

LABORATORIO 9- SEGURIDAD DE SISTEMAS

DESCRIPCIÓN

Recursos:

Se utilizarán 1 máquina física Windows 8 que será el servidor

Un modem-router TP-Link (Cualquier otro sirve por ejemplo en un CISCO se probó y funcionó de igual forma)

Una pc inalámbrica W7 , un dispositivo Android.

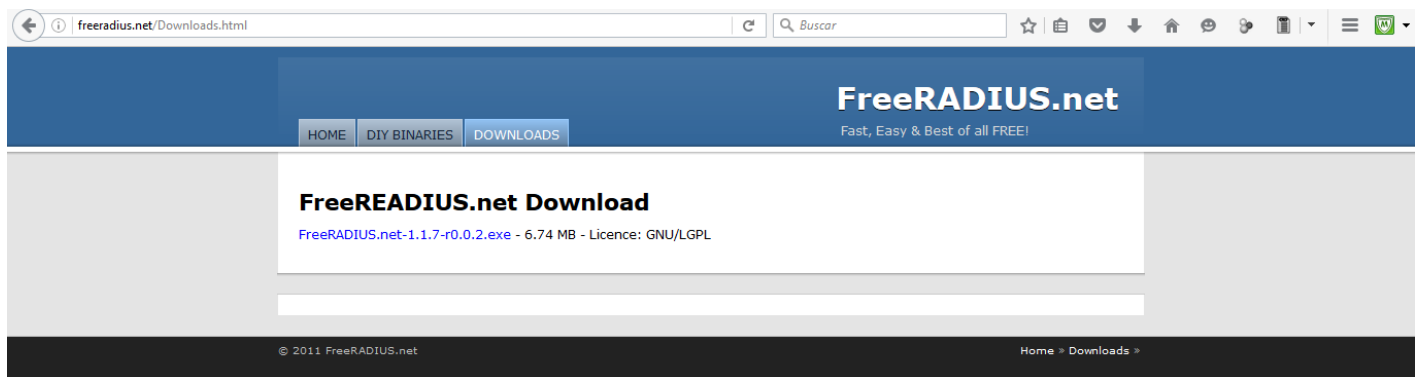
El Modem Router debe estar ya configurado con salida al Internet.

Conexión cableada: Cable amarillo: Salida a Internet (Puerto WAN), cable plomo: conexión con el servidor (Puerto LAN).

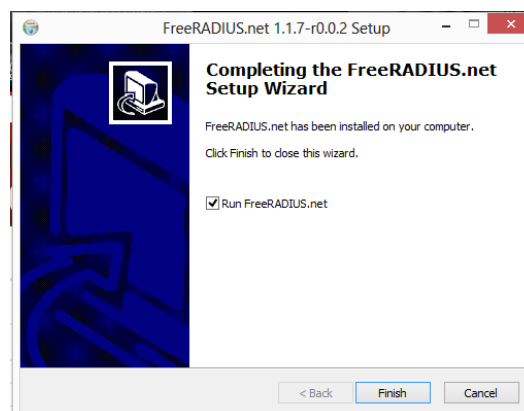


DESARROLLO

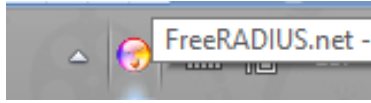
Primeramente descargamos freeradius para windows en el siguiente enlace: <http://freeradius.net/Downloads.html>



