UNIVERSIDAD LUTERANA SALVADOREÑA

FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA

LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

ASIGNATURA: REDES II

TEMA DEL PROYECTO: IMPLEMENTACIÓN DE UN PORTAL CAUTIVO WIFI (HOTSPOT)

DOCENTE: ING. MANUEL FLORES

PRESENTADO POR:

N°	APELLIDOS	NOMBRES	CARNET	PARTICIPACIÓN
1	FUNES RIVERA	NORMA MAGDALENA	FR02110904	100%
2	JIMÉNEZ VALLADARES	VERÓNICA MARLENE	JV01121165	100%
3	JUÁREZ GARCÍA	ANA MARGARITA	JG02110132	100%

SÁBADO 08 DE NOVIEMBRE DE 2014

ÍNDICE DE CONTENIDO

ÍNDICE DE ILUSTRACIONES

INTRODUCCIÓN

Un portal cautivo es una aplicación utilizada generalmente en redes inalámbricas abiertas (hotspots) para controlar el acceso a la misma, aunque también puede utilizarse en redes cableadas.

Cuando un usuario, una vez seleccionada la red WIFI y establecida la conexión inalámbrica, intenta acceder a una página web utilizando cualquier navegador, el portal cautivo captura esta solicitud y en lugar de la página solicitada le presenta al usuario la página de registro al sistema, bloqueando cualquier otro tipo de tráfico. Una vez que el usuario introduce sus datos y estos son comprobados se le permite el acceso a la red facilitándole la página web inicialmente solicitada.

El presente proyecto busca servir como guía, para la instalación y configuración de un portal cautivo WiFi, en un sistema operativo GNU/Linux, para este caso se ha usado EasyHotspot, el cual viene dentro de Ubuntu 9.04, en el cual se hace uso de diferentes servicios como el DHCP, servicios de wlan, servidor radius, entre otros con una finalidad concreta y siguiendo una serie de pasos se llega al resultado deseado que es el que a continuación se detalla:

- Objetivos tanto general como los específicos, propuestos por el grupo de trabajo y con la finalidad de cumplir cada uno de ellos.
- Marco teórico, el cual explica de manera amplia que es un portal cautivo, las tecnologías a utilizar, los servicios que se están usando, etc.
- Una información detallada de los pasos, comandos y procedimientos que se utilizaron en el desarrollo del proyecto.
- Escenarios de prueba los cuales demuestran su correcto funcionamiento.
- Conclusiones y recomendaciones a las que se llego al finalizar el proyecto.
- Bibliografía que se ha usado para obtener la información.

OBJETIVOS

OBJETIVO GENERAL

- Instalar y configurar un portal cautivo WiFi (hotspot) en un Sistema Operativo GNU/Linux.

OBJETIVOS ESPECÍFICOS

- Investigar e implementar las tecnologías involucradas en la configuración de un portal cautivo WiFi.

- Explicar paso a paso la construcción de un portal cautivo WiFi, con sus respectivos comandos y procedimientos.

- Realizar pruebas para verificar el correcto funcionamiento del portal cautivo WiFi (hotspot)

MARCO TEÓRICO

Implementación de un portal cautivo wifi (hotspot)

Un portal cautivo es un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal. El programa intercepta todo el tráfico HTTP hasta que el usuario se autentifica.

El portal se encargará de hacer que esta sesión caduque al cabo de un tiempo, también puede empezar a controlar el ancho de banda usado por cada cliente (haciendo lo que se llama Calidad de Servicio). En el contexto de las comunicaciones inalámbricas, un hotspot (punto caliente) es un lugar que ofrece acceso a Internet a través de una red inalámbrica y un enrutador conectado a un proveedor de servicios de Internet.

Usualmente, los hotspot son zonas de alta demanda de tráfico y que por tanto el dimensionamiento de su cobertura está condicionado a cubrir esta demanda por parte de un punto de acceso o varios y de este modo proporcionar servicios de red a través de un proveedor de servicios de Internet Inalámbrico (WISP).

WISP: Es un acrónimo para Wireless internet serviceprovider o proveedor de servicios de internet inalámbrico pueden ser hotspot Wi-fi, un operador con una estructura Wi-fi.

TECNOLOGÍAS WI-FI

Wi-Fi (Wireless Fidelity) es la tecnología utilizada en una red o conexión inalámbrica, para la comunicación de datos entre equipos situados dentro de una misma área (interior o exterior) de cobertura.

Las redes inalámbricas permiten la transmisión de datos a velocidades de 11 Mbps o incluso superiores, lo que proporciona rapidez suficiente para la mayoría de las aplicaciones.

En la actualidad podemos encontrarnos con dos tipos de comunicación WIFI: 802.11b, que emite a 11 Mb/seg, y 802.11g, más rápida, a 54 MB/seg.

Estándar IEEE 802.11

- Los estándares IEEE 802.11b, IEEE 802.11g e IEEE 802.11n disfrutan de una aceptación internacional debido a que la banda de 2.4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbit/s, 54 Mbit/s y 300 Mbit/s, respectivamente.

- En la actualidad ya se maneja también el estándar IEEE 802.11a, conocido como WIFI 5, que opera en la banda de 5 GHz y que disfruta de una operatividad con canales relativamente limpios. La banda de 5 GHz ha sido recientemente habilitada y, además, no existen otras tecnologías (Bluetooth, microondas, ZigBee, WUSB) que la estén utilizando, por lo tanto existen muy pocas interferencias. Su alcance es algo menor que el de los estándares que trabajan a 2.4 GHz (aproximadamente un 10 %), debido a que la frecuencia es mayor (a mayor frecuencia, menor alcance).

USO DE LOS PORTALES CAUTIVOS

Se usan sobre todo en redes inalámbricas abiertas, donde interesa mostrar un mensaje de bienvenida a los usuarios y para informar de las condiciones del acceso (puertos permitidos, responsabilidad legal). Los administradores suelen hacerlo para que sean los propios usuarios quienes se responsabilicen de sus acciones y así evitar problemas mayores. Se discute si esta delegación de responsabilidad es válida legalmente.

