2012

SEGURIDAD Y ALTA DISPONIBILIDAD

TEMA 3:
Implantación de técnicas de acceso remoto. Seguridad perimetral

Nicolás Madrid Gallego

Seguridad y alta disponibilidad

26/01/2012

Contenido

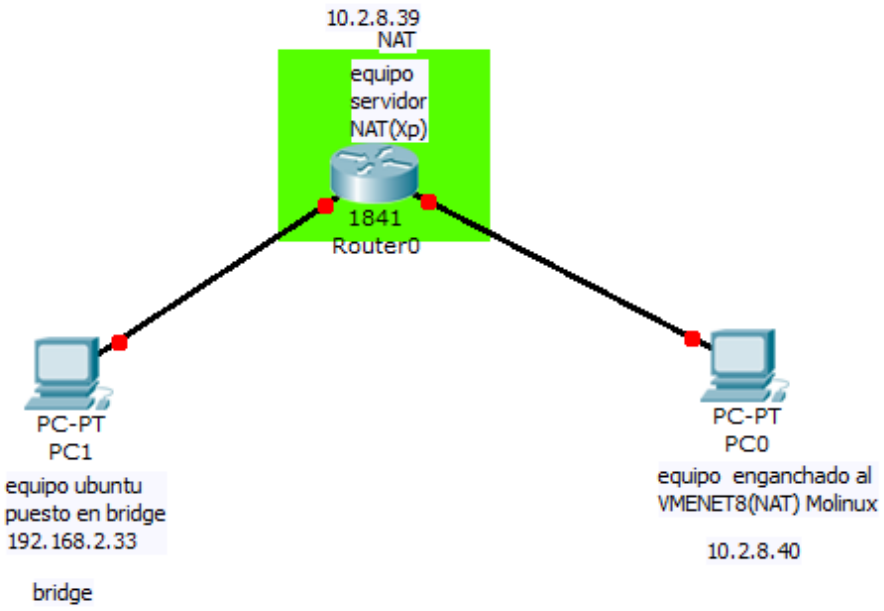
SEGURIDAD PERIMETRAL:

1.NAT:

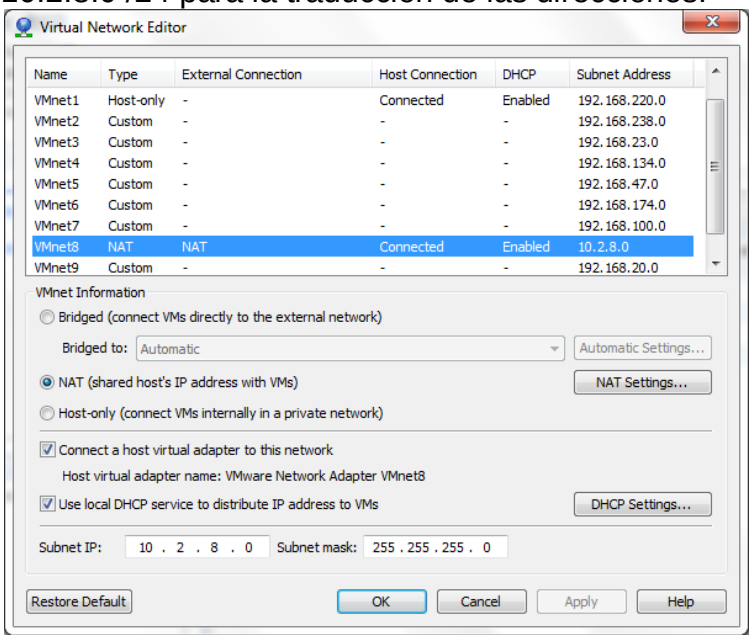
Comprobación de la seguridad perimetral a través de un NAT (Laboratorio virtual)

Nuestro escenario sera el siguiente:

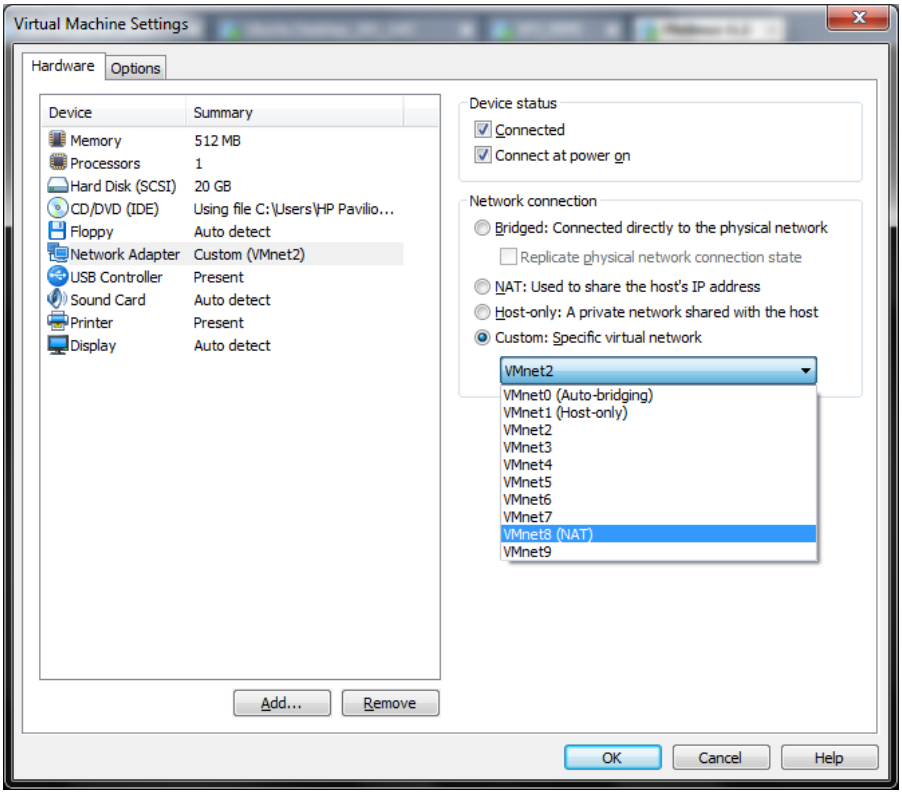
Esta práctica la realizaremos haciendo uso del NAT del VMWARE, para ello en primer lugar iremos a la pestaña edit/virtual Network Editor para ver la configuración de nuestro nat:



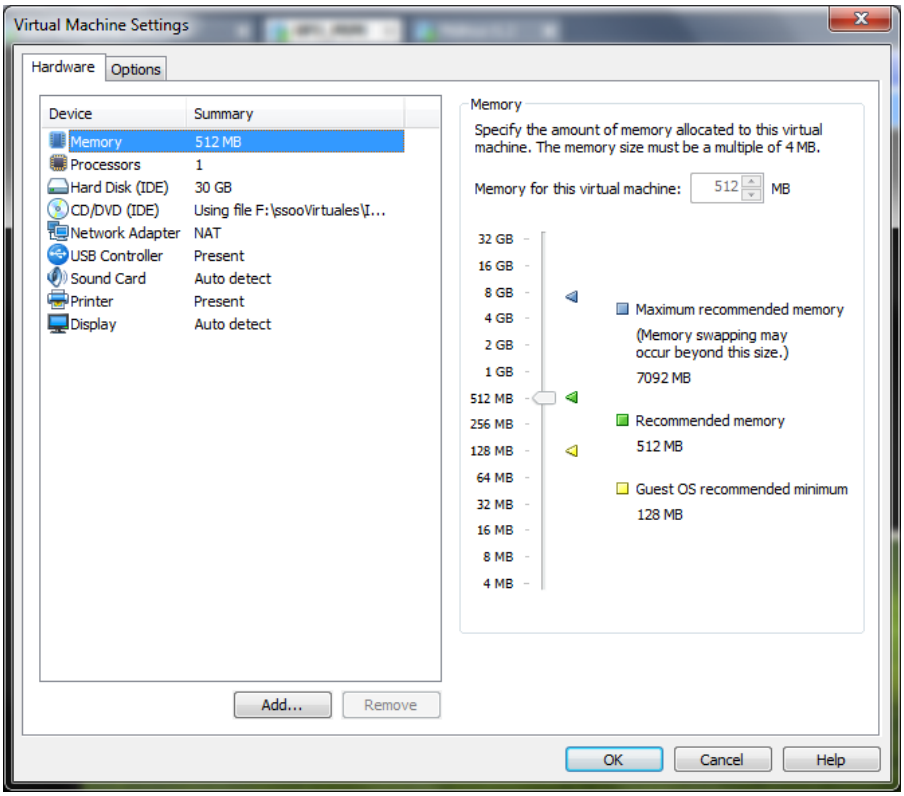
En la pantalla podremos ver que nuestro NAT usa la dirección de red 10.2.8.0 /24 para la traducción de las direcciones:



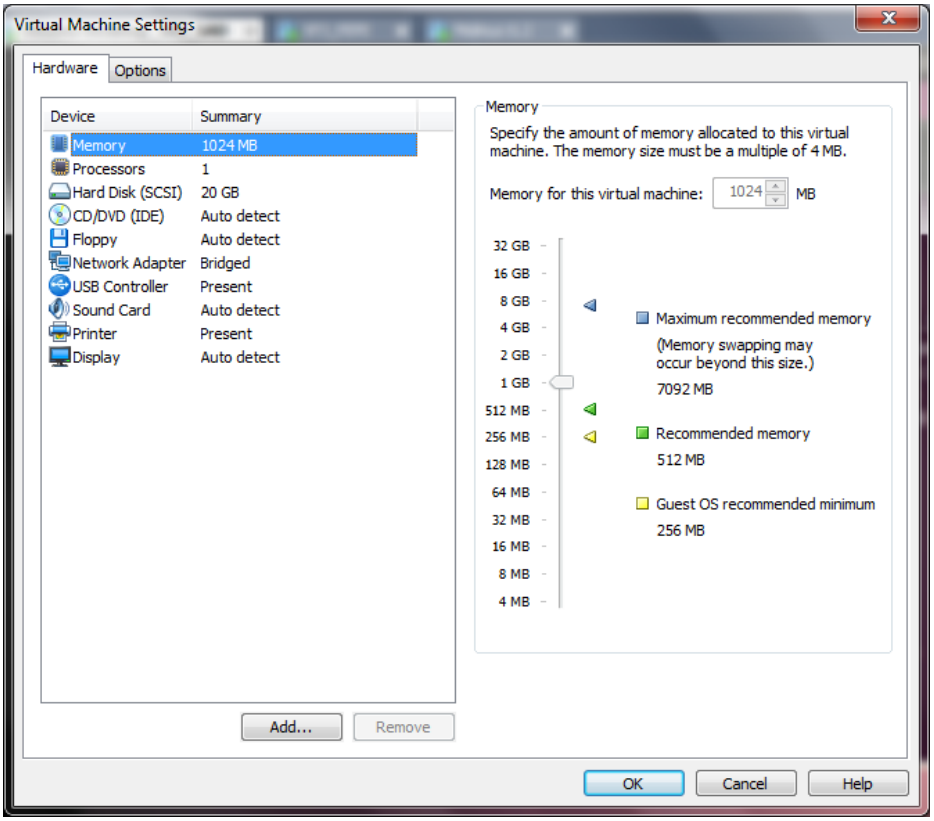
El cliente Molinux está en VMnet 8 (NAT) que actua como un switch conectado a equipo con el servidor NAT integrado.



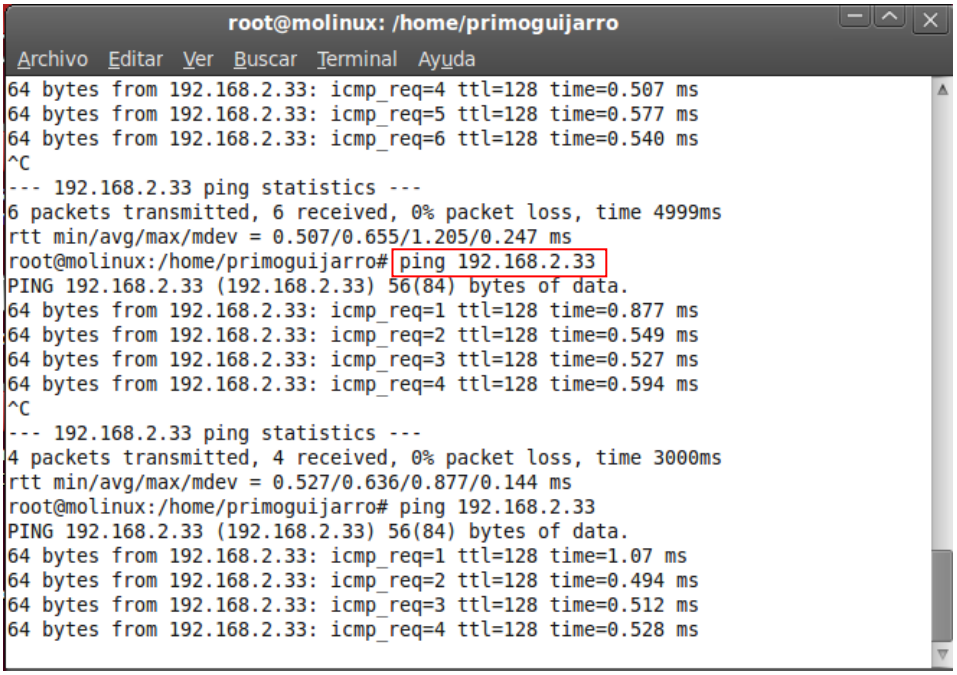
El Cliente XP, actúa como NAT:



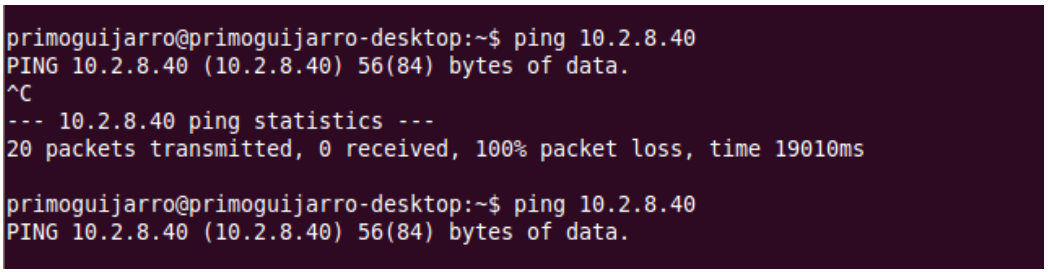
El cliente Ubuntu que esta en modo Bridge es decir esta fuera del NAT.



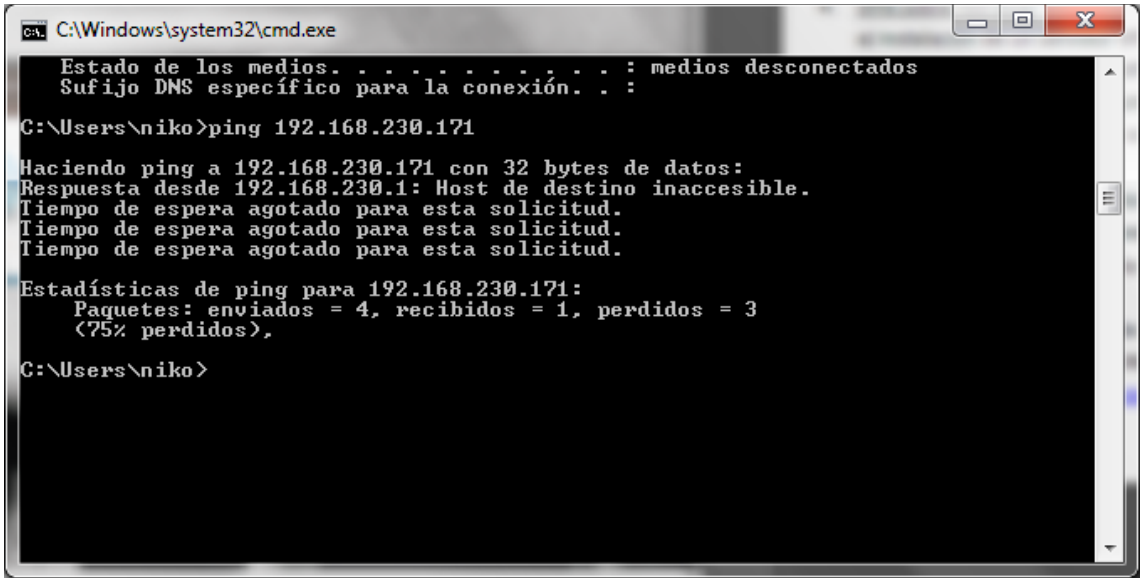
La practica será la siguiente desde el cliente Molinux en VMnet8 (NAT) realizaremos un ping al cliente Bridge(Ubuntu), de modo que nos tiene que dejar:



Sin embargo, si realizamos un ping desde el Ubuntu al Molinux, no nos debe dejar, esto quiere decir que funciona correctamente la seguridad perimetral con NAT.



Ahora probaremos a realizar un ping desde otro equipo que esta fuera de red que tiene activado el NAT:

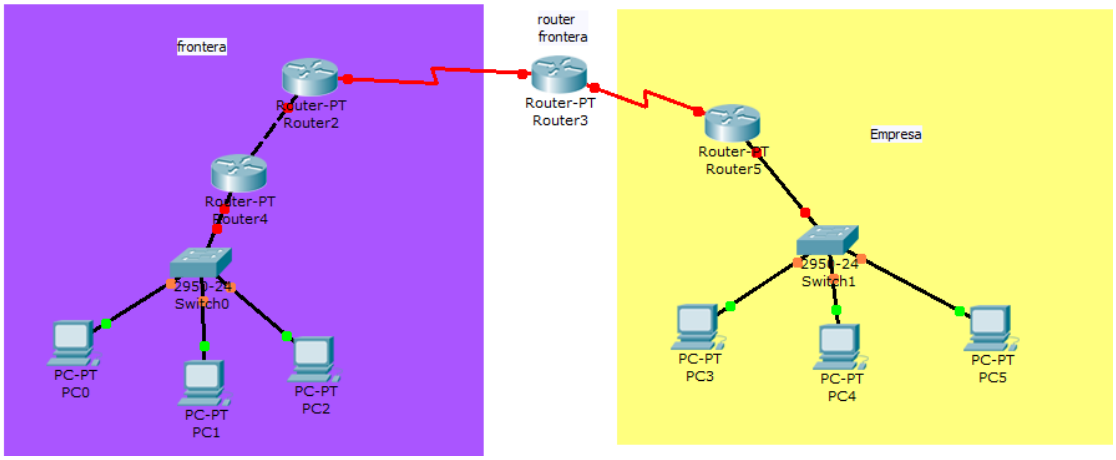


Como era de esperar el ping ha fallado puesto que al estar activado el NAT los equipos que no están integrados en la red del NAT no pueden acceder a los equipos con NAT.

2. Router frontera:

a) Planteamiento escenario CISCO Packet Tracert: esquema.

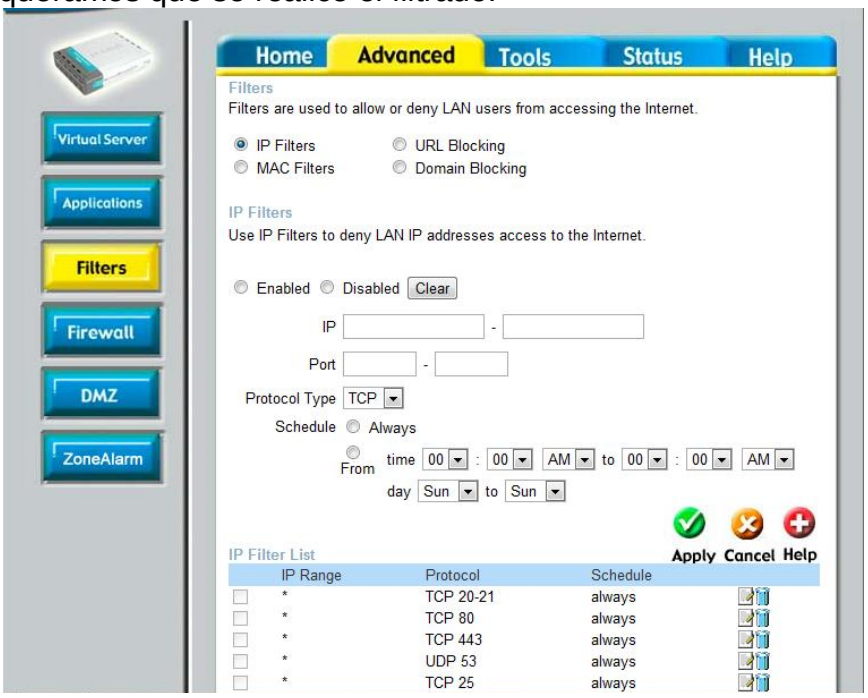
En este esquema podremos apreciar 2 empresas en la que él y entre dichas empresas podremos apreciar un router que actúa como router frontera entre ambas empresas:



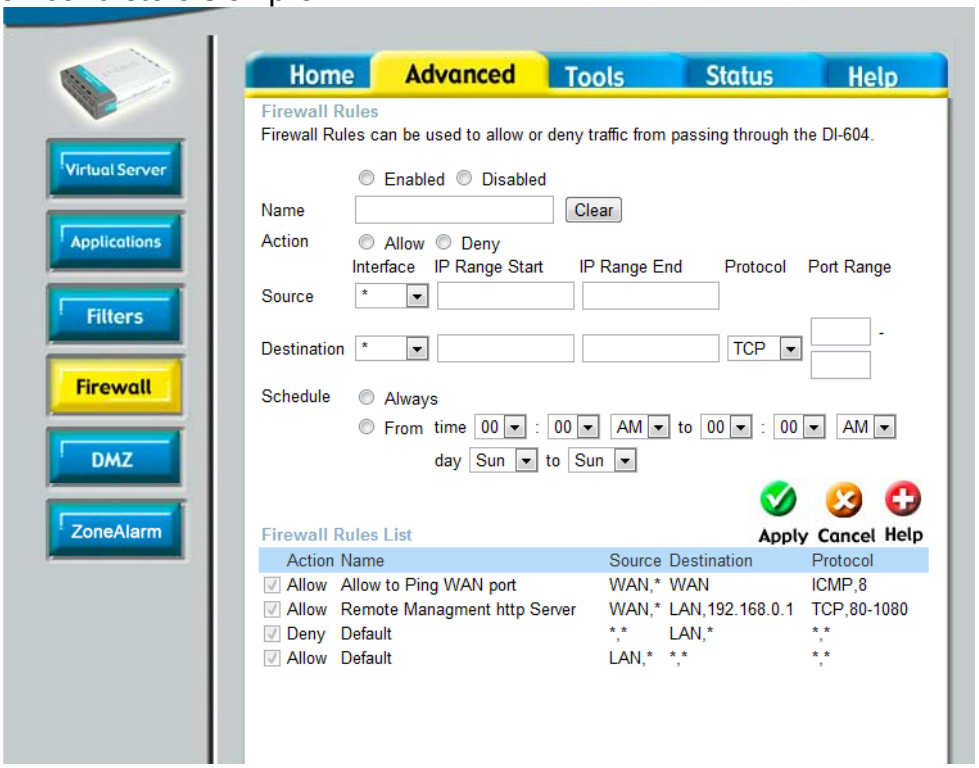
b) Realiza una comparativa entre los routers frontera atendiendo a las opciones de seguridad perimetral (NAT,Firewall,DMZ,...etc)

Router DLINK: http://support.dlink.com/emulators/di604_reve

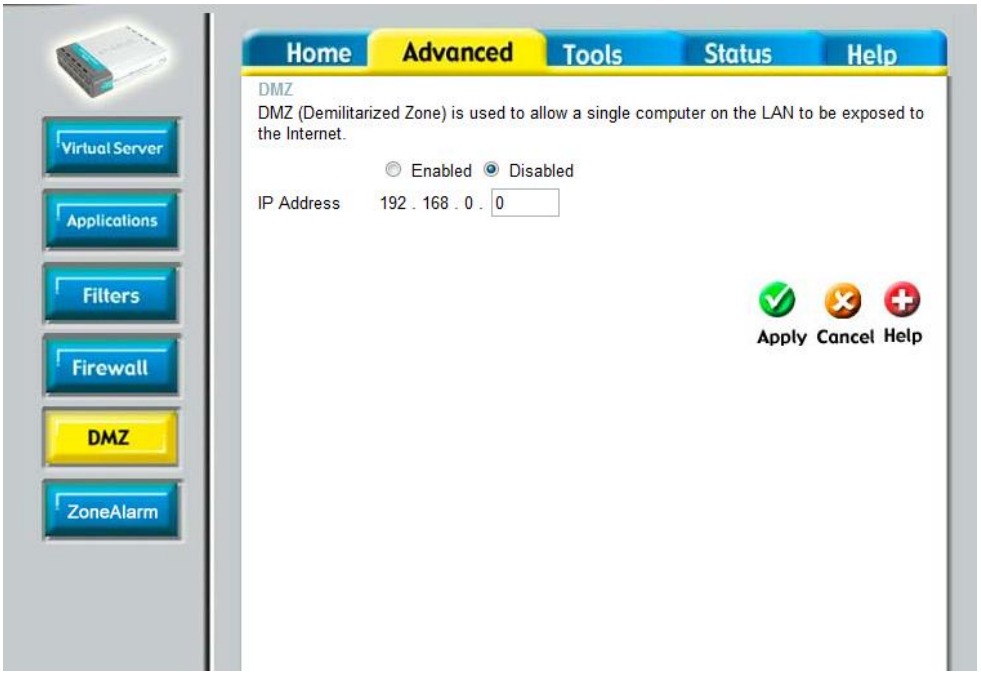
En este router podemos configurar varias opciones como son:
En primer lugar podremos implementar filtros en los que podremos bloquear ip, direcciones mac, puertos, e incluso podremos de elegir el momento y el dia que queramos que se realice el filtrado:



Otra opción de seguridad de este router en el firewall, aquí podremos permitir o denegar ciertas direcciones de origen a un destino concreto con un protocolo y unos puertos específicos y viceversa, al igual que lo que ocurría con los filtros también podremos configurar si estas configuraciones se aplicaran en un día en concreto o siempre:



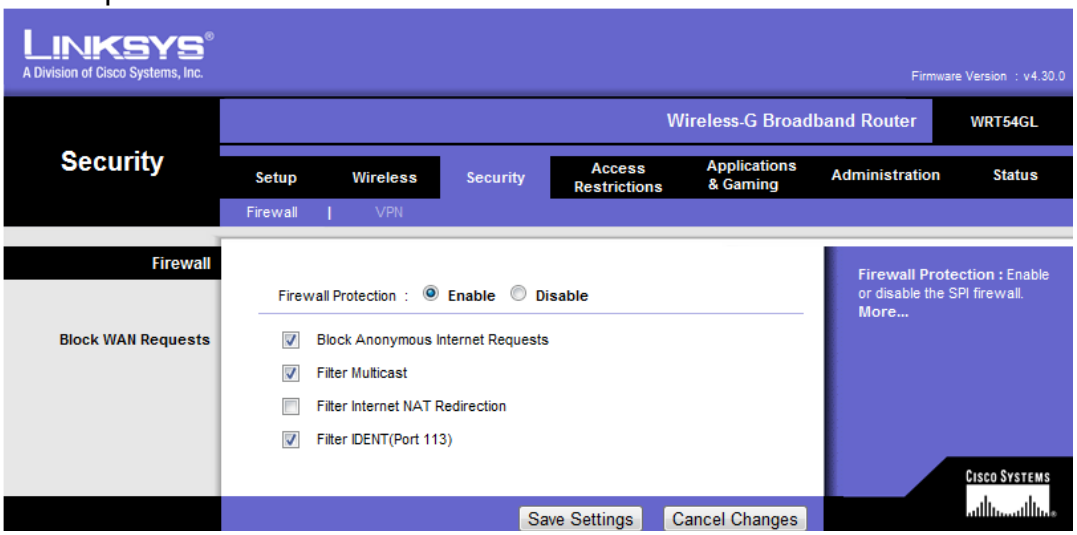
Por último podremos configurar una DMZ:



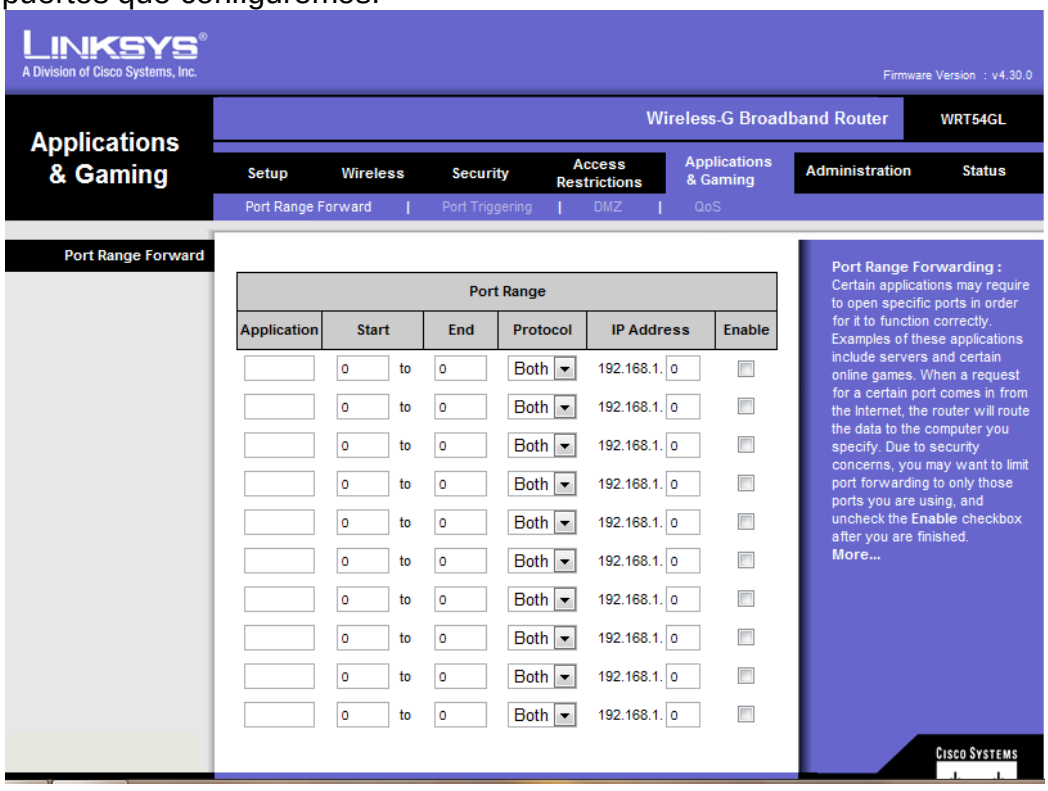
Router LINKSYS: http://ui.linksys.com/files/WRT54GL/4.30.0/Setup.htm

Este router nos ofrece varias opciones de seguridad, de las cuales podemos destacar las siguientes:

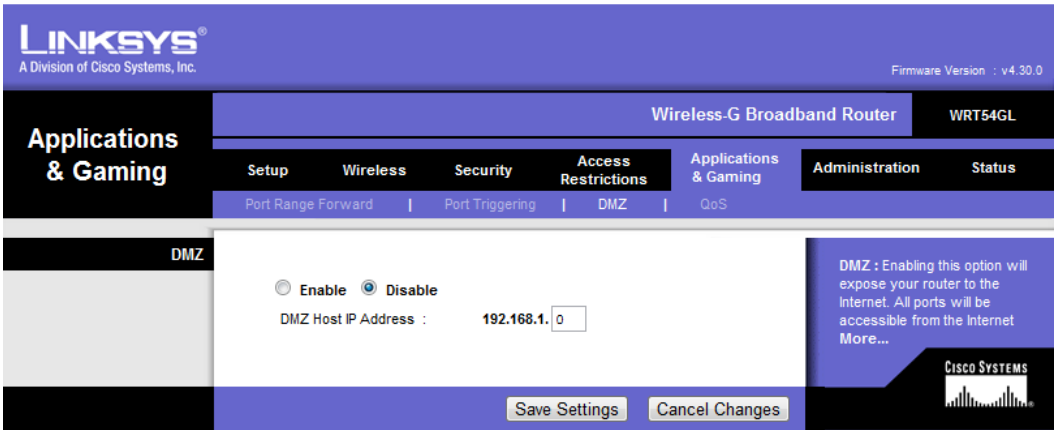
En primer lugar podemos encontrar un cortafuegos, en el cual podemos realizar varios tipos de filtros:



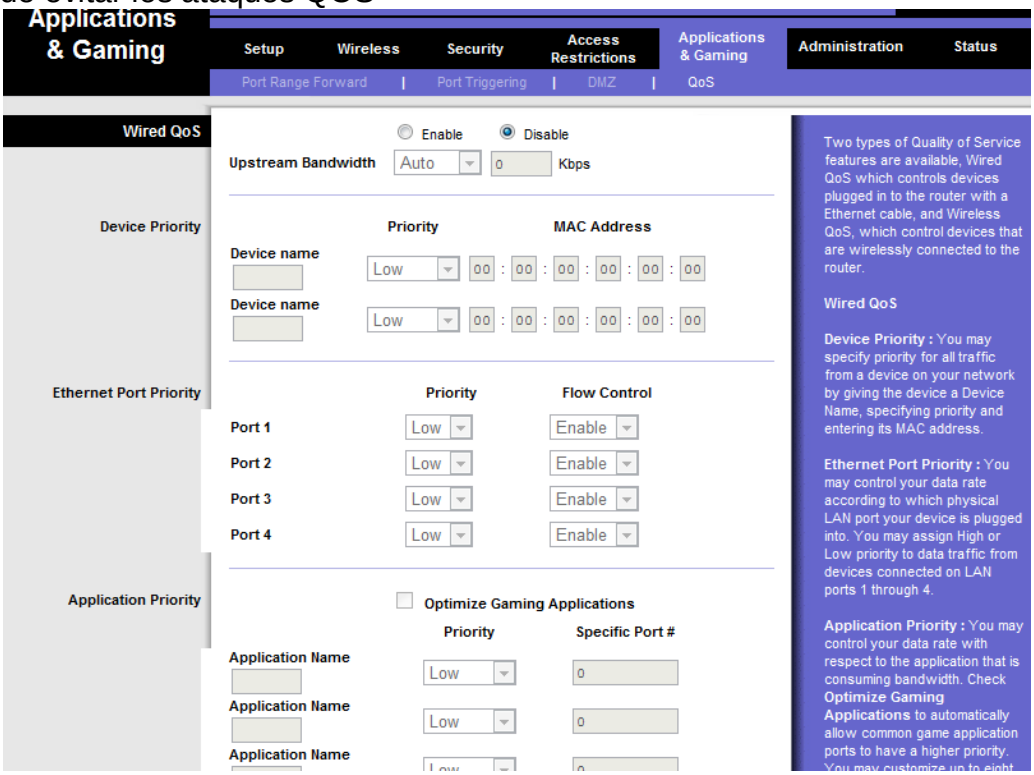
Tambien podremos realizar una serie de restricciones de acceso según los puertos que configuremos:



También podremos configurar una DMZ:

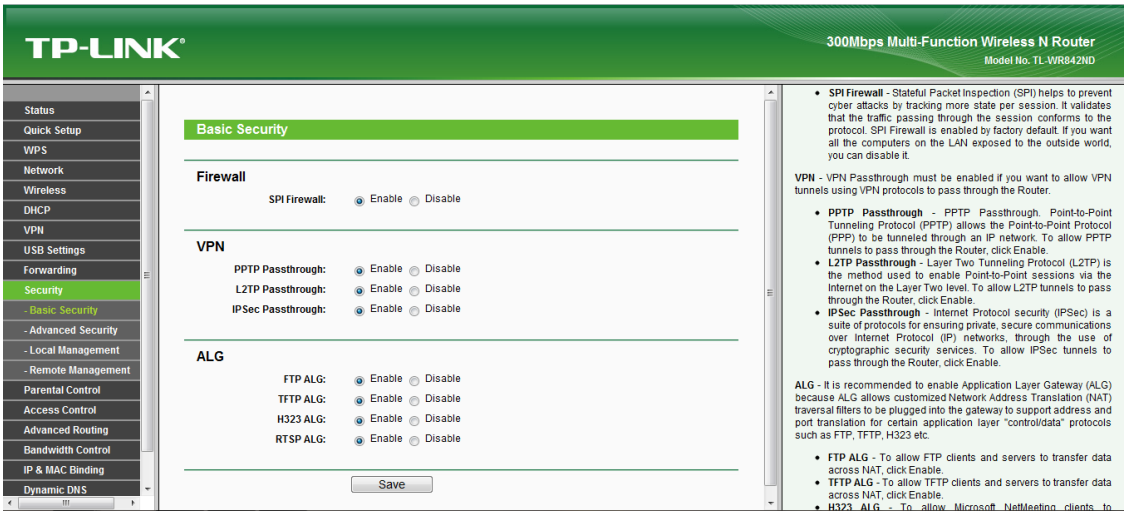


Por últimos podremos configurar unos parámetros específicos con el objetivo de evitar los ataques QOS

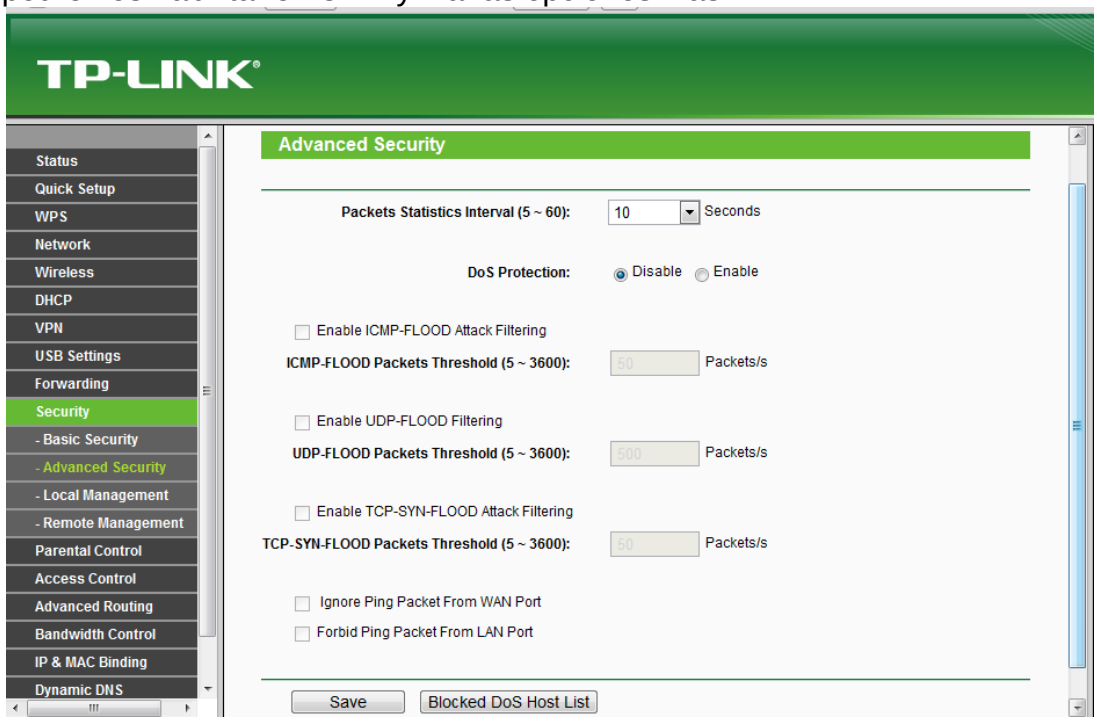


Router TP-LINK:
http://www.tplink.com/Resources/simulator/WR842ND(UN)1.0/index.htm

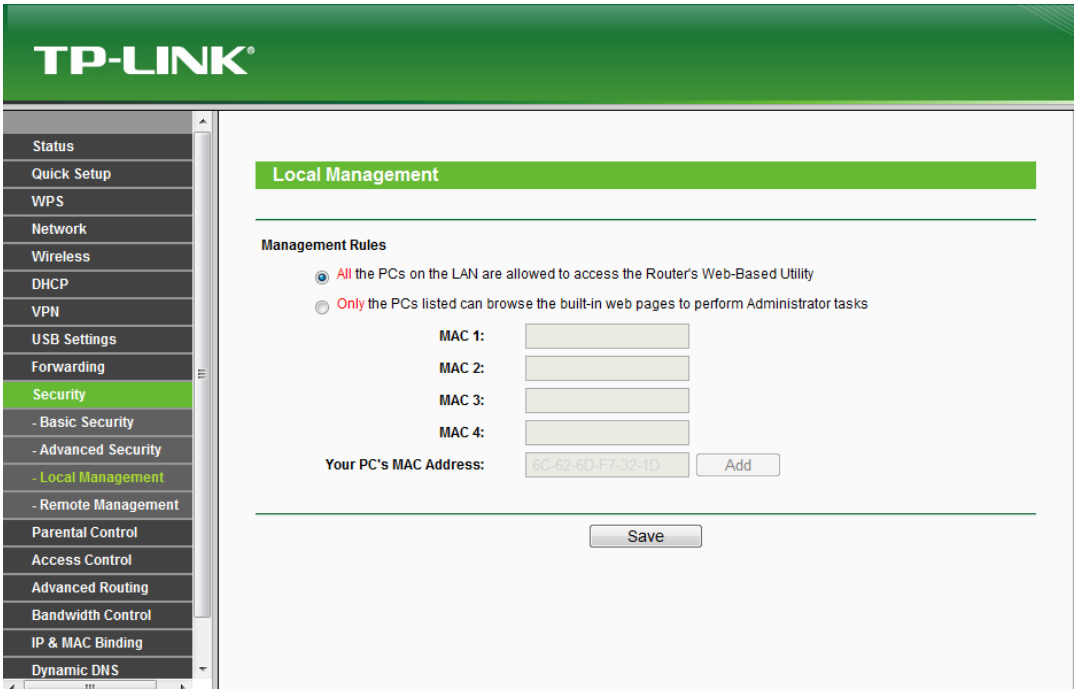
Las principales medidas de seguridad de este router son las siguientes:
En primer lugar podremos ver una sección de seguridad básica en la que podremos activar un firewall, vpn o alg pudiendo en estos 2 ultimos activar o desactivar ciertos protocolos:



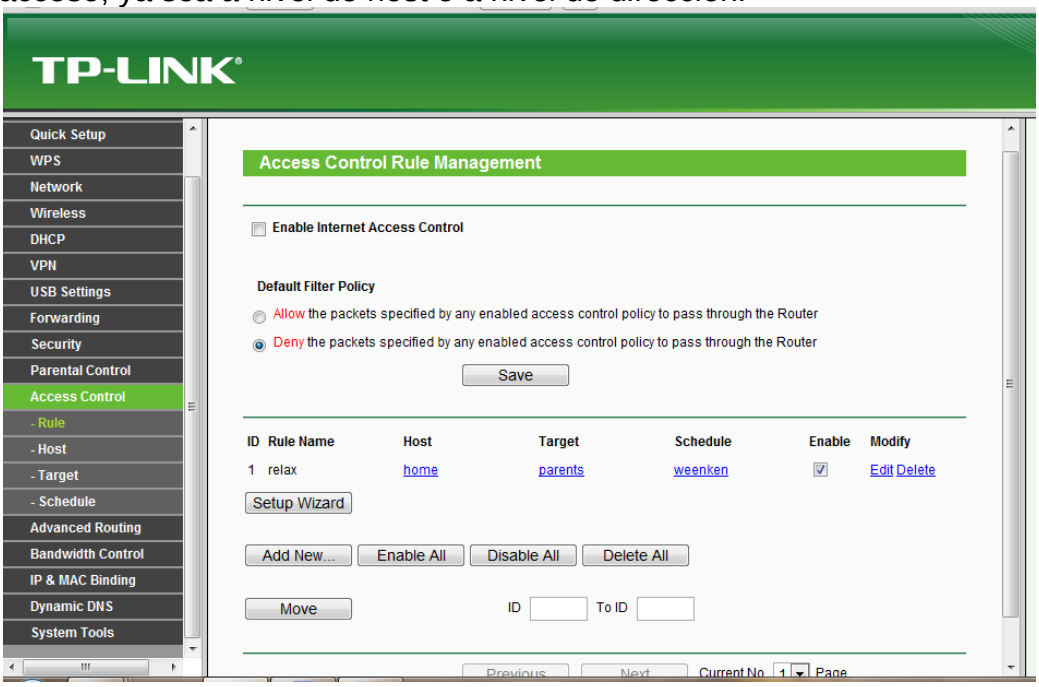
También encontramos unas opciones avanzadas de seguridad, aquí podremos habilitar el ICMP y varias opciones mas:



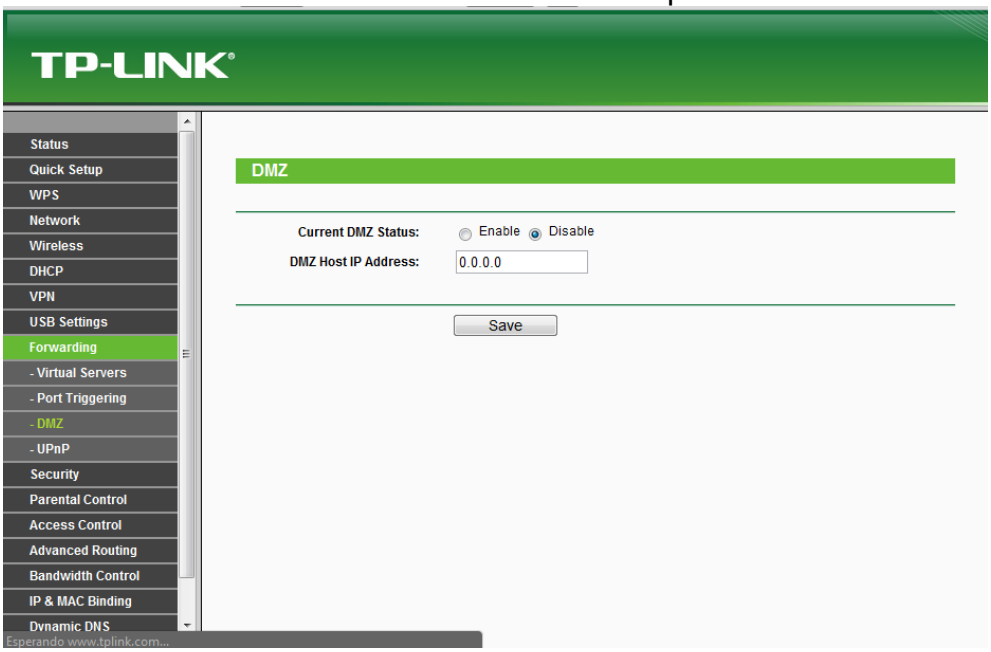
También encontramos opciones de seguridad locales en las que podremos configurar varias direcciones mac permitiendo o denegando su acceso al router



También podremos controlar el accesoa al router mediante listas de control de acceso, ya sea a nivel de host o a nivel de dirección:



Por último como en los routers anteriores también podremos definir una DMZ:



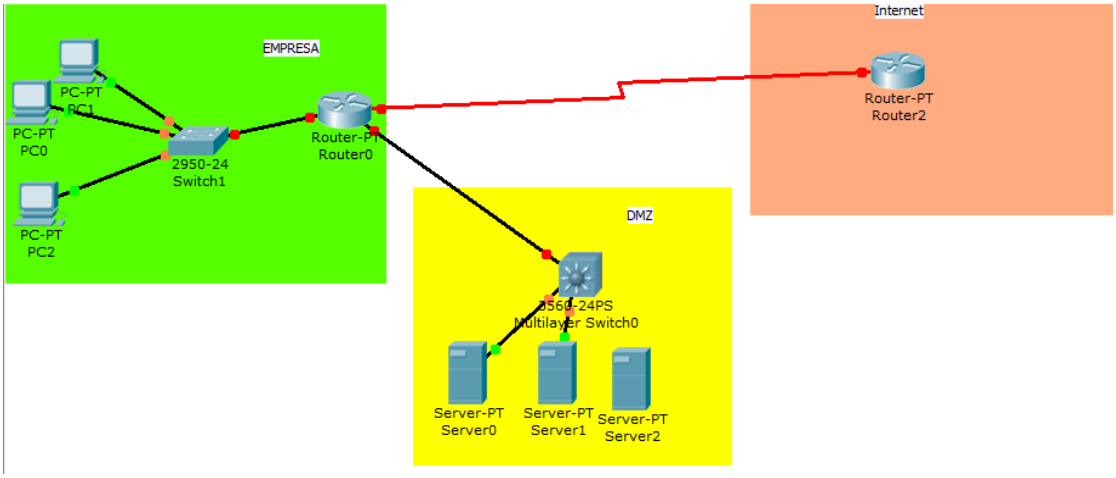
CONCLUSIÓN

Como conclusión podemos decir que aunque los 3 modelos de router tienen un gran abanico de opciones de seguridad, el que mas opciones de seguridad nos permite en el TP-LINK, por lo tanto en mi opinión este es el mejor router de los 3.

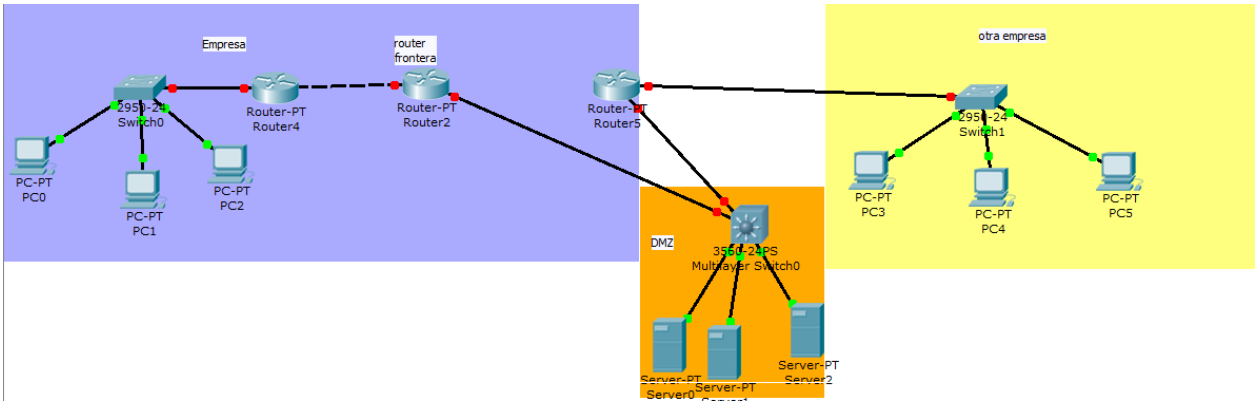
3. DMZ:

a) Planteamiento de escenarios DMZ en Cisco (Packet Tracert): esquemas.