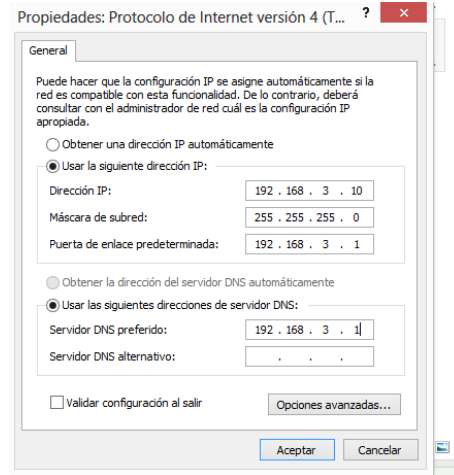
Instalamos el software



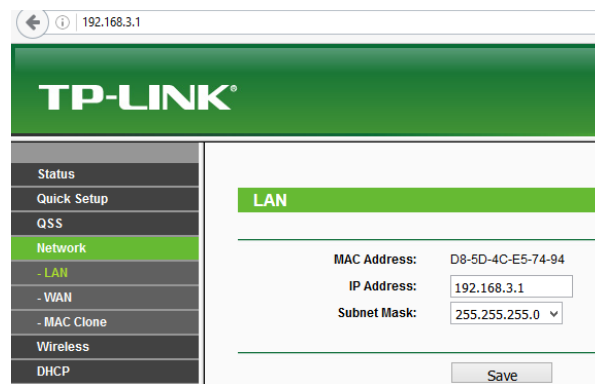
Y finalizamos. El servidor ya se estará ejecutando



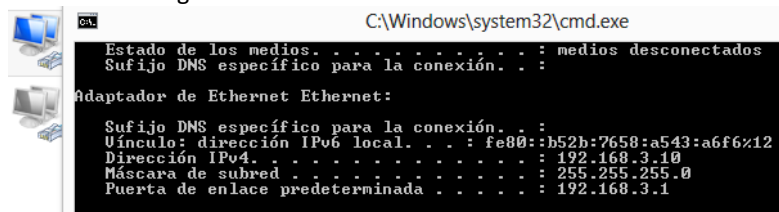
Configuramos el puerto Ethernet de la maquina servidor con direcciones estáticas, para comunicarnos con el Router Inalámbrico:



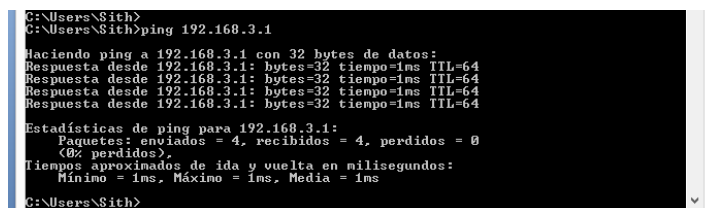
La dirección 192.168.3.1 es la Ip que fue asignada al Router para la sección LAN, que hace de gateway de la red inalámbrica:



Verificamos que la dirección estática esté asignada a nuestra PC

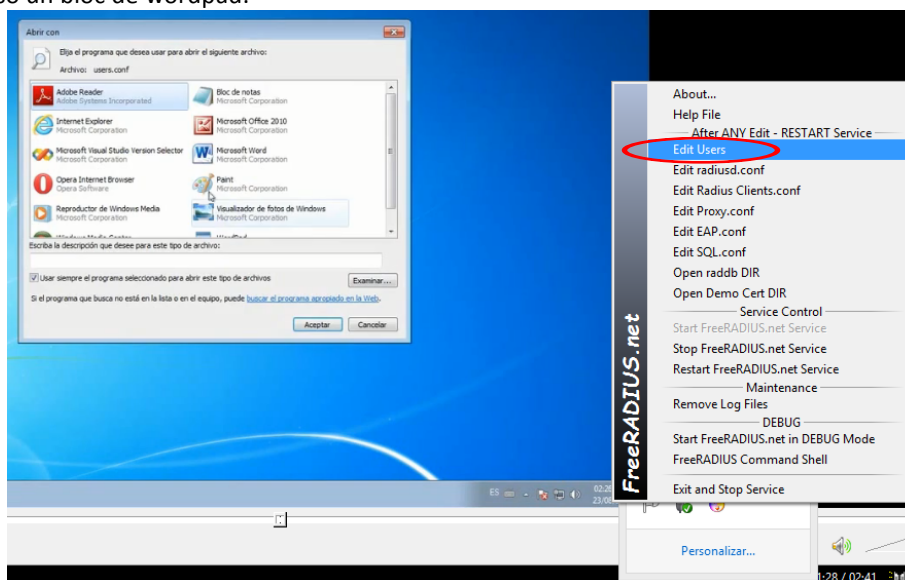


Verificamos que exista conectividad con el router



Comenzamos a configurar el servidor RADIUS (la configuración puede ser bastante extensa dependiendo a lo que se requiera, para este ejemplo nos centraremos en la creación de usuarios)

Ingresamos al menú de Radius y Edit Users, ante la solicitud de utilizar algún programa para abrir el archivo, seleccionamos el que se prefiera en este caso un bloc de wordpad.