SISTEMAS DE PORTAL CAUTIVO QUE EXISTEN

PepperSpot: Es un portal cautivo o un controlador de punto de acceso LAN inalámbrico que soporta el protocolo IPv6. Es compatible con inicio de sesión basado en la web y es compatible con WirelessProtected Access (WPA). La autentificación se realiza mediante el servidor de radio favorita (sobreIPv4 / IPv6)

MikroTikHotspot: Es muy fácil de configurar, pero hay que hacer ciertas modificaciones para evitar tener problemas en nuestra red si es que utilizamos AP's o Routers modo cliente.

Chillispotes**:** Una fuente de portal cautivo abierto o controlador de punto de acceso LAN inalámbrico. Se utiliza para la autenticación de usuarios de una LAN inalámbrica.

CoovaChilli: Es un controlador de acceso de software rica característica que proporciona un entorno de portal / jardín-vallado cautivo y utiliza RADIUS o un protocolo HTTP para el acceso de aprovisionamiento y la contabilidad. CoovaChilli es una parte integral de la CoovaAP firmware basado en OpenWRT que está especializada para las zonas activas.

WiFiDog: Es una solución de portal cautivo de código abierto. Como tal, tiene tres funciones principales:

1. Sensible a la ubicación de entrega de contenido interno o externo
2. De autenticación y autorización
3. Supervisión de la red Centralizada

FUNCIONAMIENTO

Cuando un usuario, una vez seleccionada la red WIFI y establecida la conexión inalámbrica, intenta acceder a una página web utilizando cualquier navegador, el portal cautivo captura esta solicitud y en lugar de la página solicitada le presenta al usuario la página de registro al sistema, bloqueando cualquier otro tipo de tráfico. Una vez que el usuario introduce sus datos y estos son comprobados se le permite el acceso a la red facilitándole la página web inicialmente solicitada.

Normalmente un portal cautivo consta de dos partes: Una puerta de enlace gateway y un servidor de autenticación. El gateway gestiona las reglas de cortafuegos, denegando el acceso a la red a los usuarios no identificados y estableciendo qué puertos y protocolos están permitidos a los usuarios autorizados. El gateway se conecta con el servidor de autenticación que realiza la comprobación de los datos de usuario, bien utilizando una base de datos local o consultando a un servidor Radius, para permitir o denegar el acceso a la red, así como asignar algunas restricciones como un límite de tiempo o un ancho de banda determinado.

Protocolo 802.1x: Es una norma o frameworks que provee autenticación de red. Su principal uso es la **autenticación de usuarios y dispositivos en una red cableada y/o inalámbrica.**

Es un método de seguridad que autentica el acceso al puerto del switch o el acceso a la wifi. Por tanto, podemos decir que **802.1x es un mecanismo de seguridad de acceso al medio.**

Su implementación en entornos corporativos puede ser compleja porque hay que tener en cuenta múltiples situaciones y compatibilidades.

DESCRIPCIÓN DEL PROTOCOLO 801.1X

Implica tres partes: Un suplicante, un autenticador y un servidor de autenticación. El solicitante es un dispositivo cliente (tal como un ordenador portátil) que desea conectar a la LAN / WLAN - aunque el término 'solicitante' también se utiliza indistintamente para referirse al software que se ejecuta en el cliente que proporciona credenciales para el autenticador.

El autenticador: Es un dispositivo de red, como un conmutador Ethernet o punto de acceso inalámbrico y el servidor de autenticación es típicamente un software que se ejecuta anfitrión apoyar las RADIUS y EAP protocolos. El autenticador actúa como un guardia de seguridad de una red protegida.

El suplicante: (Es decir, el dispositivo cliente) no se permite el acceso a través del autenticador para el lado protegido de la red hasta que la identidad del solicitante ha sido validado y autorizado.

Una analogía de esto es proporcionar una visa válida a la inmigración llegada del aeropuerto antes de poder entrar en el país. Con la autenticación basada en el puerto 802.1X, el suplicante proporciona credenciales, como el nombre de usuario / contraseña o certificado digital, el autenticador envía las credenciales al servidor de autenticación para su verificación.

Si el servidor de autenticación determina las credenciales son válidas, el solicitante (dispositivo cliente) se le permite acceder a los recursos situados en el lado protegido de la red.

Gateway: Es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red inicial al protocolo usado en la red de destino.

Un servidor RADIUS: Es el que gestiona el acceso a las redes. Se utiliza principalmente por los proveedores de servicios de Internet para gestionar acceso a Internet a sus clientes. El nombre RADIUS es en realidad un acrónimo de "Remote Authentication Dial In UserService" (Dial de autenticación remoto para acceso a servicios). El protocolo no sólo logra acceso a la red, sino también a la gestión de cuentas del usuario.

TECNOLOGÍAS A UTILIZAR EN LA IMPLEMENTACIÓN DE UN PORTAL CAUTIVO

- ✓ Un ordenador donde instalar el portal cautivo con 2 tarjetas de red
- ✓ Un Wireless Access Point (Punto de acceso Wifi)
- ✓ Cables de red
- ✓ Acceso a Internet
- ✓ CD de instalación de EasyHotSpot
- ✓ 2 o más PC
- ✓ 1 switch
- ✓ Sistema operativo GNU/Linux

Estas tecnologías son las necesarias para la implementación de un portal cautivo.

Un punto de acceso inalámbrico: (WAP o AP por sus siglas en inglés. Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación alámbricas para formar una red inalámbrica.

Cables de red: Es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e, 6 y 6a).

Switch: Es un dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI.

EasyHotSpot: Es un software que reúne las características necesarias para la implementación de un portal cautivo en GNU/Linux.