En este esquema podremos ver una DMZ simple en la que se observamos una zona de la empresa local, luego una zona de internet y por útimo una zona desmilitarizada donde se situan los servidores de la empresa:

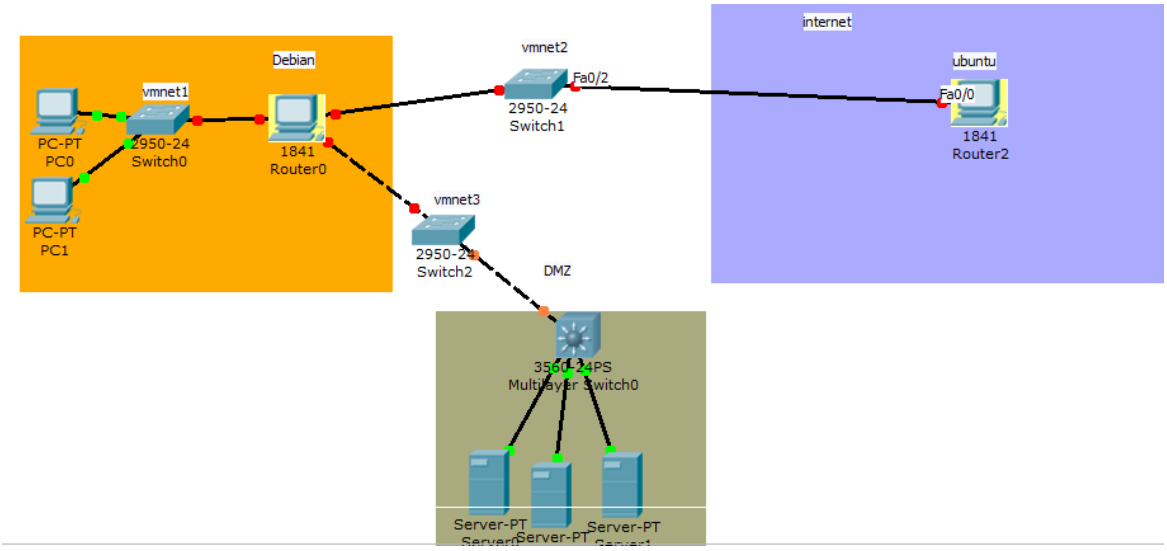


Otro esquema mas complejo es el siguiente en el que entre el router frontera de la empresa y otro router que es el que da acceso a la red a los equipos encontramos la DMZ:

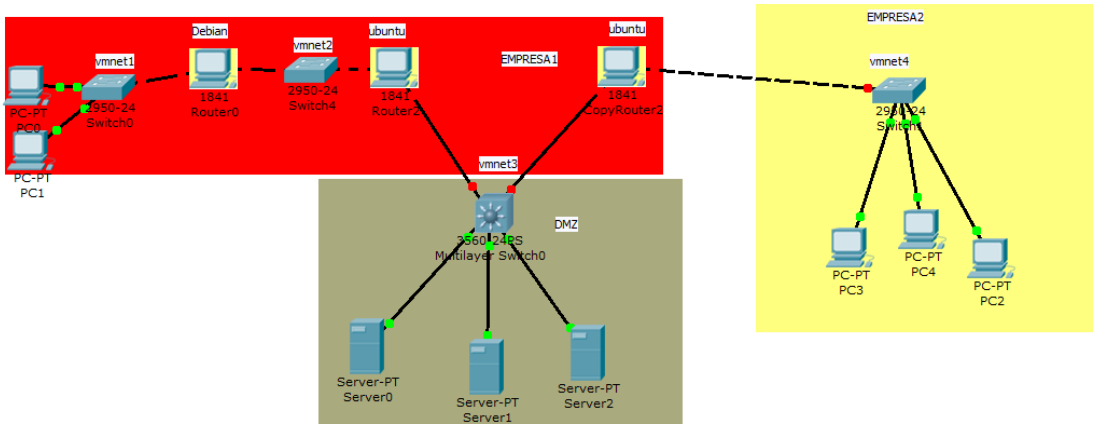


b)Planteamiento de escenarios DMZ en Linux (laboratorio virtual): esquemas.

En este esquema podremos ver una DMZ simple en la que se observamos una zona de la empresa local, luego una zona de internet y por útimo una zona desmilitarizada donde se situan los servidores de la empresa:



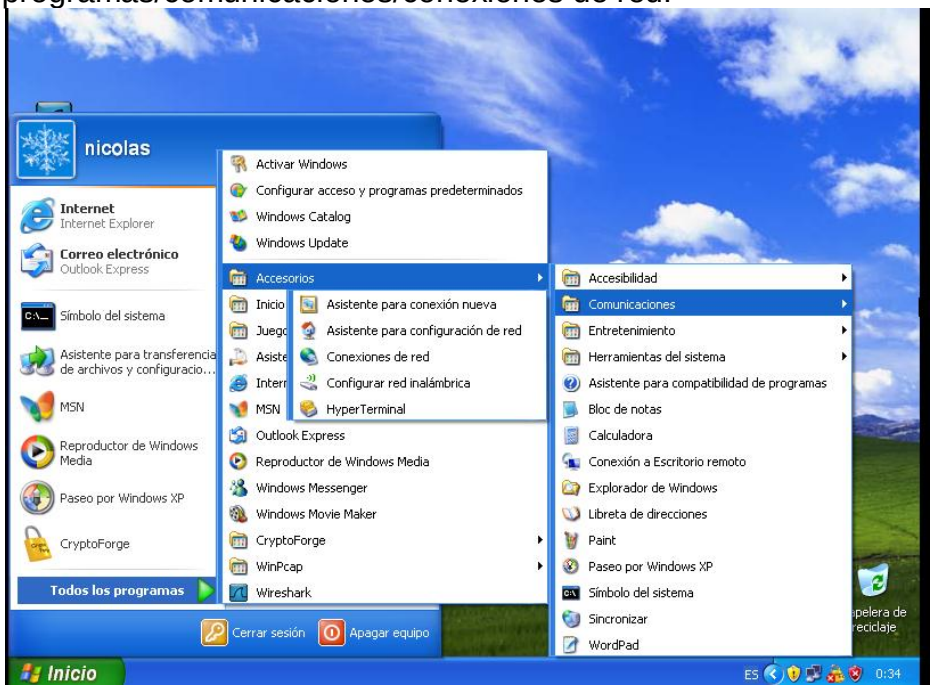
Otro esquema mas complejo es el siguiente en el que entre el router frontera de la empresa y otro router que es el que da acceso a la red a los equipos encontramos la DMZ:



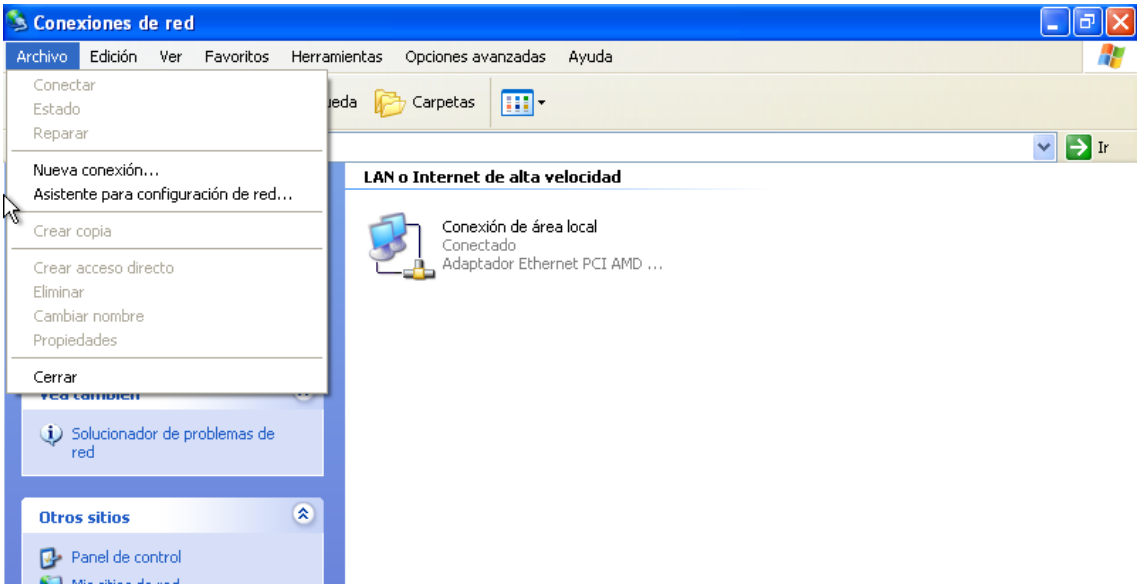
4.VPN sobre red local

a) Instalación de un servidor VPN en Windows XP.

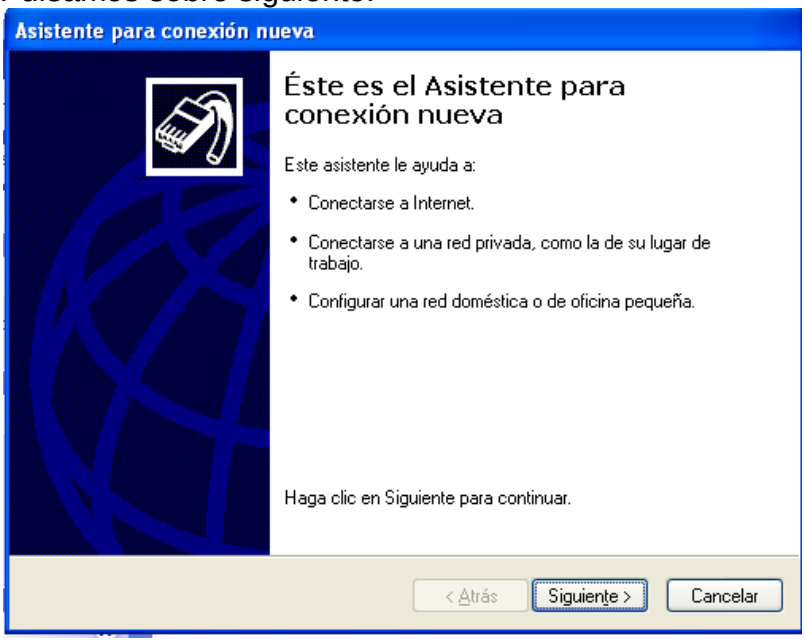
En primer lugar nos dirigimos a inicio/todos los programas/comunicaciones/conexiones de red:



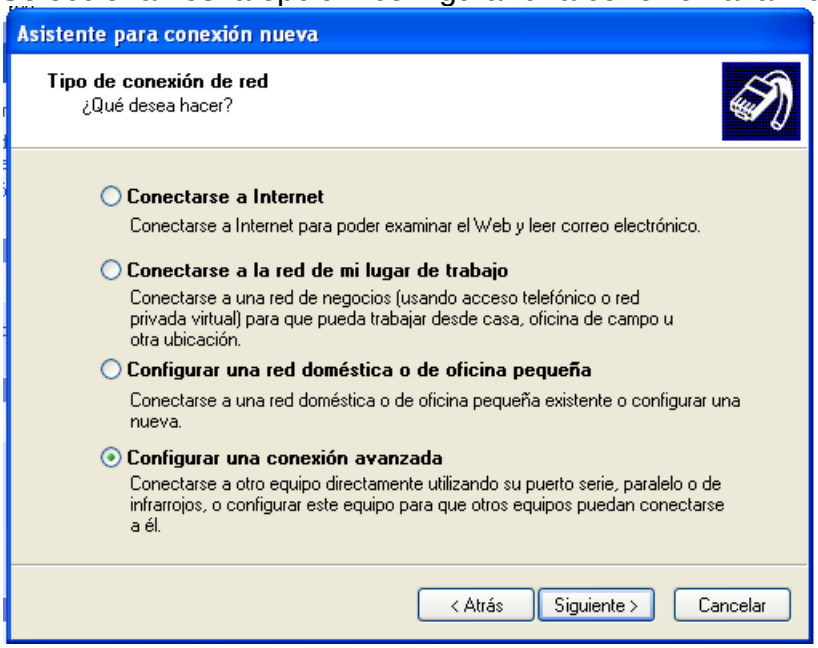
En la ventana que nos aparece nos dirigimos a archivo/nueva conexión:



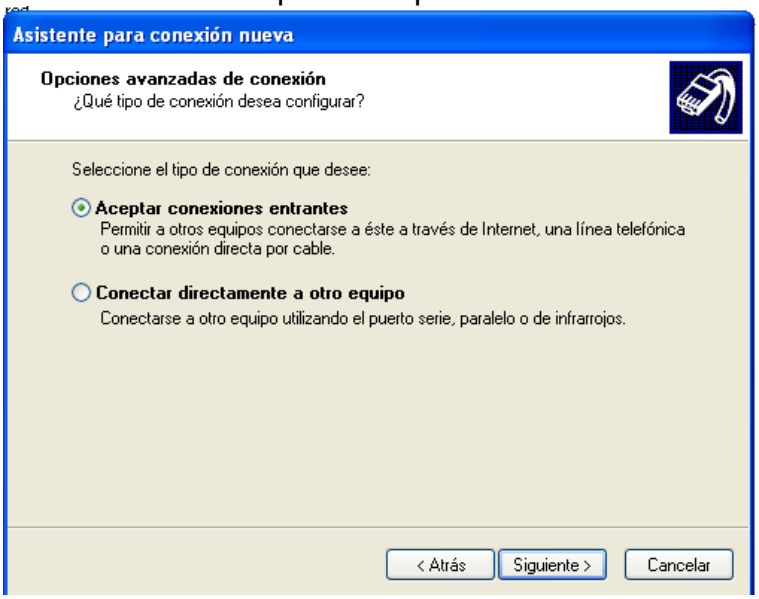
Pulsamos sobre siguiente:



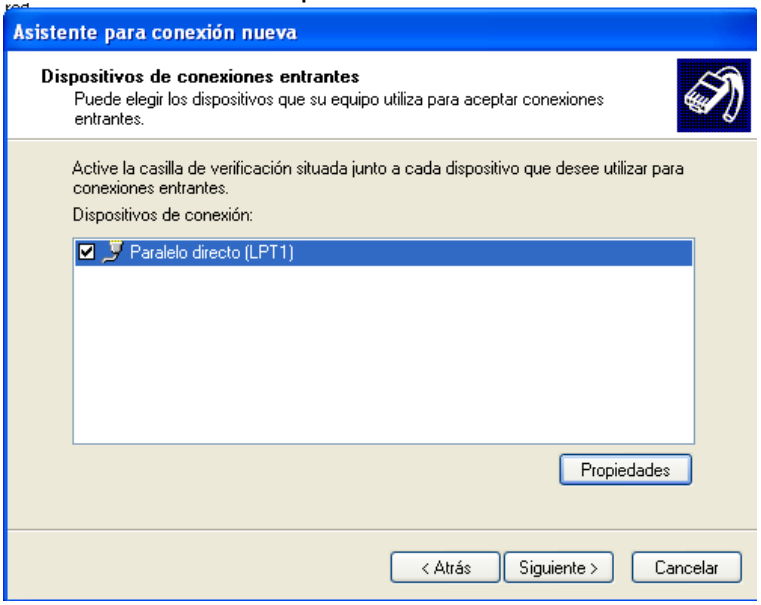
Seleccionamos la opción configurar una conexión avanzada:



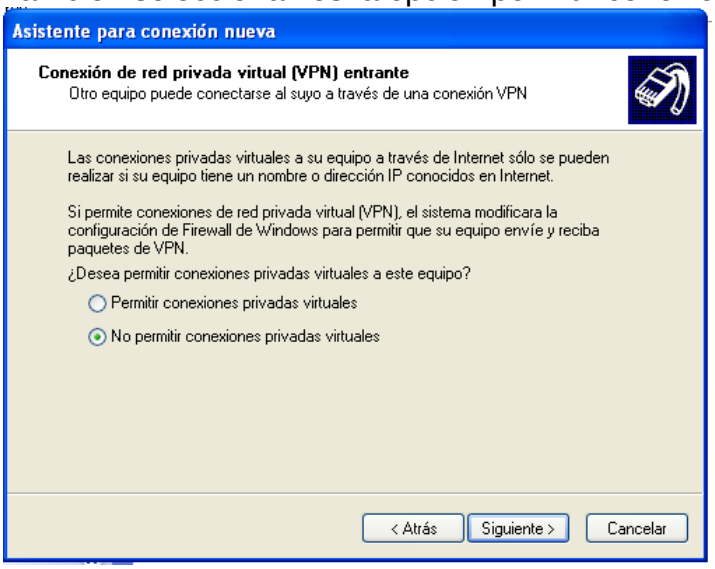
Seleccionamos la opción aceptar conexiones entrantes:



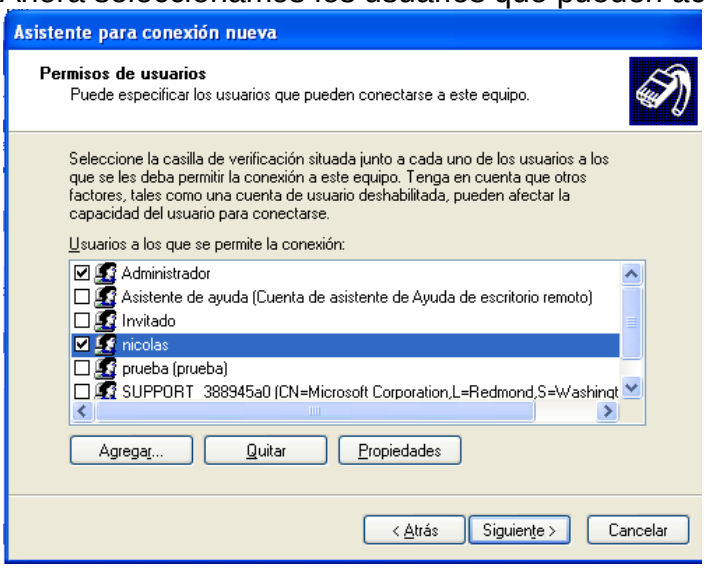
Seleccionamos el dispositivo de conexiones entrantes:



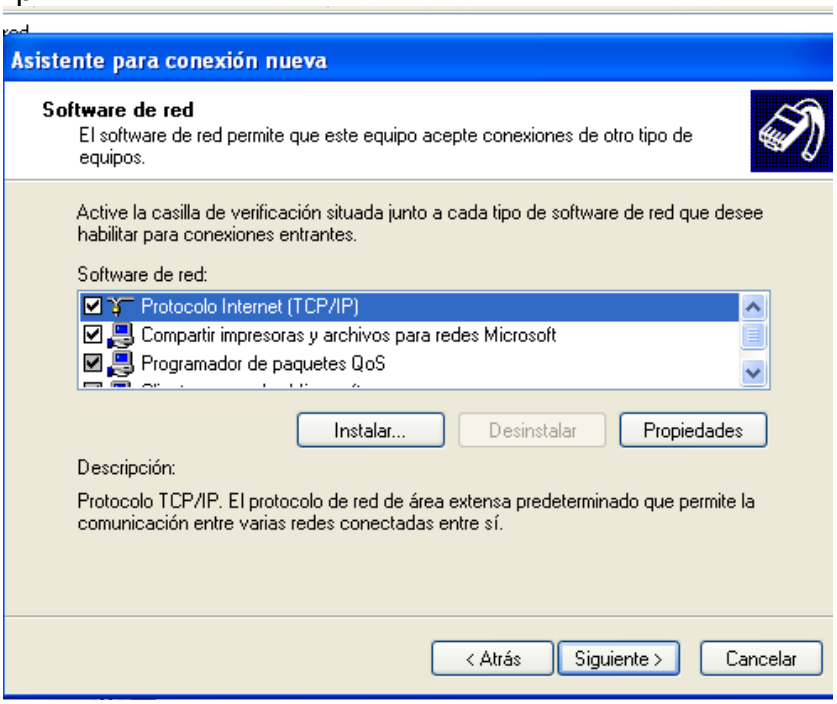
También seleccionamos la opción permitir conexiones privadas virtuales:



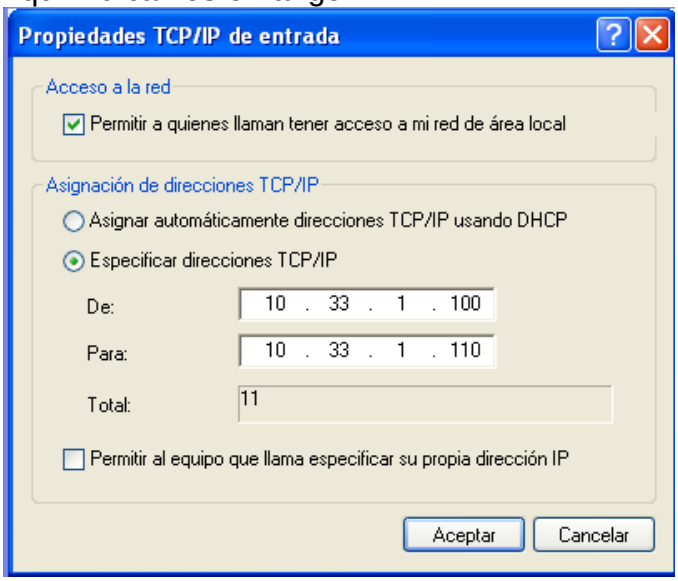
Ahora seleccionamos los usuarios que pueden acceder:



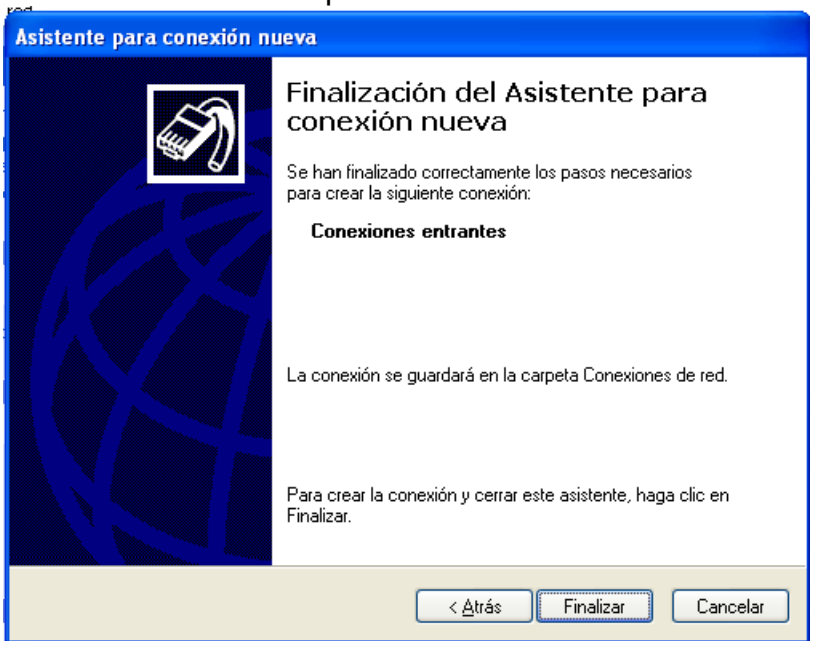
En la siguiente pantalla en el protocolo indicamos el rango de ips de nuestra vpn:



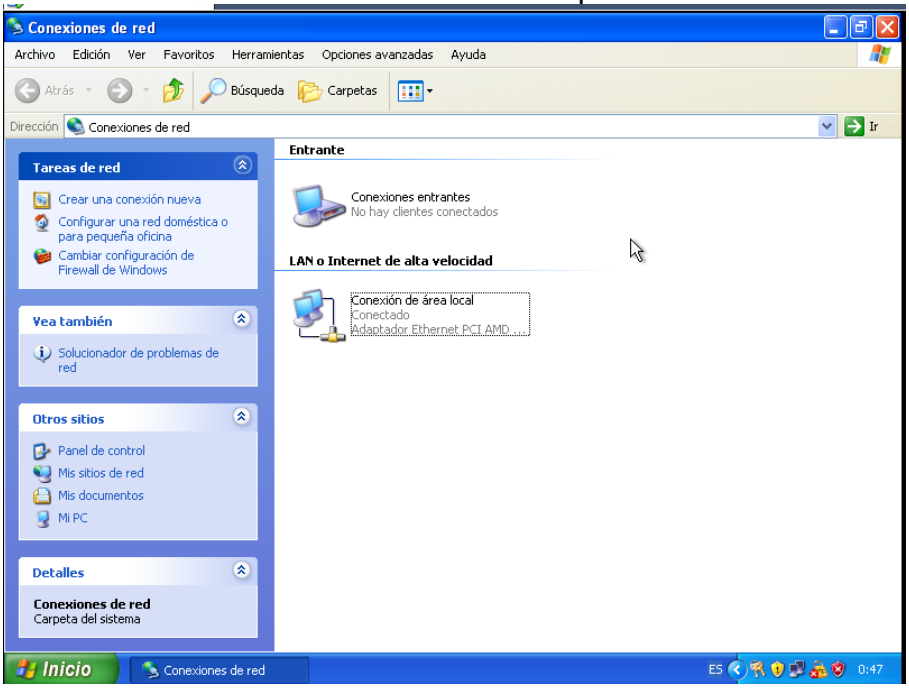
Aquí indicamos el rango:



Ahora finalizaremos el proceso:



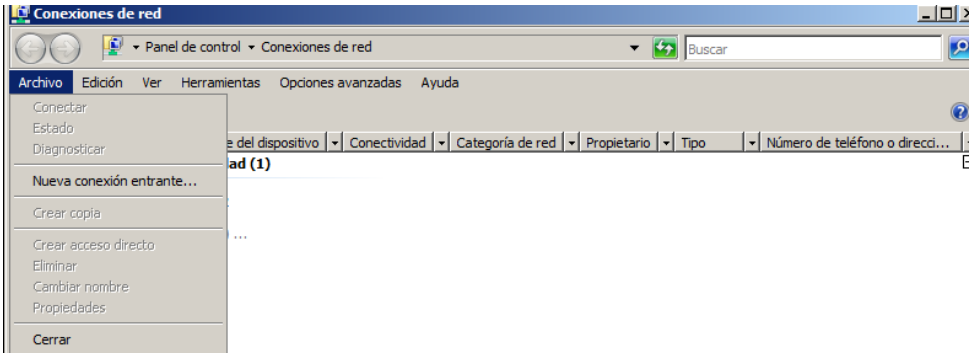
Ahora en conexiones de red nos habrá aparecido nuestra nueva VPN:



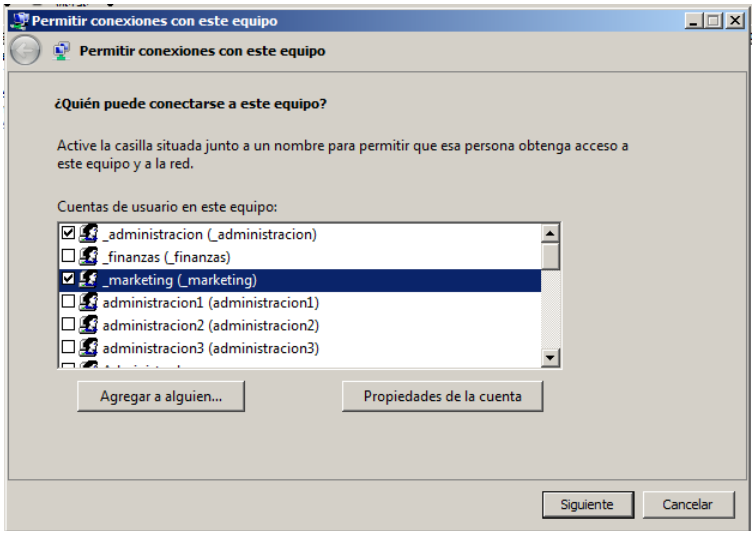
b) Instalación de un servidor VPN en Windows 2003/2008.

