión.

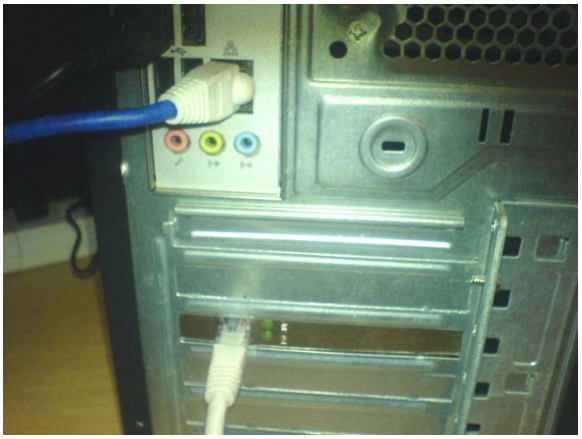


Figura: V.31: Ordenador con tarjeta de red

Como se puede observar en la zona inferior izquierda hay una ranura blanca (PCI) libre para poder conectar una tarjeta de red tipo Ethernet como la que muestra la siguiente imagen:

Figura: V.32: Tarjeta de Red

d) Se realizó la conexión de un ordenador al Switch ocultando los mismos mediante las canaletas.

En la siguiente figura se ilustra un rollo de cable tipo UTP categoría 5e utilizado para montar en canaletas desde el RJ45 del ordenador al RJ45 del Switch.

Figura: V.33: Cable UTP CATEGORIA 5e

Dicho cable se instala por el interior de la canaleta:

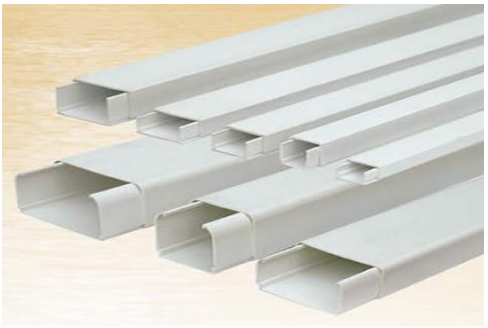


Figura: V.34: Canaletas

En el interior de la canaleta encontraremos todos los cables de cada uno de los ordenadores de la red que van hacia el Switch o concentrador para realizar la instalación completa de la red.

Figura: V.35: Switch

Se observa un cable conectado al Switch, dicho cable proviene de una clavija de pared RJ45., cada uno de los cables que lleguen a través de la canaleta hacia el Switch ocuparán los conectores del Switch como muestra la siguiente fotografía.

Figura: V.36: Conectores conectados al Switch

Las cajas RJ45 Hembras de la pared quedan como se ilustra a continuación.

Figura: V.37: Caja RJ45 hembra

2.- Una vez instalada la red cableada en Bonny 1 se realiza un estudio de campo con el fin de determinar la distancia, sus puntos georeferenciales, a través de un GPS; además la existencia de línea de vista entre los locales, obteniendo los siguientes resultados:

Ubicación Física:

- Bonny 1: Villarroel y Almagro
- Bonny 2: Primera Constituyente y Darquea

Ubicación Geográfica:

- Bonny 1: S (01º 40´ 41.1”) O (078º 38´ 50.1”)
- Bonny 2: S (01º 40´ 40.7”) O (078º 38´ 36.2”)

Mediante la observación se pudo constatar la existencia de línea de vista entre las dos sucursales determinando de esta manera la ubicación de las antenas.

3.- Interconexión entre las sucursales de Bonny Restaurant

Antenas

Luego de los datos obtenidos en el estudio de campo se procede a seleccionar los dispositivos a utilizar para el proyecto, como es conocido existe una amplia gama de antenas y dispositivos para diversas aplicaciones de campo, de acuerdo a las distancias y aplicaciones que estas tengan.

La distancia que existe entre los puntos es de 420m que equivalen a 0,42km, debido a que es una distancia menor a 5km, se escogió un par de antenas direccionales marca Ubiquiti Nanostation 5 de 14 dbi, que permitirán la transmisión y conexión entre las sucursales sin complicaciones.

A continuación se muestra un esquema del posicionamiento de los restaurantes, así como las calles donde se encuentran ubicados y la distancia entre ellos:

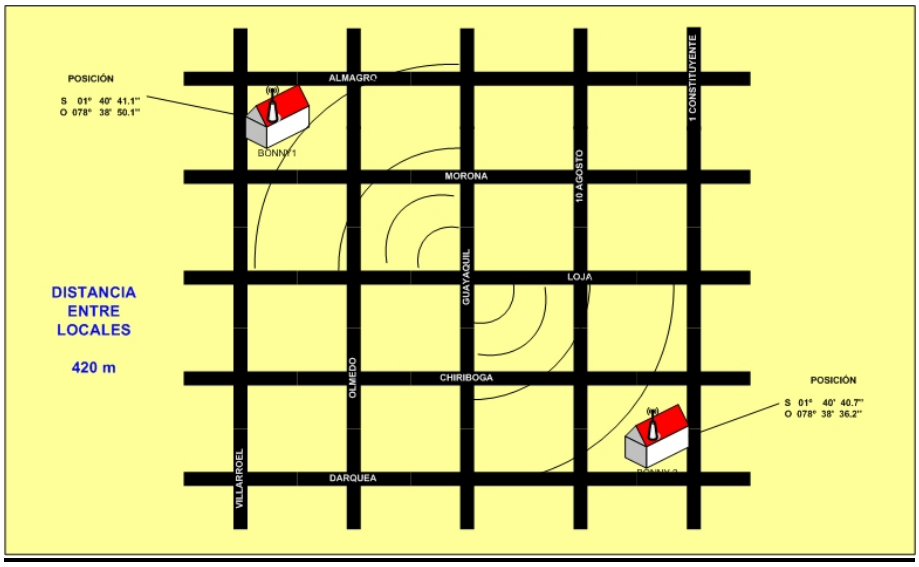


Figura: V.38: Ubicación de las antenas en la red

Las antenas Ubiquiti Nanostation son dispositivos con un diseño compacto, que permite su uso tanto en interior como en exterior. Su interface es intuitiva y permite una rápida configuración incluso para los no expertos. Es tan potente como simple.

El Nanostation presenta un diseño revolucionario, es un sistema de antenas de alta ganancia con doble polarización, una arquitectura de radio avanzada y un firmware altamente investigado y desarrollado que le permite una alta estabilidad y rendimiento compitiendo con los equipos análogos de alta gama.

Figura: V.39: Antenas Ubiquiti Nanostation

A continuación se procede a configurar cada una de las ellas, lo primero que se debe hacer es conectar con un cable de red RJ-45 directo, el primer extremo a la antena y el segundo extremo a la computadora y seguimos los siguientes pasos:

1. Primero se accede al dispositivo, mediante la dirección IP por defecto **192.168.1.20,** se ingresa esta dirección en el explorador de Internet, y aparecerá una ventana de autenticación, donde se escribe el login: por defecto es **ubnt** y el password que es por defecto **ubnt.**

2. Una vez logeado, se cambia la dirección IP (**Network** -> **Network Settings**) y se le asigna la que se vaya a utilizar, en este caso la 192.168.182.101, clic en "**CHANGE**" para aplicar los cambios.

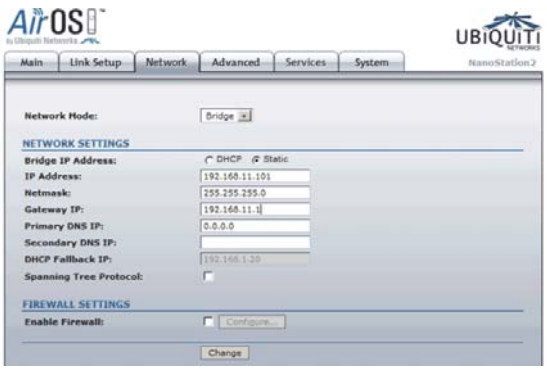


Figura: V.40: Configuración Antenas

3. A continuación se procede a configurar los parámetros del dispositivo.

En este caso se accede al menú de **"LINK SETUP"** y se configura los siguientes campos:

- **Modo inalámbrico:** Punto de acceso WDS Conexiones WDS: La dirección MAC del cliente WDS. SSID: NS1

- **Codigo de país:** Ecuador

- **Modo IEEE 802.11:** B/G Mixto

- **Anchura del espectro:** 20Mhz (Seleccionable hasta 40Mhz en NanoStation5 para obtener mayor ancho de banda)

- **Canal: 7 Seguridad**: WEP.

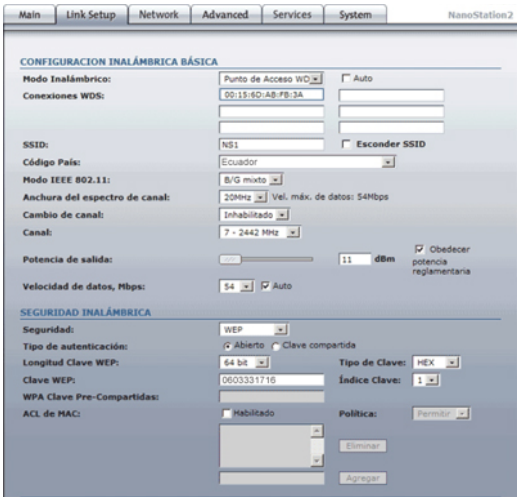


Figura: V.41: Configuración parámetros Antenas

4. Una vez configurado la primera antena como **punto de acceso WDS**, ahora se configurará la otra antena como **Estación WDS,** para esto se deben hacer estos cambios:

- En modo Estación WDS.
- Tener una IP conocida (para este ejemplo es 192.168.182.102)
- Tener un SSID conocido al que conectar (para este caso es NS1)
- Establecer encriptación, en este caso WEP.

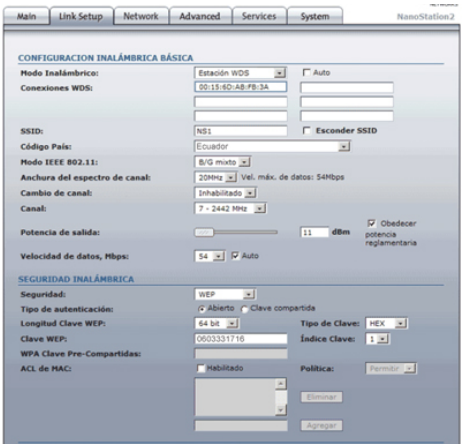


Figura: V.42: Configuración Antenas 2

5. De esta manera si las dos Antenas tienen línea de vista, Automáticamente, la estación va a reconocer la señal del Punto de acceso, logrando la interconexión entre las dos sucursales.

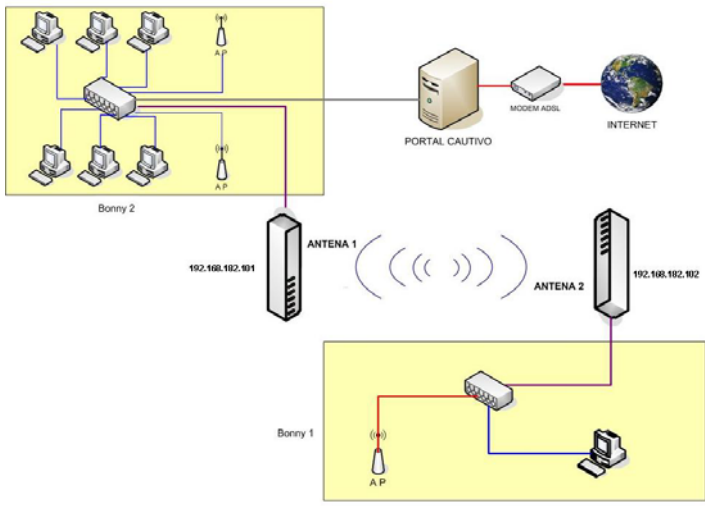


Figura: V.43: Interconectividad entre Bonny1 y Bonny2

5.4. Implementación

Para la implementación de Chillispot es necesario conocer que Chillispot está disponible para Linux y FreeBSD, también es compatible con: OpenBSD, NetBSD y Solaris, incluso Apple OSX.

Chillispot se sabe que se ejecutan en Debian, Gentoo, RedHat, Fedora, Mandrake y OpenWRT.

En términos más generales, se necesita un sistema Linux con la versión del núcleo 2.4.7 al menos, ya que Chillispot utiliza el controlador tun para las interfaces de red, el mismo que se incluye en el kernel de Linux desde la versión 2.4.7 y posteriores.

Para la instalación es necesario lo siguiente, tanto en HW como en SW.

- PC con Linux + 2 tarjetas de red. (eth0 y eth1).
- Chillispot
- FreeRADIUS
- Apache
- PHP
- MySQL

En cuanto al servidor Radius se puede utilizar uno de los siguientes servidores Radius de código abierto:

- FreeRADIUS
- OpenRadius
- Cistrón
- IC-RADIUS

En la actualidad existe una herramienta que integra todas las componentes necesarias para el funcionamiento de Chillispot lo que facilita la instalación y configuración de esta aplicación, esta herramienta es EASYHOTSPOT.´

EasyHotspot se una aplicación que corre sobre una distribución de Ubuntu, con una interfaz para el administrador del punto de acceso se construye a partir del marco CodeIgniter (es un framework PHP fácil de entender y es muy práctico para hacer uso de él en la web) y que utiliza como aplicación de portal cautivo Chillispot, con una base de datos MySql, para almacenamiento de los usuarios y de la información registrada, además EasyHotspot incrementa el servicio de facturación el mismo que puede o no implementarse en la red deseada, lo que da oportunidad a la red de Bonny Restaurant de escalar en un futuro. A continuación se detalla el paquete de EasyHotspot:

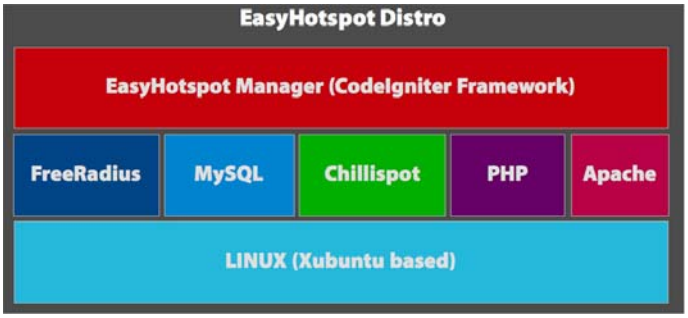


Figura: V.44: Paquete EasyHotspot

Requerimientos de Hardware para la Instalación de EasyHotspot:

TABLA V.XXI: Requerimientos de Hardware

HARDWARE MÍNIMO	HARDWARE UTILIZADO
Pentium 3 o igual	Pentium Core Dúo
512 MB de RAM	2GB de memoria RAM
5GB de espacio libre de disco duro	320 GB de espacio en disco duro
2 interfaces de red (eth0) y (eth1)	2 interfaces de red (eth0) y (eth1)
Punto de acceso inalámbrico	ROUTER TP-LINK Modelo TL-WR941ND
Switch / Hub (para usuarios que tengan conexión con cable)	Dos switch D-LINK de 8 puertos Modelo DGS-2208

Recursos Software utilizados:

TABLA V.XXII: Requerimientos Software

REQUERIMIENTOS DE SOFTWARE
FreeRadius versión 2.1.0
Chillispot versión 1.0
Apache versión 2.2.11
MySqld versión 5.0.75
PHP versión 5.2.6
EasyHotspot versión 0.2
Ubuntu Server versión 9.0.4

PROCESO DE INSTALACIÓN

EasyHotspot viene integrado con una versión live CD de Ubuntu, lo primero que se debe hacer para su instalación es descargar EasyHotspot de easyhotspot.inov.asia/index.php/download y se quema en un CD, luego arrancar desde el CD-ROM la PC.

Aparecerá el siguiente menú donde escogemos el modo de arranque de Ubuntu en este caso xforcevesa para iniciar con el modo gráfico de la aplicación y presionar enter para continuar.

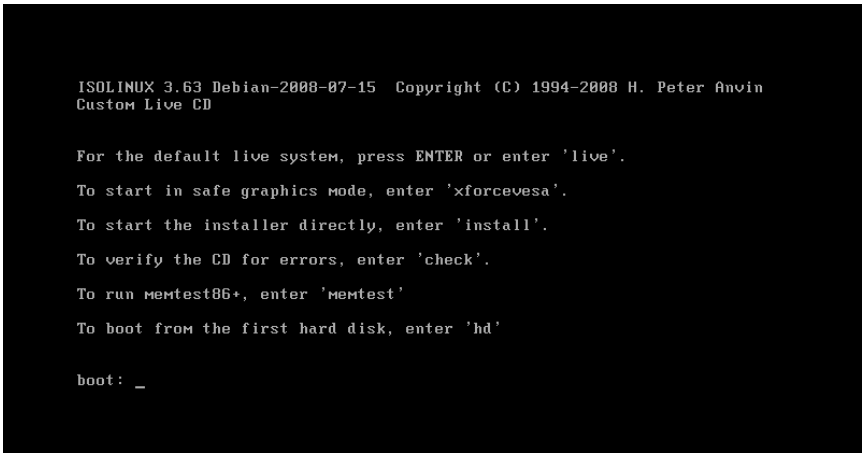


Figura: V.45: Menú de Instalación EasyHotspot

Empezara la instalación de Ubuntu.

Figura: V.46: Inicio de la Instalación

Una vez cargado el programa aparecerá una nueva pantalla donde se ingresa un nombre de usuario si no colocamos nada no importa ya que en la instalación total podremos definir el usuario y la contraseña del mismo.