DIAGRAMA DE RED

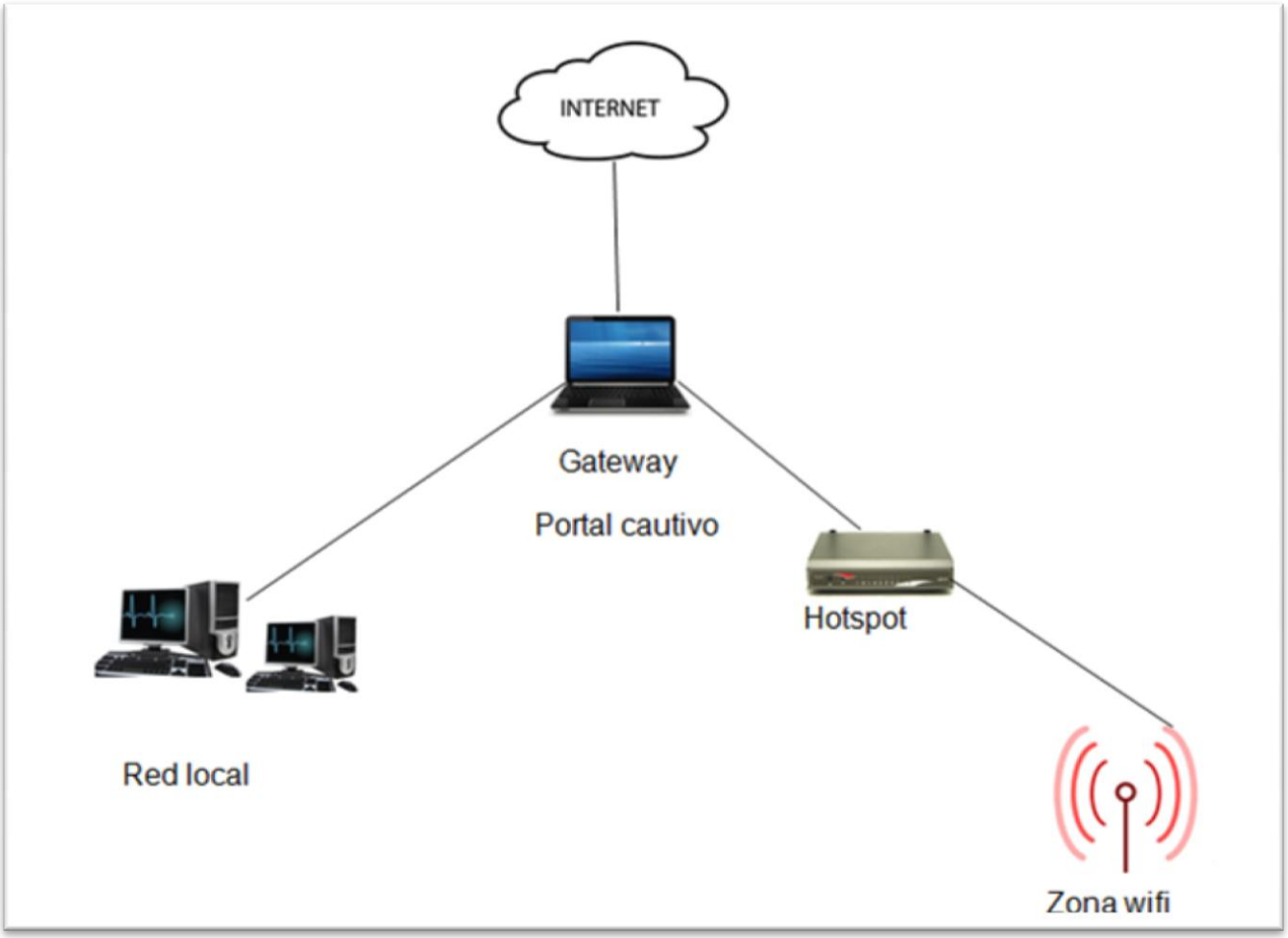


Diagrama de red

CONSTRUCCIÓN Y PASOS DEL PROYECTO

Un portal cautivo es un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal. El programa intercepta todo el tráfico HTTP hasta que el usuario se autentifica.

INSTALACIÓN DEL EASYHOTSPOT

Paso 1: Para la implementación del portal cautivo; lo primero que haremos es descargar la iso de EasyHotSpot. Este es el enlace en donde descargaremos la iso.http://es.sourceforge.jp/projects/sfnet_easyhotspot/downloads/Full_Distro/easyhotspot-distro-beta-0.2/easyhotspot.iso/

Paso 2: Insertamos el CD y esperamos que cargue, una vez haya cargado nos aparecerá una pantalla como esta donde seleccionamos el idioma y damos clic en adelante.

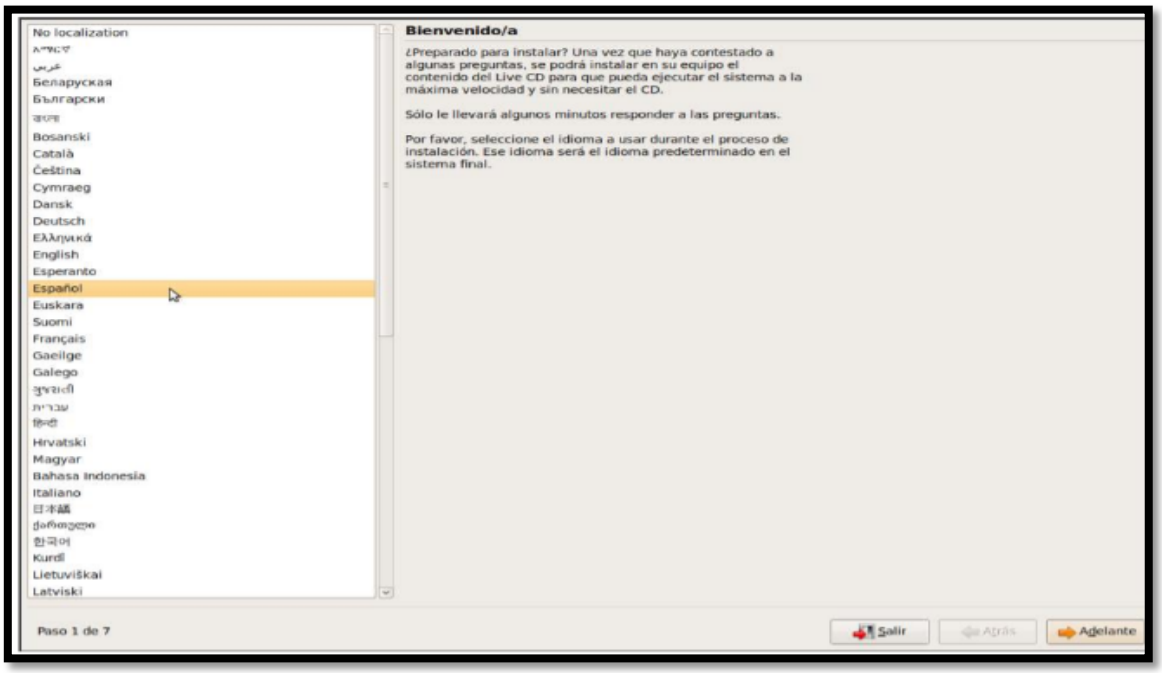


Imagen 1

Paso 3: Nos aparecerá una pantalla donde esta un mapa en el vamos a seleccionar el país que nos corresponda.