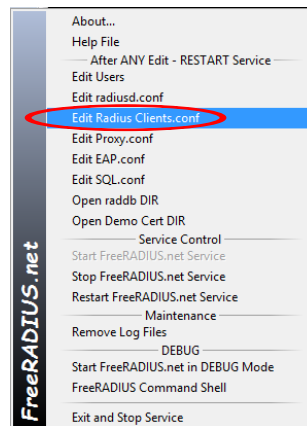
Agregamos los usuarios que se requieran más sus contraseñas, en el ejemplo solo 2.

users.conf - WordPad

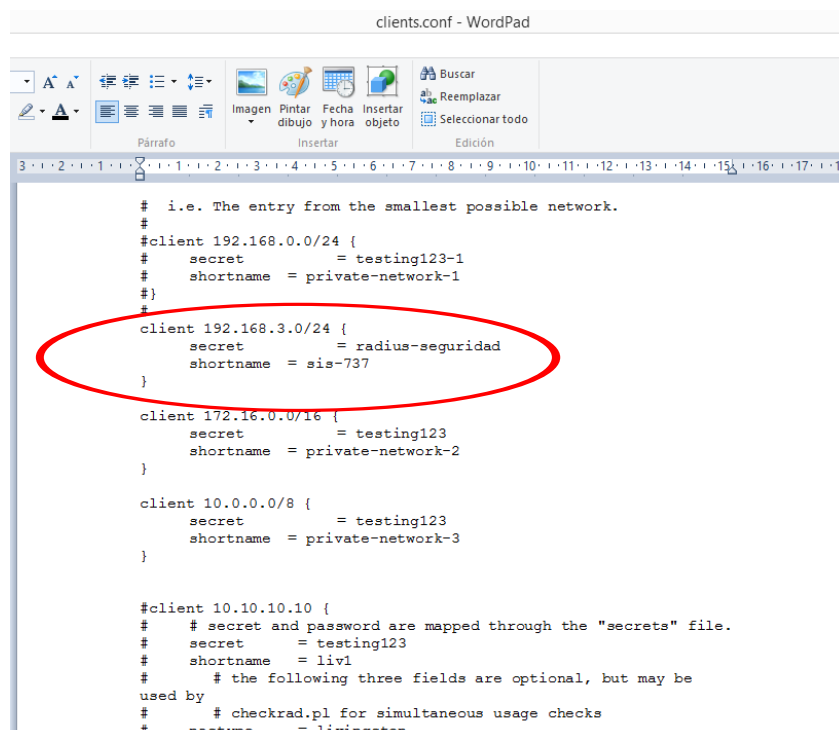
```
#  
  
##### RFC3580 #####  
## Also the "eap.conf" MUST be modified to include the follow  
## line:  
## "use_tunneled_reply = yes"  
## the default is "use_tunneled_reply = no"  
## this allow the "Tunnel*" AV's to be passed outside the eap  
## tunnel  
## otherwise the switch will NOT see the VLAN to place the  
## port into  
### Comments added by Jeff Reilly ###  
  
alex User-Password == "alex"  
sith User-Password == "sith"  
  
FreeRADIUS.net-Client User-Password == "demo"  
  
rfc3580 User-Password == "demo"  
Tunnel-Type = "VLAN",  
Tunnel-Medium-Type = "IEEE-802",  
Tunnel-Private-Group-Id = "1",  
Reply-Message = "Hello, %u"  
  
#  
# This is a complete entry for "steve". Note that there is no  
# Fall-Through  
# entry so that no DEFAULT entry will be used, and the user  
# will NOT  
# get any attributes in addition to the ones listed here.  
#
```