Figura: V.47: Nombre de Usuario EasyHotspot

Ahora aparecerá el modo gráfico de Ubuntu.

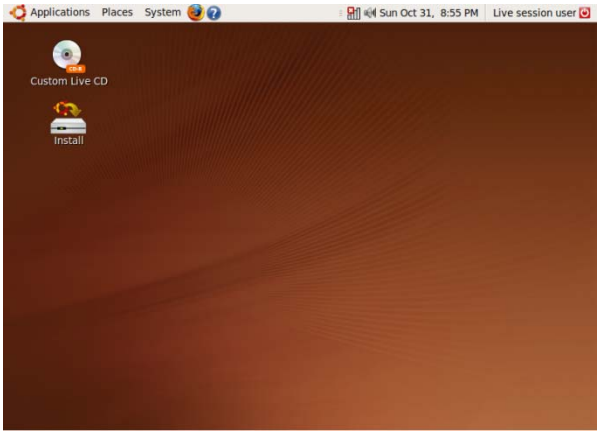


Figura: V.48: Modo Grafico EasyHotspot

Dando clic en el acceso del escritorio install para instalar en el equipo el contenido del Live CD para que este se ejecute en el sistema sin necesidad del CD y empezaremos a instalar Ubuntu y EasyHotspot.

Primero aparecerá una pantalla de Bienvenida donde se selecciona el idioma que tendrá el sistema en este caso Español y presionamos la tecla adelante para continuar.

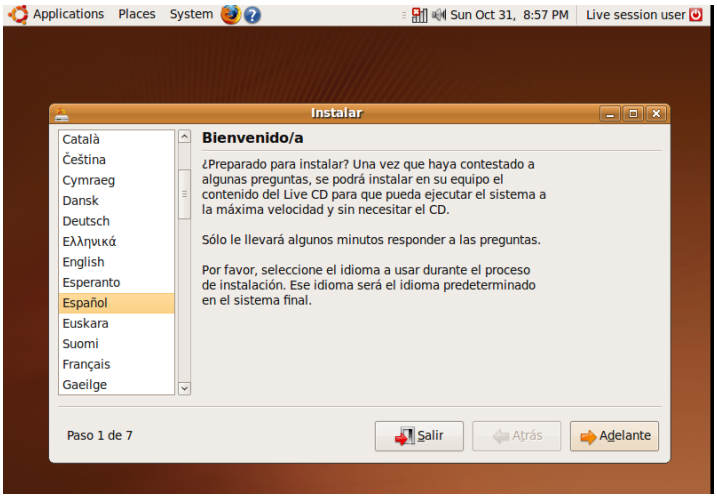


Figura: V.49: Pagina de bienvenida de la Instalación

A continuación seleccionar nuestra zona horaria en este caso región es América y Ciudad Guayaquil clic en Adelante y continuar con la instalación.

Figura: V.50: Selección de Zona Horaria

Se escoge la distribución de nuestro teclado en este caso Latín América y clic en Adelante para continuar.

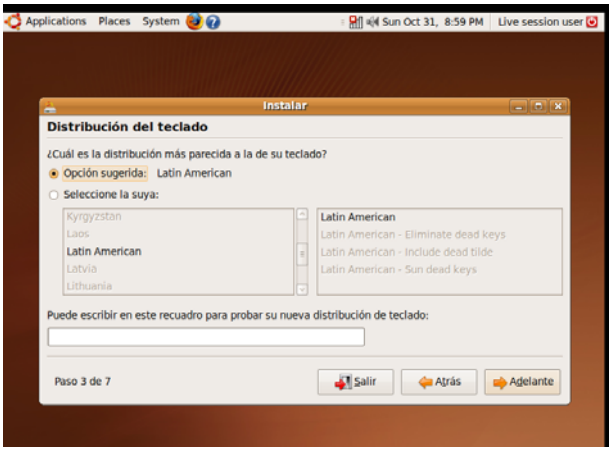


Figura: V.51: Distribución del Teclado

Se procede con la preparación del espacio en disco y la instalación de Ubuntu clic en adelante y continuar.

Figura: V.52: Especificación de particiones e instalación

Una vez instalado aparecerá una nueva ventana donde se especifica el nombre del usuario la contraseña clic en Adelante y se sigue con la instalación.

Figura: V.53: Especificación de usuario y contraseña Ubuntu

Ya especificado la zona horaria, el nombre y contraseña del usuario y la partición se procede a Instalar Ubuntu.

Figura: V.54: Instalación Ubuntu

Aparecerá la siguiente pantalla de instalación

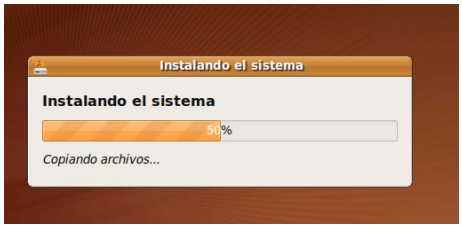


Figura: V.55: Proceso de Instalación

Terminada la instalación aparecerá un mensaje de aprobación, se escoge Reiniciar ahora para que la instalación se complete.

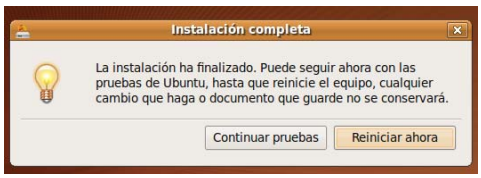


Figura: V.56: Instalación Completa

CONFIGURACIÓN DEL ROUTER TP-LINK TL-WR941ND

Una vez reiniciada la máquina se procede a configurar el Router para continuar con la configuración de Easyhotspot.

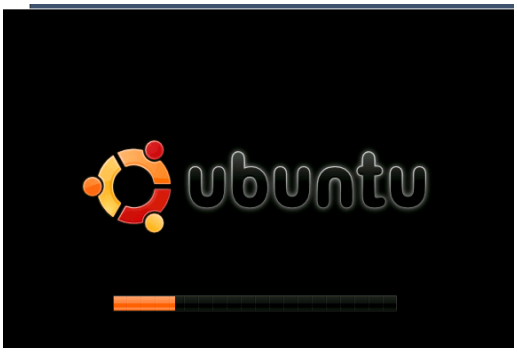
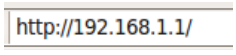


Figura: V.57: Iniciando Ubuntu

Lo primero que se hará es configura las interfaces de red, como se dijo anteriormente se debe tener 2 interfaces un eth0 y un eth1, en este caso eth0 será nuestra fuente de conexión con Internet la misma que será dinámica, por el MODEM ADSL de nuestro proveedor de servicios CNT. En cambio la interfaz eth1 actuará como interfaz de distribución, esta no será configurada, solo debe ser conectada al Router.

A continuación se accede al Router mediante el navegador de Ubuntu Mozilla se digita la dirección por defecto del Router 

con usuario admin y password admin.

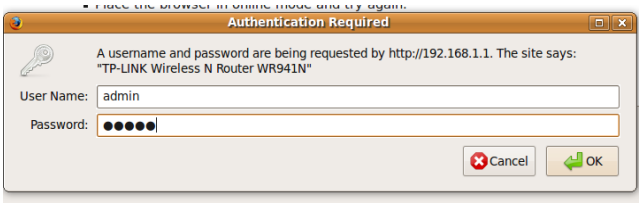


Figura: V.58: Autenticación para el Router

Una vez autenticado se ingresa a la configuración del Router:

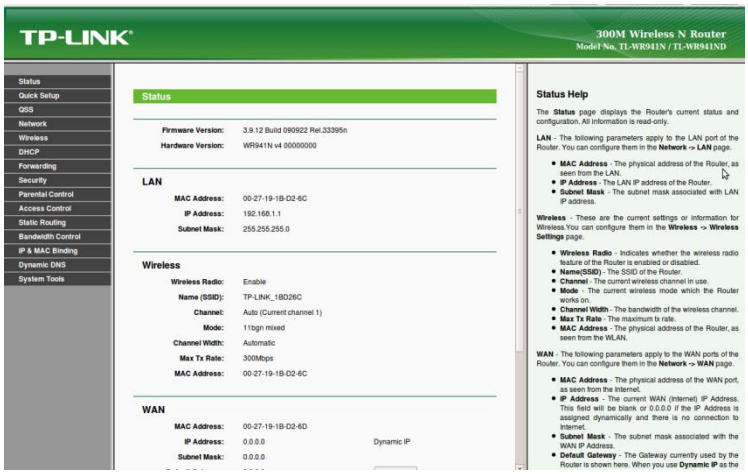


Figura: V.59: Interfaz del Router

A continuación se configura el Router se escoge la opción Wireless, y luego Wireless Settings, y empezar la configuración:

TABLA V.XXIII: Parámetros de Configuración del Router

Parámetros	**Valor**
SSID (identificador de la red)	Bonny
Región	Ecuador
Channel	Auto
Mode	11bpn
Channel Width	Automatic
Max Tx Rate	300Mbps

Y se procede a guardar los cambios dando click en ***save***:

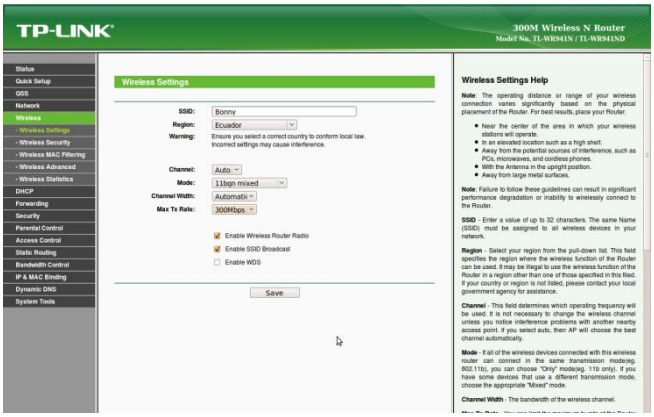


Figura: V.60: Configuración de los parámetros Router

Reiniciar el Router para actualizar los cambios realizados

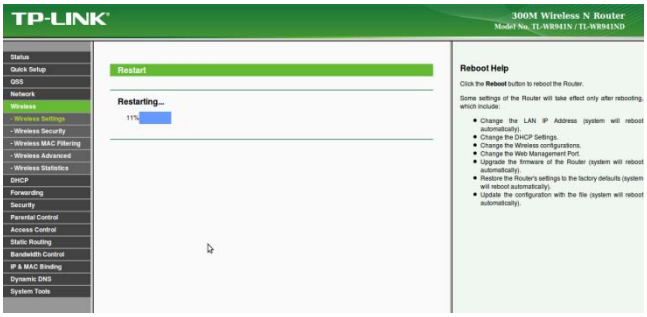


Figura: V.61: Actualización de los cambios en el Router

Deshabilitar DHCP, cifrado y la función del Router en su punto de acceso ya que Chillispot tiene su propio servidor DHCP de tal forma que el Router se vuelve transparente para la ejecución del portal.

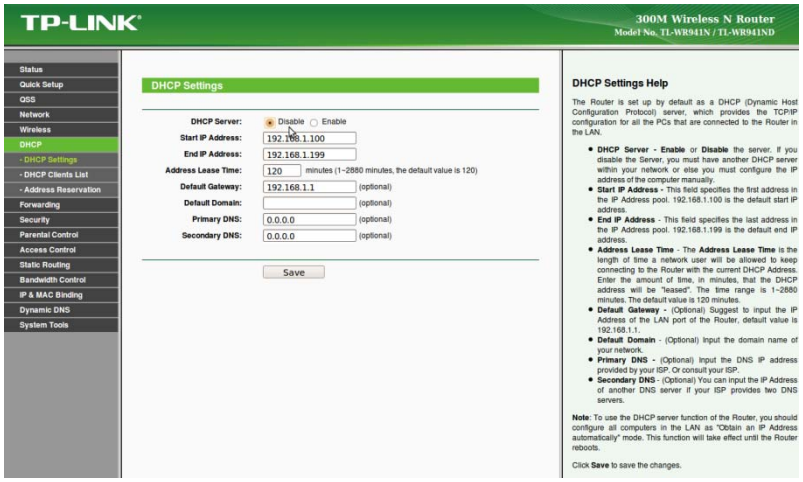


Figura: V.62: Deshabilitando el Router

Se reinicia el Router para que se concreten los cambios

Figura: V.63: Reiniciar el Router

CONFIGURACIÓN DE EASYHOTSPOT

Una vez configurado el Router se ingresa al explorador Mozilla y se escribe http://localhost/easyhotspot para proceder a la configuración de Easyhotspot, ya que este trae una preconfiguración y una interfaz Web para gestionar la administración de usuarios, aparecerá una pantalla de autenticación donde por defecto el usuario es **admin**, y la contraseña es **admin123.**

En EasyHotspot se diferencian dos tipos de usuarios:

- Admin: Este usuario se encarga del plan de facturación, el precio, asignación ancho de banda y configuración del sistema
- Cajero: Este usuario maneja las cuentas de usuarios, generación de vales, facturas, estadísticas de la red.

Los mismos que pueden ser manejados por el mismo administrador.

ADMIN

La primera página que se muestra es la página principal del administrador donde se puede ver la información del punto de acceso y la información del sistema que nos permite verificar si todo está funcionando correctamente.

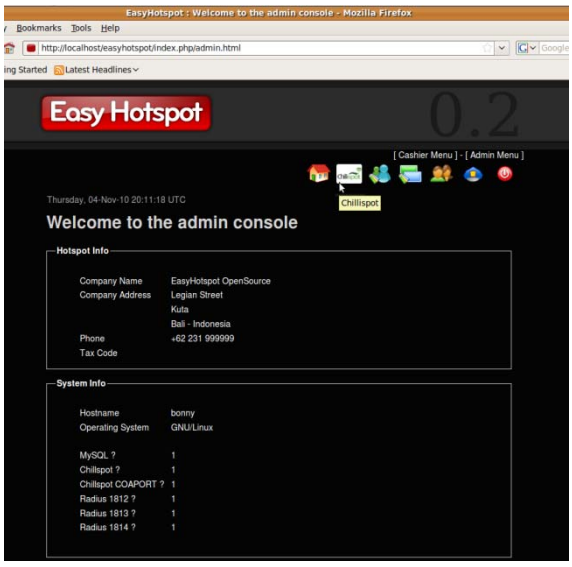


Figura: V.64: Come Admin EasyHotspot

Configuración De Chillispot

Dentro del admin se escoge la opción chillispot y se configura los siguientes campos:

- Radius Server 1 (Es la dirección del servidor RADIUS principal por defecto es **127.0.0.1**)

- Radius Server 2 (Es la dirección del servidor RADIUS secundarios, por defecto también es **127.0.0.1**)

- Radio Secreto (es la frase secreta entre el servidor RADIUS y Chillispot en este caso **esasyhotspot**)

- Interfaz DHCP (Es la interfaz que se desea utilizar para la interfaz del hotspot en este caso es **eth1**)

- Servidor UAM (Dirección del portal cautivo esta es **https://192.168.182.1/cgi-bin/hotspotlogin.cgi**)

- Secreto UAM(Es la frase secreta entre la página de inicio de sesión y Chillispot en este caso **easyhotspot**)

- Página de inicio del cliente (Dirección de la página donde se le redirecciona por primera vez al cliente para el logeo)

- URL permitidas(Son las URL que los clientes pueden ver sin necesidad de logeo, en este caso se coloca a la página de Bonny Restaurant para que conozcan los servicios que el Restaurant ofrece en este caso www.bonnyrestaurant.com)

- Rango DHCP(es el rango de la IP que podrá dar el DHCP en este caso **192.168.182.0/24**)

- COAPORT es el puerto por donde actúa el portal cautivo en este caso 3**799**

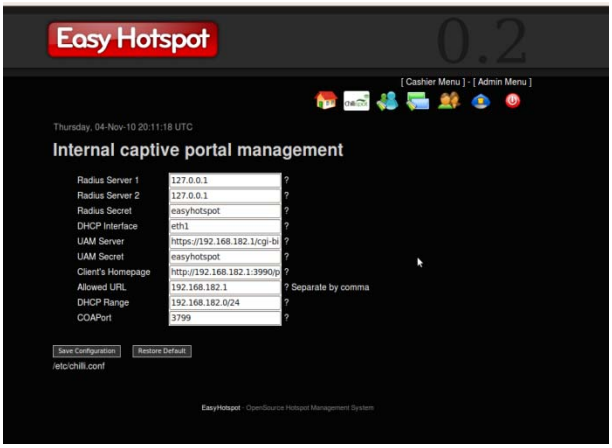


Figura: V.65: Configuración Chillispot EasyHotspot

Ajuste Postpago 

En esta opción si se desea se puede establecer la tarifa a cobrar ya sea que se cobre por MB o por tiempo de uso, el tiempo de espera de la cuenta inactiva, la tasa de ancho de banda tanto para la descarga como para la subida de archivos. Esta configuración se le asigna a cada cliente postpago creado.

Figura: V.66: Ajustes Postpago EasyHotspot

Plan de Facturación 

En esta opción se configura el plan de facturación si así lo desea, para crear un nuevo plan de facturación modificar los campos debajo de la lista de plan de facturación existentes, los mismos que pueden ser eliminados dando clic en X, modificados dando clic en el icono lápiz.