EN WS2008

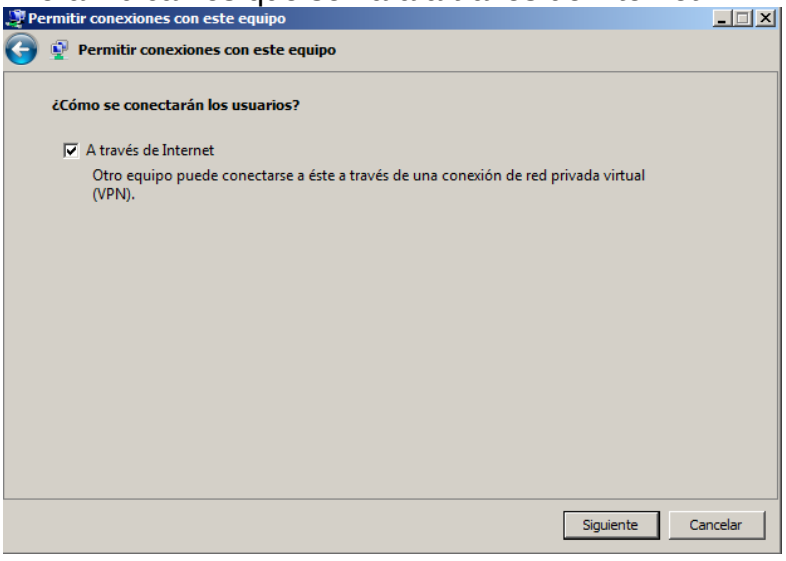
EN primer lugar nos dirigimos a conexiones de red, una vez allí seleccionamos la configurar conexión de red y seleccionamos la opción nueva conexión entrante:



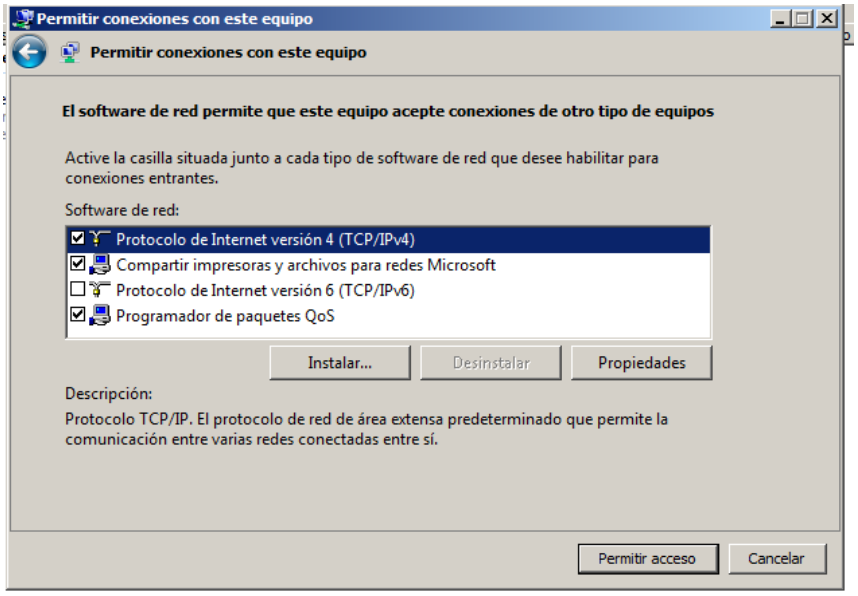
Ahora seleccionamos los usarios autorizados:



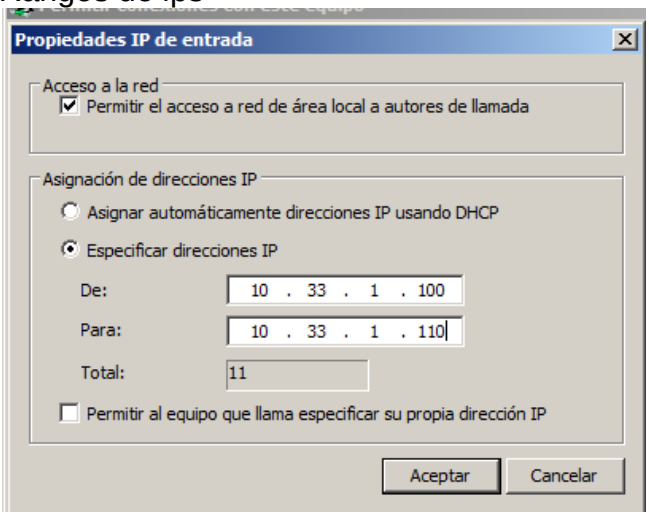
Ahora indicamos que se hara a través de internet:



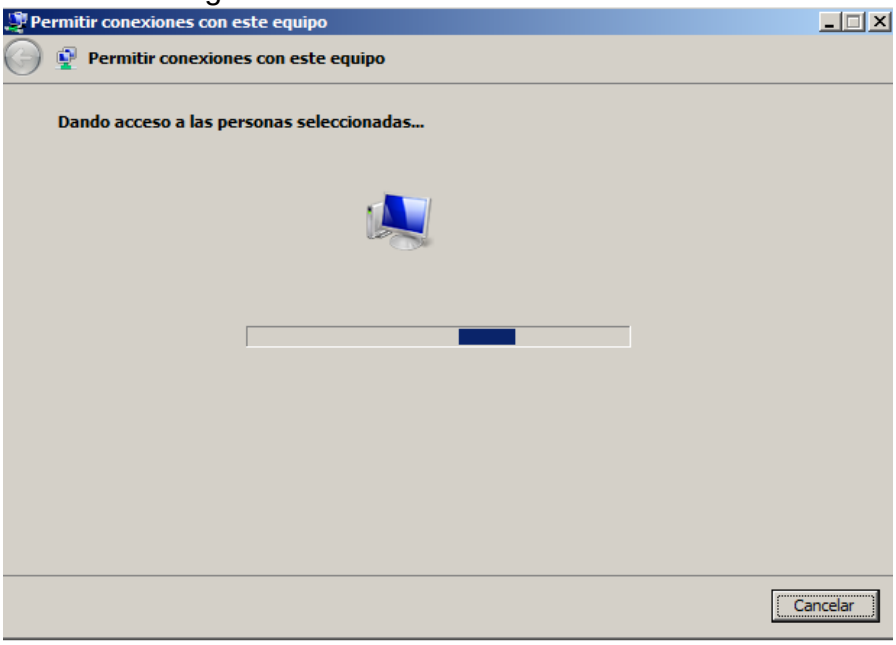
En esta pantalla configuramos el protocolo TPC para indicar el rango de ips de servidor VPN:



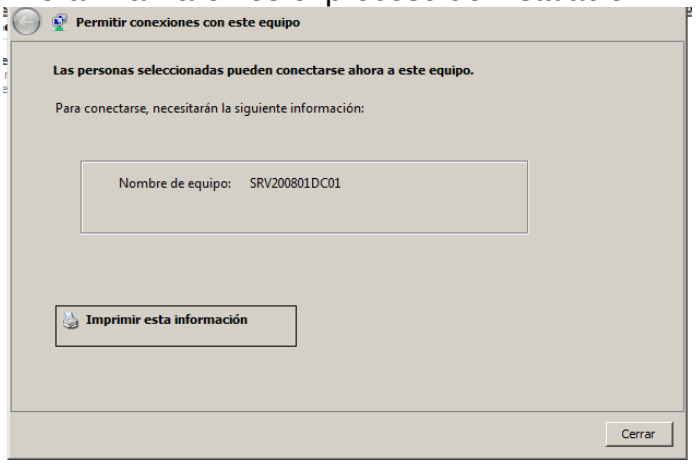
Rangos de ips



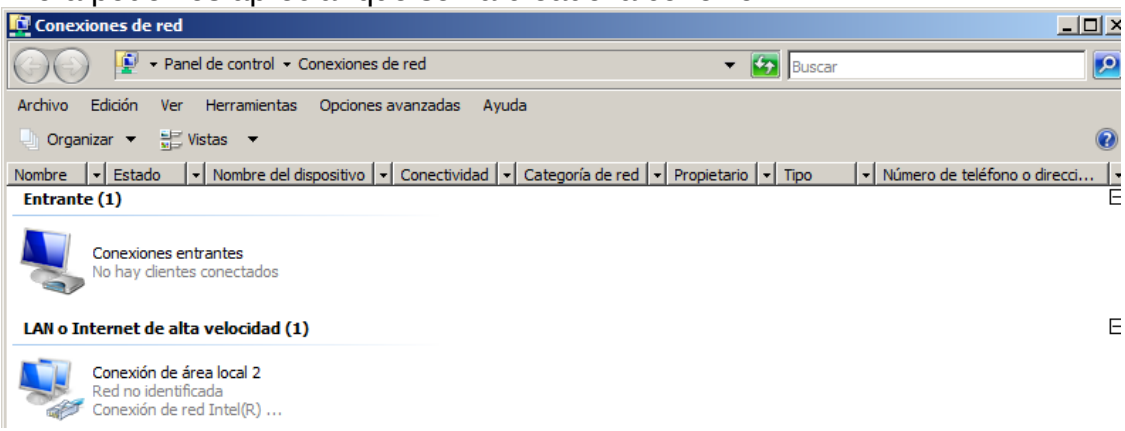
Ahora se configurara nuestra VPN:



Ahora finalizaremos el proceso de instalación:



Ahora podemos apreciar que se ha creado la conexión VPN:



c) Instalación de un servidor VPN en GNU/Linux

Primero instalaremos el paquete pptpd:

```
root@molinux1:/etc/apache2# apt-get install pptpd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  bcrelay
Se instalarán los siguientes paquetes NUEVOS:
  bcrelay pptpd
0 actualizados, 2 se instalarán, 0 para eliminar y 134 no actualizados.
Necesito descargar 116kB de archivos.
Se utilizarán 446kB de espacio de disco adicional después de esta operación
¿Desea continuar [S/n]? s
0% [Conectando a repositorios.molinux.info]
```

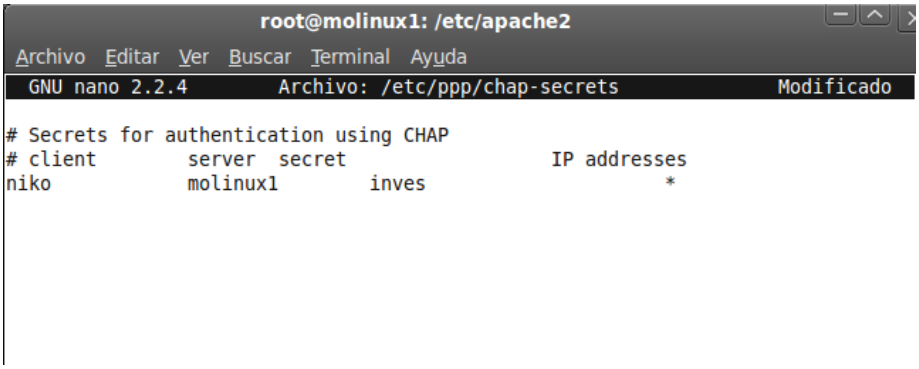
Una vez instalado accederemos y modificaremos el archivo /etc/ppp/pptpd-options con los valores remarcados en la imagen:

```
  GNU nano 2.2.4        Archivo: /etc/ppp/pptpd-options

################################################################################


# Authentication

# Name of the local system for authentication purposes
# (must match the second field in /etc/ppp/chap-secrets entries)
name molinux1
require-mschap-v2
require-mppe-128
ms-dns 10.33.1.1
ms-dns 8.8.8.8
proxyarp
nodefaultroute
lock
# Optional: domain name to use for authentication
# domain mydomain.net

# Strip the domain prefix from the username before authentication.
```

Ahora en el archivo /etc/pptpd.conf introducimos las siguientes líneas:

```
root@molinux1: /etc/apache2
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
  GNU nano 2.2.4          Archivo: /etc/pptpd.conf

#       4. If you give a single localIP, that's ok - all local IPs will
#          be set to the given one. You MUST still give at least one remote
#          IP for each simultaneous client.
#
# (Recommended)
#localip 192.168.0.1
#remoteip 192.168.0.234-238,192.168.0.245
# or
#localip 192.168.0.234-238,192.168.0.245
#remoteip 192.168.1.234-238,192.168.1.245

ppp /usr/sbin/pppd
option /etc/ppp/pptpd-options
localip 10.33.1.1
remoteip 10.33.1.20-50



                        [ 86 líneas escritas ]
^G Ver ayuda ^O Guardar   ^R Leer Fich ^Y RePág.    ^K Cortar Tex^C Pos actual
^X Salir     ^J Justificar^W Buscar    ^V Pág. Sig. ^U PegarTxt  ^T Ortografía
```

Ahora en /etc/ppp/chap-secrets y agregamos un nombre de usuario que deseamos permitir:



Ahora reiniciamos el servicio:

```
root@molinux1:/etc/apache2# /etc/init.d/pptpd restart
Restarting PPTP:
Stopping PPTP: pptpd.
Starting PPTP Daemon: pptpd.
```

COnfiguracion de un cliente Linux:

Ahora introducimos los datos del servidor VPN y el nombre de usuario y contraseña:

Ahora habilitaremos la configuración VPN creada:

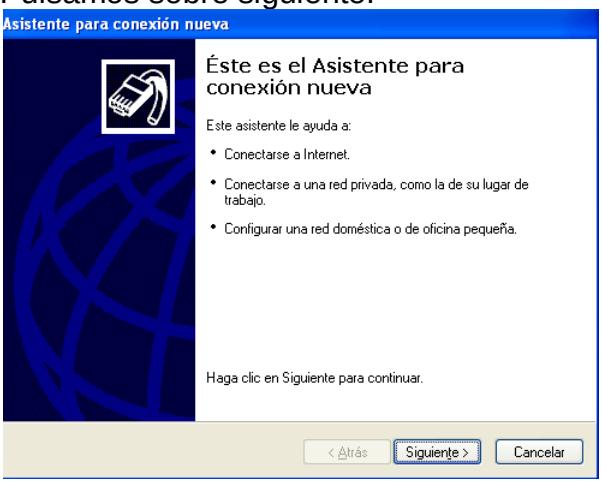
Configuración de cliente en WINDOWS XP:

d) Conexión desde un cliente Windows y GNU/Linux VPN a un servidor VPN.

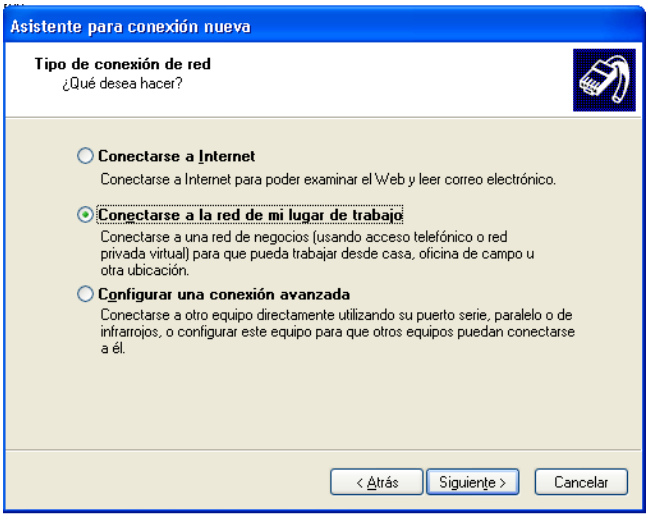
EN WINDOWS XP:

En primer lugar nos dirigimos a conexiones de red; una vez allí pulsamos sobre la opción nueva conexión de red:

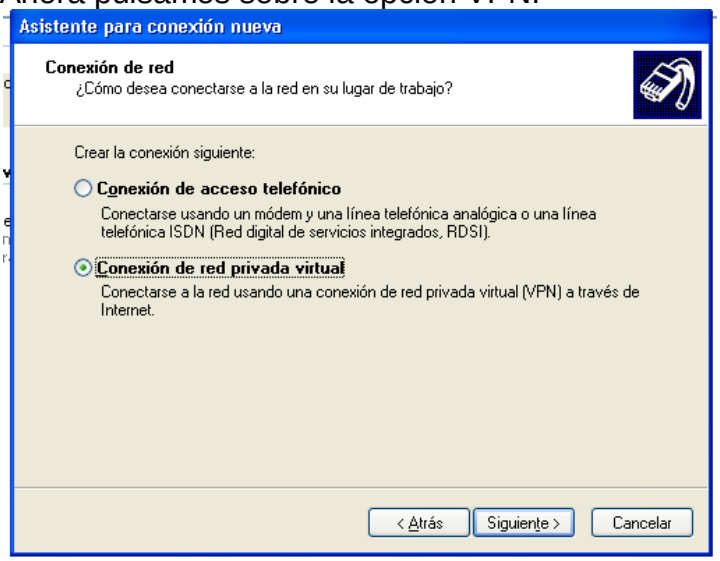
Pulsamos sobre siguiente:



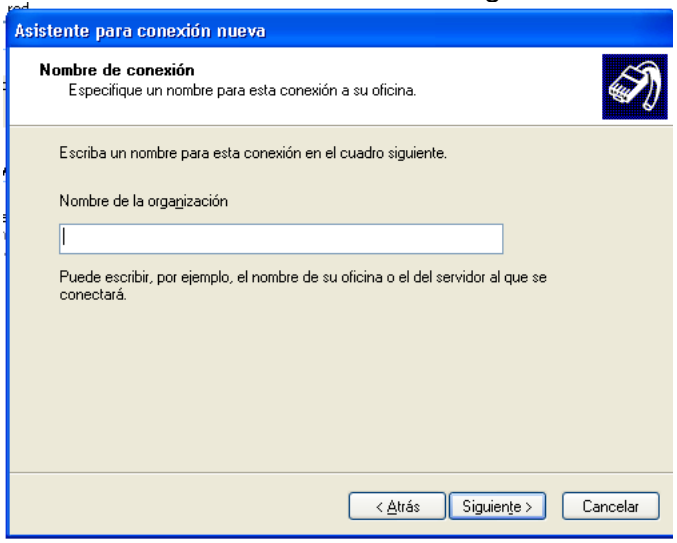
Ahora pulsamos la opción conectarse a la red de mi lugar de trabajo:



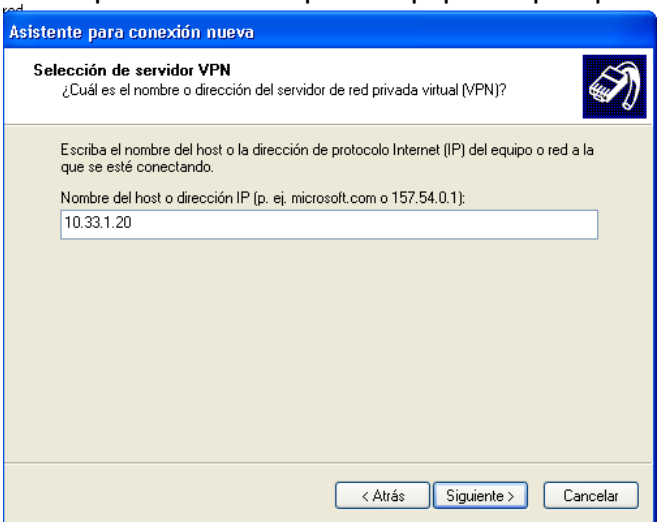
Ahora pulsamos sobre la opción VPN:



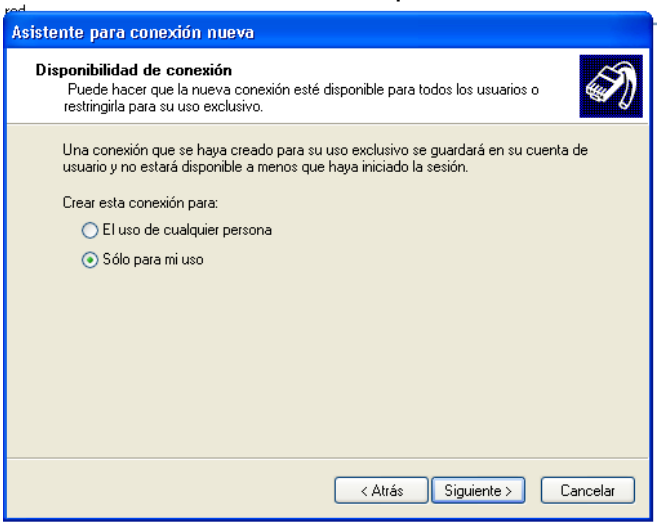
Ahora le damos un nombre a la organización:



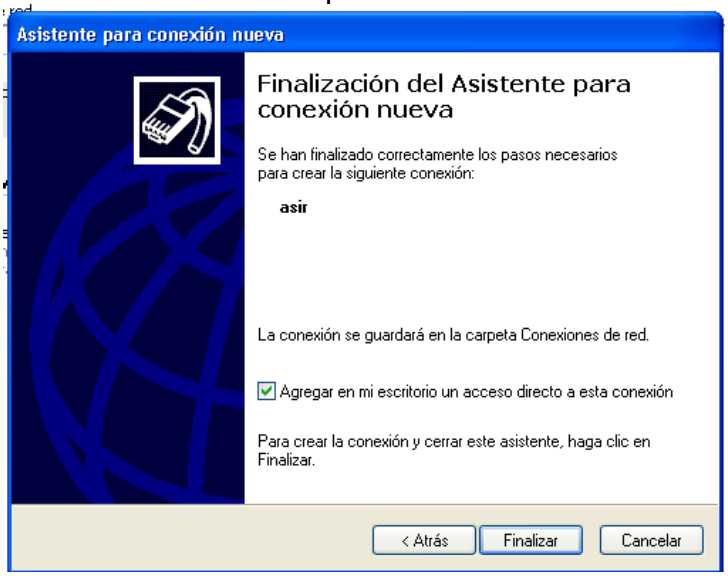
Ahora pondremos la ip del equipo al que queremos conectarnos:



Ahora seleccionaremos la opción crear esta conexión solo para este usuario:

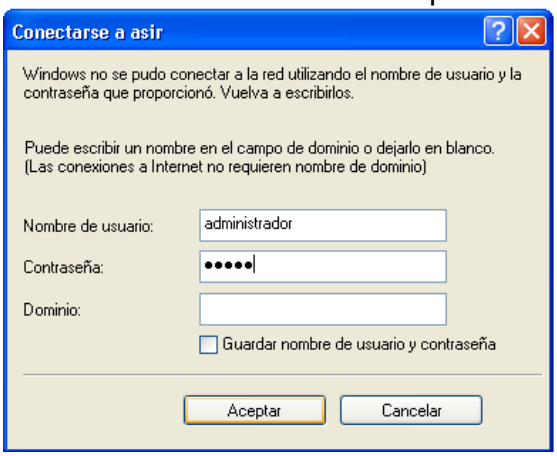


Ahora finalizaremos el proceso:

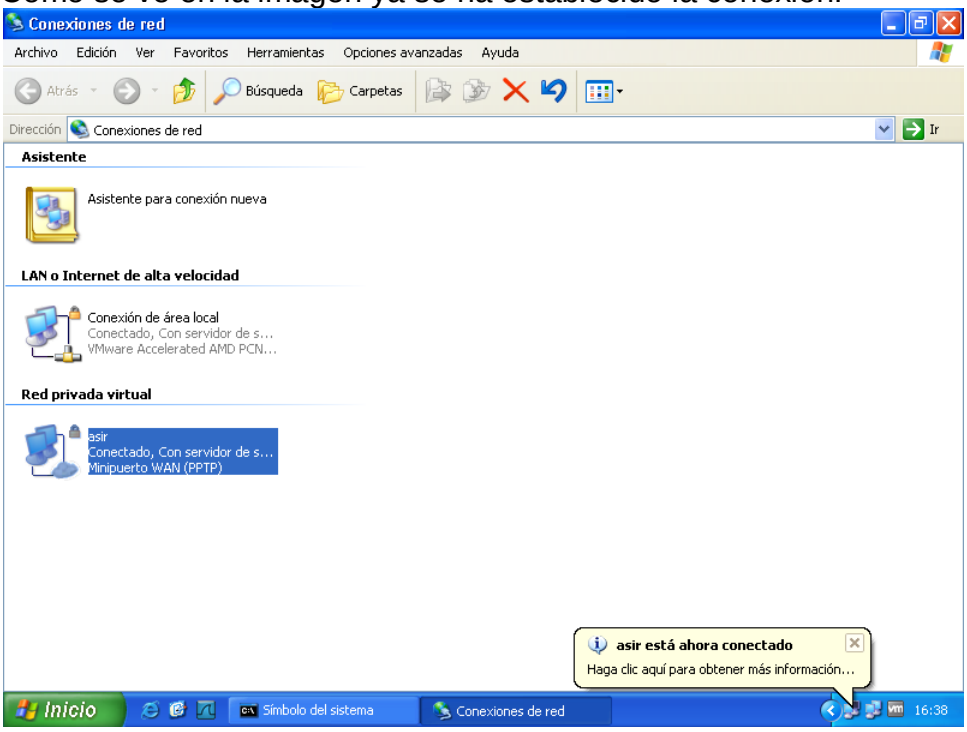


Ahora pondremos el nombre de usuario y contraseña:

Ahora deberemos de volver a poner la contraseña:

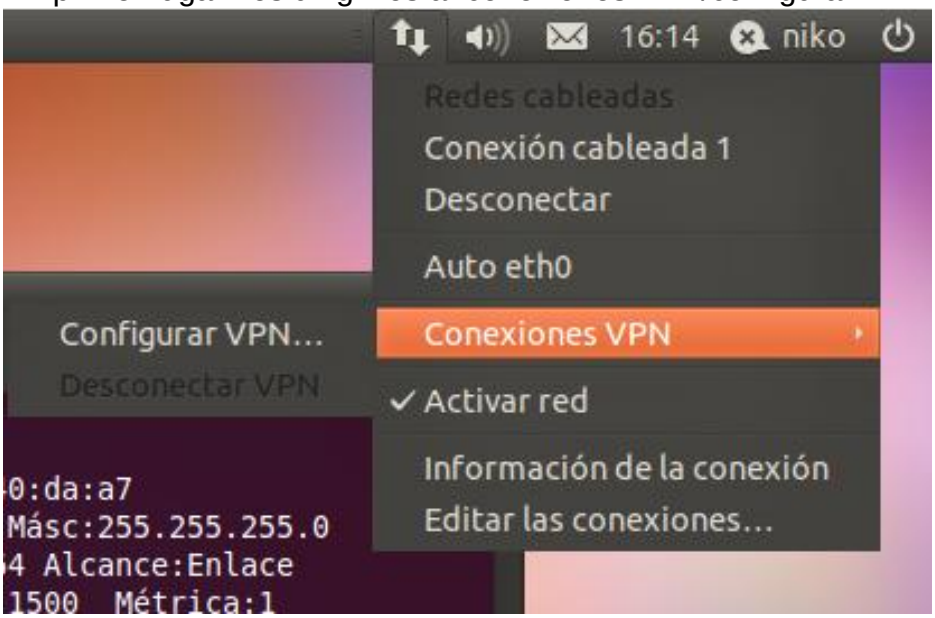


Como se ve en la imagen ya se ha establecido la conexión:

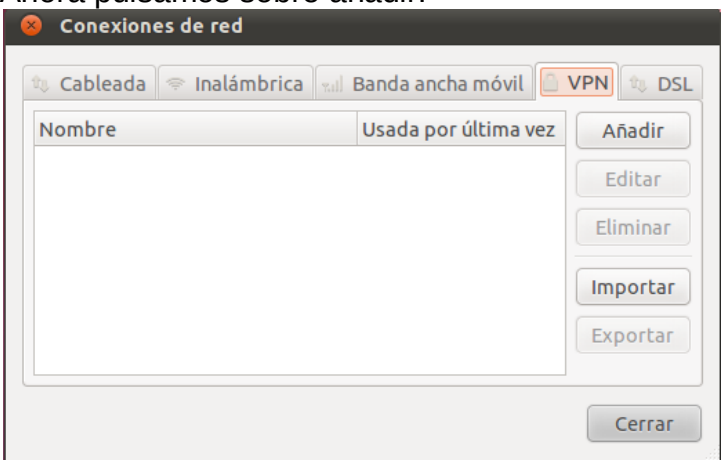


Cliente en Ubuntu:

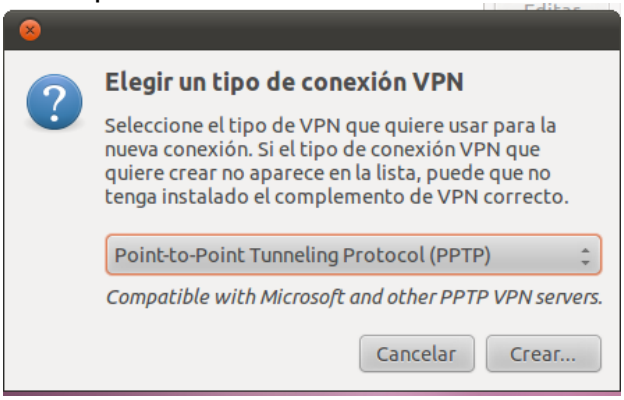
EN primer lugar nos dirigimos a conexiones VPN/configurar VPN:



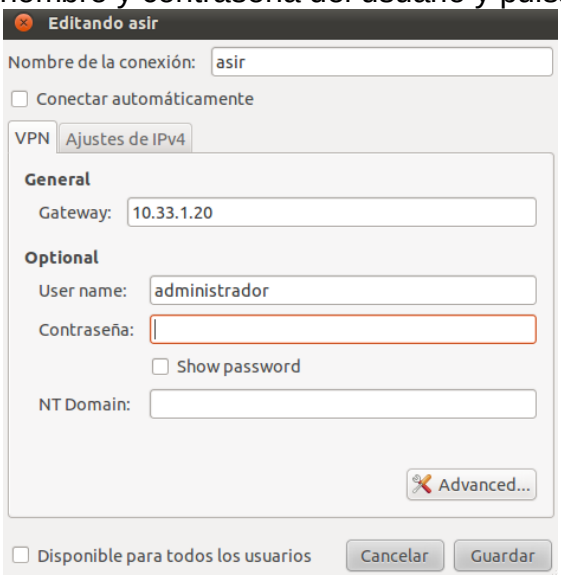
Ahora pulsamos sobre añadir:



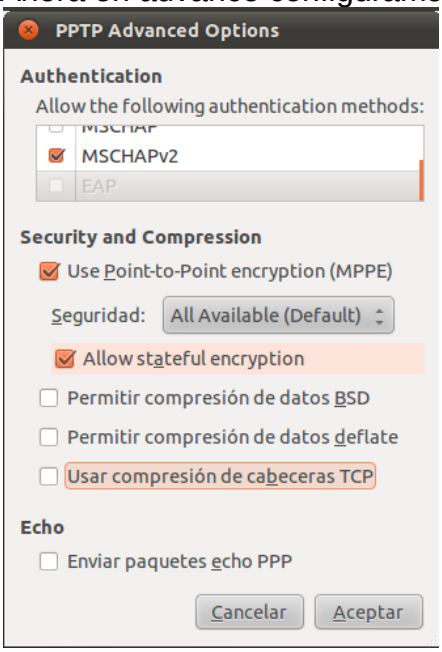
Ahora pulsamos sobre crear:



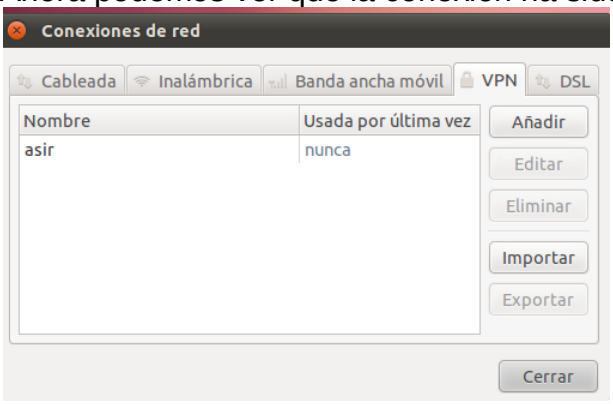
Ahora rellenamos los siguientes campos con la dirección del servidor VPN y el nombre y contraseña del usuario y pulsamos sobre guardar:



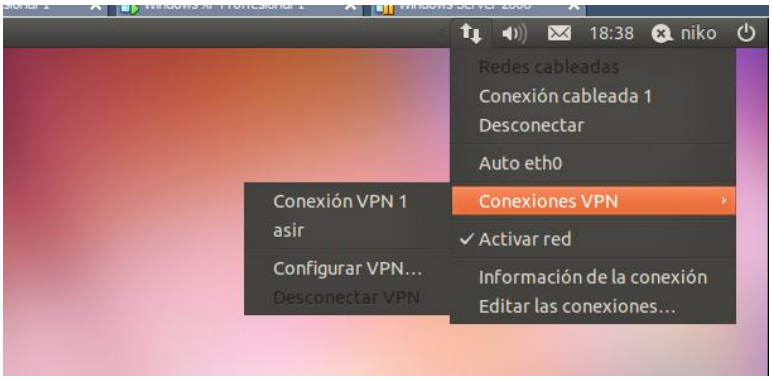
Ahora en advance configuramos lo que aparece en pantalla:



Ahora podemos ver que la conexión ha sido creada:



Ahora la activaremos, para ello nos dirigimos a conexiones VPN y seleccionamos asir:



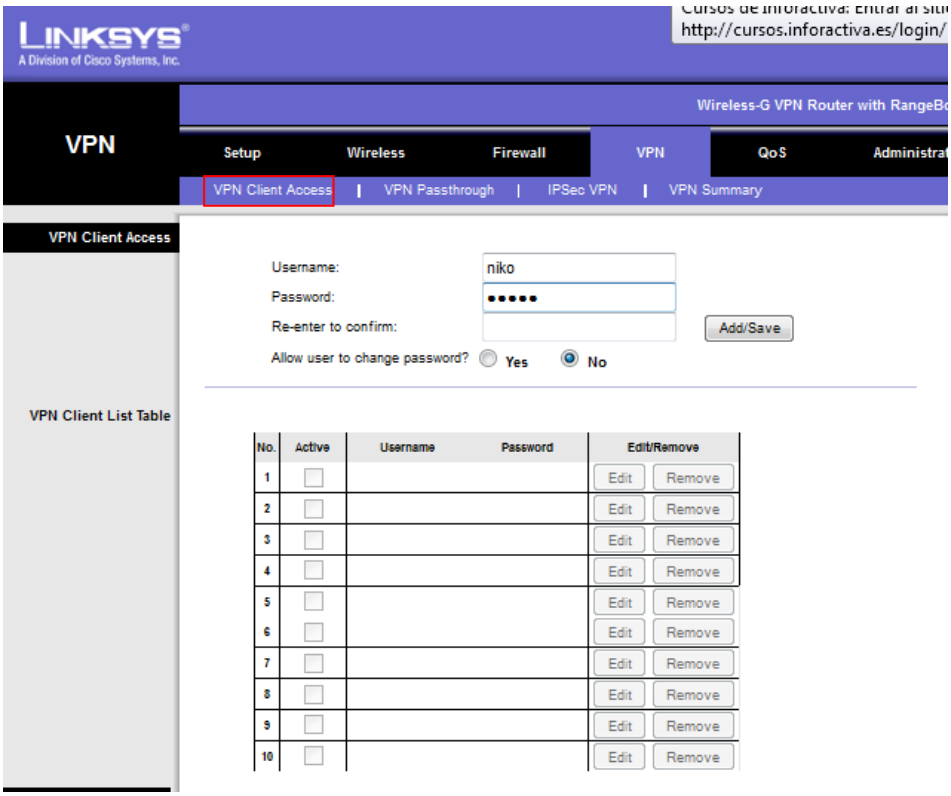
5. VPN de acceso remoto

b) Configurar el router Linksys RV200 como un servidor VPN de acceso remoto.

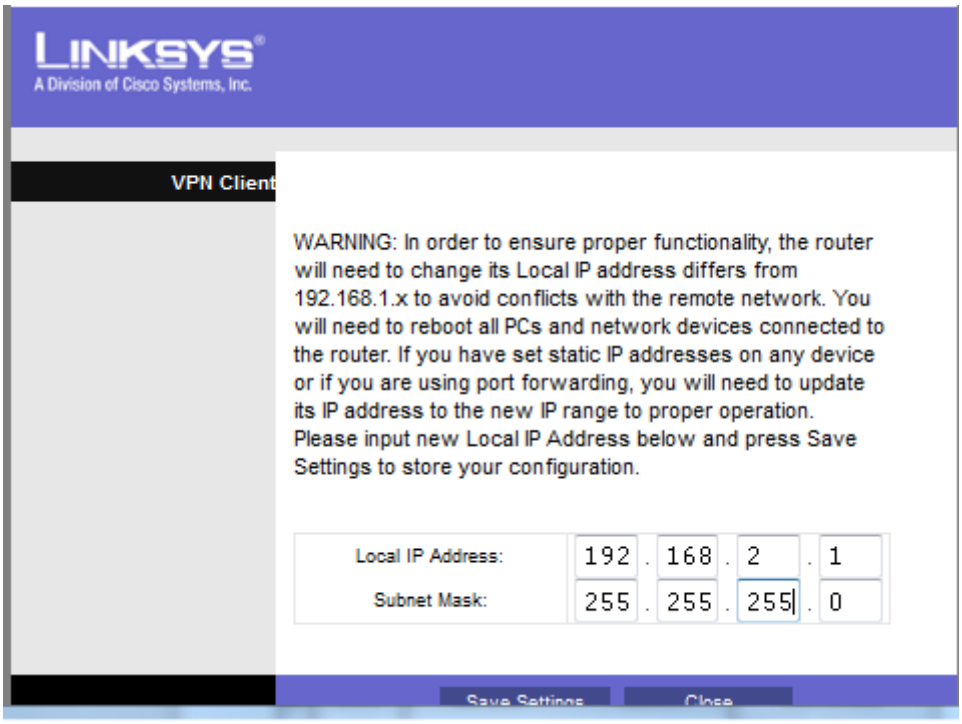
Utiliza el simulador

http://ui.linksys.com/files/WRV200/1.0.29/SetupDHCP.htm

En primer lugar crearemos el usuario niko con la contraseña inves:



Ahora configuramos la dirección IP del cliente y pulsamos sobre settings:

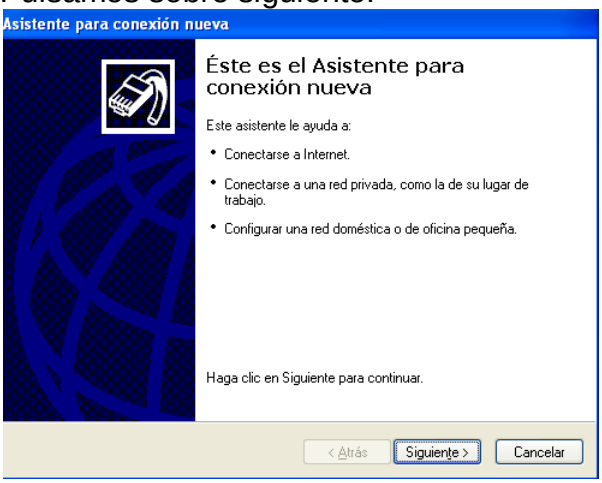


c) Configura tu cliente VPN en Windows.

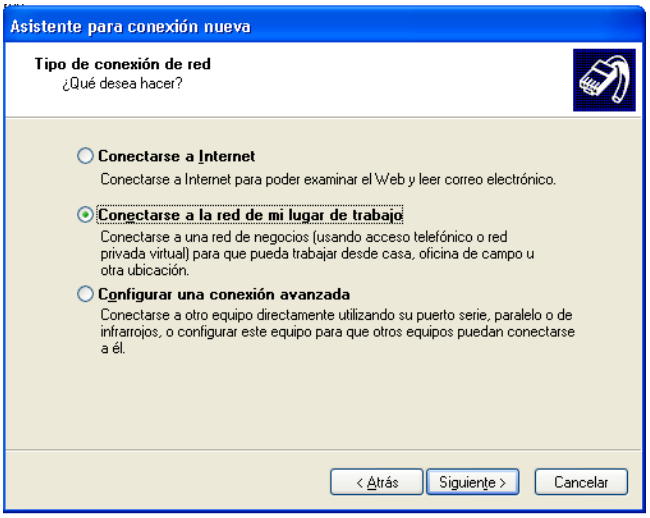
EN WINDOWS XP:

En primer lugar nos dirigimos a conexiones de red; una vez allí pulsamos sobre la opción nueva conexión de red:

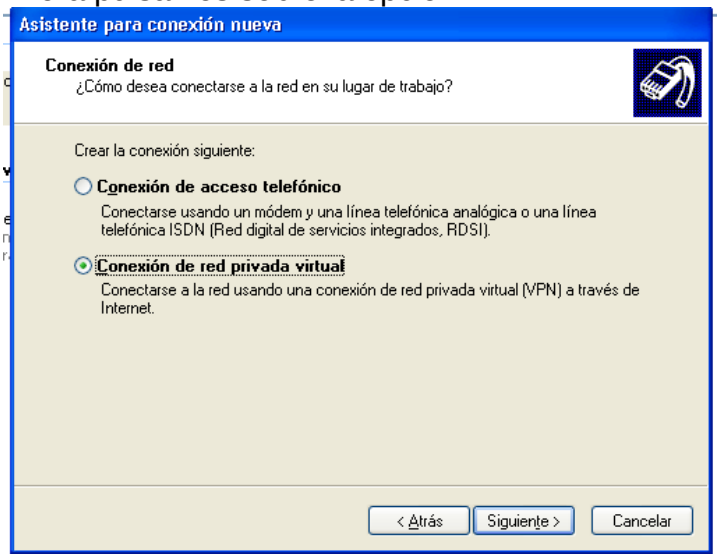
Pulsamos sobre siguiente:



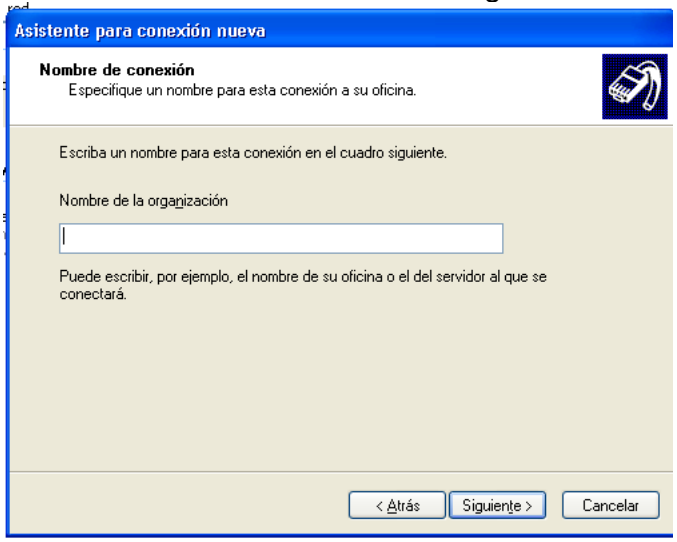
Ahora pulsamos la opción conectarse a la red de mi lugar de trabajo:



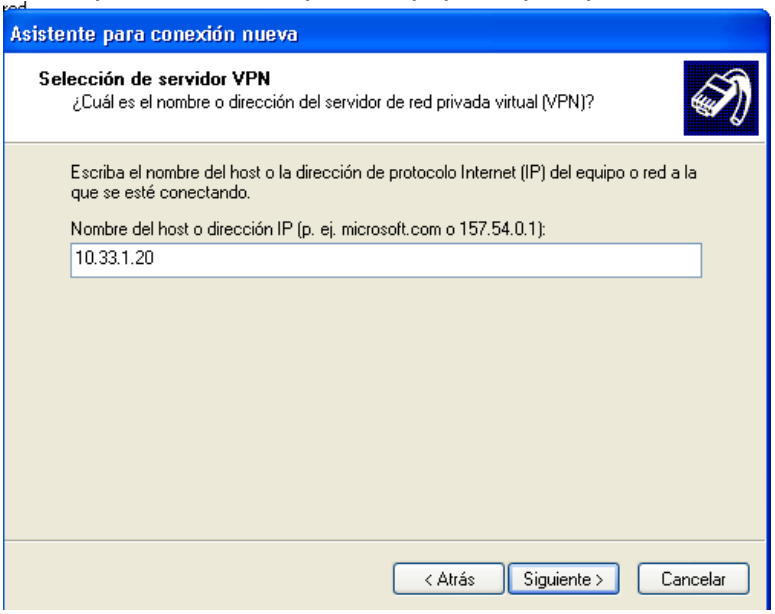
Ahora pulsamos sobre la opción VPN:



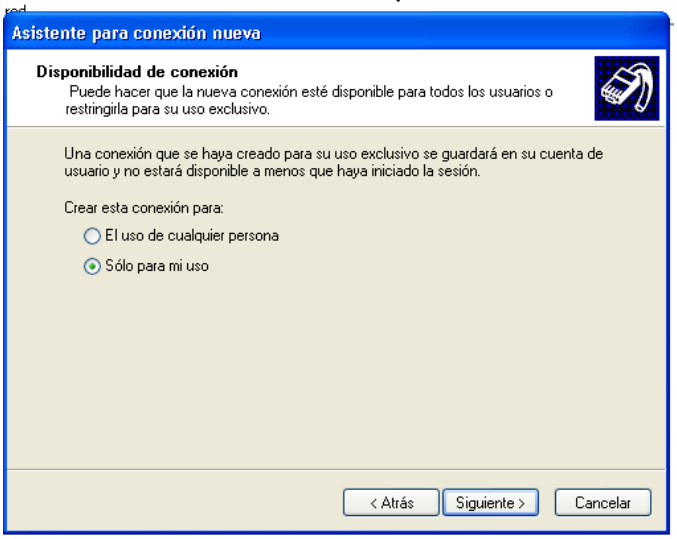
Ahora le damos un nombre a la organización:



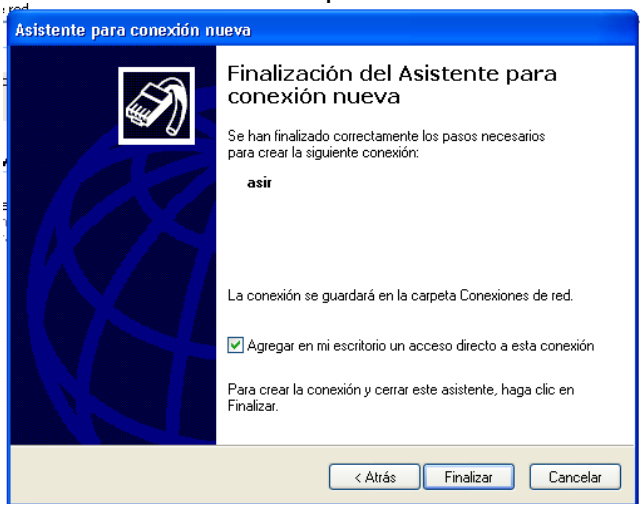
Ahora pondremos la ip del equipoal que queremos conectarnos:



Ahora seleccionaremos la opción crear esta conexión solo para este usuario:

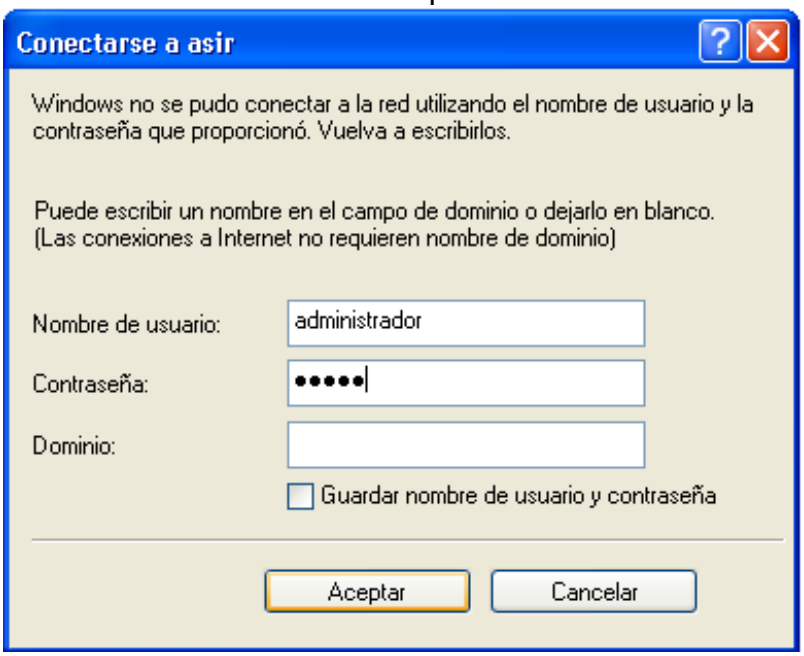


Ahora finalizaremos el proceso:

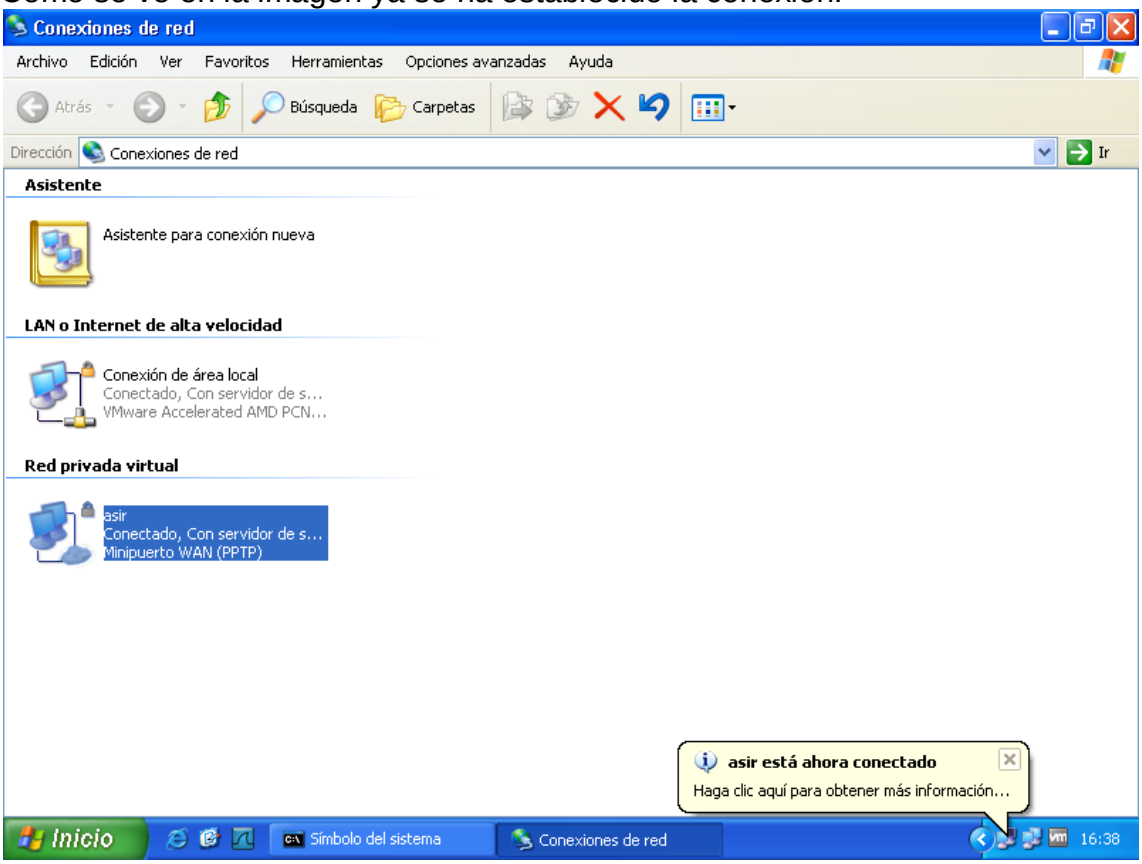


Ahora pondremos el nombre de usuario y contraseña:

Ahora deberemos de volver a poner la contraseña:



Como se ve en la imagen ya se ha establecido la conexión:

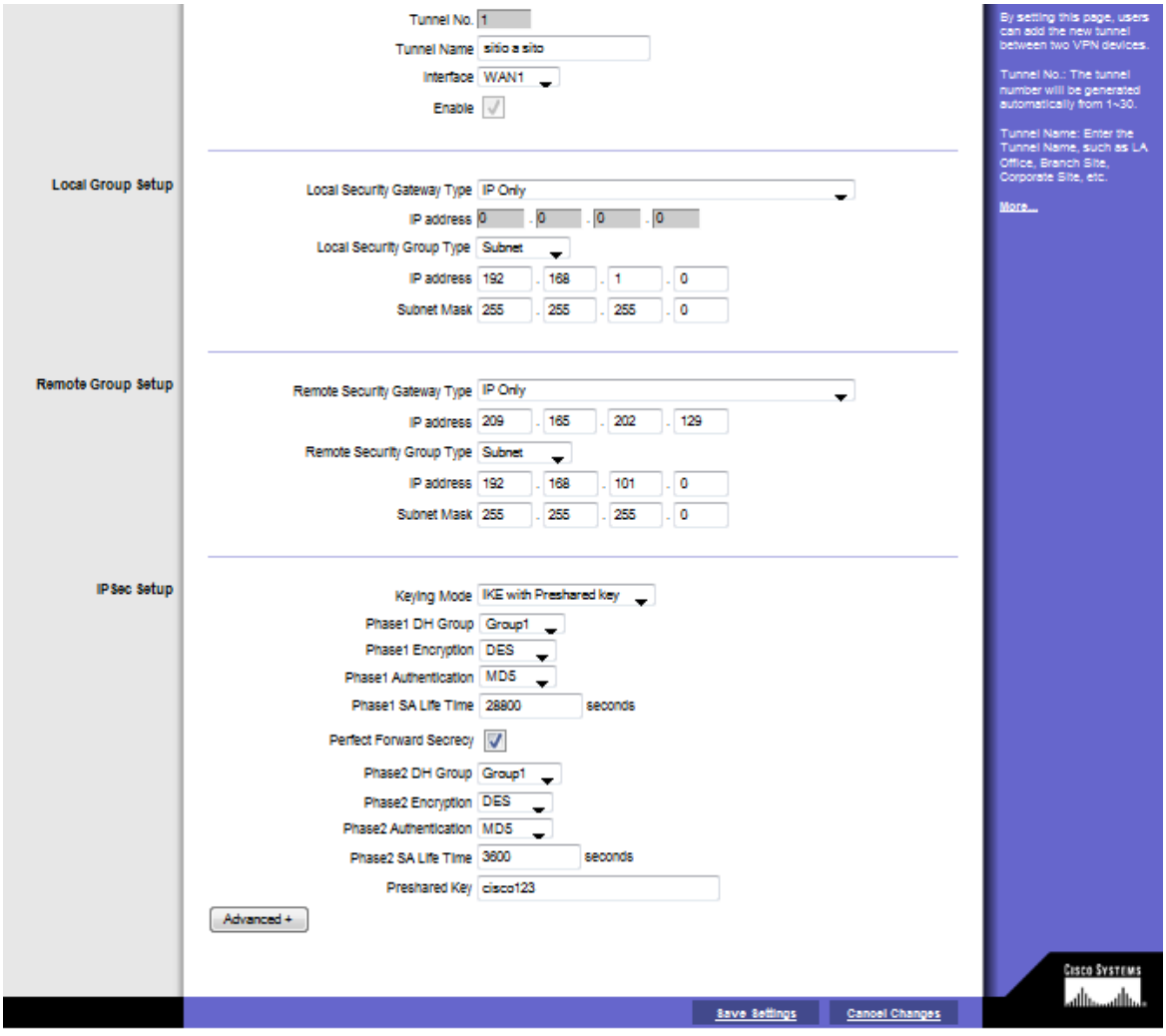


REDES PRIVADAS VIRTUALES

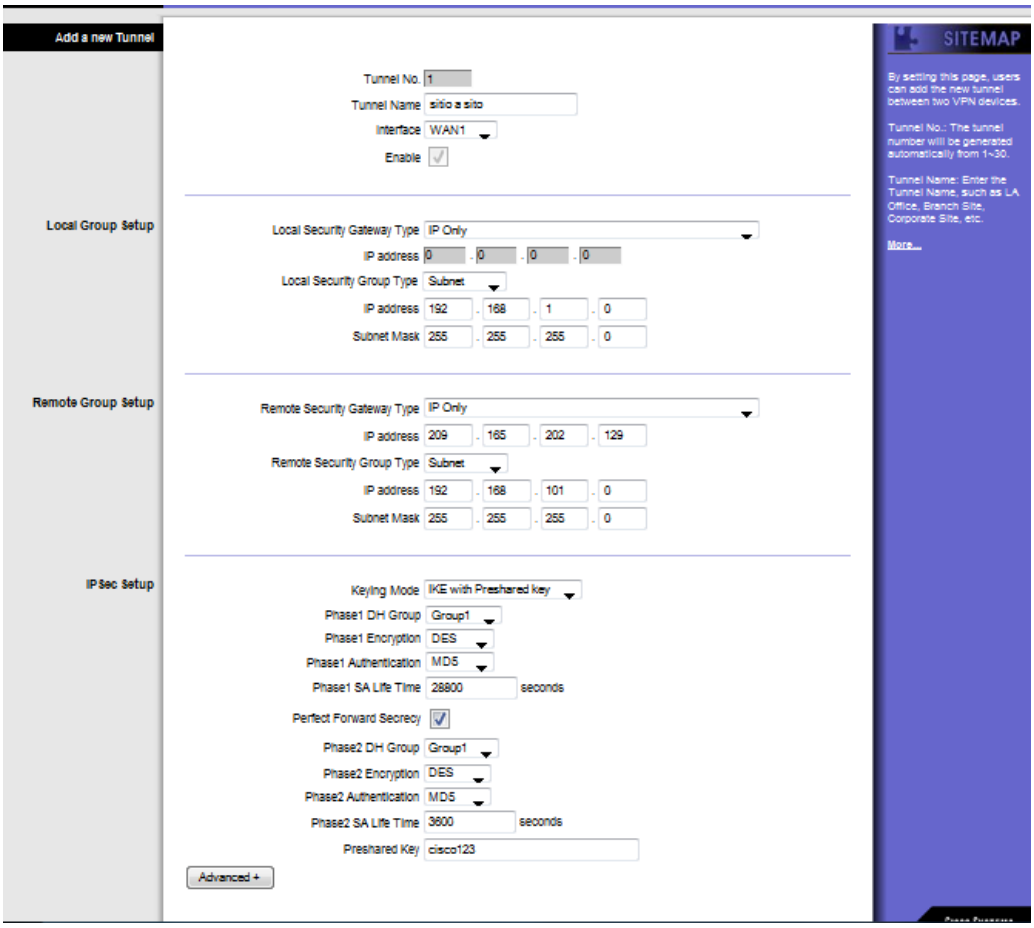
6. VPN sitio a sitio

b) En cada sitio existe un router Linksys RV042.
Configurar cada sitio - **router Linksys RV042** utilizando el simulador
http://ui.linksys.com/files/RV042/1.2.3/home.htm

CONFIGURACIÓN ROUTER **Central:**



CONFIGURACIÓN ROUTER **SUCURSAL**



TECNICAS DE CIFRADO: COMUNICACIONES SEGURAS

7. SSH

a) Instalación del servidor SSH en GNU/Linux

En primer lugar deberemos de introducir el comando apt-get install openssh-server:

```
niko@ubuntu1:~$ sudo apt-get install openssh-server
sudo: unable to resolve host ubuntu1
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```

Una vez instalado el openssh-server los clientes ssh podrán acceder a nuestro equipo con cualquier usuario dado de alta en el equipo que actua como servidor ssh.

b) Conexión al servidor SSH mediante cliente GNU/Linux y cliente Windows.

EN LINUX

Para realizar una conexión deberemos de introducir en el terminal ssh niko@10.33.1.5 y posteriormente introducir la contraseña del usuario niko como aparece en la imagen:

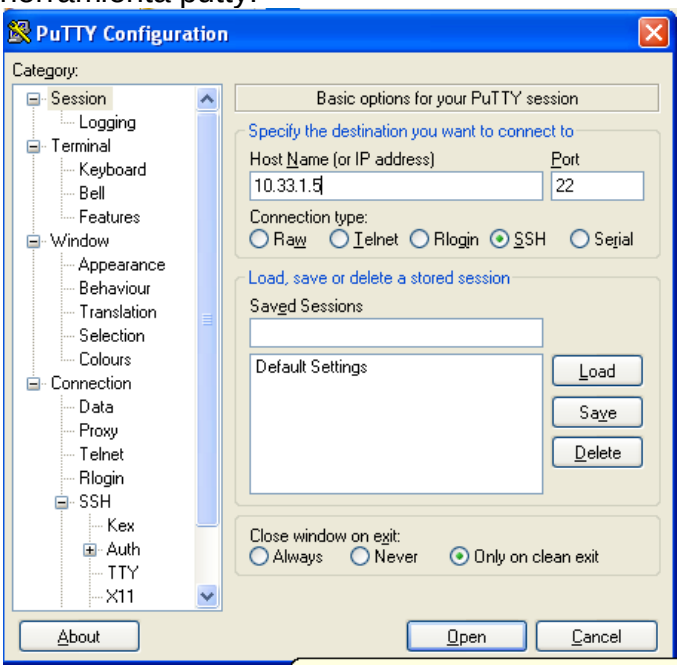
```
root@molinux1:/home/niko# ssh niko@10.33.1.5
niko@10.33.1.5's password:
Welcome to Ubuntu 11.04 (GNU/Linux 2.6.38-8-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release 'oneiric' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Jan 11 19:10:44 2012 from ubuntu1-20.local
niko@ubuntu1:~$
```

Ahora podemos hacer labores administrativas de forma remota:

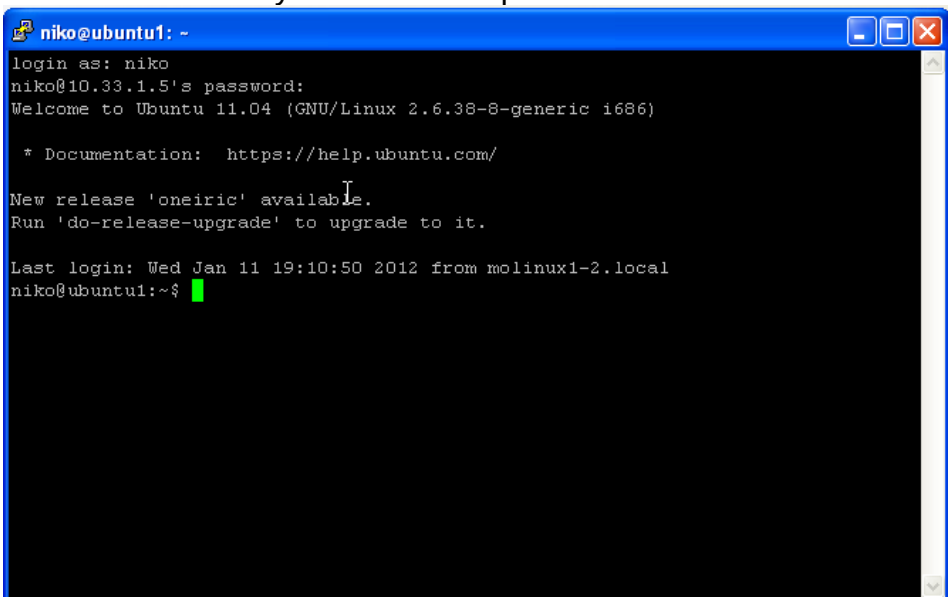
```
niko@ubuntu1:~$ ls
Descargas   Escritorio        Imágenes  Plantillas  Vídeos
Documentos  examples.desktop  Música    Público
niko@ubuntu1:~$
```

EN WINDOWS

Para poder realizar una conexión en Windows deberemos de instalar la herramienta putty:



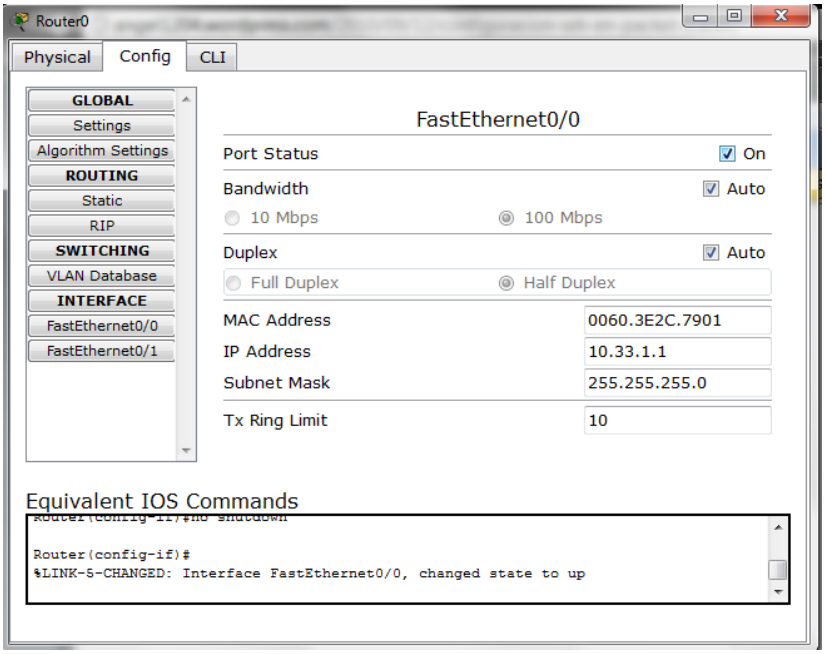
Ahora nos aparecerá una ventana en la que deberemos de proceder a poner el nombre de usuario y la contraseña para establecer la conexión ssh:



Ahora podemos realizar tareas administrativas en nuestros equipos.

c) Escenario CISCO: Conexión segura a la administración de un router.

En primer lugar configuraremos la interfaz f0/0 del router:



Ahora deberemos de configurar un nombre en el router:

```
Router(config)#hostname niko
```

Ahora deberemos de **Configurar dominio y generar llaves rsa mediante los siguientes comandos:**

(config)# ip domain-name asir01.
(config)# crypto key generate rsa
How many bits in the modulus [512]: 1024

Aqui podemos apreciar su aplicacion:

```
Router(config)#ip domain-name asir01.
```

```
niko(config)#crypto key generate rsa
The name for the keys will be: niko.asir01.
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:   How many bits in the modulus [512]: 1024
% A decimal number between 360 and 2048
How many bits in the modulus [512]: % A decimal number between 360 and 2048
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

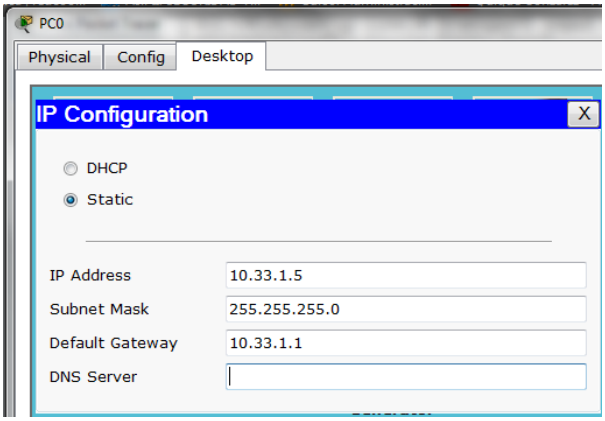
Ahora deberemos de **Especificar que protocolos se dejan pasar por la línea VTY:**

```
niko(config)#line vty 0 4
*mar 1 0:5:53.937:  %SSH-5-ENABLED: SSH 1.99 has been enabled
niko(config-line)#transport input ssh
```

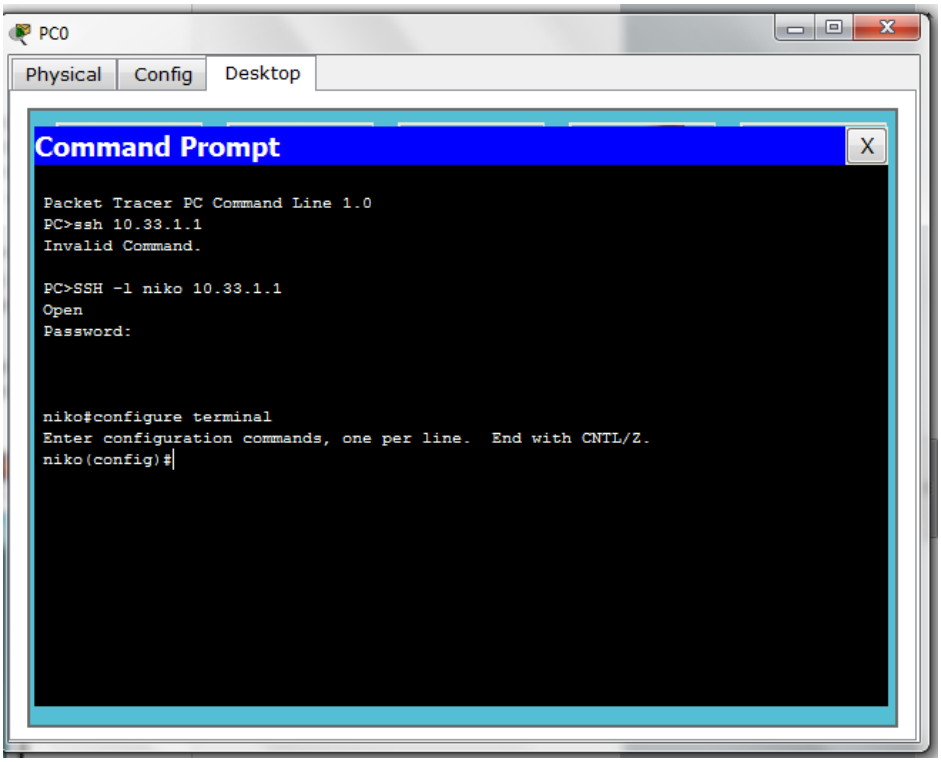
Ahora deberemos de dar de dar de alta a un usuario con su contraseña:

```
niko(config-line)#login local
niko(config-line)#username niko privilege 15 password inves
niko(config)#
```

Configuración del equipo cliente:
En primer lugar configuraremos la tarjeta de red del equipo:



Ahora nos dirigimos a la consola de comandos y ejecutamos el comando SSH –l niko 10.33.1.1. Posteriormente introducimos la contraseña y ya habremos accedido de forma remota al router de forma segura:

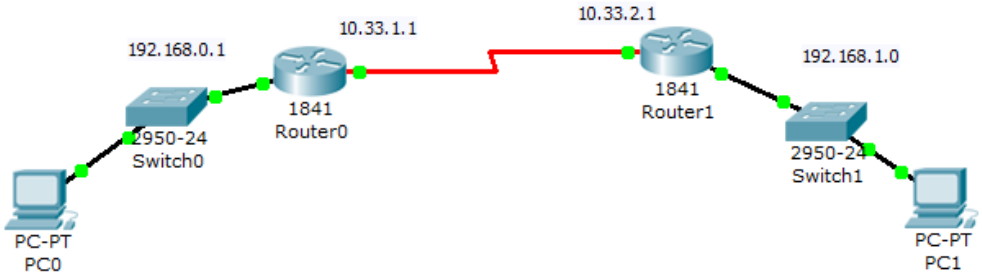


SERVIDORES DE ACCESO REMOTO

8. Protocolos de autenticación:

a) Escenarios CISCO: Interconexión de redes mediante protocolos PPP,PAP,CHAP.