Guardamos y cerramos

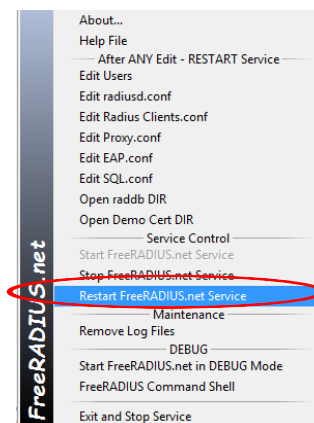
Posteriormente ingresamos a Edit Radius Clients.conf, donde se definirá la dirección de red



Establecemos la dirección de red: **192.168.3.0 /24**, la contraseña que se utilizará para autenticar el servidor con el router: **radius-seguridad** y el nombre abreviado **sis-737** (este no será necesario para este ejemplo)



Guardamos, cerramos y reiniciamos el servidor



Ahora realizamos la configuración en el router, lo primero usamos como identificador de la red: **Sis-737** y guardamos

TP-LINK

192.168.3.1

Wireless Settings

SSID: Sis-737

Region: Bolivia

Warning: Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

Channel: Auto

Mode: 11bgn mixed

Channel Width: Auto

Max Tx Rate: 300Mbps

☒ Enable Wireless Router Radio

☒ Enable SSID Broadcast

☐ Enable WDS

Save

En seguridad wireless seleccionamos la que nos permite utilizar RADIUS. Indicamos la dirección Ip del servidor Radius y introducimos la contraseña que colocamos en la configuración del servidor: **radius-seguridad**

TP-LINK

192.168.3.1

Wireless Security

Type: Automatic

WEP Key Format: Hexadecimal

Key Selected

Key 1: Disabled

Key 2: Disabled

Key 3: Disabled

Key 4: Disabled

☒ WPA/WPA2

Version: Automatic

Encryption: Automatic

Radius Server IP: 192.168.3.10

Radius Port: 1812 (1-65535, 0 stands for default port 1812)

Radius Password: radius-seguridad

Group Key Update Period: 0 (in second, minimum is 30, 0 means no update)

☐ WPA-PSK/WPA2-PSK

Version: WPA2-PSK

Encryption: Automatic

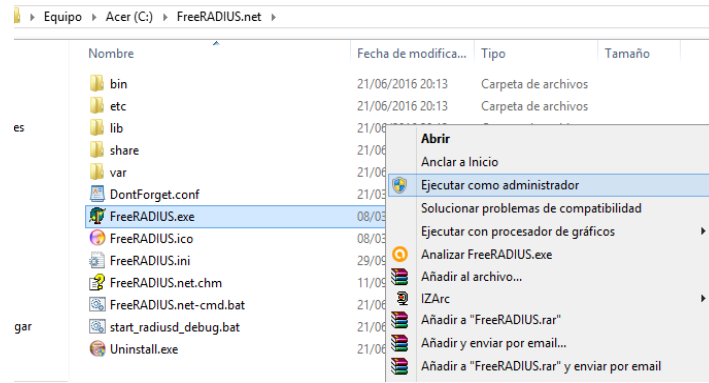
Guardamos y reiniciamos el dispositivo

Reboot

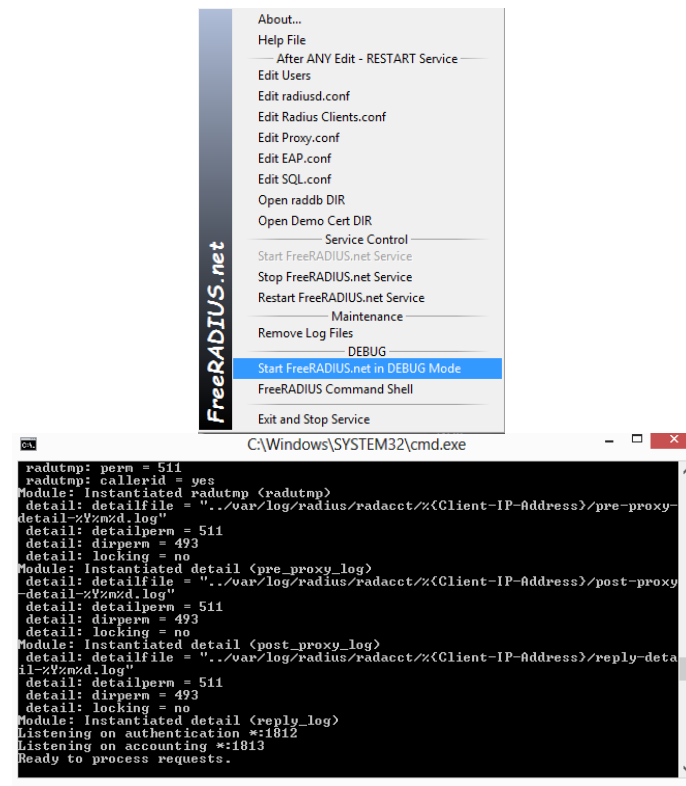
Click this button to reboot the device.