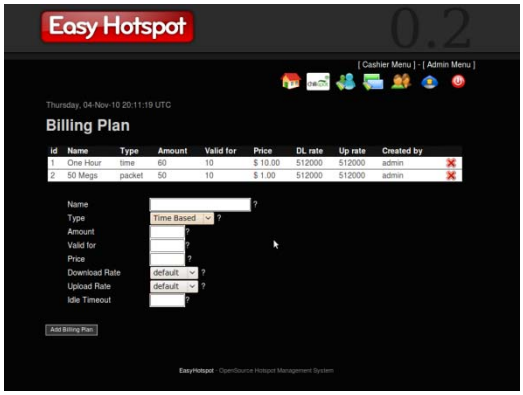


Figura: V.67: Plan de Facturación EasyHotspot

Gestión de Cajero 

Tanto el Administrador como el usuario Caja son los mismos, la diferencia está en el rol de usuario, en esta opción como Administrador se muestra la lista de cajeros.

Figura: V.68: Gestión de Cajeros EasyHotspot

Gestión del Administrador 

Muestra la lista de administradores y su rol.

Figura: V.69: Gestión del Administrador EasyHotspot

Cerrar Sesión 

Es la opción que el usuario cierre la sesión

CAJERO 

Se puede iniciar sesión como usuario cajero después de haber creado una cuenta caja en el administrador.

Figura: V.70: Página de Bienvenida del Cajero EasyHotspot

Administración de cuentas postpago

En esta opción permite la creación, eliminar y modificar un usuario, imprimir comprobante. Si una cuenta ha sido cerrada, no puede ser usada de nuevo, una cuenta puede ser creada por tiempo o por volumen o MB.

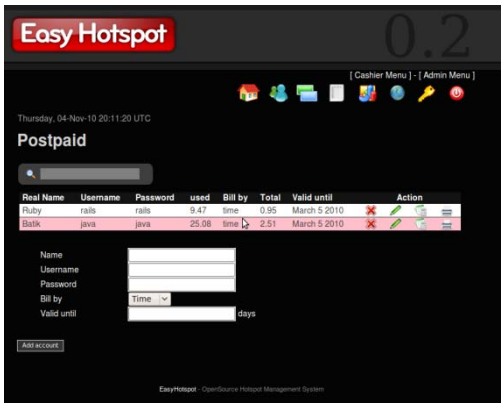


Figura: V.71: Administración de cuentas Postpago Cajero EasyHotspot

Bono de Gestión

Mediante esta opción se pueden generar bonos e imprimirlos para que los clientes puedan acceder a la red. Por lo general, este método es usado en cafés, centros comerciales, hoteles, restaurantes o cualquier lugar donde las personas suelen ser móviles. El cajero tiene opción de imprimir cupones.

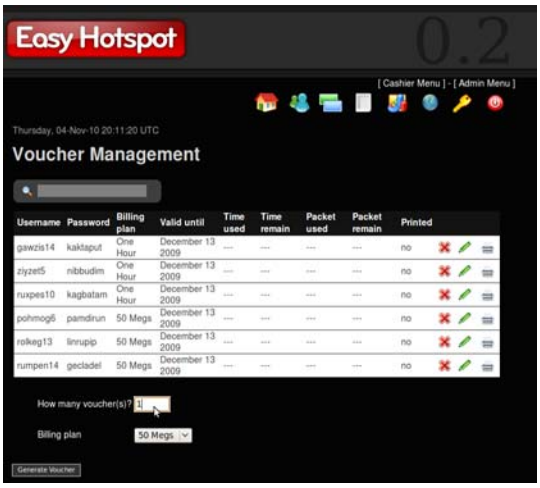


Figura: V.72: Bono de Gestión Cajero EasyHotspot

Gestión Invoice 

Esta opción permite ver todos los detalles de las facturas impresas.

Figura: V.73: Gestión Invoice Cajero EasyHotspot

Estadísticas 

Dando clic en esta opción se pueden ver estadísticas de los cupones, planes de facturación y cuentas creadas.

Figura: V.74: Estadísticas Cajero EasyHotspot

Usuarios en Línea 

Esta opción forza a los clientes a desconectarse.

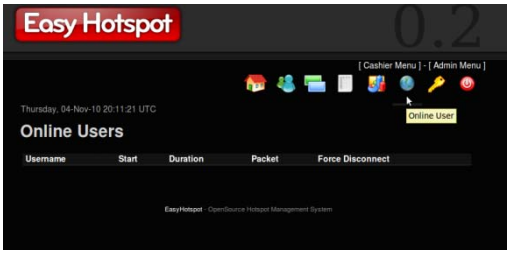


Figura: V.75: Estadísticas Cajero EasyHotspot

Cambiar contraseña 

Mediante esta opción se puede cambiar la contraseña del cajero

Figura: V.76: Cambiar contraseña Cajero EasyHotspot

Cerrar Sesión 

Es la opción que el usuario cajero cierre la sesión

CONFIGURACIÓN DE LA INTERFAZ DEL USUARIO

Para la configuración de la interfaz del usuario ingresar a **/opt/local/web/easyhotspot/hotspot/hotspotlogin.cgi** y modificar el código para adaptarlo a las necesidades de la red o de la empresa en este caso de Bonny Restaurant.

Previo a esto debemos seguir los siguientes pasos:

- Lo primero que se hará es descargar el siguiente archivo de http://smk-karya-budi.sch.id/data/zip/hotspot.zip, haciendo doble clic para extraer el archivo.

- Luego se accederá a la carpeta de los archivos descargados y se colocará en la ruta /opt/local/web/easyhotspot/ htdocs /public, de esta forma se redireccionará del archivo que mostrara la interfaz gráfica hacia este destino accediendo a **hotspologin.cgi** y cambiando http://192.168.182.1/public por http://192.168.182.1/easyhotspot/public.

- Una vez hecho esto se copia la carpeta wp-login.php_files descargado en el directorio /opt/local/web/easyhotspot/ htdocs /public. Luego se abre la carpeta y se configura el archivo wp-admin.css.

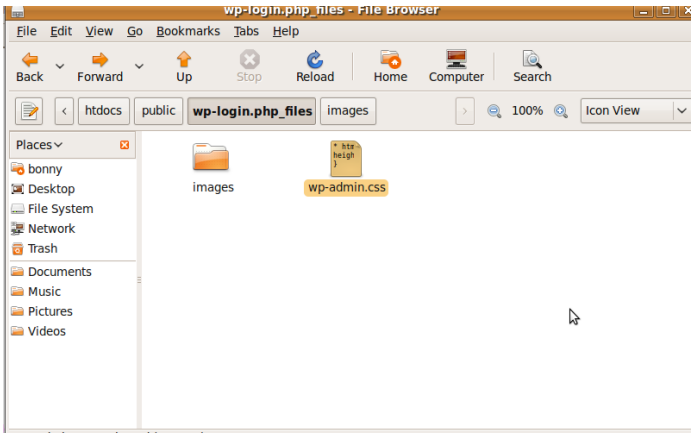


Figura: V.77: Carpeta wp-login.ph_files

- Debido a que este directorio no posee permisos suficientes se deberá asignar por completo ingresando la siguiente línea de comando en el terminal:

sudo chmod 777 / opt / local / web / easyhotspot –R

- Una vez dado permisos se configura wp-admin.css adaptándolo a las necesidades de la interfaz

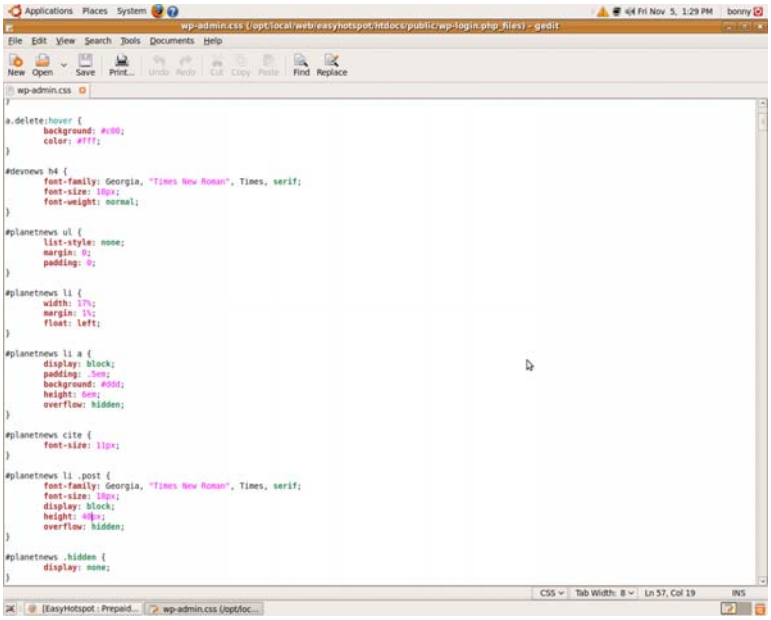


Figura: V.78: Archivo wp-admin.css

- Ahora se abre el directorio /opt/local/web/easyhotspot/hotspot

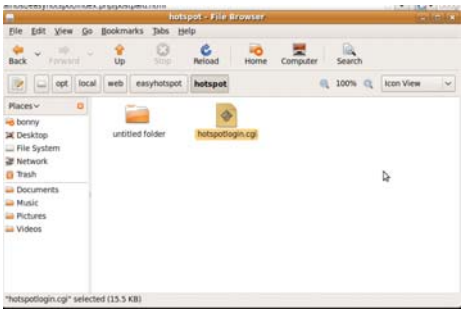


Figura: V.79: Directorio /opt/local/web/easyhotspot/hotspot

- Se abre el archivo hotspotlogin.cgi y se configura el contenido de la interfaz del usuario de la siguiente manera:

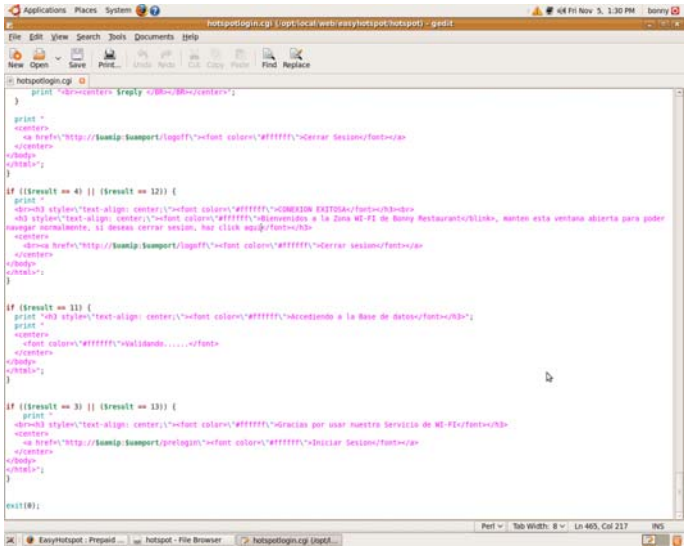


Figura: V.80: Archivo de Configuración de Interfaz Usuario

- A continuación se mostrará la interfaz que tendrá el usuario para el Logeo a la red de Bonny Restaurant.

Figura: V.77: Interfaz Usuarios

CLIENTE

El cliente es aquel que desea hacer uso de la red, y pude conectarse a ella ya sea de forma inalámbrica o por cable, EasyHotspot le otorga un IP y redirecciona al cliente a una página de registro pero este no puede hacer uso de la red mientras no se registre:

Figura: V.78: Interfaz de logeo Usuarios

El usuario deberá ingresar sus datos de una cuenta postpago creada por el administrador, y aparecerá la siguiente pantalla de espera hasta que se verifiquen los datos.

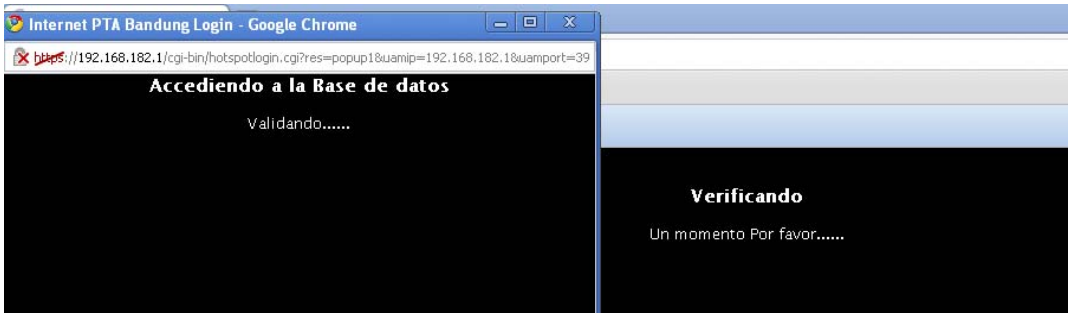


Figura: V.79: Comprobando Datos Usuarios

Si los campos validados son correctos se muestra un splash que le confirme la conexión y en la parte superior veremos el tiempo que transcurre de la conexión:

Figura: V.80: Interfaz de Conexión Exitosa

La cuenta del usuario se puede cerrar de las siguientes maneras:

- Escriba 'http://splash' en la barra de direcciones y se cerrará la sesión
- Si no cerro el 'splash' de logeo puede dar click aquí y cierra sesión
- Escriba en el navegador web http://192.168.182.1:3990/logoff
- El tiempo de la cuenta expiró
- Si el usuario está inactivo por un tiempo limitado por el Administrador.

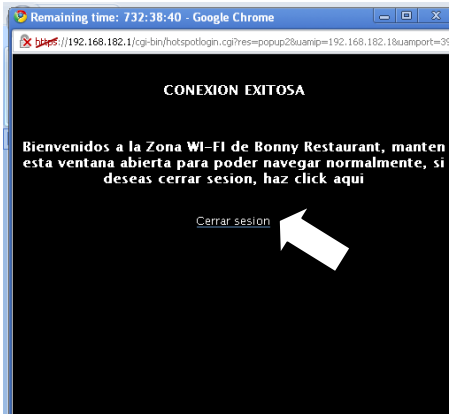


Figura: V.81: Cerrar sesión usuario

En caso de que el usuario ingrese una cuenta no correcta se enviará el siguiente mensaje pidiéndole que intente de nuevo:

Figura: V.82: Interfaz de Conexión Fallo

5.5. Pruebas

PRUEBA DE FUNCIONALIDAD DE LA APLICACIÓN

Para realizar las pruebas de funcionalidad de la aplicación, se utilizaron distintos tipos de dispositivos con los cuales los clientes buscarán conectarse a la red y usando dos tipos de conexión una inalámbrica y por cable.

- Prueba 1

  Para está prueba se utilizó una Laptop Toshiba y una laptop HP y la aplicación funciono correctamente, el usuario quiso hacer uso del internet y fue redireccionado a la página de logeo, y una vez logeado tuvo acceso a la red.

Figura: V.83: Prueba 1 (Toshiba y HP)

- Prueba 2

Para esta prueba se utilizaron celulares con soporte para WI-FI en este caso un Nokia 5800 y un Blackberry curve, los cuales mediante el uso de la red inalámbrica trataron de acceder a la red y fueron redireccionados a la página de logeo al igual que en la Prueba 1, y solo una vez logeado pudo hacer uso de la red.

Figura: V.84: Prueba 2 (Nokia 5800 y un Blackberry curve)

- Prueba 3

Para la prueba número 3 se uso un iPod touch que hizo uso de la red inalámbrica para acceder y al igual que en la prueba 1 y 2 fue redireccionado y solo una vez logeado tuvo acceso a la red.

Figura: V.85: Prueba 3 iPod touch

- Prueba 4

Para esta prueba se utilizo una PC de escritorio conectada a la red a través de un cable directo RJ45 al Router Inalámbrico y se trato de acceder a la red pero de la misma forma que en la red inalámbrica fue redireccionado al logeo y solo una vez registrado pudo tener acceso a la red.

Figura: V.86: Prueba 4 PC escritorio red cableada

PRUEBA DE SEGURIDAD DE LA APLICACIÓN

La redes inalámbricas siempre han estado expuestas a ciertas amenazas por usuarios que buscan tener una conexión a Internet de manera gratuita o sencillamente por uso investigativo, toda red inalámbrica siempre es vulnerable hacia

uno u otro tipo de software que ayuda exclusivamente a descifrar claves WEP, WPA o WPA-PSK, y otras que también ayudan a realizar auditorías a estas redes.

Puesto que la red inalámbrica esta implementada con una aplicación de Portal Cautivo, Se va a usar algunas herramientas para constatar que la red inalámbrica, a pesar de no tener clave WEP o WPA, ofrece una seguridad que es difícil de captar por usuarios ajenos a la red.

La herramienta que se utiliza es Wireshark que es un analizador de protocolos, es un software libre, y se ejecuta sobre la mayoría de sistemas operativos como Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac OS X, así como en Microsoft Windows, la misma que permite ver todo el tráfico que pasa a través de una red, en este caso el trafico que se envía entre el servidor y el Portal.

Este análisis se realizó con siguiente ambiente de prueba:

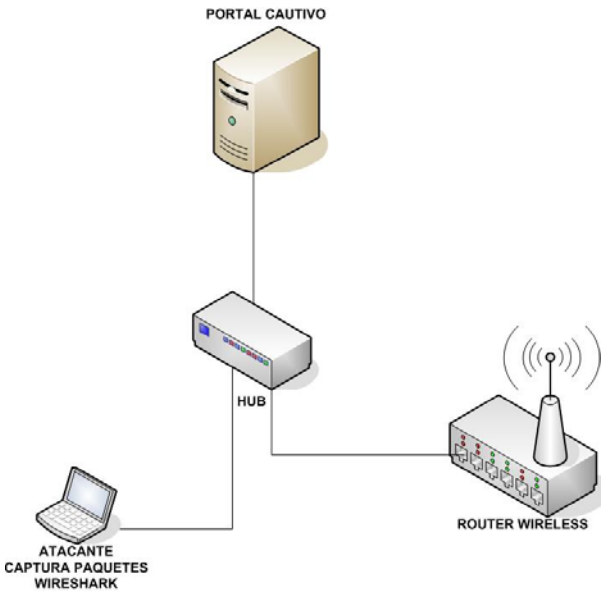


Figura: V.87: Ambiente de prueba de seguridad de la aplicación

Donde se ha usado un HUB como mediador entre el Portal Cautivo el Router Inalámbrico con el objetivo de capturar los paquetes enviados y recibidos por el portal, todo esto por medio de un cliente que posee instalado la herramienta Wireshark.