Paso 4: En este paso hay que poner mucha atención ya que aquí se hará el particionado del disco.

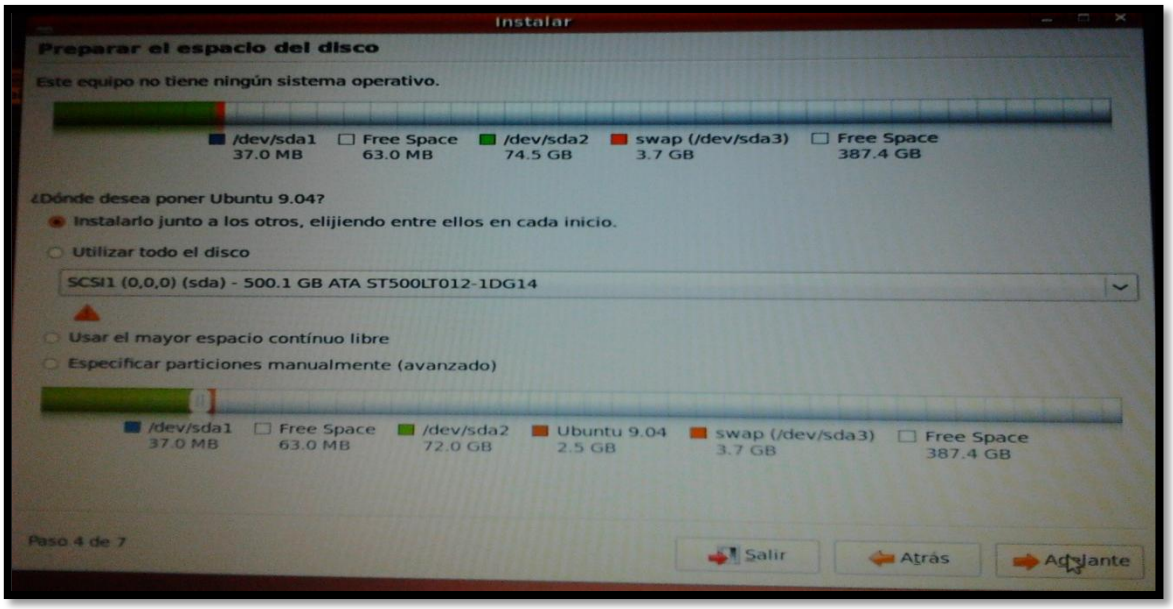


Imagen 2

Paso 5: Aquí configuramos la cuenta de usuario, nombre de inicio de sesión, contraseña y nombre del equipo.

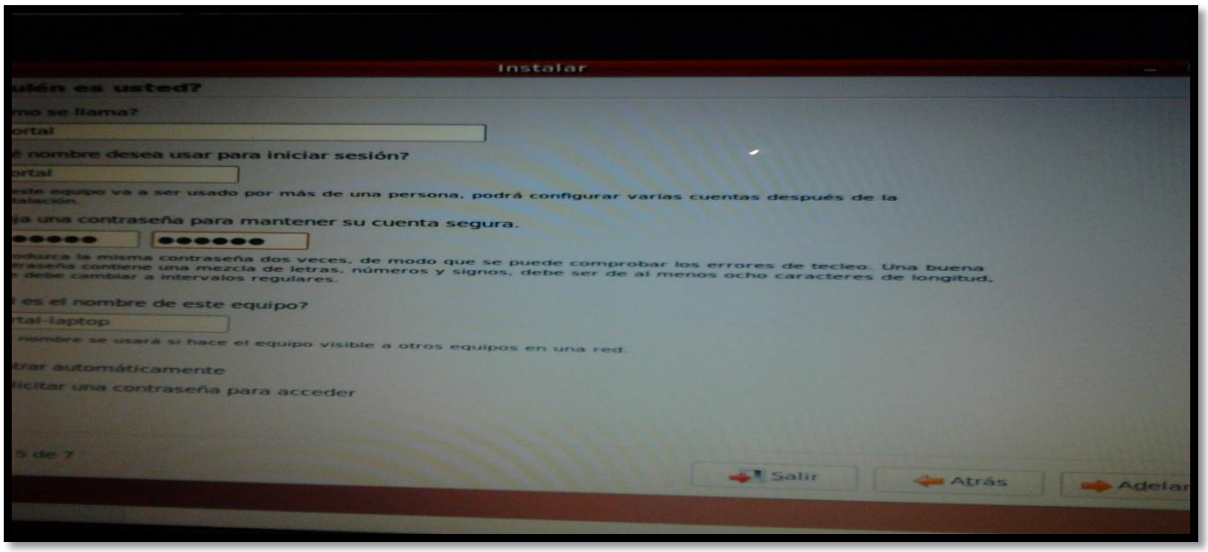


Imagen 3

Paso 6: Una vez completada la configuración de instalación damos clic en instalar.