Reboot

Dependiendo al Sistema Operativo puede existir problemas con los permisos, por lo tanto es importante iniciar FreeRadius como Administrador



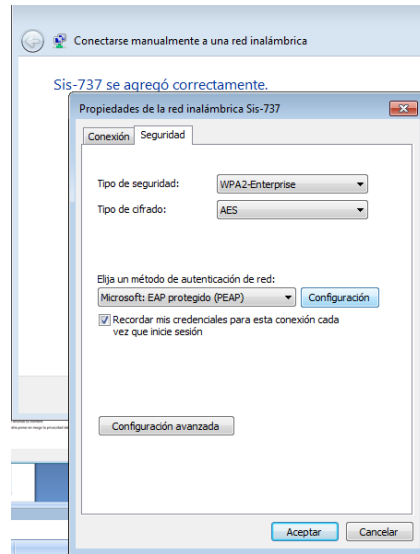
Iniciar FreeRadius en modo depurador ayudará a ver las transacciones entre cliente y servidores, se recomienda iniciarlo de este modo. Se abrirá una consola donde podrá ver los respectivos logs.



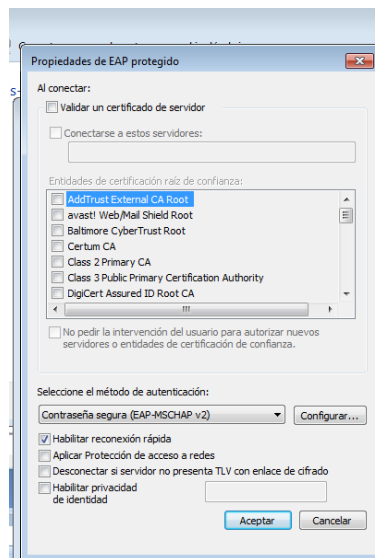
Finalmente si intentamos realizar una conexión con el router, nos bloqueará la conexión ya que detectará que hay un servidor Radius en la red y el perfil de conexión del cliente no está configurado para autenticación en Radius. Para configurar un perfil de conexión de un cliente Windows seguimos los siguientes pasos en la máquina cliente (**Se utilizó un equipo con W7** para las demás versiones los pasos son los mismos):

1. Entramos en panel de control, centro de redes y recursos compartidos.
2. Configurar una nueva conexión de red- Conectarse manualmente a una red inalámbrica
3. Escribimos -> Nombre de la red: "Sis-737" / Tipo de seguridad: WPA2-Enterprise / Tipo de cifrado: AES / Marcamos la opción: Iniciar esta configuración manualmente. Y pulsamos siguiente.
4. Aparece "Sis-737 se agregó correctamente". Pulsamos sobre "Cambiar la configuración manualmente"
5. En la pestaña Conexión, dejamos la configuración por defecto.