Obteniendo como resultados **ANEXO E**, el uso de algunos protocolos estos son:

- **TCP:** Permite enviar flujo de datos desde el servidor al cliente
- **UDP:** Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión
- **DNS:** Asigna nombres de dominio a los conexiones de los clientes que ingresan a la red.
- **TLS:** Es un protocolo criptográfico que permite la comunicación segura por la red.
- **HTTPS:** Es un protocolo de red basado en el protocolo HTTP pero destinado a la transferencia segura de datos de Hipertexto.

Mediante el uso de Wireshark se ha podido conocer todos los paquetes y protocolos transmitidos en la ejecución de la aplicación, de donde se puede concluir que la red de Bonny Restaurant con la implementación de la aplicación de portal cautivo posee un alto grado de seguridad contra usuarios ajenos a la red ya que toda la información transmitida entre el servidor, el portal, el cliente es encriptada mediante el protocolo TLS, por lo cual es complicado descifrar las claves de cada usuario. Además no puede haber dos conexiones con el mismo tipo de usuario.

5.6. Demostración Hipótesis

Para la demostración de la Hipótesis ha sido dada en base a opiniones recolectadas en encuestas ver **ANEXO A**, **ANEXO B y ANEXO C** dirigida a dos tipos de usuario el Administrador quien es el que administrará la red (Administradores de Bonny Restaurant) y el Usuario quien es el que hará uso de la misma (clientes del Restaurant), y una vez recolectada esta información se aplica el método estadístico T de Student para la comprobación de la hipótesis.

Se realizaron tres tipos de encuesta dos para los Administradores y una para los usuarios, en cuanto a la determinación de la población se tomó de la siguiente manera.

- Para los Usuarios Administradores se realizó con totalidad de la población en este caso 6 personas que son quienes Administran el Restaurant y estarán a cargo de la aplicación, las encuestas realizadas tienen como objetivo conocer el antes y el después del funcionamiento de la red.

- En cuanto a los Usuarios se determinó que al Restaurant llegan entre clientes nacionales y extranjeros un promedio de 80 en la una sucursal y 100 en la otra, sacando como promedio semanal un total de 480 personas en Bonny 1 y 600 personas en Bonny2 con un total de población de 1080 personas por ambas sucursales.

  N=Población 1080

  E=0.1; Límite de error

  σ = 0.5; Varianza

  Z=1.96; Nivel de confianza

$$n = \frac{N\sigma^2 Z^2}{(N-1)E^2 + \sigma^2 Z^2}$$

$$n = \frac{1080(0.5)^2(1.96)^2}{(1080-1)(0.1)^2 + (0.5)^2(1.96)^2}$$

$$n = 88.27 encuestasrealizadas$$

Representación de los resultados Obtenidos Encuesta Usuarios:

TABLA V.XXIV: Resultados de la Encuesta Realizada a Usuarios

Preguntas	**Repuestas**				
Está de acuerdo con que Bonny Restaurant brinde un servicio de Internet Gratuito	*NO*				*SI*
	0				88
Ha tenido usted problemas para conectarse a esta Red	*SI*				*NO*
	18				70
Cómo fue la velocidad de navegación del Internet del Restaurant	*Muy lenta*	*Lenta*	*Aceptable*	*Buena*	*Rápida*
	0	0	30	50	8
Se siente inseguro al navegar por la red de Bonny	*SI*				*NO*
	9				79
Puede acceder a la red de Bonny Restaurant desde su dispositivo sin problema	*NO*				*SI*
	0				88
Está de acuerdo con que se requiera de autenticación para el uso de Internet por motivos de seguridad y calidad de servicio	*NO*				*SI*
	15				73
TOTAL	42	0	30	50	406
PORCENTAJE	8%	0%	6%	9%	77%

TABLA V.XXV: Resultados de la Encuesta Realizada a Administradores Antes de Implementar un portal cautivo

Preguntas	Respuestas			
1)Cree usted necesario la implementación de un portal cautivo para mejorar la administración en la red de Bonny Restaurant	*NO*			*SI*
	0			6
2)La red actual de Bonny Restaurant permite distribuir el ancho de banda de acuerdo a las necesidades del usuario	*NO*		*Algo*	*SI*
	4		2	0
3)La red actual de Bonny Restaurant le permite llevar un control de los usuarios conectados y los recursos utilizados	*NO*			*SI*
	6			0
4) Piensa usted que un Portal cautivo provee mejor seguridad y acceso a la red inalámbrica de Bonny	*NO*			*SI*
	0			6
5) Llevar un control de los recursos, seguridad y usuarios en la actualidad resulta.	*Muy Difícil*	Difícil	Fácil	*Muy Fácil*
	4	2	0	0
6)Desearía implementar una herramienta que le permita mejorar la administración y gestión de la red inalámbrica de Bonny Restaurant	*NO*			*SI*
	0			6
7)Está satisfecho con las prestaciones que presta la red actual de Bonny Restaurant	*NO*			*SI*
	6			0
TOTAL	20	3	2	18
PORCENTAJE	47.62%	7.14%	4.76%	42.86%

TABLA V.XXVI: Resultados de la Encuesta Realizada a Administradores

Preguntas	Respuestas			
1)Se facilita la administración de los usuarios de la red con la implementación del Portal Cautivo	*NO*			*SI*
	0			6
2)Piensa usted que con la implementación del portal cautivo mejora la distribución del ancho de banda para los usuarios	*NO*		*Algo*	*SI*
	0		2	4
3)Le permite la aplicación realizar estadísticas de los usuarios conectados y sus fuentes	*NO*			*SI*
	0			6
4)Piensa usted que el Portal cautivo proveerá mejor seguridad y acceso a la red inalámbrica de Bonny	*NO*			*SI*
	0			6
5)Piensa usted que la interfaz del portal cautivo al manejarla es	*Muy Difícil*	Difícil	Fácil	*Muy Fácil*
	0	0	1	5
6)Le brinda la aplicación las herramientas necesarias para facilitar su administración	*NO*			*SI*
	0			6
7)Está satisfecho con las prestaciones que brinda el portal cautivo utilizado para la solución	*NO*			*SI*
	0			6
TOTAL	0	0	3	39
PORCENTAJE	0%	0%	7.14%	92.86%

Resultados Finales:

- Con los datos obtenidos en la encuesta realizada a los administradores de la red de Bonny Restaurant antes de la implementación de una aplicación para portal cautivo, se tuvo como resultado que la red no posee ninguna herramienta que facilita la administración ni la gestión de los recursos ni de usuarios y que desearían implementar una herramienta que se ajuste a sus necesidades y que les permita brindar un servicio de calidad.

- Mientras que los resultados obtenidos de la encuesta realizadas a los Administradores y a los usuarios la red de Bonny Restaurant con la implementación de un portal cautivo, se dedujo que la aplicación seleccionada para la implementación de portal cautivo es la que ofrece mejores prestaciones y características para satisfacer las necesidades de la red, ya que los usuarios están en un 77% satisfechos con el servicio de la red, y los administradores un 92.86% totalmente conformes y un 7.14% conformes con los resultados conseguidos en la red tales como, mejor administración de usuarios, distribución de ancho de banda, monitoreo de la red, interfaces amigables, adaptables y fáciles de manejar e intuir, compatibilidad con todos los dispositivos usados en la actualidad por los clientes de Bonny Restaurant para acceder a Internet.

Una vez obtenidos los resultados de las encuestas se procede a demostrar la hipótesis;

La selección de una aplicación para la implementación de un portal cautivo, empleando interconectividad entre los locales del Restaurant Bonny, permitirá administrar la seguridad de acceso de los usuarios a la red inalámbrica corporativa del Restaurant.

A través de los métodos Estadísticos en este caso el método T –Student, debido a que la población específica, con dos tipos de muestras una antes de la implementación aplicación para portales cautivos y una después. De donde:

Ha (Hipótesis alternativa)= La administración de acceso de los usuarios a la red corporativa de Bonny Restaurant a mejorado con la implementación de una aplicación para portal cautivo.

Ho (Hipótesis Nula)= La administración de acceso de los usuarios a la red corporativa de Bonny Restaurat es igual o menor que la administración de acceso otorgada por la aplicación para la implementación de un portal cautivo.

Nivel de Significación:

Por todo valor de probabilidad igual o menor que 0.05 se acepta Ha y se rechaza Ho

Zona de Rechazo:

Por todo valor de probabilidad mayor que 0.05 se acepta Ho y se rechaza Ha.

Con la ayuda de la tabla de T-Student se determinó el grado de libertad que tendrá nuestro estudio en este caso para 0.05 con una muestra de 6 administradores -1 es de 2.0150.

Ahora se procede a calcular la t calculada de la siguiente manera **ANEXO D**:

TABLA V.XXVII: Tabla Datos para aplicación de T Student

Administrador	Encueta Antes	Encueta Después	$(X1-\overline{X1})^2$	$(X2-\overline{X2})^2$
1	17	7	1	0.25
2	17	7	1	0.25
3	19	7	1	0.25
4	19	7	1	0.25
5	18	8	0	0.25
6	18	9	0	2.25
	$\sum X = 108$	$\sum X = 45$	$\sum (X-\overline{X})^2 = 4$	$\sum (X-\overline{X})^2 = 3.5$

Se determinó también la varianza, desviación estándar y la media aritmética obteniendo los siguientes resultados:

Determinación de la media aritmética:

$$\overline{X1} \equiv \frac{\sum X1}{N} \qquad \overline{X2} \equiv \frac{\sum X2}{N}$$

$$\overline{X1} \equiv 18 \qquad \overline{X2} \equiv 7.5$$

La desviación estándar se obtuvo de la siguiente manera:

$$S = \sqrt{\frac{\sum (X1 - \overline{X1})^2}{N1 - 1}} \qquad S = \sqrt{\frac{\sum (X2 - \overline{X2})^2}{N2 - 1}}$$

$$S1 = 1.26 \qquad S2 = 1.565$$

La varianza se obtuvo de la siguiente manera:

$$S^2 1 = (S1)^2 \qquad S^2 2 = (S2)^2$$

$$S^2 1 = 1.6 \qquad S^2 2 = 2.45$$

Una vez obtenido la media aritmética, la varianza y la desviación estándar se procede a obtener el valor estadístico del procedimiento usando la siguiente fórmula:

$$t = \frac{\overline{X1} - \overline{X2}}{S_{X1'X2}}$$

$$S_{X1-X2} = \sqrt{\frac{N1 * S1^2 + N2 * S2^2}{N1 + N2 - 2}} * \sqrt{\left(\frac{1}{N1} + \frac{1}{N2}\right)}$$

$$S_{X1-X2} = \sqrt{\frac{6 * 1.6 + 6 * 2.45}{6 + 6 - 2}} * \sqrt{\left(\frac{1}{6} + \frac{1}{6}\right)}$$

$$S_{X1-X2} = \sqrt{\frac{9.6 + 14.7}{10}} * \sqrt{\frac{1}{3}}$$

$$S_{X1-X2} = 0.899$$

$$t = \frac{18 - 7.5}{0.899}$$

$$t = 11.67$$

El valor t calculado (11.67), se comparan con la tabla, y se observa qu**e al valor crítico (tt) de 2.015** corresponde a una probabilidad de 0.05. De esta manera, el estadístico t 11.67 tiene una probabilidad menor que 0.05.

Decisión

Como el valor de el t calculado tiene un probabilidad menor que la t origen se rechaza Ho y se acepta Ha.

Interpretación:

La administración de acceso a los usuarios a la red corporativa de Bonny Restaurant implementado una aplicación para portal cautivo difieren notoriamente de la administración anterior ya que esta ha mejorado, y puede ser aplicado en cualquier lugar donde se desee llevar una administración del acceso de los usuarios a la red.

CONCLUSIONES

Al finalizar el Estudio de aplicaciones para la implementación de Portales Cautivos, se han obtenido las siguientes conclusiones:

- La implementación de un portal cautivos en una red inalámbrica ofrece una mejor administración y control de los usuarios de la red

- La implementación de un portal cautivo es sumamente de bajo costo pero de alto alcance ya que a más de la seguridad y el fácil uso de la autenticación, existe la posibilidad de generar ingresos de facturación por uso del Internet.

- Existen varias aplicaciones para implementar portales cautivos, cada uno de estos ofrecen varias prestaciones al usuario administrador por lo que no se puede establecer el mejor de una manera generalizada, si se debería escoger uno, se lo haría por el que mejor se ajuste a las necesidades de la empresa, institución o lugar donde se lo vaya a implementar.

- Para la implementación del portal cautivo en Bonny Restaurant, se utilizó Easy Hotspot, que no es más que un paquete basado en Chillispot que permite unir a todos los requerimientos necesarios para el funcionamiento de la aplicación agilitando el tiempo de configuración y de implementación.

- Todo portal cautivo, está expuesto a todo tipo de amenazas como escaneos, snifing, o intrusos que deseen capturar claves (man-in-the-middle), que a diferencia de otras seguridades, éstos solo cubren accesos no deseados por lo que será muy complicado pero no imposible para las amenazas lograr acceder a la red, a pesar también que los datos siempre viajan encriptados.

- Un portal Cautivo para nuestro caso es una de las mejores soluciones que se pudo implementar en el restaurant, tanto por la afluencia de personas que buscan seguridad, calidad y fácil acceso al Internet, provocando así una excelente presentación de la Empresa.

RECOMENDACIONES

- Gracias a la tecnología inalámbrica y la constante evolución que han tenido dispositivos que la usan, los lugares de mayor afluencia de personas, deberían implementar un portal cautivo en su red ya que mediante éste, ayudaría a controlar a sus usuarios como también de brindar un servicio de calidad de Internet.

- Para el análisis comparativo, de los portales cautivos, se deben tomar en cuenta parámetros válidos, que puedan al final ser evaluados, además deben ser orientados a características que permitan la comprobación de la hipótesis.

- Debido a que los portales cautivos poseen escasa información en sus páginas web, es recomendable acceder a blogs y foros relacionados a estos, ya que podemos tener contacto con otras personas que tal vez tienen la solución y respuesta a nuestra inquietud.

- Un portal cautivo como todo tipo de seguridad inalámbrica está expuesto a toda amenaza, por lo que si se desea fortalecer la seguridad en base al portal, se recomienda reforzarlo con un servidor Proxy seguro con un squid y ssl de forma que todas las peticiones al web estén encriptados.

- Ya que la mayor parte de portales cautivos son implementados en software libre (LINUX), es recomendable tener conocimientos básicos sobre el uso de estos comandos, debido a que todas las configuraciones se las hace en modo consola.

- Actualmente se encuentra en pruebas la versión NANO del portal cautivo EASYHOTSPOT, que ofrece mejores características, implementa la ubicación geográfica por usuario a través de google maps, además de personalización de la página de presentación, etc.

RESUMEN

Este Proyecto de Investigación tiene como objetivo realizar un Estudio Comparativo de las Aplicaciones para implementar Portales Cautivos, seleccionar la que brinde mejores prestaciones y aplicarla a la red de Restaurant Bonny, ubicado en la Ciudad de Riobamba, Provincia de Chimborazo.

En el análisis se utilizaron 4 tipos de portales, considerados los más importantes por sus prestaciones, estos son: CHILLISPOT, WIFIDOG, NOCAT y ZEROSHELL, se analizaron características como administración, monitoreo, lenguaje, configuración, conectividad, calidad funcionalidad, entre otros, a través de los Métodos: Deductivo, Experimental, Científico y Comparativo, obteniendo como resultado a CHILLISPOT con un 83 %, como mejor candidato para la implementación en la red de Restaurant Bonny, WIFIDOG con un 77%, NOCAT con un 52% y ZEROSHELL con un 50%. Para la implementación se usó la Herramienta EASYHOTSPOT, basada en CHILLISPOT, para el manejo de la interfaz, la implementación se la realizó en la distribución de Linux UBUNTU SERVER. Además se emplearon dos antenas de 14dbi para enlazar las sucursales del Restaurant Bonny, ubicadas en las calles Villarroel y Almagro y 1era Constituyente y Darquea, separadas a 420 m de distancia, con la finalidad de compartir el servicio de internet. Una vez implementada la aplicación, se determinó mediante el uso de encuestas que la solución ha mejorado en un 77% la calidad de servicio y un 86% las necesidades de los Administradores de la red.

Se concluye que la solución de implementar Un Portal Cautivo en Restaurant Bonny es totalmente factible, ya que permitió administrar la seguridad y controlar el acceso de Internet a los usuarios que usan la red inalámbrica.

Es recomendable implementar este tipo de aplicaciones en todos los lugares que brinden el servicio de Internet inalámbrico Abierto, como restaurantes, aeropuertos, parques, malls, etc, para dar un servicio de Internet controlado y de calidad.

SUMMARY

This investigation Project deals with carrying out a Comparative Study of the Applications to implement Captive Gates, select the one giving the best service and apply it to the network of the Restaurant Bonny, located in Riobamba city, Chimborazo Province.