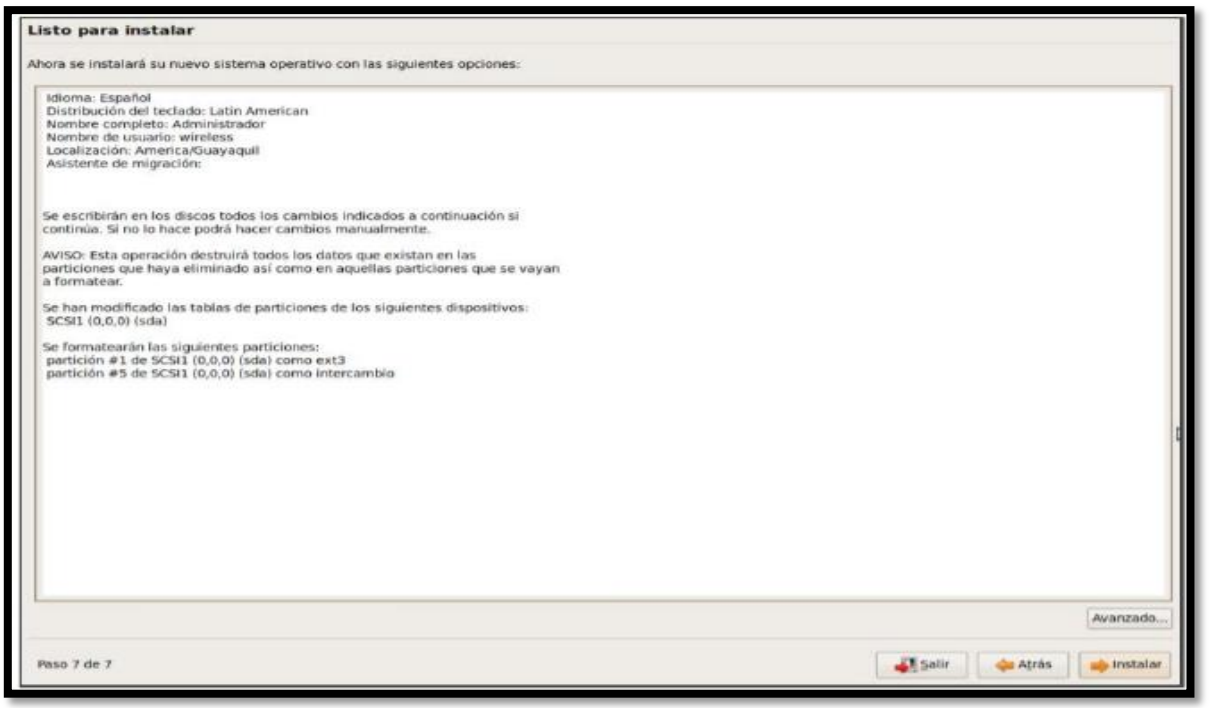


Imagen 4

Paso 7: Luego de que la instalación ha finalizado reiniciamos el equipo

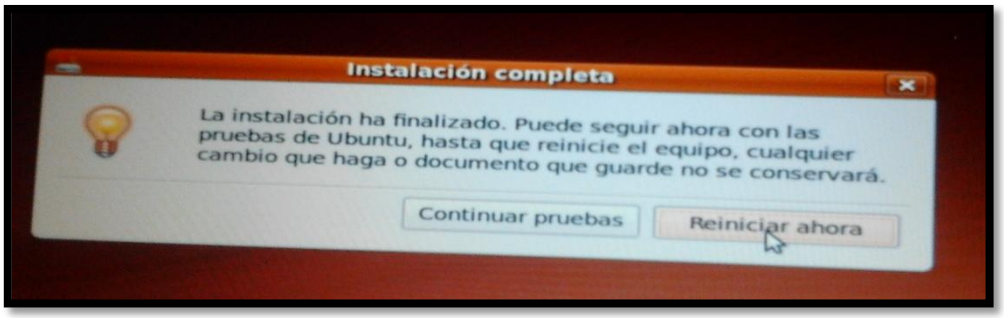


Imagen 5

Paso 8: Una vez completada la instalación de EasyHotSpot, nos direccionamos a la URL y digitamos localhost/easyhotspot/

Imagen 6

El EasyHotSpot viene con dos tipos de administración unos de ellos es el Administrador (Admin Menú). La función que realiza este administrador es el de la configuración, precio y sistema.

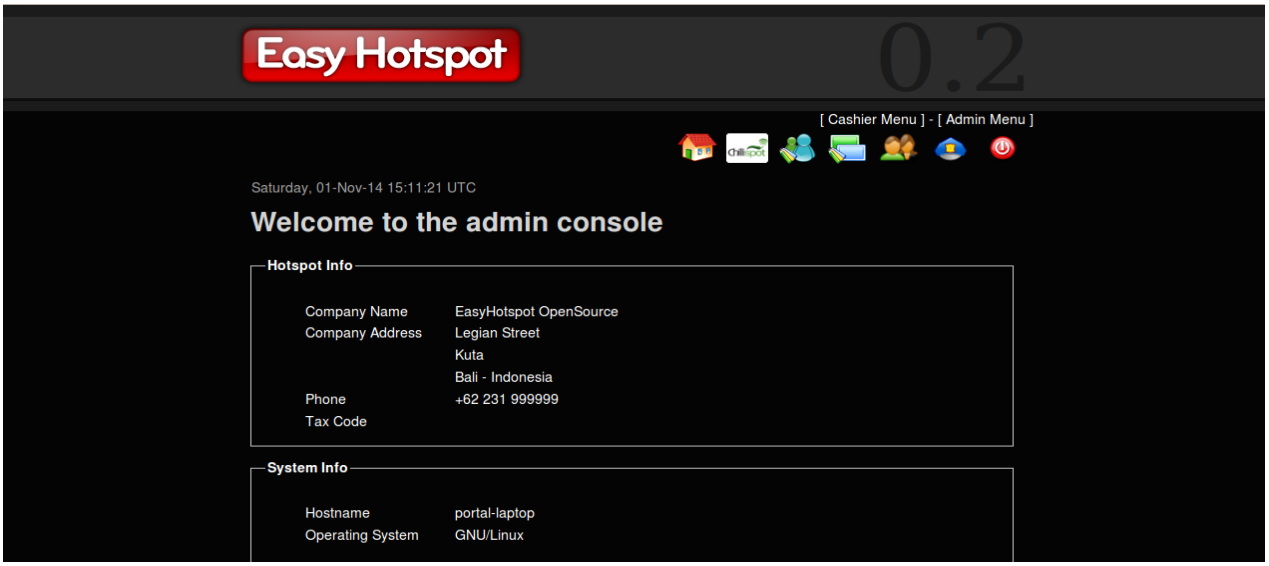


Imagen 7

Configuración del servicio de red (chillispot): En esta página se procede a editar la configuración básica para el punto de acceso:

Imagen 8

En esta sección se puede configurar:

Radius Server 1: (Dirección de servidor RADIUS primario, por defecto 127.0.0.1).
Radius Server 2: (Dirección del servidor RADIUS secundario, por defecto 127.0.0.1).
Radius Secret: Frase secreta entre el servidor RADIUS y Chillispot.
DHCP Interface: (Selección de la interfaz que desea utilizar como Hotspot) en nuestro caso hemos utilizado la Wlan0.
UAM Server: Dirección de portal cautivo almacenado.
UAM Secret: Frase secreta entre la página de inicio de sesión y la página Chillispot.
Client's Homepage: (Dónde quiere redirigir su cliente por primera vez.
Allowed URL: URL que los clientes pueden navegar sin loguearse, no se debe poner espacios.
DHCP Range: Servicio DHCP para los clientes

Administración de cajeros (Cashier Menú)

En esta otra página es esencialmente para cajeros aquí podemos editar, añadir y eliminar a los usuarios que deseen agregarse en nuestro portal.

Imagen 9

Postpaid Account Management (administración de cuentas de postpago)

Aquí es donde los cajeros crean a los usuarios de postpago. Si los clientes deciden cerrar su sesión, el cajero cerrará e imprimirá la factura haciendo clic en el detalle de uso de sesión. Una cuenta de postpago puede manejarse de dos maneras: tiempo y volumen.

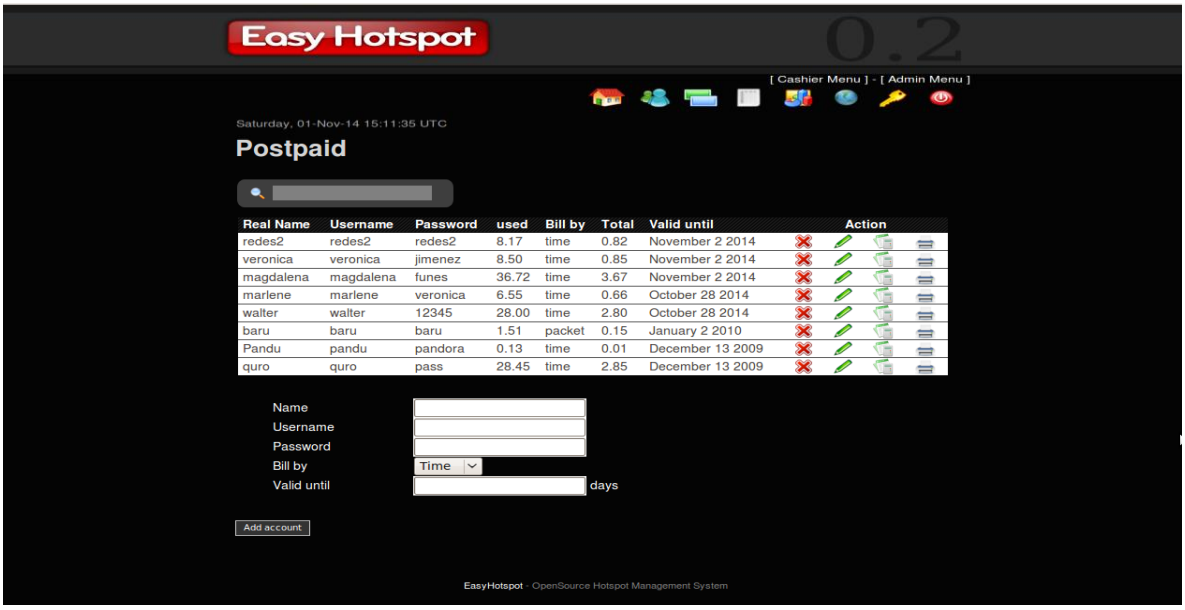


Imagen 10

PASOS PARA EL FUNCIONAMIENTO DE LA RED

Para que la red inalámbrica funcionara en la implementación del portal cautivo se realizo una serie de pasos. Ya que cuando se instalo el EasyHotSpot no funciono.

Este problema sucedió porque la versión del EasyHotSpot está un poco defasada

Paso 1: El comando **lspci** sirve para encontrar detalles del hardware de nuestra computadora. En este caso lo que necesitamos es saber el modelo de la tarjeta.

```
root@portal-laptop:/home/portal# lspci
```

```
00:1d.0 USB Controller: Intel Corporation 82801G (ICH7 Family) USB UHCI Controll
er #1 (rev 01)
00:1d.1 USB Controller: Intel Corporation 82801G (ICH7 Family) USB UHCI Controll
er #2 (rev 01)
00:1d.2 USB Controller: Intel Corporation 82801G (ICH7 Family) USB UHCI Controll
er #3 (rev 01)
00:1d.7 USB Controller: Intel Corporation 82801G (ICH7 Family) USB2 EHCI Control
ler (rev 01)
00:1e.0 PCI bridge: Intel Corporation 82801 Mobile PCI Bridge (rev e1)
00:1f.0 ISA bridge: Intel Corporation 82801GBM (ICH7-M) LPC Interface Bridge (re
v 01)
00:1f.1 IDE interface: Intel Corporation 82801G (ICH7 Family) IDE Controller (re
v 01)
00:1f.2 SATA controller: Intel Corporation 82801GBM/GHM (ICH7 Family) SATA AHCI
Controller (rev 01)
00:1f.3 SMBus: Intel Corporation 82801G (ICH7 Family) SMBus Controller (rev 01)
06:00.0 Network controller: Broadcom Corporation BCM4311 802.11b/g WLAN (rev 01)
08:08.0 Ethernet controller: Realtek Semiconductor Co., Ltd. RTL-8139/8139C/8139
C+ (rev 10)
```

Imagen 11

Paso 2: Una vez que se han encontrado los detalles del hardware de nuestra computadora procedemos a buscar el modelo de la tarjeta broadcom.

apt-cache search broadcom ⟶ La función de este comando es buscar un paquete determinado.

```
root@portal-laptop:/home/portal# apt-cache search broadcom
b43-fwcutter - Utility for extracting Broadcom 43xx firmware
bcm5700-source - module source for Broadcom's bcm5700 ethernet driver
```