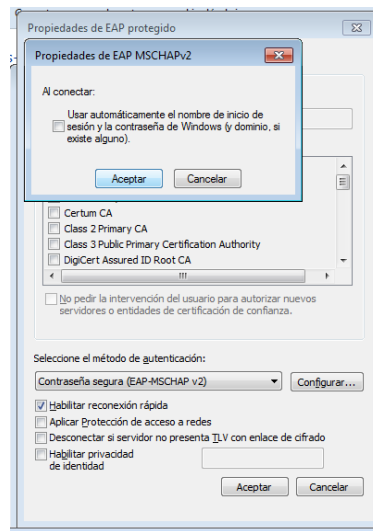
6. Sobre la pestaña Seguridad -> Tipo de conexión: WPA2-Enterprise / Tipo de cifrado: AES / Elija un método de autenticación de red: Microsoft EAP protegido (PEAP)



7. Pulsamos sobre el botón configuración y aparece una ventana llamada "Propiedades de EAP protegido. Aquí desmarcamos la opción: Validar un certificado de servidor, en caso de querer dicha opción tendríamos que habilitar uno en nuestro servidor en /freeradius/certs. En seleccione el método de autenticación elegimos: Contraseña segura (EAP-MSCHAP v2) / Marcamos la opción: Habilitar re conexión rápida

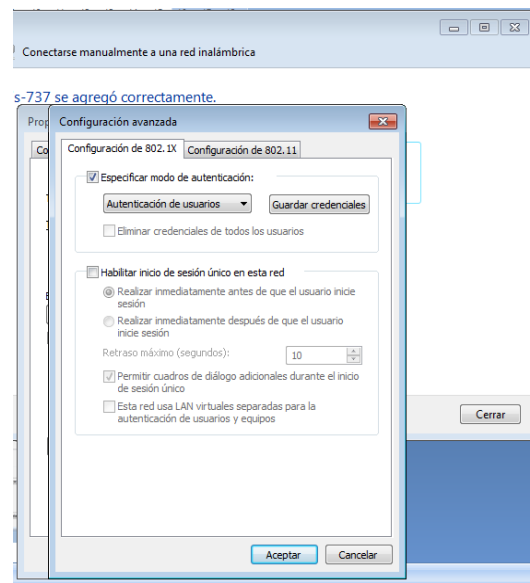


8. Pulsamos sobre el botón configurar y desmarcamos la opción: Usar automáticamente el nombre de inicio de sesión y la contraseña de Windows (y dominio, si existe alguno) y pulsamos aceptar.

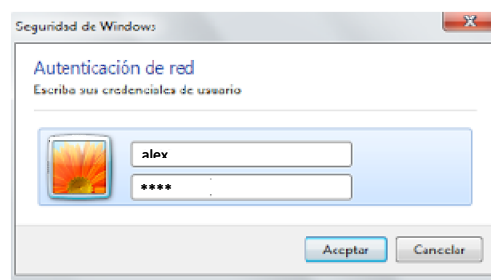


Regresamos a la anterior pantalla y pulsamos aceptar.

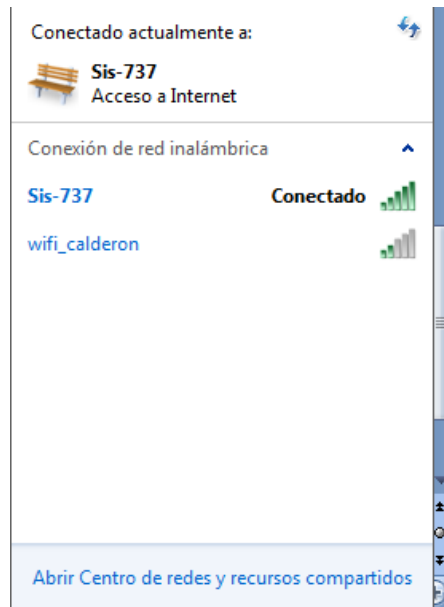
9. Por último pulsamos en Configuración avanzada y seleccionamos el modo de autenticación “Autenticación de usuarios”