In the analysis 4 gate types were used, considered to be the most important for their service; these are: CHILLISPOT, WIFIDOG, NOCAT and ZEROSHELL. Characteristics such administration, monitoring, language, configuration, connectivity, quality, functionality among others were analyzed through the deductive, experimental, scientific and comparative methods obtaining the CHILLISPOT with an 83 % as the best candidate for the implementation in the Restaurant Bonny network, WIFIDOG with 77%, NOCAT with 52 % and ZEROSHELL with 50 %. For the Implementation the EASYHOTSPOT tool was used based on CHILLISPOT for the interface, handling the implementation was carried out in the Linux UBUNTU SERVER distribution. Moreover two 14 dbi antennas were used to link branches of the Bonny Restaurant located on the streets Villarroel and Almagro and Primera Constituyente and Darquea separated art 420m to share the internet service. Implemented the application, it was determined, through the use of questionnaires that the solution had improved by 77% the service quality and 86% the needs of the network administrators.

It is concluded that the solution of implementing a captive gate in the Bonny Restaurant is totally feasible as it permitted to administer security and control the internet access of the users using the wireless network. It is recommended to implement this type of applications in all places giving the open wireless Internet Service, such as restaurants, airports, parks, malls, etc., to provide controlled quality Internet service.

ANEXOS

ANEXO A

ENCUESTA SOBRE EL SERVICIO DE WIRELESS EN BONNY RESTAURANT

Estimado Cliente: Estamos trabajando para que el servicio de Internet Inalámbrico de Bonny Restaurant sea de la mejor calidad posible, Por esta razón le rogamos que responda a la siguiente Encuesta con sinceridad y responsabilidad ya que es de primordial importancia para acercarnos a este propósito.

1.- ¿Está de acuerdo con que Bonny Restaurant brinde un servicio de Internet Gratuito?

SI [ ] NO [ ]

2.- ¿Ha tenido usted problemas para conectarse a esta Red?

SI [ ] NO [ ]

3.- ¿Cómo fue la velocidad de navegación del Internet del Restaurant?

Muy Lenta [ ] Lenta [ ] Aceptable [ ] Buena [ ] Rápida [ ]

4.- ¿Qué uso le da usted al Internet de Bonny?

Ver Videos [ ] Descargas [ ]

Revisar Correo [ ] Redes sociales [ ]

Buscar información [ ] OTROS [ ]

5.- ¿Se siente inseguro al navegar por la red de Bonny?

SI [ ] NO [ ]

Por qué _____

6.- ¿Que rango de tiempo usa usted el Internet inalámbrico del restaurant?

1 - 15min [ ] 16 – 30min [ ] 31 – 45min [ ] más de 45 minutos [ ]

7.- ¿Qué tipo de dispositivo usa usted para conectarse a la red inalámbrica?

Laptop o Netbook [ ] Teléfono Celular con WLAN [ ] OTROS [ ]

8.- ¿Puede acceder a la red de Bonny Restaurant desde su dispositivo sin problema?

SI [ ] NO [ ]

9.- ¿Está de acuerdo con que se requiera de autenticación para el uso de Internet por motivos de seguridad y calidad de servicio?

SI [ ] NO [ ]

Por qué _____

PERFIL DE LA PERSONA (GENERAL)

ORIGEN O NACIONALIDAD:_____

INDIQUE EL TRABAJO QUE REALIZA ACTUALMENTE:_____

LUGAR, CIUDAD O CONDADO DE RESIDENCIA:_____

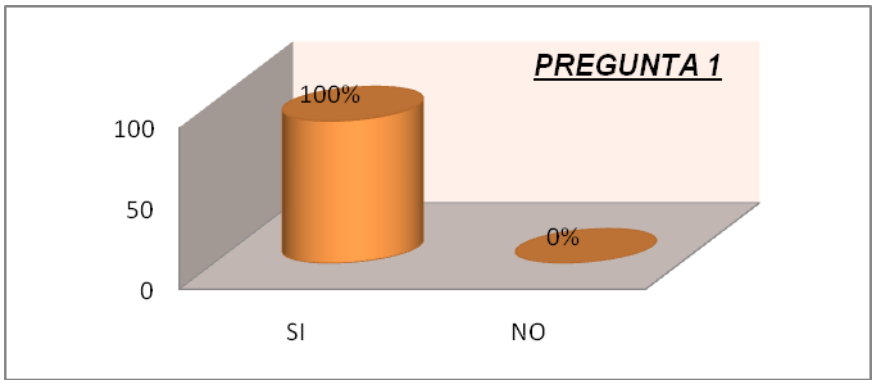
Muchas gracias por su colaboración!

RESULTADOS

ENCUESTA USUARIOS

1.- ¿Está de acuerdo con que Bonny Restaurant brinde un servicio de Internet Gratuito?

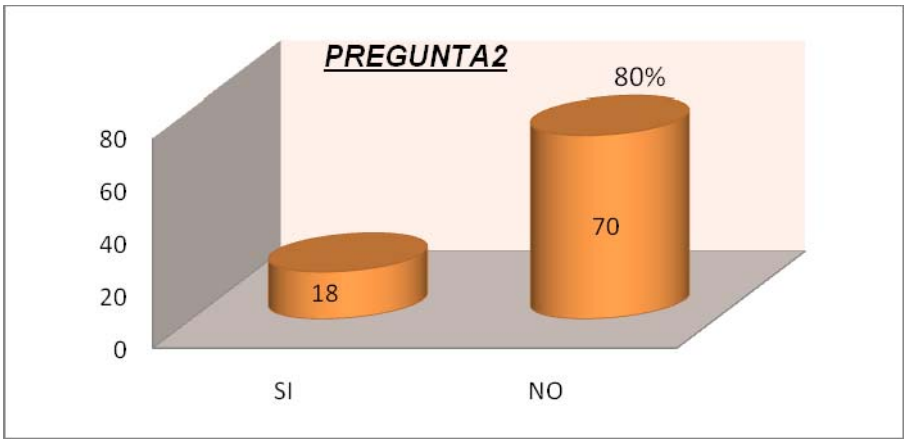
De las encuestas realizadas se obtuvieron los siguientes resultados:



Que en un 100% los clientes de Bonny Restaurant están agradecidos y de acuerdo con la implementación de servicio de Internet gratuito en sus instalaciones ya que en la actualidad todo las comunicaciones tanto personales como empresariales son vía a Internet.

2.- ¿Ha tenido usted problemas para conectarse a esta Red?

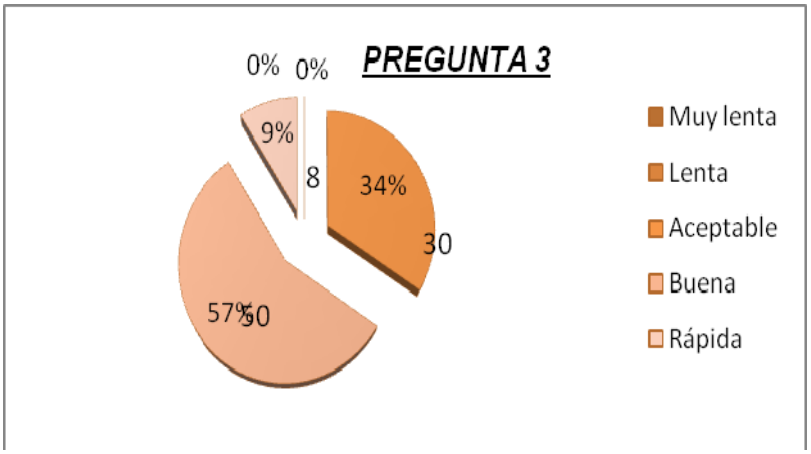
Esta pregunta se realiza con el fin de conocer que tan amigable y que tan fácil es la aplicación para el cliente obteniendo los siguientes resultados:



De los resultados se concluye que tan solo un 20% de los clientes tienen problemas al conectarse a la red mientras que un 80% de clientes del Restaurant no presentan problemas al interactuar con la aplicación, por lo que podemos concluir que la aplicación es sencilla, y amigable para el cliente ya que el porcentaje de rechazo es mínimo.

3.- ¿Cómo fue la velocidad de navegación del Internet del Restaurant?

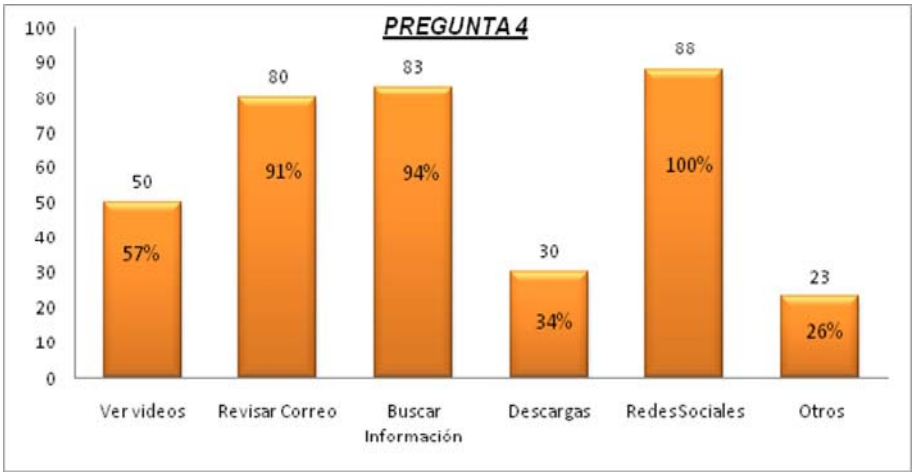
Con esta pregunta se determina la calidad de servicio de Internet que la red de Bonny Restaurant está brindando a sus clientes:



De los datos obtenidos de las encuestas podemos decir que la velocidad de navegación en la red de Bonny Restaurant es buena y está sobre los rangos aceptables para la satisfacción del cliente ya que un 34% opina que la velocidad es aceptable, un 57 % que es buena, un 9% que es rápida, un 0% que es lenta y muy lenta lo que nos demuestra que el servicio satisface a los clientes.

4.- ¿Qué uso le da usted al Internet de Bonny?

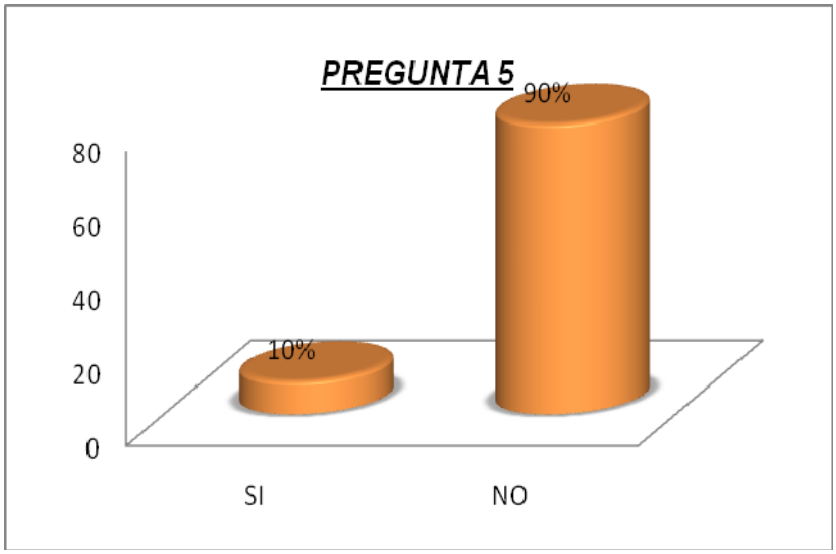
Se realizo esta pregunta con el fin de determinar la demanda de ancho de banda que tienen los clientes de la red de Bonny Restaurant.



De los resultados obtenidos se concluye que en un 100% los clientes utilizan la red para acceder a redes sociales, en un 94% para buscar información, en un 90,9% para revisar correo, en un 57% ver videos, un 34% a realizar descargas y un 26% para otras actividades por lo cual podemos decir que el ancho de banda requerido por la mayor parte de los clientes es básico y que existen usos no tan representativo que requieren de mayor uso de ancho de banda de bajada para descargas y acceso a videos, de los cuales se debe tomar precaución para que no terminen saturando la red.

5.- ¿Se siente inseguro al navegar por la red de Bonny?

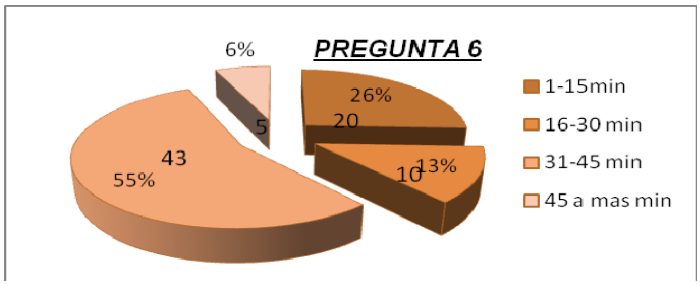
Mediante esta pregunta se pretende confirmar y determinar el grado de seguridad e inseguridad que siente el cliente al acceder a la red de Bonny Restaurant.



Con los datos obtenidos en la encuesta se puede determinar que el 90% de los clientes se sienten seguros de acceder y hacer uso de la red de Bonny Restaurant y solo un 10% de los clientes tienen inseguridad y dado que la inseguridad que siente los clientes es mínima se puede deducir que la seguridad de la red es buena.

6.- ¿Que rango de tiempo usa usted el Internet inalámbrico del restaurant?

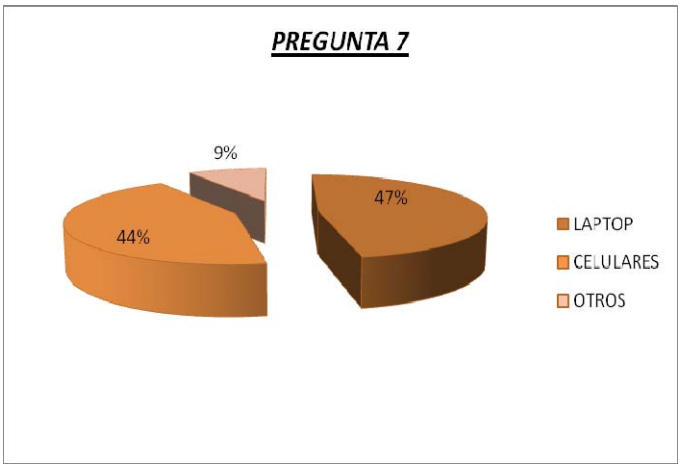
Con los resultados de esta pregunta se conocerá el tiempo promedio que un cliente hace uso de la red.



Al ver los resultados obtenidos se concluye que el tiempo promedio de uso de la red por parte de los clientes de Bonny Restaurant es de 31 minutos a 45 minutos ya que esta fue la opción que obtuvo 55% aceptación, seguido por los clientes que usan 1 a 15 minutos con un porcentaje de 26%, continuando con los clientes que utilizan la red por un período de 16 a 30 minutos con un porcentaje de 13% y finalmente un 6% representado por grupo pequeño de usuarios que utilizan la red por un período de más de 45 minutos. En promedio podríamos decir que la red es usada por los clientes un período de 1 a 45 minutos.

7.- ¿Qué tipo de dispositivo usa usted para conectarse a la red inalámbrica?

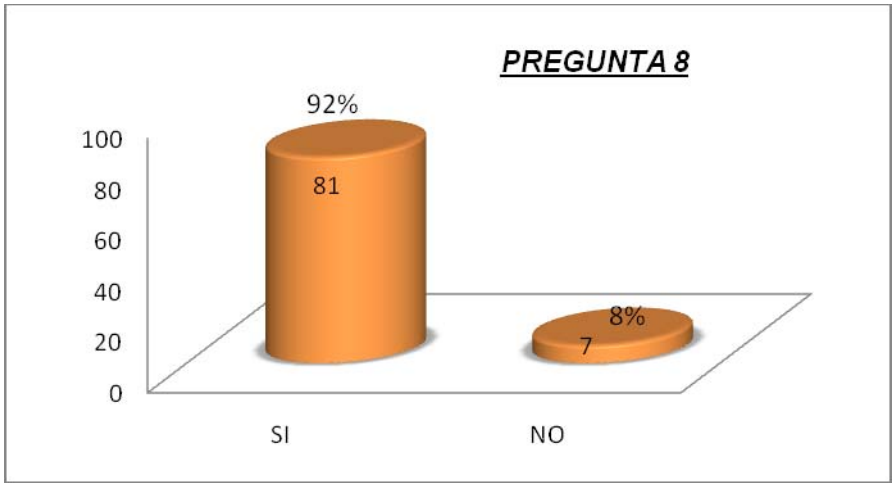
Esta pregunta tiene como objetivo determinar la compatibilidad de la aplicación con los dispositivos inalámbricos o PDAs que son las herramientas con las que los clientes acceden a la red de Bonny



De los resultados obtenidos podemos decir que un 47% de los usuarios de la red utilizan sus laptops para acceder a la misma, un 44% hace uso de sus teléfonos y un 9% de otros dispositivos, es decir la aplicación es compatible con los dispositivos que los clientes de Bonny Restaurant poseen para acceder a la red.

8.- ¿Puede acceder a la red de Bonny Restaurant desde su dispositivo sin problema?