Imagen 12

Paso 3: cuando tengamos identificado el modelo de nuestra tarjeta procedemos a la instalación con el siguiente comando. **apt-get install b43-fwcutter**

```
root@portal-laptop:/home/portal# apt-get install b43-fwcutter
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  b43-fwcutter
0 upgraded, 1 newly installed, 0 to remove and 153 not upgraded.
Need to get 16.7kB of archives.
After this operation, 111kB of additional disk space will be used.
Get:1 http://old-releases.ubuntu.com jaunty/main b43-fwcutter 1:011-5 [16.7kB]
Fetched 16.7kB in 1s (14.1kB/s)
Preconfiguring packages ...
Selecting previously deselected package b43-fwcutter.
(Reading database ... 104178 files and directories currently installed.)
Unpacking b43-fwcutter (from .../b43-fwcutter_1%3a011-5_i386.deb) ...
Processing triggers for man-db ...
```

Imagen 13

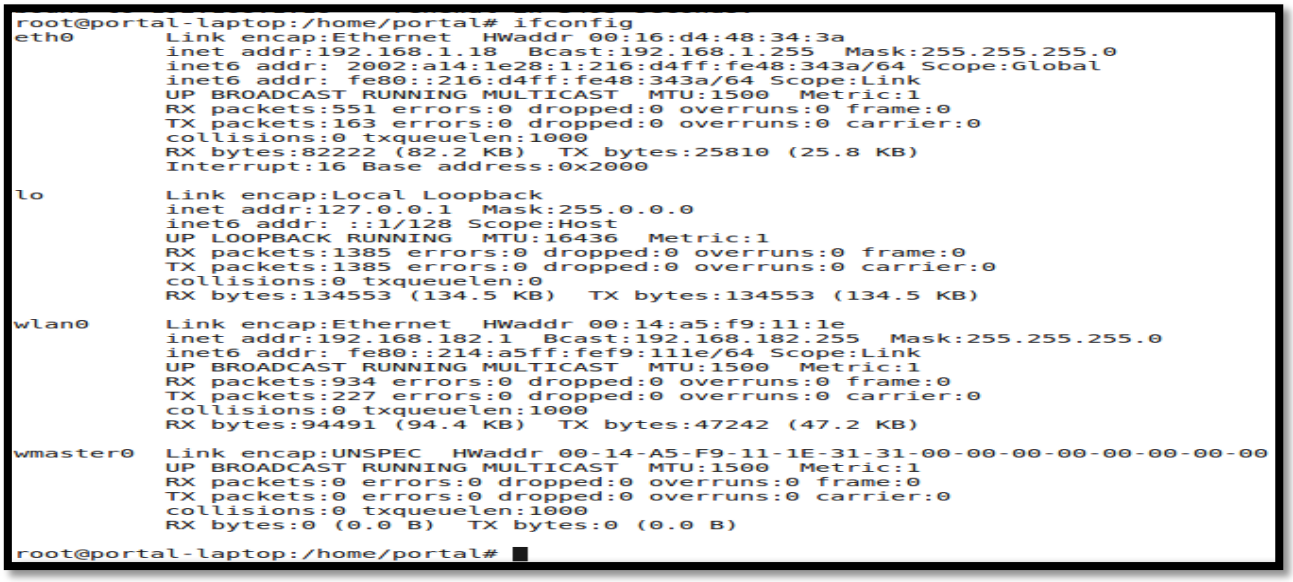
Paso 4: Cuando ya tengamos instalado el modelo de nuestra tarjeta procedemos a la actualización de los repositorios. Y lo hacemos con el comando **nano /etc/apt/sources.list**

```
root@portal-laptop:/home/portal# nano /etc/apt/sources.list
root@portal-laptop:/home/portal# apt-get update
Get:1 http://old-releases.ubuntu.com jaunty Release.gpg [189
```

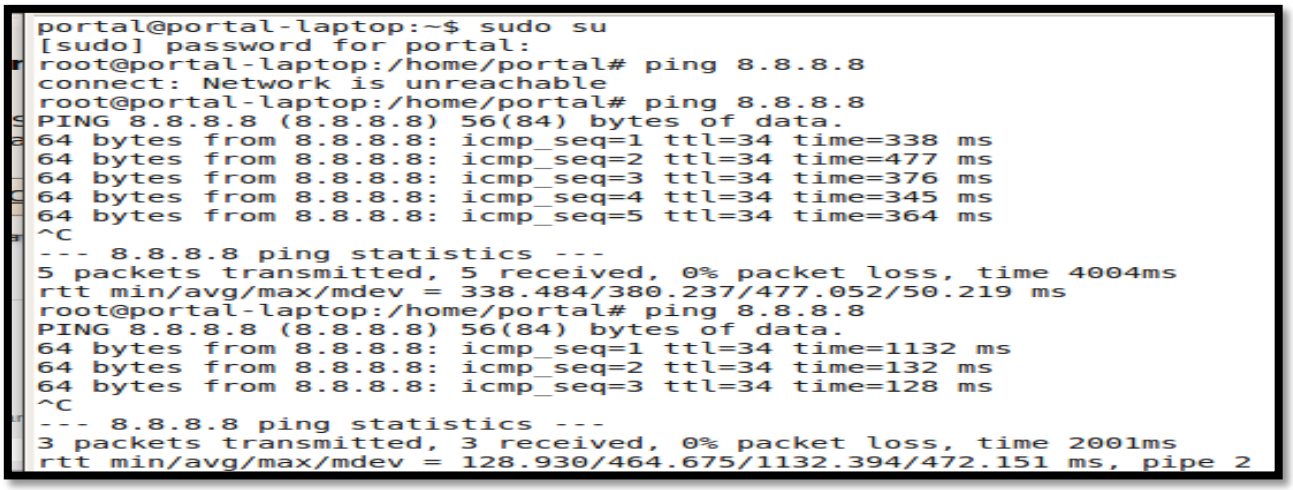
Luego actualizamos la lista de repositorios con el siguiente comando **apt-get update**

```
root@portal-laptop:/home/portal# apt-get update
Get:1 http://old-releases.ubuntu.com jaunty Release.gpg [189B]
Ign http://old-releases.ubuntu.com jaunty/main Translation-en_US
Ign http://old-releases.ubuntu.com jaunty/restricted Translation-en_US
Ign http://old-releases.ubuntu.com jaunty/universe Translation-en_US
Ign http://old-releases.ubuntu.com jaunty/multiverse Translation-en_US
Get:2 http://old-releases.ubuntu.com jaunty-updates Release.gpg [198B]
Ign http://old-releases.ubuntu.com jaunty-updates/main Translation-en_US
Ign http://old-releases.ubuntu.com jaunty-updates/restricted Translation
```

Con el comando **ifconfig** se verifico cuales interfaces de redes se tenían.