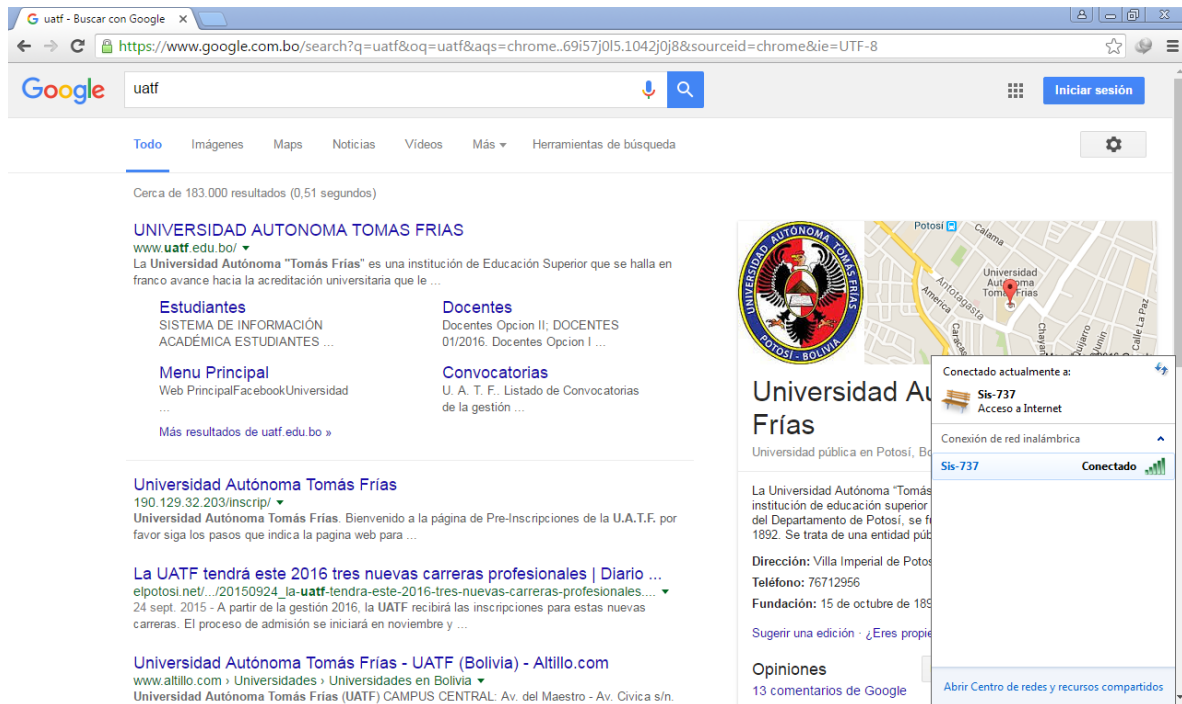
Elegimos aceptar, guardamos los cambios y nos volvemos a conectar al punto de acceso. Ahora nos pedirá el usuario y contraseña para comprobarlo en el servidor Radius, a través de nuestro router. Ingresamos alguno de los usuarios creados más su contraseña.



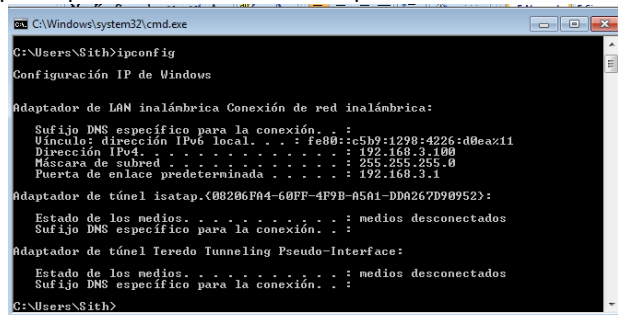
La pc se conecta a la red previa autenticación del servidor Radius



Probamos accediendo a una página web



Verificamos la dirección IP recibida por la pc cliente mediante DHCP por el router



Ahora conectaremos un dispositivo móvil, en este caso un teléfono con S.O. Android, de igual forma debemos agregar una red nueva y configurar los parámetros: para este dispositivo se utilizará el segundo usuario creado en Radius