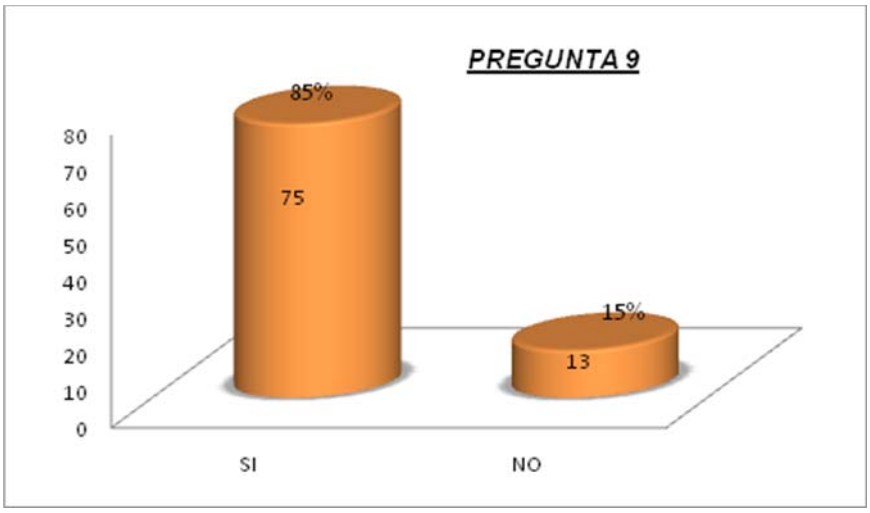
Aquí se quiere determinar si la aplicación da problemas en alguno de los dispositivos que el cliente puede utilizar para su conexión con la red inalámbrica de Bonny Restaurant.



Con los resultados obtenidos se concluye que la aplicación es compatible y funciona sin complicaciones en un 92% de dispositivos que han sido usados por los clientes para el acceso a la red y un 8% de los dispositivos han tenido alguna complicación para acceder a la red.

9.- ¿Está de acuerdo con que se requiera de autenticación para el uso de Internet por motivos de seguridad y calidad de servicio?

Mediante esta pregunta se busca determinar si el usuario se siente molesto por el requerimiento de autenticación o si e) porque sabe que es una medida de seguridad que le brindará un mejor servicio de red.



Luego de analizar los resultados obtenidos se concluye que el 85% de los usuarios de la red están de acuerdo con el uso de autenticación para el acceso a la red y un 15% no está de acuerdo o le parece molestoso el uso de autenticación para acceder a la red.

ANEXO B

ENCUESTA SOBRE EL SERVICIO DE WIRELESS EN

BONNY RESTAURANT ANTES DE IMPLEMENTAR UNA APLICACIÓN PARA PORTAL CAUTIVO

Estimado Administrador: Esta encuesta tiene como finalidad conocer los principales problemas de administración, gestión de usuarios que tiene en la actualidad la red de Bonny. Por esta razón le rogamos que responda a las preguntas con sinceridad y responsabilidad ya que es de primordial importancia para acercarnos a este propósito.

1.- ¿Cree usted necesario la implementación de un portal cautivo para mejorar la administración en la red de Bonny Restaurant?

SI [ ] NO [ ]

2.- ¿La red actual de Bonny Restaurant permite distribuir un ancho de banda adecuado a las necesidades del usuario?

SI [ ] ALGO [ ] NO [ ]

3.- ¿La red actual de Bonny Restaurant le permite llevar un control de los usuarios conectados y los recursos utilizados?

SI [ ] NO [ ]

4.- ¿Piensa usted que el Portal cautivo proveerá mejor seguridad y acceso a la red inalámbrica de Bonny?

SI [ ] NO [ ]

5.- ¿Llevar un control de los recursos, seguridad y usuarios en la actualidad resulta?

MUY FACIL [ ] FACIL [ ] DIFICIL [ ] MUY DIFICIL [ ]

6.- ¿Desearía implementar una herramienta que le permita mejorar la administración y gestión de la red inalámbrica de Bonny Restaurant?

SI [ ] NO [ ]

7.- ¿Está satisfecho con las prestaciones que presta la red actual de Bonny Restaurant?

SI [ ] NO [ ]

PERFIL DE LA PERSONA (GENERAL)

INDIQUE EL TRABAJO QUE REALIZA EN EL RESTAURANT:_____

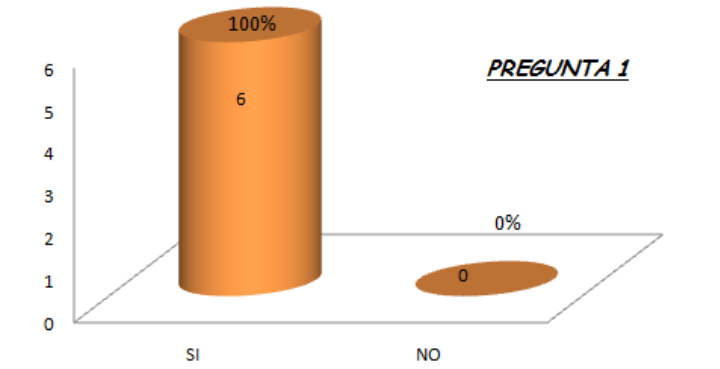
INDIQUE LA INTERACCIÓN QUE TENDRA CON LA APLICACIÓN:_____

RESULTADOS

ENCUESTA ADMINISTRADORES ANTES DE LA IMPLEMENTACIÓN DEL PORTAL CAUTIVO

1.- ¿Cree usted necesario la implementación de un portal cautivo para mejorar la administración en la red de Bonny Restaurant?

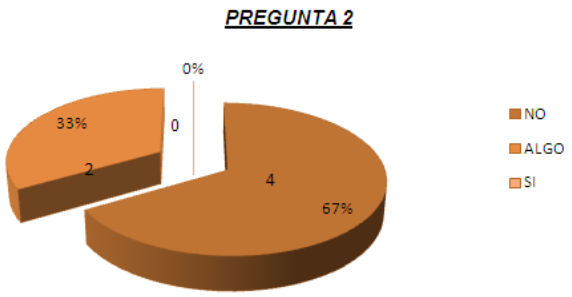
Esta pregunta tiene como objetivo determinar la aceptación que los administradores tienen con la implementación de una aplicación para portal cautivo para mejorar la administración de la red de Bonny Restaurant.



Mediante los datos obtenidos se determina que los administradores están 100% de acuerdo en implementar una aplicación para portal cautivo para mejorar la administración de la red de Bonny Restaurant.

2.- ¿La red actual de Bonny Restaurant permite distribuir un ancho de banda adecuado a las necesidades del usuario?

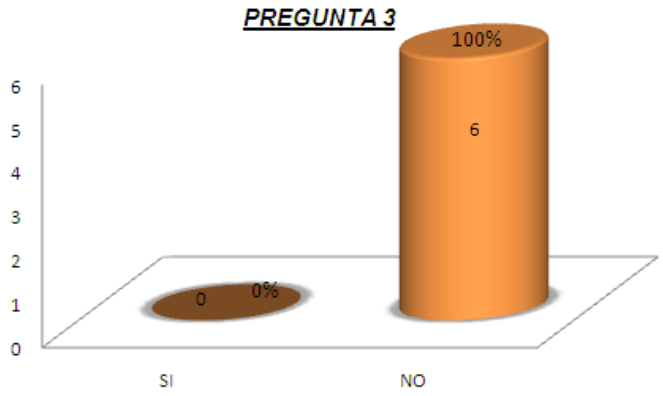
El objetivo de esta pregunta es conocer los alcances que tiene la red actual del Bonny Restaurant.



De donde se concluye que un 67% de los administradores coinciden en que es imposible establecer un ancho de banda adecuado para los clientes y un 33% se puede controlar en algo la distribución del ancho de banda, ya que con la red actual es imposible conocer que cliente consume mayor ancho de banda y establecer un control por usuario.

3.- ¿La red actual de Bonny Restaurant le permite llevar un control de los usuarios conectados y los recursos utilizados?

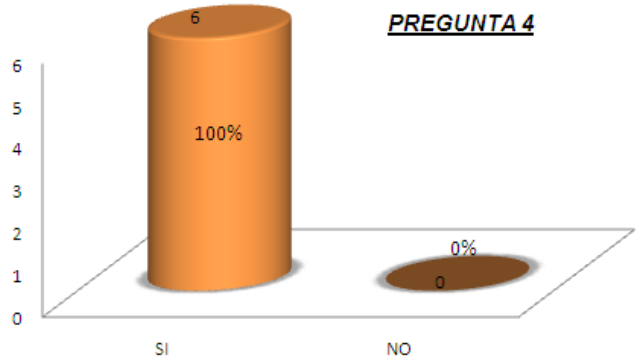
Con esta pregunta se trata de conocer el control actual que tiene la red sobre los usuarios y los recursos que esta dispone.



Mediante los resultados obtenidos se concluye que el 100% de los administradores de la red confirman que no existe un control y una herramienta que les permita gestionar y administrar la red de Bonny Restaurant.

4.- ¿Piensa usted que el Portal cautivo proveerá mejor seguridad y acceso a la red inalámbrica de Bonny?

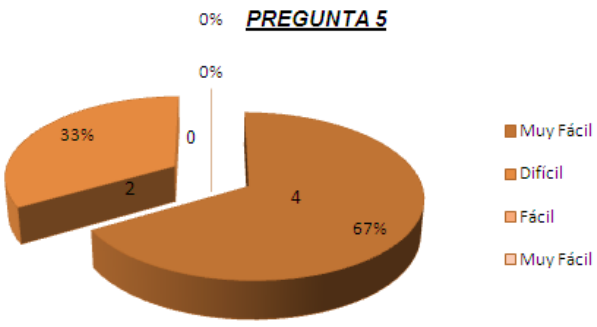
Mediante esta pregunta se determina la aceptación que los administradores de la red tendrán con la aplicación seleccionada para mejorar las debilidades actuales de la red de Bonny Restaurant.



Con estos resultados se puede concluir que el 100% de los administradores están de acuerdo con implementar una aplicación que les permita mejorar el servicio y la administración de la red.

5.- ¿Llevar un control de los recursos, seguridad y usuarios en la actualidad resulta?

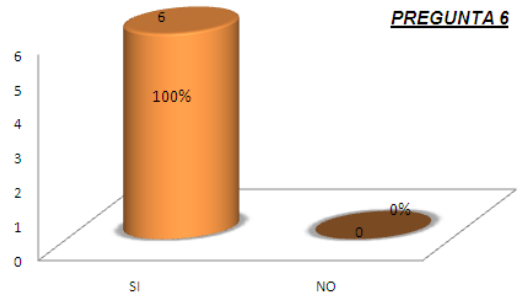
El objetivo de esta pregunta es conocer la dificultad o facilidad que tienen los administradores para controlar la red de Bonny Restaurant.



Como resultado se obtuvo que para 67% de los administradores es Muy Difícil llevar un control de la red y un 33% que es Difícil poder llevar un control tanto de seguridad, recursos y usuarios con la actual estructura de la red.

6.- ¿Desearía implementar una herramienta que le permita mejorar la administración y gestión de la red inalámbrica de Bonny Restaurant?

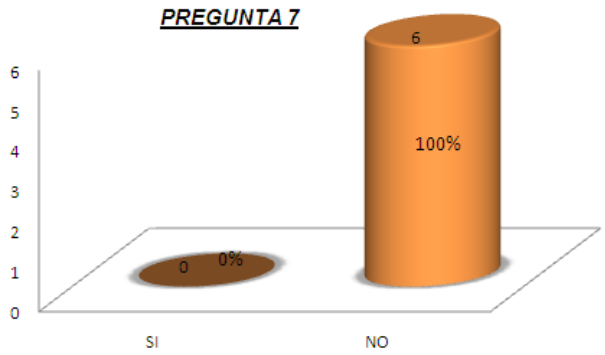
Esta pregunta tiene como objetivo conocer si los administradores de la red de Bonny Restaurant desean implementar una herramienta que mejore la administración y control de la red inalámbrica.



Mediante los resultados se concluye que el 100% de los administradores de la red desean que se implemente una herramienta que les permita mejorar la administración y control de la red inalámbrica de Bonny Restaurant.

7.- ¿Está satisfecho con las prestaciones que presta la red actual de Bonny Restaurant?

Mediante esta pregunta se pretende conocer la satisfacción que tienen los administradores de la red de Bonny Restaurant con la estructura actual y sus prestaciones.



Con los resultados obtenidos en las encuestas realizadas a los administradores de la red de Bonny Restaurnat se conoce que el 100% de ellos está insatisfecho con las prestaciones que tiene la red actualmente.

ANEXO C

ENCUESTA SOBRE EL SERVICIO DE WIRELESS EN

BONNY RESTAURANT

Estimado Administrador: Esta encuesta tiene como finalidad conocer si la aplicación que funciona actualmente en el Restaurant le brinda las facilidades y las herramientas para administrar la red y sus usuarios y si cumple con las necesidades requeridas por Restaurant. Por esta razón le rogamos que responda a las preguntas con sinceridad y responsabilidad ya que es de primordial importancia para acercarnos a este propósito.

1.- ¿Se facilita la administración de los usuarios de la red con la implementación del Portal Cautivo?

SI [ ] NO [ ]

2.- ¿Piensa usted que con la implementación del portal cautivo mejora la distribución del ancho de banda para los usuarios?

SI [ ] ALGO [ ] NO [ ]

3.- ¿Le permite la aplicación realizar estadísticas de los usuarios conectados y sus fuentes?

SI [ ] NO [ ]

4.- ¿Piensa usted que el Portal cautivo provee mejor seguridad y acceso a la red inalámbrica de Bonny?

SI [ ] NO [ ]

5.- ¿Piensa usted que la interfaz del portal cautivo al manejarla es?

MUY FACIL [ ] FACIL [ ] DIFICIL [ ] MUY DIFICIL [ ]

6.- ¿Le brinda la aplicación las herramientas necesarias para facilitar su administración?

SI [ ] NO [ ]

7.- ¿Está satisfecho con las prestaciones que brinda el portal cautivo utilizado para la solución?

SI [ ] NO [ ]

PERFIL DE LA PERSONA (GENERAL)

INDIQUE EL TRABAJO QUE REALIZA EN EL RESTAURANT:_____

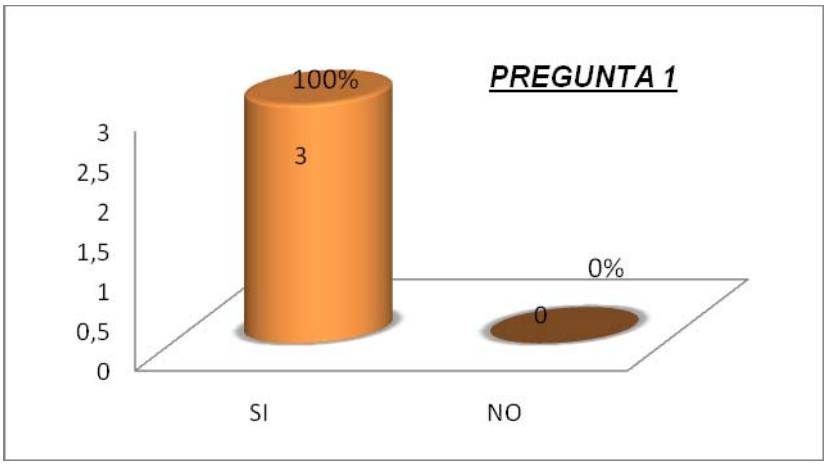
INDIQUE LA INTERACCIÓN QUE TENDRA CON LA APLICACIÓN:_____

RESULTADOS

ENCUESTA ADMINISTRADOR

1.- ¿Se facilita la administración de los usuarios de la red con la implementación del Portal Cautivo?

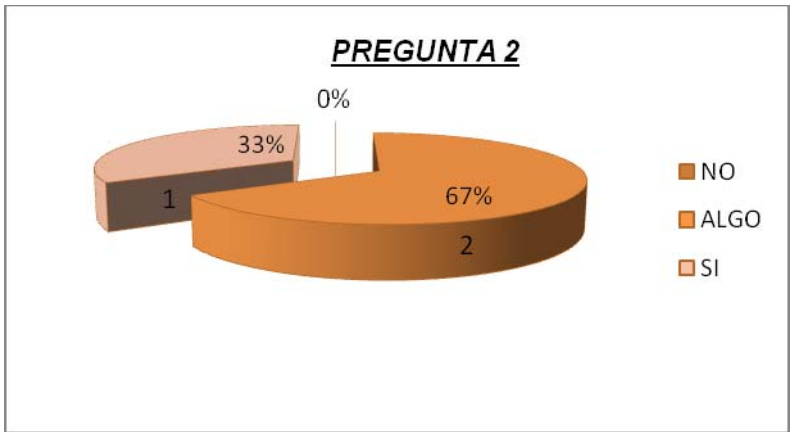
Mediante los resultados de esta pregunta podremos conocer si la implementación del Portal Cautivo que se selecciono satisface las necesidades del administrador de la red.



Como podemos ver en el gráfico el 100% de los administradores opinó que la aplicación les facilita la administración de los usuarios de la red.

2.- ¿Piensa usted que con la implementación del portal cautivo mejora la distribución del ancho de banda para los usuarios?

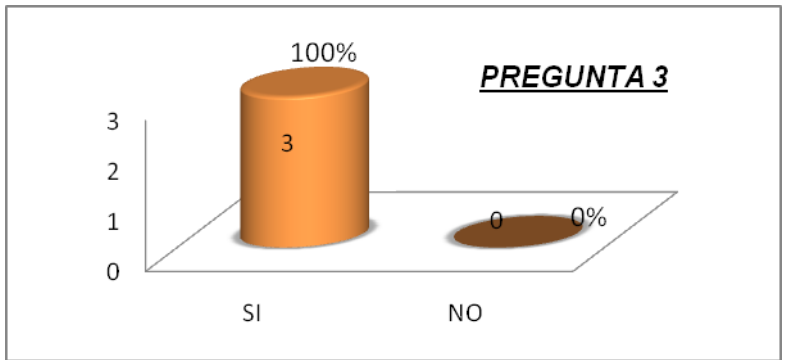
Con el uso de esta pregunta se desea conocer si el administrador puede asignar ancho de banda a los clientes según él lo vea necesario.