Paso 5: Con el comando **ping 8.8.8.8** verificamos que haya comunicación a internet.



ESCENARIO DE PRUEBAS DEL PROYECTO

Esta pantalla es la que le aparecerá al usuario luego de haber sido registrado por el administrador del portal cautivo. En el cual podrá acceder con el usuario y la contraseña que se le ha asignado y luego podrá navegar por internet.

Imagen 14

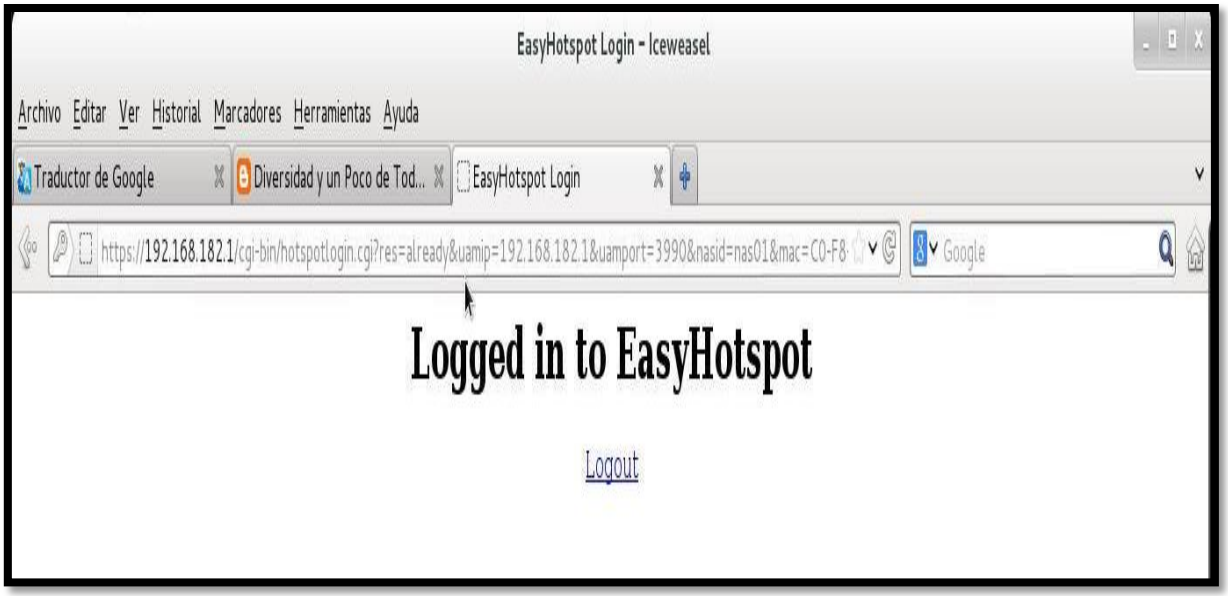


Imagen 15

BUENAS PRÁCTICAS PARA LA CONSTRUCCIÓN DEL PROYECTO

La computadora que se use como servidor tiene que ser un modelo antiguo. El easyhotspot es una distro de Ubuntu versión 9.04 por lo que al instalarlo en un modelo de computadora reciente causa problemas con la red cableada e inalámbrica.

Al momento de cambiar el idioma del sistema easyhotspot se debe tener en cuenta que al reiniciar la máquina da error, por lo que no muestra más la página de bienvenida.

Una máquina cliente no debe tener instalado el servidor DHCP, al momento de realizar las pruebas ya que dos servidores DHCP no pueden establecer conexión.

La iso de easyhotspot debe ser almacenada en un Cd o Dvd, ya que si se utiliza otro tipo de almacenamiento como USB no lo reconocerá al momento de arrancar desde el dispositivo.

CONCLUSIONES

Después de haber desarrollado el proyecto portal cautivo con el software EasyHotSpot podemos concluir que:

- ✓ Al momento de elegir el software con el que se trabajara se tiene que tener en cuenta que la computadora en la que se instalara el EasyHotSpot tiene que ser un poco antigua ya que el sistema está un poco obsoleto.

- ✓ Cuando ya se haya instalado el software se tiene que verificar si la red funciona al menos la cableada ya que es un problema que se da si la PC en la que se instala el EasyHotSpot no es muy antigua.

- ✓ Es importante tener en cuenta que al almacenar la iso del EasyHotSpot se tiene que guardar en un CD o DVD ya que al guardar en otros dispositivos al momento de ser instalados se tiene problema.

- ✓ Los portales cautivos wifi son de mucha utilidad ya que podemos controlar los usuarios de la red y pueden acceder solo a los que el administrador desee.

RECOMENDACIONES

- ✓ Analizar los requerimientos básicos para la implementación de un portar cautivo, pues es de tener en cuenta que el EasyHotSpot es un software antiguo y por lo tanto la computadora en la que se instalara tiene que ser antigua.

- ✓ Verificar si la red funciona correctamente.

- ✓ Se deberán cambiar los repositorios del sistema pues están un poco obsoletos.

- ✓ Es importante descargar la iso de la página oficial de EasyHotSpot.

- ✓ Se deben de tener los conocimientos básicos de Linux. Pues el EasyHotSpot es una distro de Ubuntu 9.4.

BIBLIOGRAFÍA

Titulo: Portal cautivo

Autor: Desconocido

URL: http://es.wikipedia.org/wiki/Portal_cautivo

Fecha de consulta: 18/07/2014

Titulo: Como crear tu portal cautivo

Autor: Ana Ibáñez

URL: http://recursostic.educacion.es/observatorio/web/es/equipamiento-tecnologico/redes/1005-como-crear-tu-portal-cautivo-con-easy-hotspot

Fecha de consulta: 18/07/2014