Agregar red

Nombre de red (SSID)
Sis-737

Seguridad
802.1x EAP

Método de EAP

CANCELAR GUARDAR

Agregar red

Método de EAP
PEAP

Autenticación de fase 2
Ninguno

Certificado de CA

CANCELAR GUARDAR

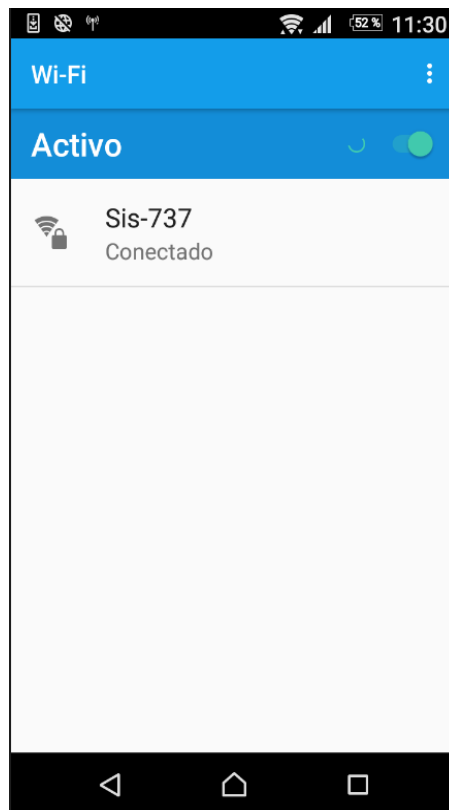
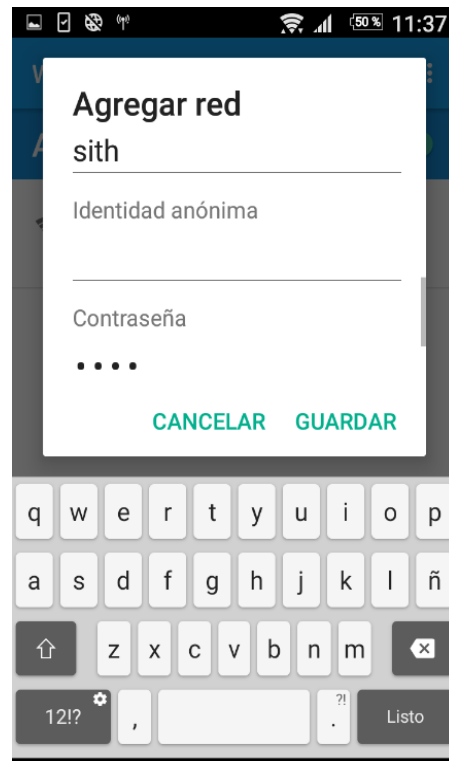
Agregar red

Certificado de CA
(sin especificar)

Identidad
sith

Identidad anónima

CANCELAR GUARDAR



Para comprobar ingresamos al router y listamos los equipos que se encuentran conectados a el

The screenshot shows the web interface of a TP-LINK 300M Wireless N Router (Model No. TL-WR841N / TL-WR841ND) accessed via a web browser at 192.168.3.1. The interface has a green header with the TP-LINK logo and router model information. On the left is a navigation menu with options like Status, Quick Setup, QSS, Network, Wireless, DHCP, and various advanced settings. The main content area is titled 'DHCP Clients List' and displays a table of connected clients. The table has columns for ID, Client Name, MAC Address, Assigned IP, and Lease Time. Two clients are listed: 'Akatsuki' with IP 192.168.3.100 and 'android-4d3a57f582c5d95e' with IP 192.168.3.101. A 'Refresh' button is located below the table. To the right of the table is a 'DHCP Clients List Help' section explaining the fields and providing a disclaimer that values cannot be changed.

| ID | Client Name | MAC Address | Assigned IP | Lease Time |
|----|--------------------------|-------------------|---------------|------------|
| 1 | Akatsuki | 00-24-2C-54-F8-67 | 192.168.3.100 | 01:33:28 |
| 2 | android-4d3a57f582c5d95e | 40-B8-37-BB-F0-AD | 192.168.3.101 | 01:52:09 |

Efectivamente tenemos los dos equipos que se conectaron la PC W7 y el Móvil a partir de los usuarios creados en Radius.

EVALUACIÓN

- 1.- Realice la instalación de Radius, utilice como SSID el nombre de su grupo para diferenciar del resto de dispositivos en la defensa en clase.
- 2.- Realizar las capturas de pantallas para asociar un equipo con un sistema operativo basado en LINUX o en MAC (elija el que vea conveniente)