Mediante los resultados obtenidos se puede concluir que la aplicación ayuda al administrador en un 67% en la distribución del ancho de banda y un 33% que si mejora por completo la distribución del ancho de banda a los usuarios. Es decir que la aplicación ayuda al administrador a la distribución del ancho de banda de alguna manera.

3.- ¿Le permite la aplicación realizar estadísticas de los usuarios conectados y sus fuentes?

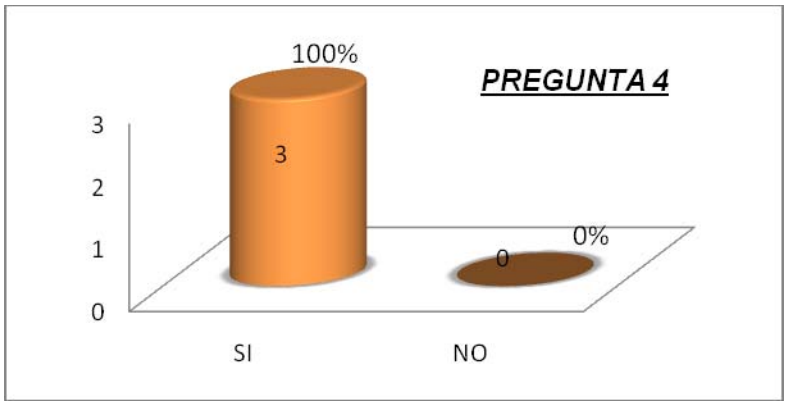
Esta pregunta se realizo para conocer si la aplicación cumple a cabalidad con el requerimiento de monitoreo de la red.



De lo cual se obtuvo el siguiente resultado en un 100% los administradores afirmaron que las estadísticas que presenta la aplicación cumplen con los requerimientos de la red.

4.- ¿Piensa usted que el Portal cautivo provee mejor seguridad y acceso a la red inalámbrica de Bonny?

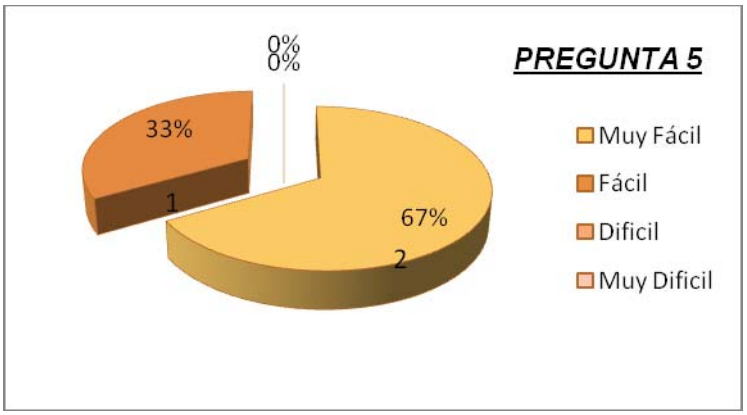
Mediante esta pregunta podemos determinar si los administradores se sienten seguros con la aplicación, y con el acceso a la red que esta utiliza.



Con los resultados se concluye que el 100% de los administradores de la red se siente seguro al usar la aplicación, y están 100% de acuerdo con la forma de autenticación que utiliza el Portal.

5.- ¿Piensa usted que la interfaz del portal cautivo al manejarla es?

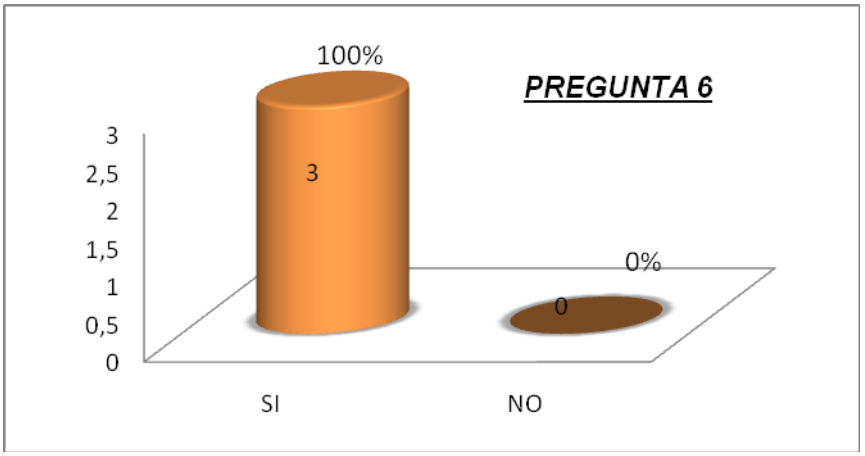
Con esta pregunta se busca determinar si la interfaz es amigable con el usuario, si es sencilla e intuitiva.



Dados los resultamos se puede ver que la interfaz es muy fácil de utilizaren un 67% y es fácil en un 33% por lo que concluimos con que la interfaz presenta amigabilidad con el usuario, es fácil de entender y es totalmente intuitiva.

6.- ¿Le brinda la aplicación las herramientas necesarias para facilitar su administración?

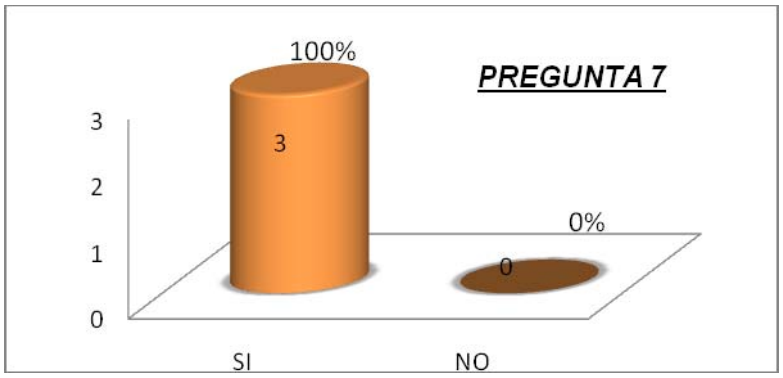
Mediante esta pregunta se trata de conocer si las herramientas de administración que posee la aplicación satisfacen las expectativas de los administradores de la red.



Con los resultados obtenidos se puede decir que la aplicación presenta el 100% de prestaciones para cumplir a cabalidad con las necesidades de la red de Bonny Restaurant.

7.- ¿Está satisfecho con las prestaciones que brinda el portal cautivo utilizado para la solución?

Esta pregunta tiene como finalidad dar a conocer la satisfacción de los administradores con la aplicación.



El resultado se puede ver es que la aplicación es 100% satisfactoria para los administradores de la red de Bonny Restaurant.

ANEXO D

DEMOSTRACIÓN DE LA HIPOTESIS

Para la demostración de la hipótesis se realizaron dos tipos de encuesta dirigida a los 6 administradores de la red de Bonny Restaurant antes de Implantar la aplicación para portal cautivo y después de implantar la aplicación.

A los datos obtenidos por medio de estas encuestas le hemos dado un valor de significancia de acuerdo a las respuestas de la misma, mediante el uso de la siguiente tabla de valoración:

Cuantitativa	**4**	**3**	**2**	**1**
Cualitativa	NO		ALGO	SI
	Muy Difícil	Difícil	Fácil	Muy Fácil

De donde se obtuvo los siguientes resultados:

Administrador 1

Pregunta	Antes	Después
1	1	1
2	2	1
3	4	1
4	1	1
5	4	1
6	1	1
7	4	1
Total	17	7

Administrador 2

Pregunta	Antes	Después
1	1	1
2	2	1
3	4	1
4	1	1
5	4	1
6	1	1
7	4	1
Total	17	7

Administrador 3

Pregunta	Antes	Después
1	1	1
2	4	1
3	4	1
4	1	1
5	4	1
6	1	1
7	4	1
Total	19	7

Administrador 4

Pregunta	Antes	Después
1	1	1
2	4	1
3	4	1
4	1	1
5	4	1
6	1	1
7	4	1
Total	19	7

Administrador 5

Pregunta	Antes	Después
1	1	1
2	4	2
3	4	1
4	1	1
5	3	1
6	1	1
7	4	1
Total	18	8

Administrador 6

Pregunta	Antes	Después
1	1	1
2	4	2
3	4	1
4	1	1
5	3	2
6	1	1
7	4	1
Total	18	9

Una vez obtenidos los resultados de las encuestas procedemos a demostrar la hipótesis;

> La selección de una aplicación para la implementación de un portal cautivo, empleando interconectividad entre los locales del Restaurant Bonny, permitirá administrar la seguridad de acceso de los usuarios a la red inalámbrica corporativa del Restaurant.

A través de los métodos Estadísticos en este caso se selecciona T -Student debido a que la población específica, con dos tipos de muestras una antes de la implementación aplicación para portales cautivos y una después. De donde:

Ha (Hipótesis alternativa)= La administración de acceso de los usuarios a la red corporativa de Bonny Restaurant a mejorado con la implementación de una aplicación para portal cautivo.

Ho (Hipótesis Nula)= La administración de acceso de los usuarios a la red corporativa de Bonny Restaurat es igual o menor que la administración de acceso otorgada por la aplicación para la implementación de un portal cautivo.

Nivel de Significación:

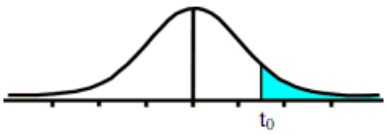
Por todo valor de probabilidad igual o menor que 0.05 se acepta Ha y se rechaza Ho

Zona de Rechazo:

Por todo valor de probabilidad mayor que 0.05 se acepta Ho y se rechaza Ha.

Con la ayuda de la tabla de T-Student se determina el grado de libertad que tendrá nuestro estudio en este caso para 0.05 con una muestra de 6 administradores -1 es de 2.0150.

Tabla t-Student



Grados de libertad	0.25	0.1	0.05	0.025	0.01	0.005
1	1.0000	3.0777	6.3137	12.7062	31.8210	63.6559
2	0.8165	1.8856	2.9200	4.3027	6.9645	9.9250
3	0.7649	1.6377	2.3534	3.1824	4.5407	5.8408
4	0.7407	1.5332	2.1318	2.7765	3.7469	4.6041
5	0.7267	1.4759	2.0150	2.5706	3.3649	4.0321
6	0.7176	1.4398	1.9432	2.4469	3.1427	3.7074
7	0.7111	1.4149	1.8946	2.3646	2.9979	3.4995
8	0.7064	1.3968	1.8595	2.3060	2.8965	3.3554
9	0.7027	1.3830	1.8331	2.2622	2.8214	3.2498
10	0.6998	1.3722	1.8125	2.2281	2.7638	3.1693
11	0.6974	1.3634	1.7959	2.2010	2.7181	3.1058
12	0.6955	1.3562	1.7823	2.1788	2.6810	3.0545
13	0.6938	1.3502	1.7709	2.1604	2.6503	3.0123
14	0.6924	1.3450	1.7613	2.1448	2.6245	2.9768
15	0.6912	1.3406	1.7531	2.1315	2.6025	2.9467
16	0.6901	1.3368	1.7459	2.1199	2.5835	2.9208
17	0.6892	1.3334	1.7396	2.1098	2.5669	2.8982

Una vez determinados p de 0.05 con un grado de libertad de 2.1250 procedemos a determinar las medias, la desviación estándar y la t calculada de la siguiente manera:

Administrador	Encueta Antes	Encueta Después	$(X1-\overline{X1})^2$	$(X2-\overline{X2})^2$
1	17	7	1	0.25
2	17	7	1	0.25
3	19	7	1	0.25
4	19	7	1	0.25
5	18	8	0	0.25
6	18	9	0	2.25
	$\sum X = 108$	$\sum X = 45$	$\sum (X-\overline{X})^2 = 4$	$\sum (X-\overline{X})^2 = 3.5$

De donde:

t= valor estadístico del procedimiento

$\overline{X}$ = Valor promedio o media aritmética de las diferencias entre los momentos antes y después

S= Desviación estándar de las diferencias entre los momentos antes y después.

S^2= Varianza

Determinación de la media aritmética:

$$\overline{X1} \equiv \frac{\sum X1}{N} \qquad \overline{X2} \equiv \frac{\sum X2}{N}$$

$$\overline{X1} \equiv \frac{108}{6} \qquad \overline{X2} \equiv \frac{45}{6}$$

$$\overline{X1} \equiv 18 \qquad \overline{X2} \equiv 7.5$$

La desviación estándar se obtiene de la siguiente manera:

$$S = \sqrt{\frac{\sum (X1 - \overline{X1})^2}{N1 - 1}} \qquad S = \sqrt{\frac{\sum (X2 - \overline{X2})^2}{N2 - 1}}$$

$$S = \sqrt{\frac{8}{6-1}} \qquad S = \sqrt{\frac{12.25}{6-1}}$$

$$S1 = 1.26 \qquad S2 = 1.565$$

La varianza se obtiene de la siguiente manera:

$$S^2 1 = (S1)^2 \qquad S^2 2 = (S2)^2$$

$$S^2 1 = (1.26)^2 \qquad S^2 2 = (1.565)^2$$

$$S^2 1 = 1.6 \qquad .5$$

Una vez obtenido la media aritmética, la varianza y la desviación estándar se procede a obtener el valor estadístico del procedimiento usando la siguiente fórmula:

$$t = \frac{\overline{X1} - \overline{X2}}{S_{X1'X2}}$$

$$S_{X1-X2} = \sqrt{\frac{N1 * S1^2 + N2 * S2^2}{N1 + N2 - 2}} * \sqrt{\left(\frac{1}{N1} + \frac{1}{N2}\right)}$$

$$S_{X1-X2} = \sqrt{\frac{6 * 1.6 + 6 * 2.45}{6 + 6 - 2}} * \sqrt{\left(\frac{1}{6} + \frac{1}{6}\right)}$$

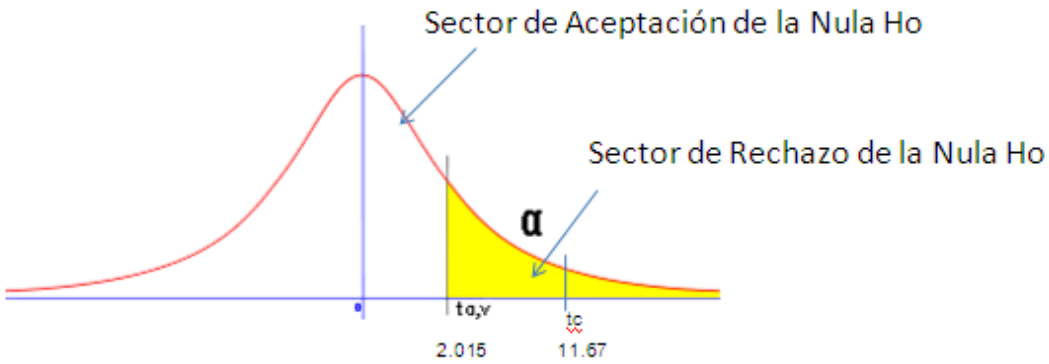
$$S_{X1-X2} = \sqrt{\frac{9.6 + 14.7}{10}} * \sqrt{\frac{1}{3}}$$

$$S_{X1-X2} = 0.899$$

$$t = \frac{18 - 7.5}{0.899}$$

$$t = 11.67$$

El valor t calculado (11.67), se comparan con la tabla, y se observa qu**e al valor crítico (tt) de 2.015** corresponde a una probabilidad de 0.05. De esta manera, el estadístico t 11.67 tiene una probabilidad menor que 0.05.



Decisión

Como el valor de el t calculado tiene un probabilidad menor que la t origen se rechaza Ho y se acepta Ha.

Interpretación:

La administración de acceso a los usuarios a la red corporativa de Bonny Restaurant implementado una aplicación para portal cautivo difieren notoriamente de la administración anterior ya que esta ha mejorado, y puede ser aplicado en cualquier lugar donde se desee llevar una administración del acceso de los usuarios a la red.

ANEXO E

PRUEBAS DE SEGURIDAD DE LA RED

WIRESHARK

Es una herramienta gráfica de código abierto que es utilizada por los administradores de la red para identificar y analizar el tipo tráfico en un momento determinado, se utiliza para dar solución a problemas de la red y para análisis. Originalmente fue llamado **Ethereal**, en mayo de 2006 el proyecto pasó a llamarse Wireshark debido a problemas de marca.

CARACTERÍSTICAS DE WIRESHARK:

- Disponible para UNIX, LINUX, WINDOWS Y Mac OS
- Captura los paquetes directamente desde la interfaz de la red
- Permite obtener un detalle de la información de los protocolos utilizando los paquetes capturados.
- Tiene capacidad de importar y exportar los paquetes capturados hacia otros programas.
- Filtra los paquetes que cumplan con un criterio definido previamente.
- Realiza la búsqueda de los paquetes que cumplan con un criterio definido previamente.

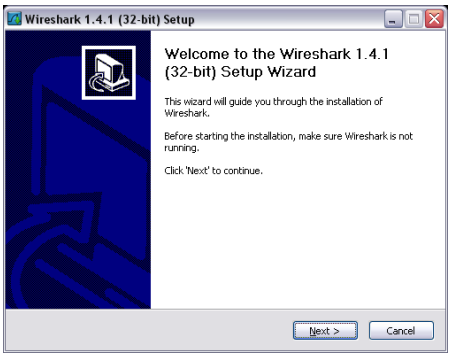
- Permite obtener estadísticas.

- Sus funciones gráficas son muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos.

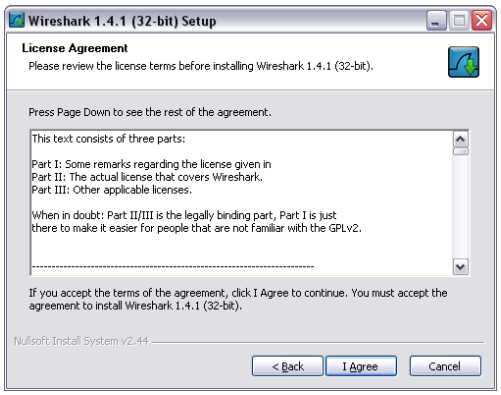
PROCESO DE INSTALACIÓN

Lo primero que se debe hacer es descargar el programa desde WireShark.org, una vez hecho esto daremos doble clic y procederá la instalación:

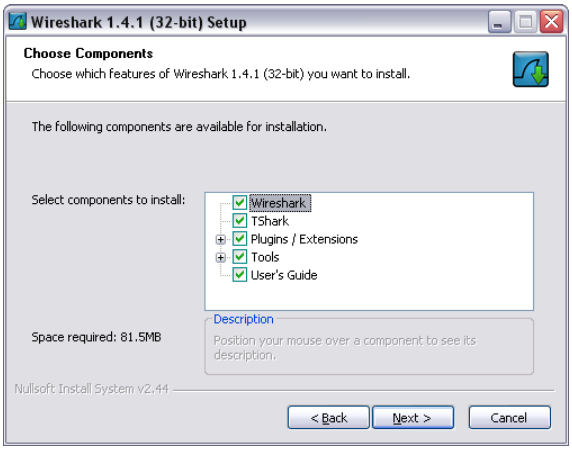
Empezará la instalación, presionar **Next** para continuar



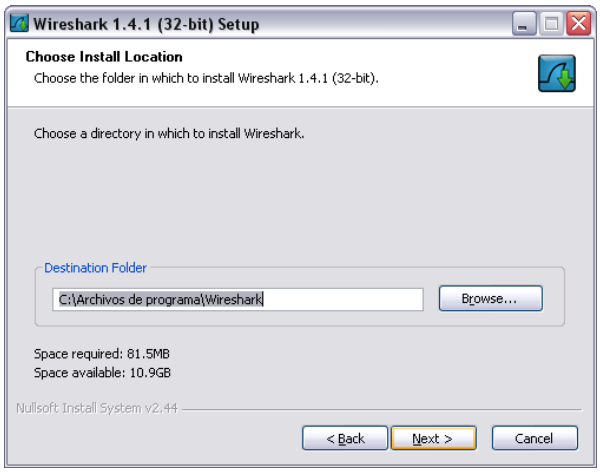
A continuación presionar I Agree para aceptar las condiciones y continuara la instalación:



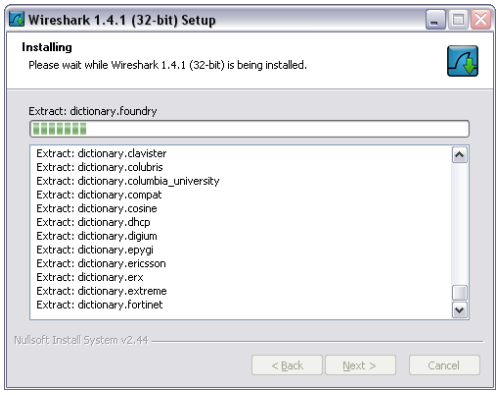
Ahora seleccionamos los componentes a instalar **Next** para continuar:



Escogemos la ruta de instalación y **Next** para continuar con la instalación:



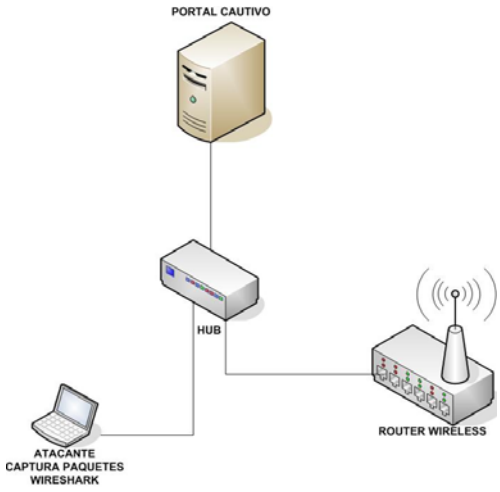
Continuará la instalación:



Una vez terminada la instalación Wireshark presionamos **Finish** y estará listo para ser usado.

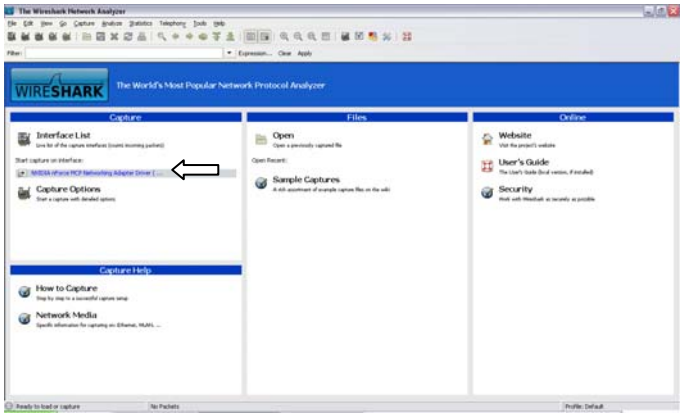
DIAGRAMA FISICO AMBIENTE DE PRUEBA

Para realizar la captura de paquetes se conecta el servidor a un HUB, mediante el uso de un cable directo RJ45, este HUB va conectado también al ROUTER TP-LINK inalámbrico, y a una PC cliente donde se encuentra instalado el capturador de paquetes Wireshark de la siguiente manera:

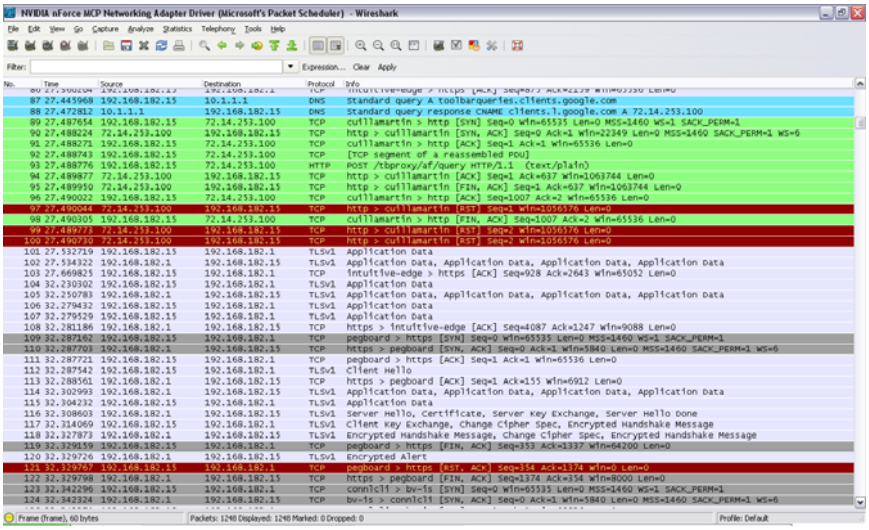


Una vez estructurado el ambiente de prueba se pone a correr la herramienta que se usara para hacer el análisis de la red en este caso Wireshark, lo primero que se debe hacer es escoger la

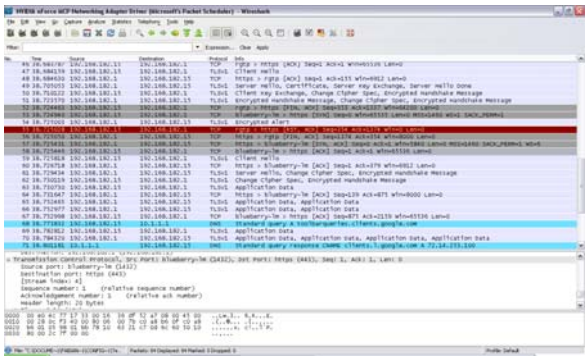
interfaz de la cual se capturará los paquetes en este caso va a ser la tarjeta de red de la computadora donde se instalo la herramienta.



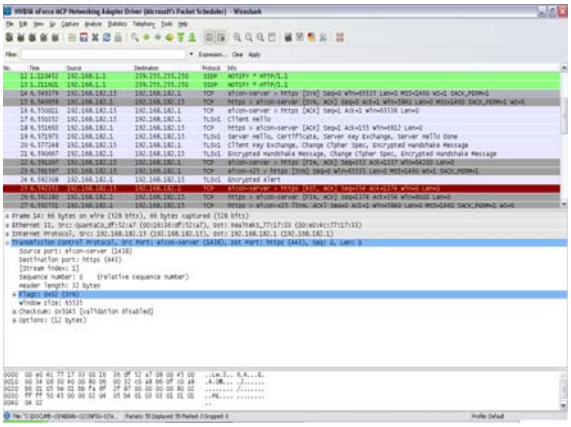
Una vez que se ha seleccionado la interfaz se muestra la captura de los paquetes transmitidos en este caso:



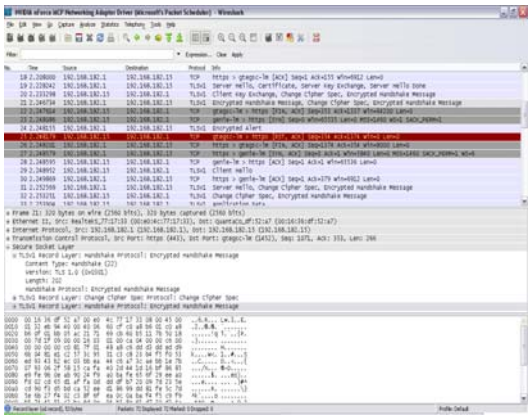
Luego accedemos desde el cliente al WIFI y es redireccionado a la página de presentación login, como podemos ver los protocolos transmitidos en el redireccionamiento TCP, TLS y DNS:



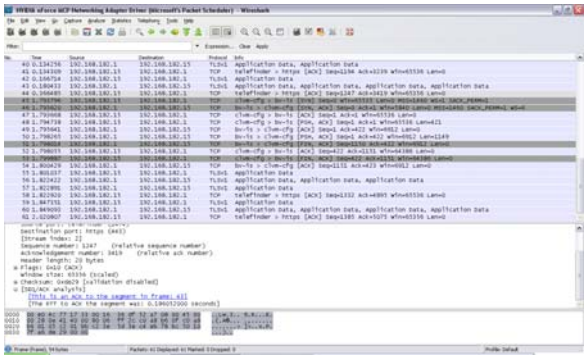
Ahora el usuario tratará de registrarse ingresando su Nombre de Usuario y Password, presiona login y estos son los paquetes enviados, protocolo HTTPS, TCP, TLS y cómo se pude ver toda la información es encriptada mediante el protocolo TLS (Seguridad de la capa de transporte) es un protocolo criptográfico que proporciona comunicaciones seguras por una red:

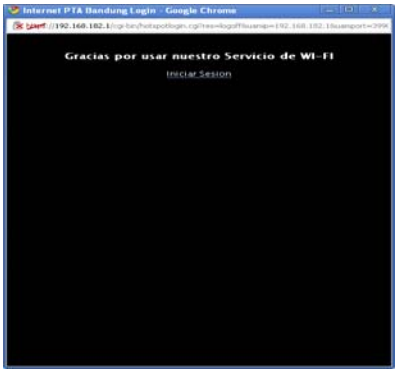


El cliente fue autenticado correctamente se conecta a la red y hace uso de la red, estos son los protocolos transmitidos para mantener la conexión, TCP y TLS



Una vez que el usuario deja de necesitar la red desea desconectarse al hacerlo los protocolos transmitidos son, TCP y TLS:





GLOSARIO

SSID

Es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red.

DHCP

Es un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después**.**

CHAP

Es un método de autentificación usado por servidores accesibles vía PPP. CHAP verifica periódicamente la identidad del cliente remoto usando un intercambio de información de tres etapas. Esto ocurre cuando se establece el enlace inicial y puede pasar de nuevo en cualquier momento de la comunicación. La verificación se basa en un secreto compartido mediante una contraseña.

ARP

Es un protocolo de nivel de red responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

HTTP

El protocolo de transferencia de hipertexto, fue desarrollado por la World Wide Web Consortium, su función es definir la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.

MAC

Es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una Ethernet de red. Se conoce también como la dirección física de un dispositivo de red.

MD5

Es un algoritmo de reducción criptográfico de 128 bits ampliamente usado para brindar cierta seguridad en las claves de red.

MIC

Es un mensaje (código de integridad MIC) que verifica la integridad de los datos de las tramas.

PGP

Es un programa desarrollado por Phil Zimmermann cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

PPP

Es el protocolo que permite establecer una comunicación a nivel de la capa de enlace entre dos computadoras. Generalmente, se utiliza para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un módem telefónico

RSN

RSN es una nueva arquitectura para redes inalámbricas que además de tener una arquitectura más compleja, RSN proporciona soluciones seguras y escalables para la comunicación inalámbrica.

SNIFFER

Es un programa para monitorear y analizar el tráfico en una red de computadoras, detectando los cuellos de botellas y problemas que existan en ella. Un sniffer puede ser utilizado para "captar", lícitamente o no, los datos que son transmitidos en la red.

TKIP

Es también llamado hashing de clave WEP WPA, incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricos.

WIRESHARK

Antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

BIBLIOGRAFÍA

- REDES INALÁMBRICAS

  http://www.maestrosdelweb.com/editorial/redeswlan/

- REDES INALÁMBRICAS

  http://www.albertolsa.com/wp-content/uploads/2009/07/alberto-los-santos-seguridad-en-wi-fi.pdf

- REDES INALAMBRICAS

  http://www.monografias.com/trabajos12/reina/reina.shtml

  ]

- 802.1x

  http://dns.bdat.net/seguridad_en_redes_inalambricas/x75.html

  [Consulta: 2010 02 18]

- 802.1x

  http://cita2003.fing.edu.uy/articulosvf/59.pdf

  [Consulta: 2010 02 19]

- 802.1x

  http://www.sans.org/reading_room/whitepapers/wireless/consideraciones_para_la_implementacion_de_802_1x_en_wlans_1607

  [Consulta: 2010 02 23]

- EAP y FreeRADIUS

  http://www.linux-magazine.es/issue/05/Radius.pdf

  [Consulta: 2010 03 03]

- FreeRADIUS

  http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/995/4/T10761CAP2.pdf

  [Consulta: 2010 03 03]

- RADIUS

http://technet.microsoft.com/es-

es/library/cc781821(WS.10).aspxhttp://www.alegsa.com.ar/Dic/radius.php

[Consulta: 2010 03 04]

- RADIUS

http://www.radiusdoc.com/Toc-1.htm

[Consulta: 2010 03 04]

- PORTALCAUTIVO

http://wndw.net/pdf/wndw-es/chapter6-es.pdf
[Consulta: 2010 03 04]

- PORTAL CAUTIVO

http://rosariowifi.com.ar/portales.html

[Consulta: 2010 03 04]

- VULNERABILIDADES DE LAS REDES INALÁMBRICAS

http://www.informatica-hoy.com.ar/redes-inalambricas-wifi/Vulnerabilidades-de-las-redes-WIFI.php
[Consulta: 2010 03 11]

- VULNERABILIDADES DE LAS REDES INALÁMBRICAS

http://wikiole.com/ordenadores/seguridad/vulnerabilidad-en-redes.html
[Consulta: 2010 03 11]

- WIFIDOG

http://www.bcwireless.net/moin.cgi/WifiDog&ei=9IG7S5fDKIbs9gT3nIH4Bw&sa=X&oi=translate&ct=result&resnum=1&ved=0CAcQ7gEwADgU&prev=/search%3Fq%3Dwifidog%26start%3D20%26hl%3Des%26sa%3DN
[Consulta: 2010 03 05]

- WIFIDOG

http://delta.cs.cinvestav.mx/~fraga/Cursos/Seguridad/2008/Wireless_Portals_

with_Wifidog.pdf

[Consulta: 2010 03 05]

- WIFIDOG

http://dev.wifidog.org/

[Consulta: 2010 03 05]

- NOCAT

http://www.slideshare.net/vilmazapana/seguridad-en-redes-inalambricas-presentation

[Consulta: 2010 03 08]

- NOCAT

http://anuiesnoroeste.uson.mx/rscn/reuniones/06/memorias/aut_redes_inalambricas.pdf

[Consulta: 2010 03 12]

- ZEROSHELL

http://www.taringa.net/posts/downloads/2234886/Crea-un-router-linux-en-tu-pc_-ZeroShell.html

[Consulta: 2010 04 02]

- ZEROSHELL

http://www.zeroshell.net/license/

[Consulta: 2010 04 06]

- ZEROSHELL

http://www.nomatch.es/media/2246/cursozeroshell.pdf

[Consulta: 2010 04 21]

- CHILLISPOT

http://www.chillispot.info/

[Consulta: 2010 09 08]

- CHILLISPOT

http://jpill.wordpress.com/2008/08/11/46/

[Consulta: 2010 09 10]

- EASYHOTSPOT

http://easyhotspot.inov.asia/index.php/documentation

[Consulta: 2010 09 11]