Configuración de PPP:



En primer lugar configuraremos las direcciones de red de los enlaces seriales:

Ahora estableceremos la encapsulación ppp:

```
Router(config-if)#interface Serial0/0/0
Router(config-if)#ip address 10.33.2.1 255.0.0.0
Router(config-if)#encapsulation ppp
```

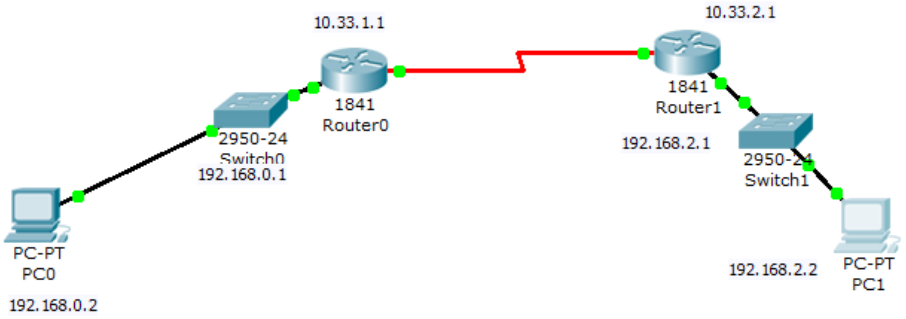
Ahora estableceremos la encapsulación ppp en el router inverso:

```
Router(config)#interface Serial0/1/0
Router(config-if)#ip address 10.33.1.1 255.0.0.0
Router(config-if)#encapsulation ppp
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
```

Ahora comprobaremos su funcionamiento con un ping:

```
Router#ping 10.33.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.33.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/38/40 ms
```

Autenticación con PAP



Como utilizaremos el escenario base anterior no realizare configuración de ips. Ahora realizaremos la configuración de la autenticación PAP:

```
Router(config)#username niko password inves
Router(config)#interface Serial0/1/0
Router(config-if)#encapsulation ppp
Router(config-if)#ppp authentication pap
Router(config-if)#ppp pap sent-username niko1 password inves
Router(config-if)#
```

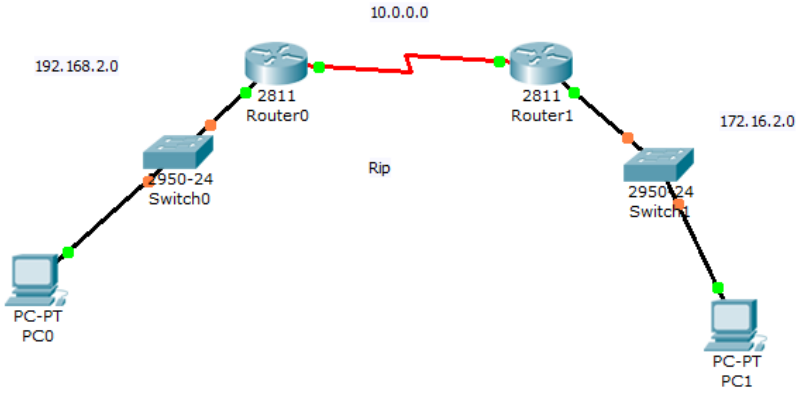
Ahora realizamos lo mismo en el router contrario:

```
Router(config)#username niko1 password inves
Router(config)#interface Serial0/0/0
Router(config-if)#encapsulation ppp
Router(config-if)#ppp authentication pap
Router(config-if)#ppp pap sent-username niko password inves
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
```

Ahora probaremos el funcionamiento de la autenticación con un ping:

```
Router#ping 10.33.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.33.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/6 ms
```

PPP con autenticación CHAP



Como utilizaremos el escenario base anterior no realizare configuración de ips. Ahora realizaremos la configuración de la autenticación chap:

```
R1(config)#username R2 password inves
R1(config)#int s0/1/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication CHAP
```

Ahora realizamos lo mismo en el router contrario:

```
Router(config)#hostname R2
R2(config)#username R1 password inves
R2(config)#int s0/1/0
R2(config-if)#encapsulation ppp
R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up


R2(config-if)#ppp authentication CHAP
```

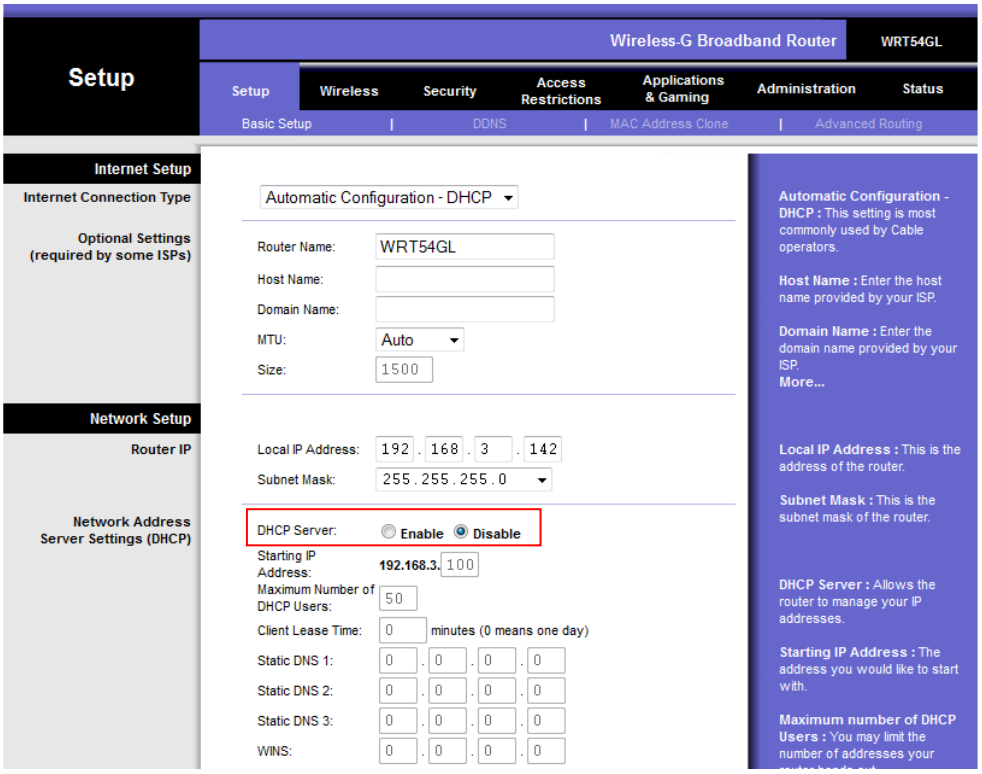
SERVIDORES DE ACCESO REMOTO

9. Servidores de autenticación

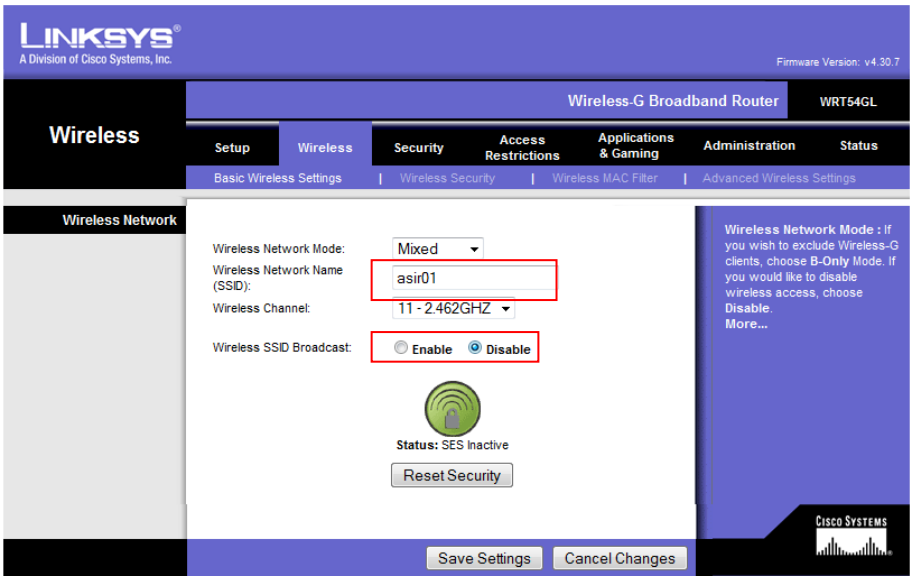
a) REDES INALÁMBRICAS: WPA Personal

- Configurar router inalámbrico Linksys WRT54GL en modo seguro: *(Cambia el SSID por defecto y desactivar el broadcasting SSID, deshabilitar DHCP, cambiar nombre de usuario y contraseña, activar el filtrado de MAC, WPA2, cifrado TKIP+AES).*
- Configurar la tarjeta de red de un cliente inalámbrico con dichas medidas de seguridad y comprobar la autenticación a dicho router inalámbrico.

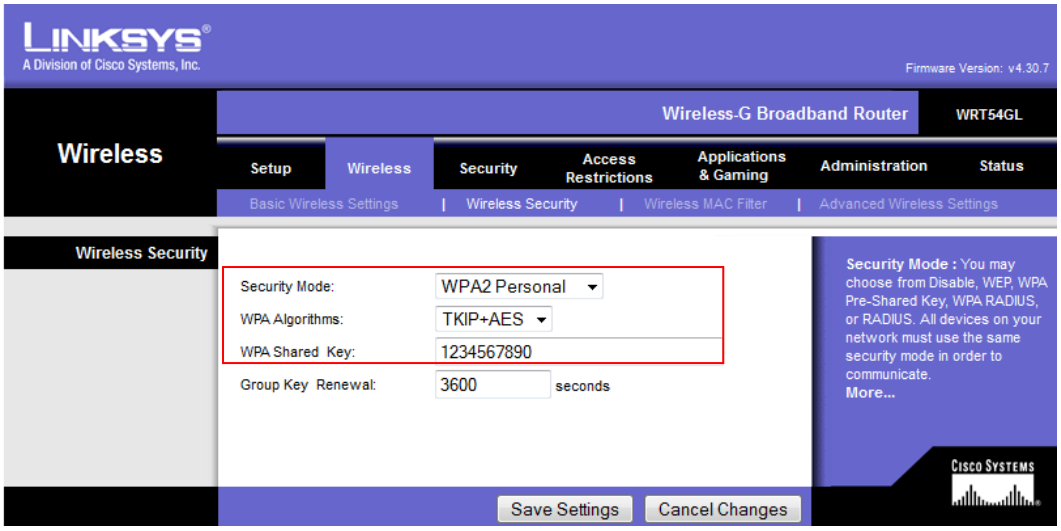
Una vez accedido al menú de administración de nuestro router inalámbrico procede a deshabilitar el dhcp, para ello en la pestaña setup/basic setup seleccionamos el botón radio disable en la sección dhcp server:



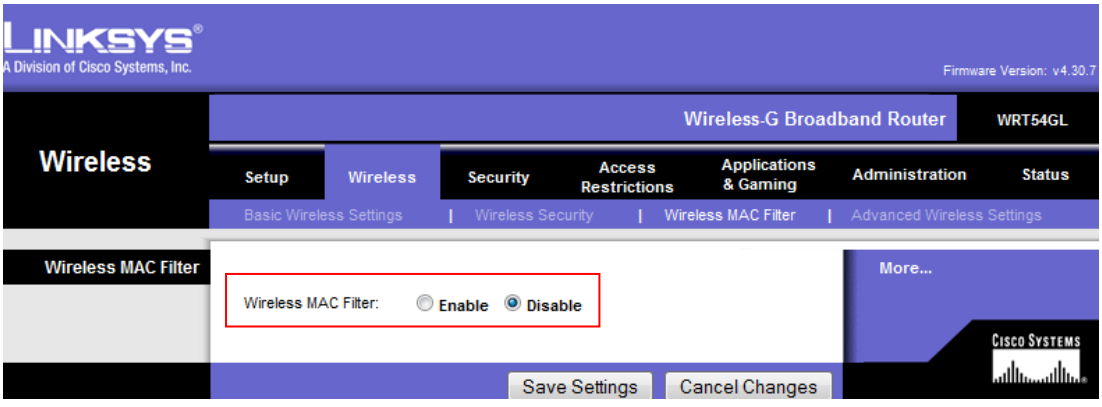
Ahora nos dirigiremos a la pestaña wireless /basic wireless Settings y allí elegimos el nombre deseado de SSID, asu vez desactivamos la difusión del SSID:



Ahora en la pestaña wirelss security el modo de seguridad y la contraseña de acceso:



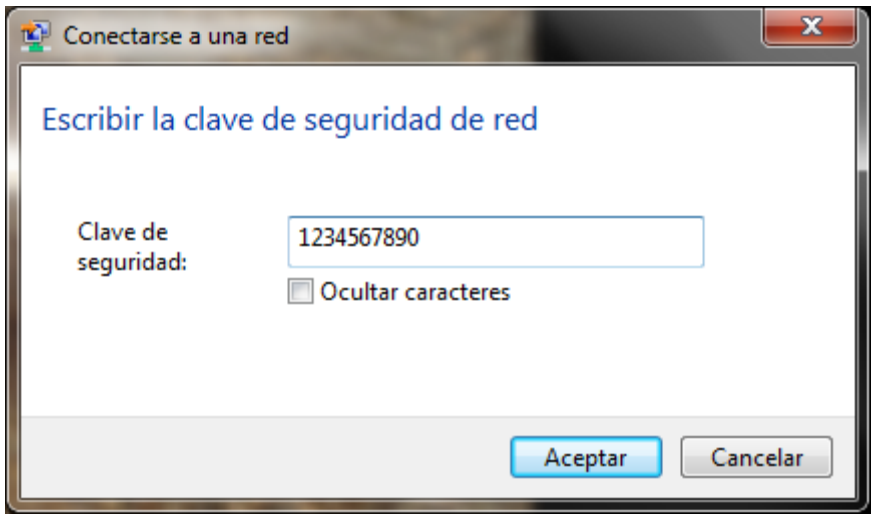
Ahora activamos el filtrado de mac:



Acceso con un cliente w7:

En primer lugar elegimos la red a la que nos queremos conectar:

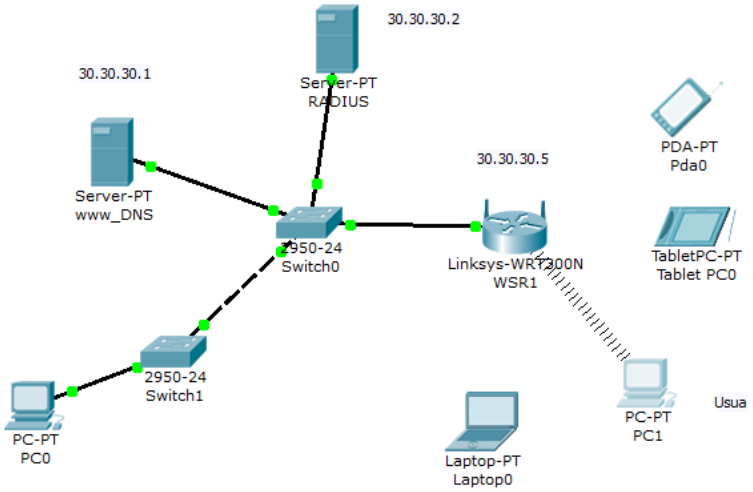
Ahora introducimos la contraseña :



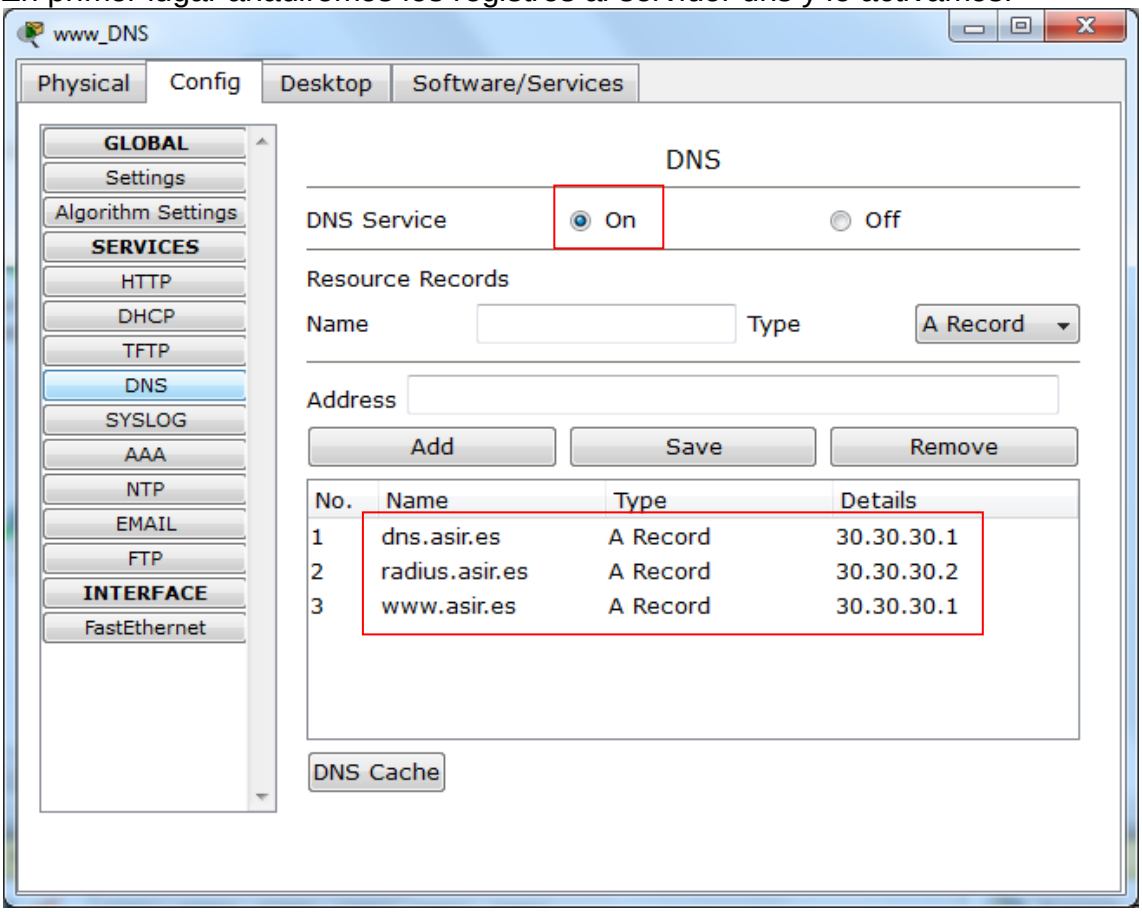
b) SERVIDOR RADIUS:

1.- Simulación de un entorno de red con servidor RADIUS CISCO en el Packet Tracert Router.

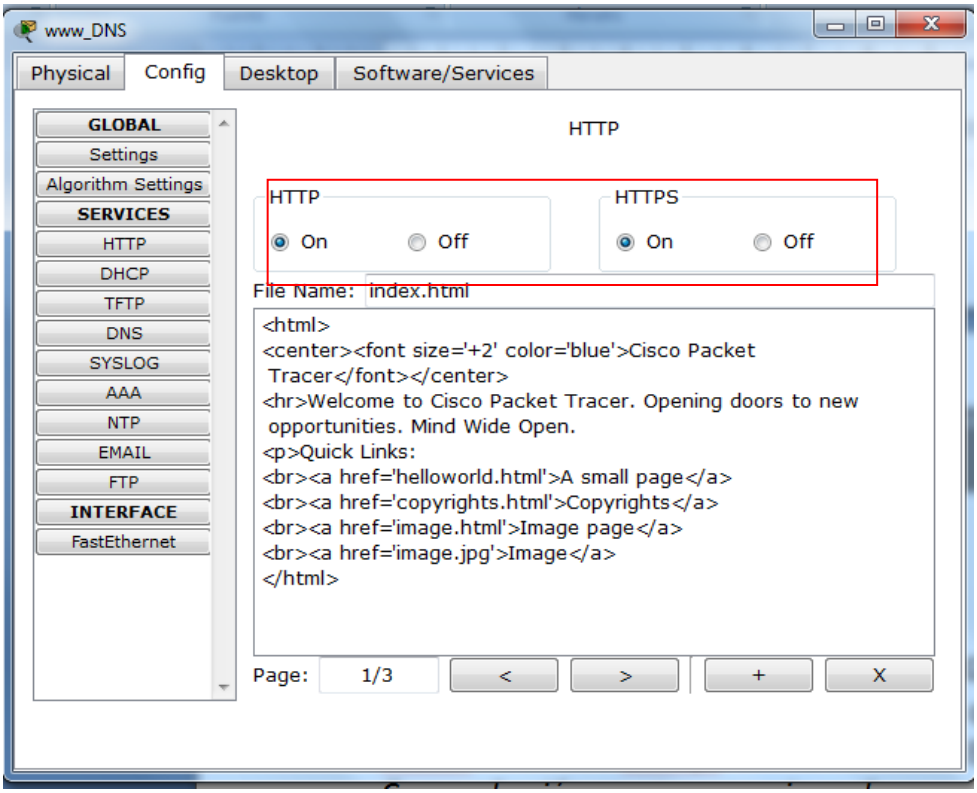
En primer lugar presentaremos el escenario:



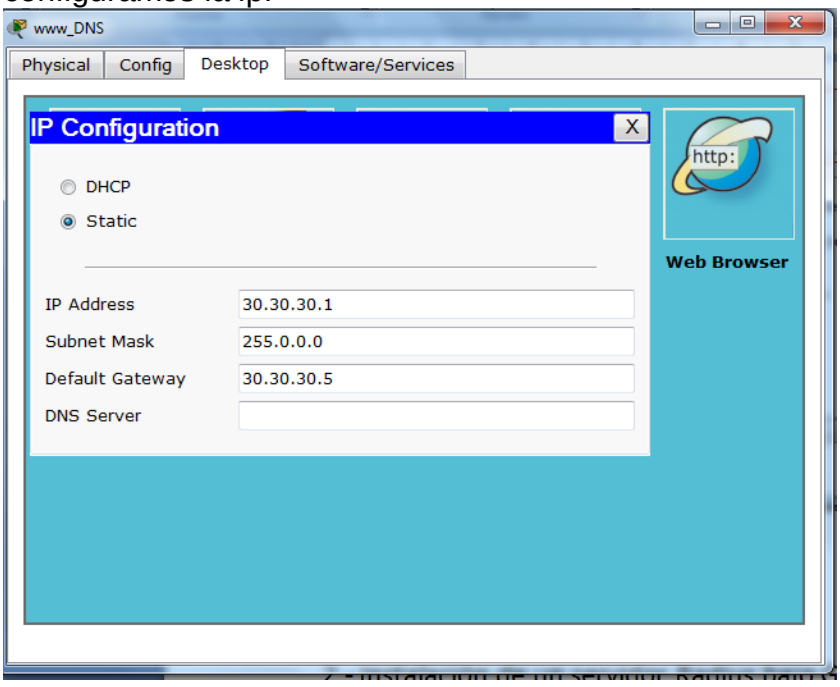
Ahora realizaremos la configuración del servidor DNS y http:
En primer lugar añadiremos los registros al servidor dns y lo activamos:



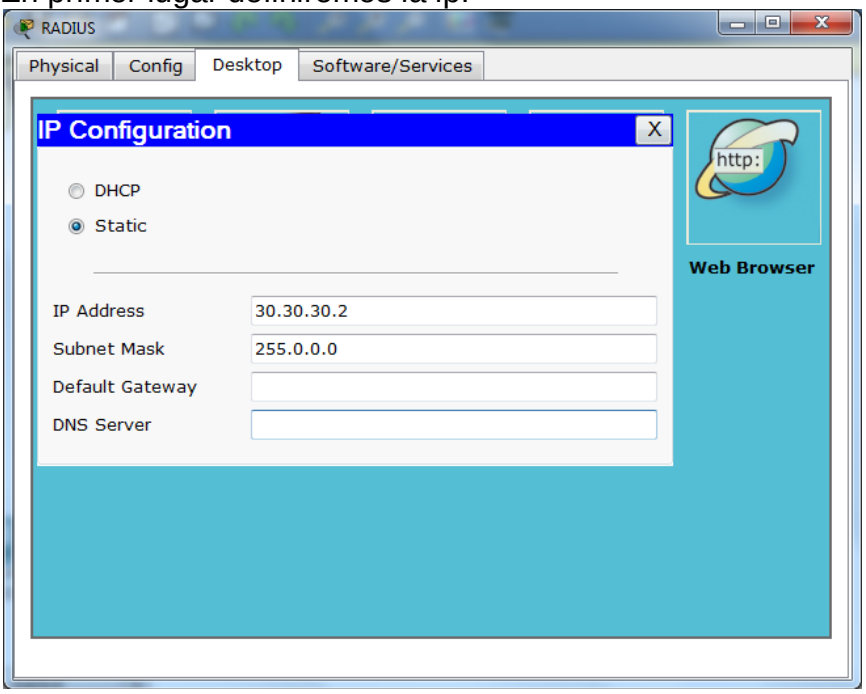
Ahora configuramos el servidor web:



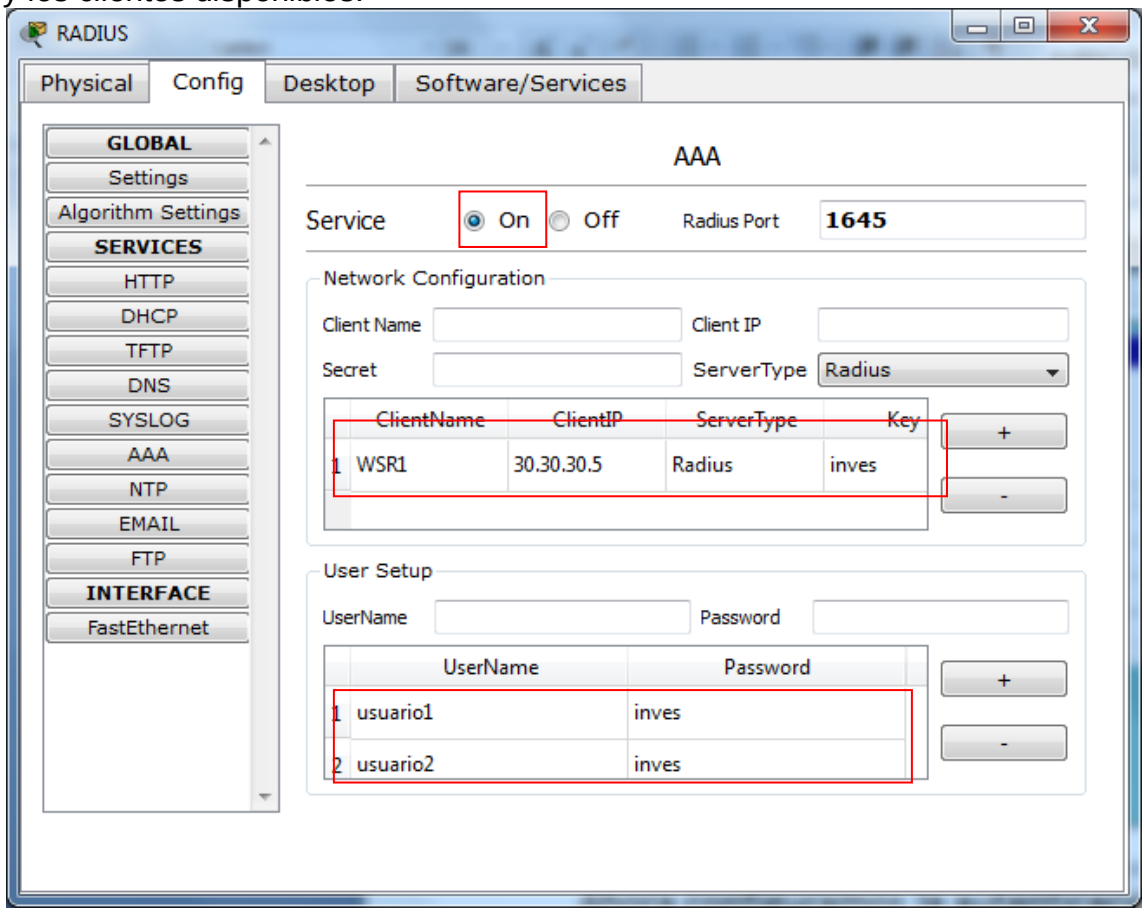
Por último configuramos la ip:



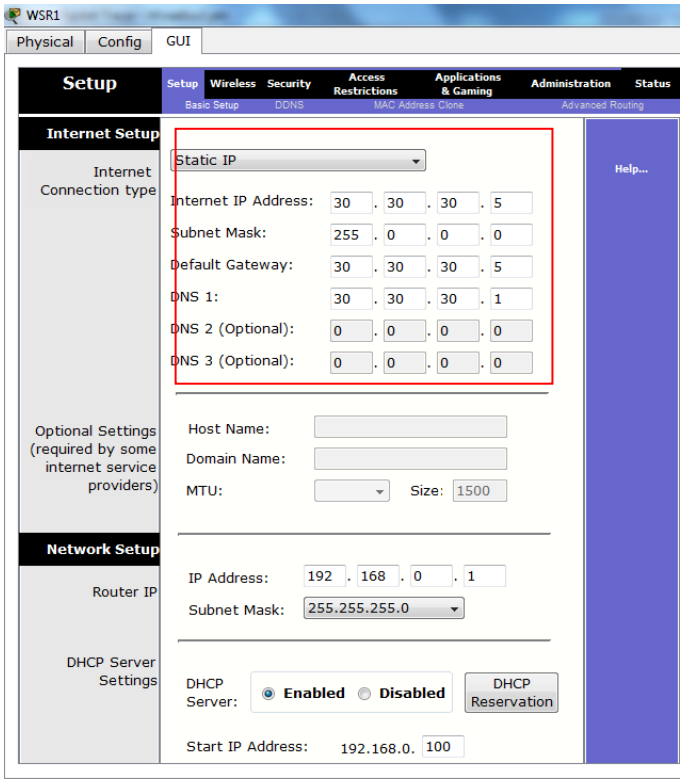
Ahora configuramos el servidor radius:
En primer lugar definiremos la ip:



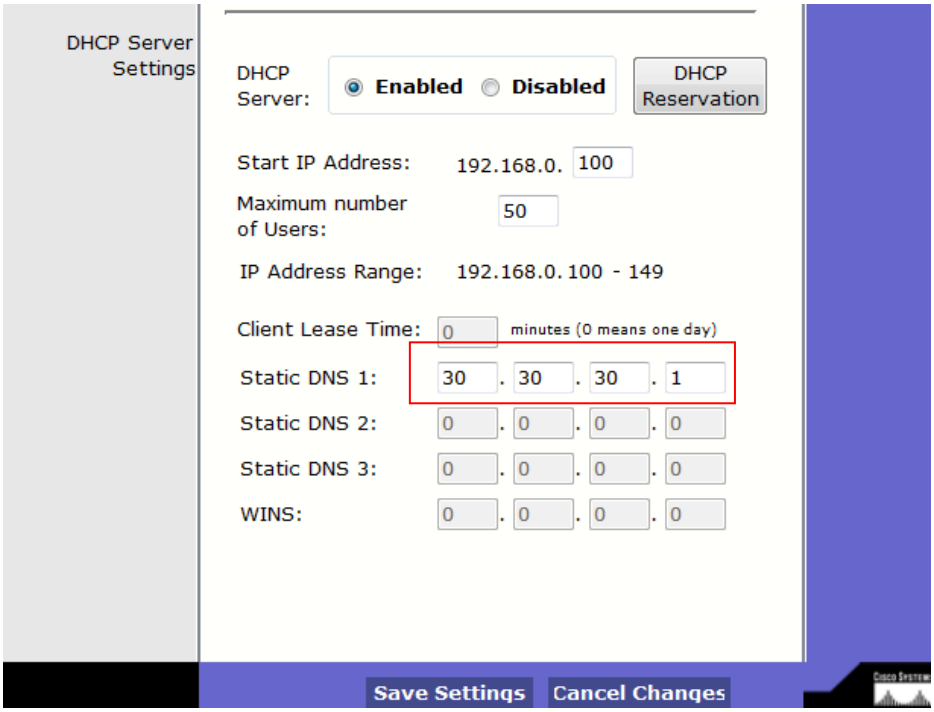
Ahora configuramos la autenticación radius añadiendo los usuarios autorizados y los clientes disponibles:



Una vez realizados los pasos anteriores configuramos el router:
En primer lugar configuramos la ip estatica, en las que a su vez indicaremos la dirección del servidor DNS:

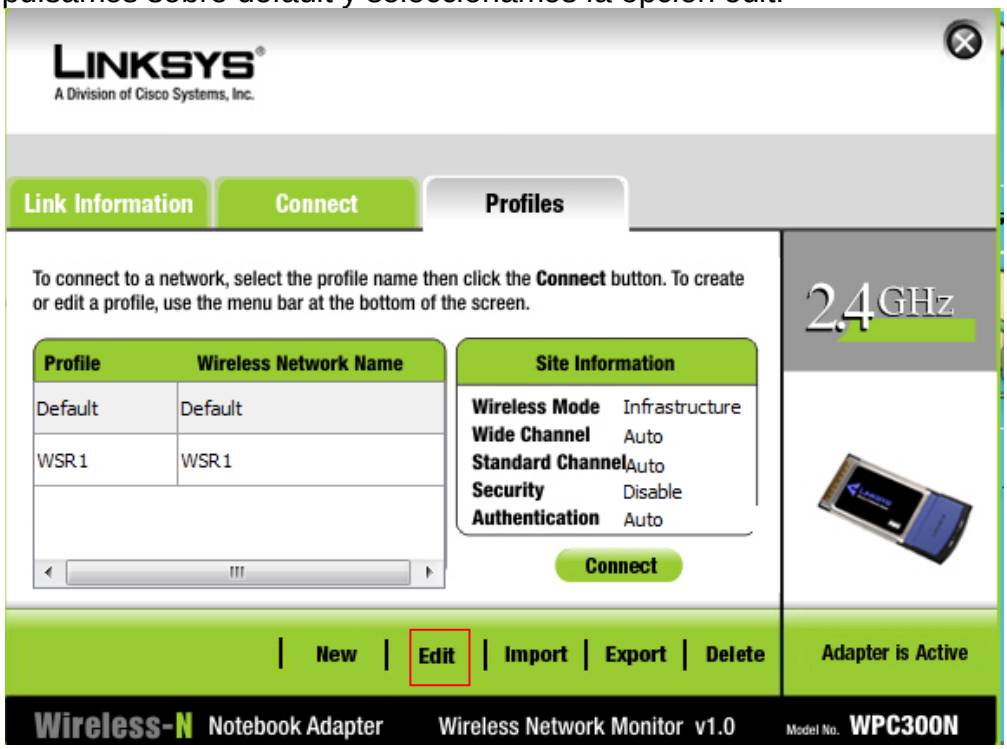


En la configuración del dhcp configuramos los rangos de ips y la dirección del dns:

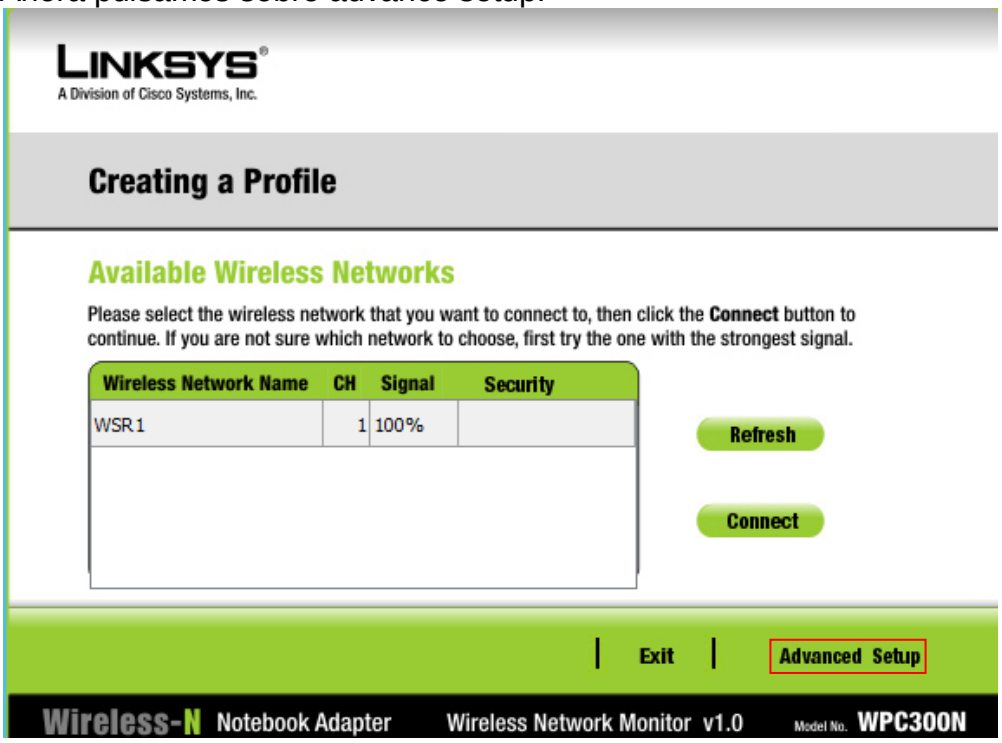


Ahora configuraremos el router como cliente radius:

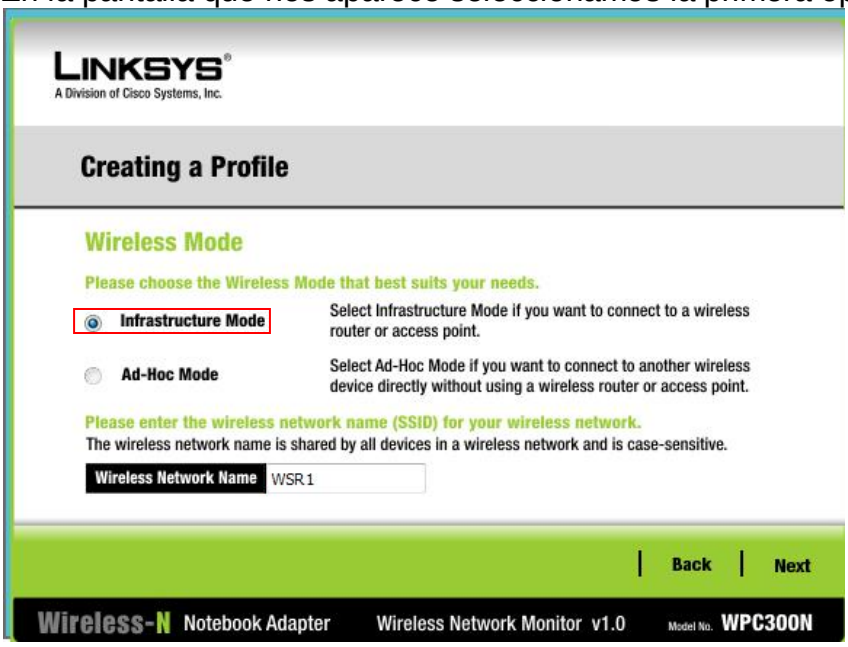
Ahora configuraremos los clientes:
En primer lugar nos dirigimos a los perfiles de la tarjeta wifi, una vez allí pulsamos sobre default y seleccionamos la opción edit:



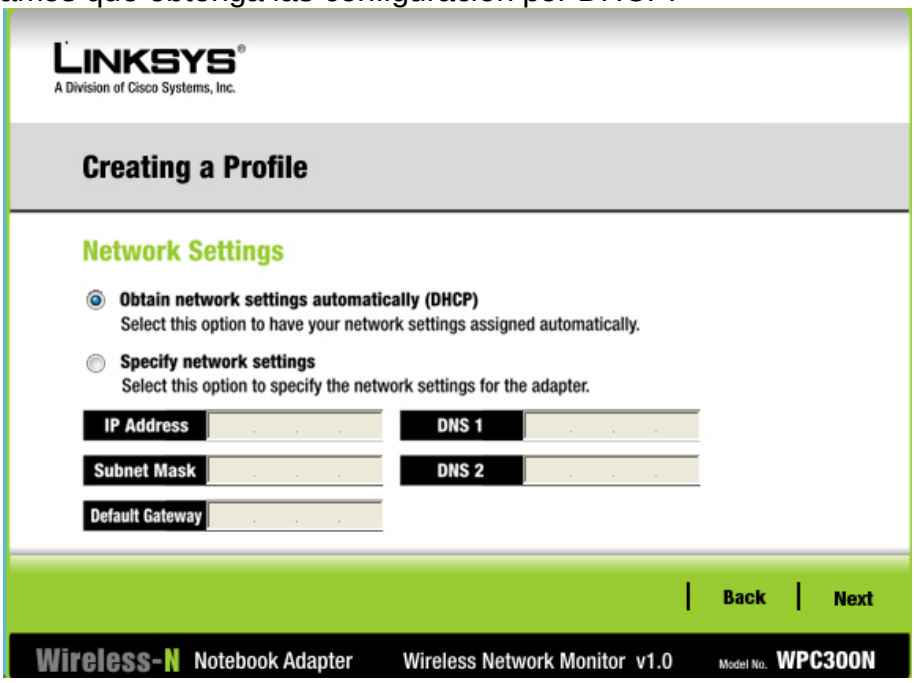
Ahora pulsamos sobre advance setup:



En la pantalla que nos aparece seleccionamos la primera opción:



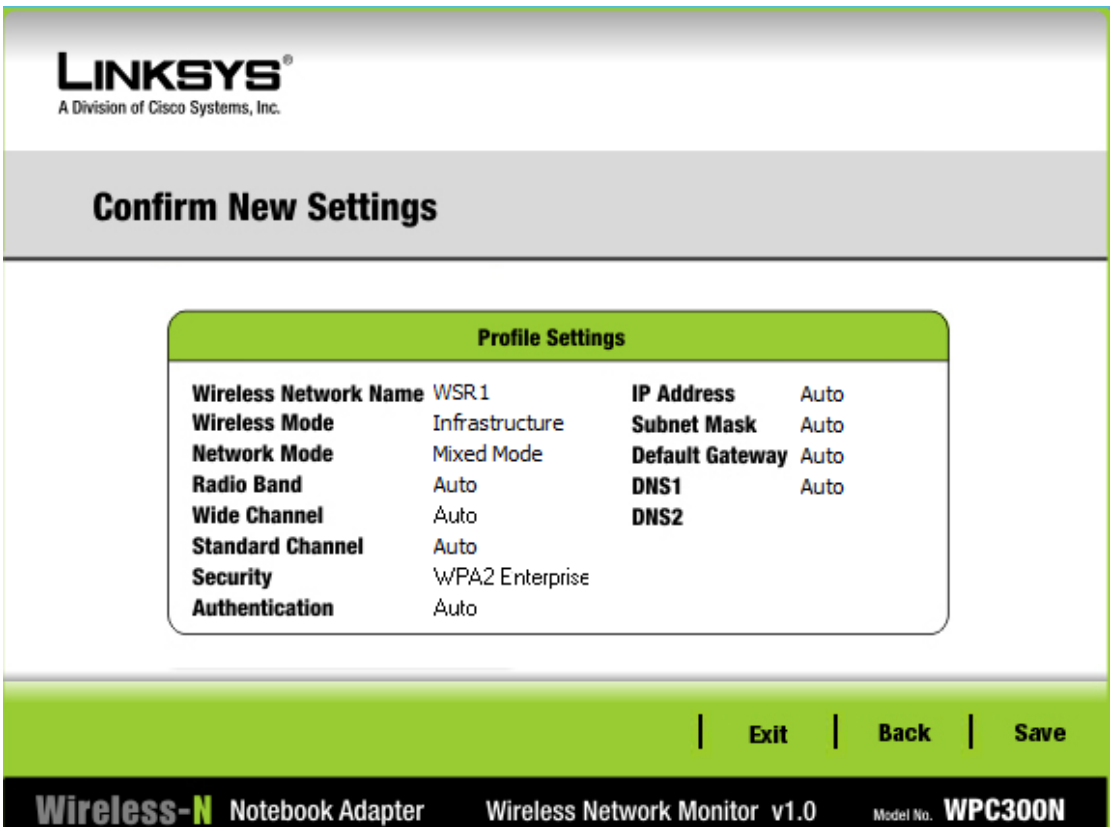
Le indicamos que obtenga las configuración por DHCP:



Configuramos la seguridad WPA2 Enterprise:

Ahora introducimos la cuenta de usuario que esta dada de alta en el sevidor radius:

Una vez realizado estos pasos la configuración del radius abra finalizado.

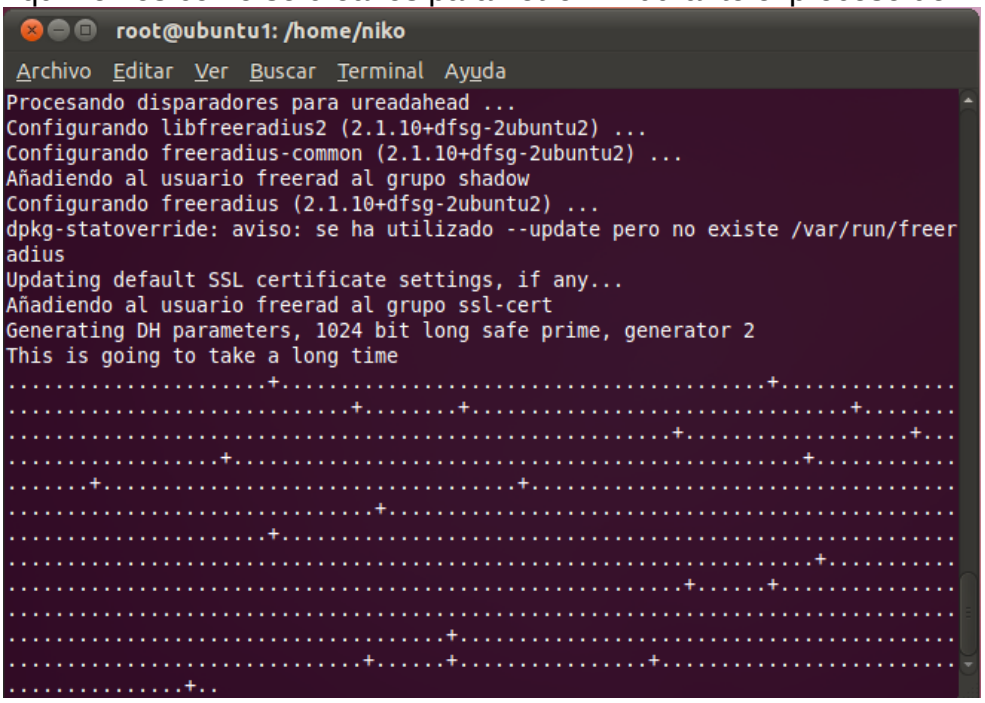


2.- Instalación de un servidor Radius bajo GNU/LINUX (freeradius) , para autenticar conexiones que provienen de un router de acceso Linksys WRT54GL: WPA Empresarial. *Comprobación en un escenario real.*

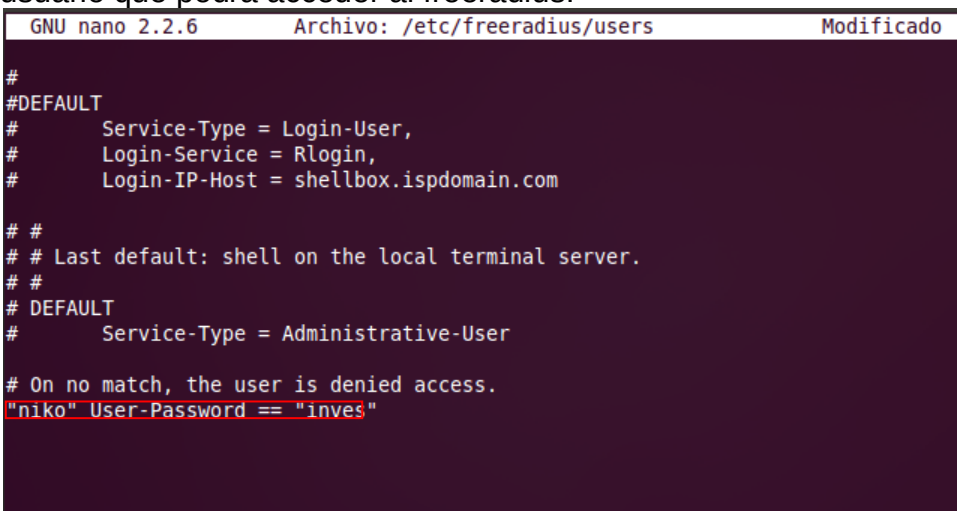
En primer lugar instalaremos el freeradius:

```
root@ubuntu1:/home/niko# apt-get install freeradius
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```

Aquí vemos como se crea los parámetro DH durante el proceso de instalación:



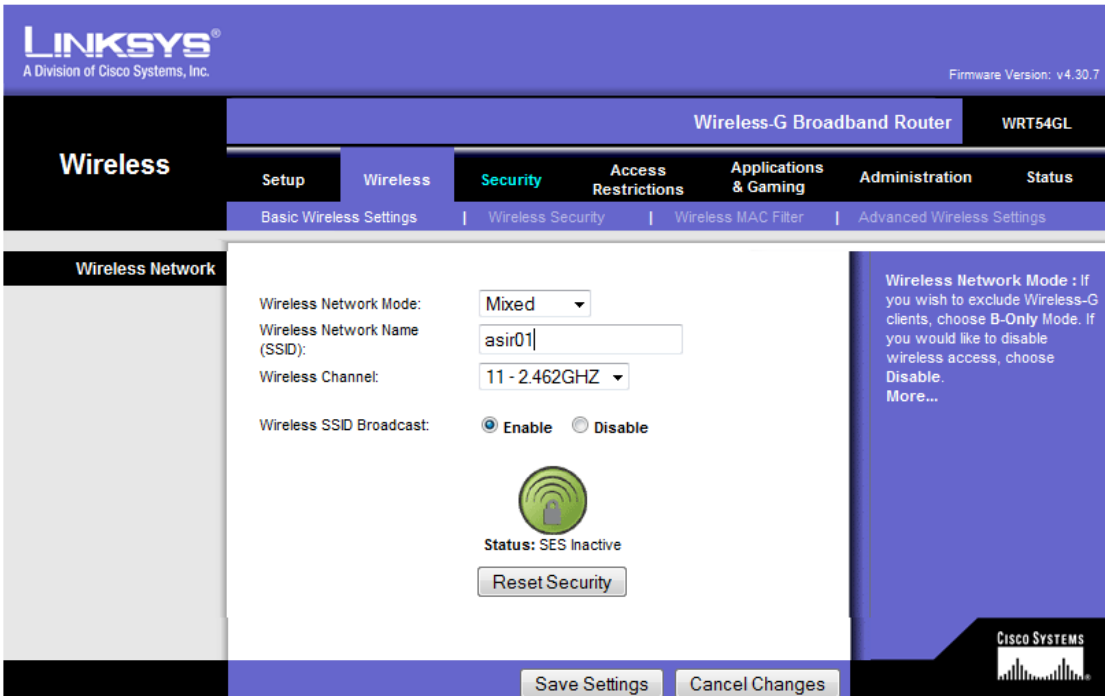
Ahora nos dirogimos al archivo /etc/freeradius/users y añadimos el nombre del usuario que podrá acceder al freeradius:



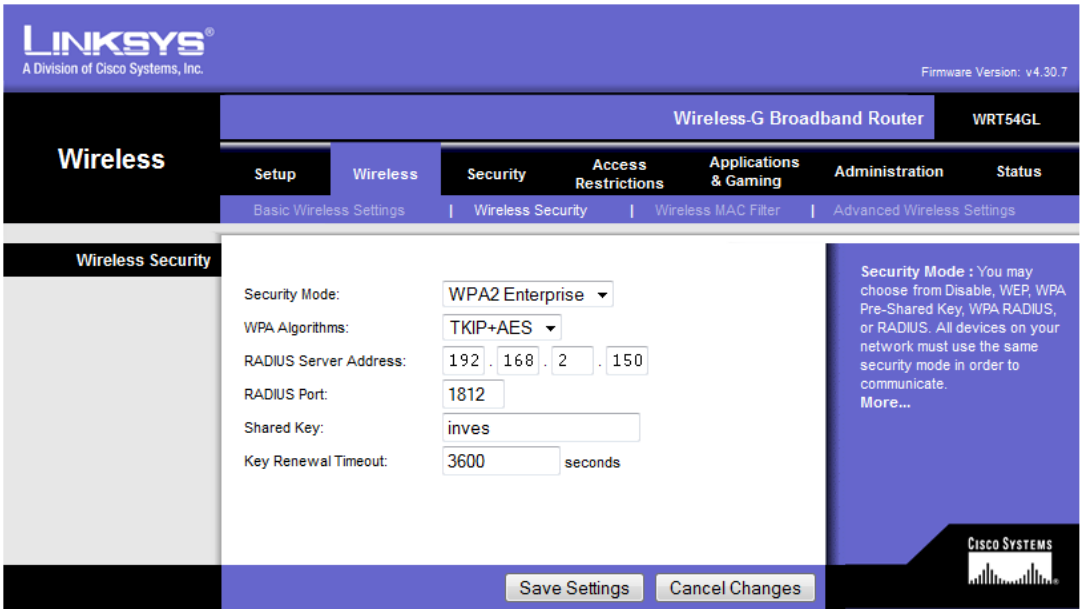
Ahora nos dirigiremos al archivo /etc/freeradius/clients.conf y una vez allí introducimos la dirección del cliente radius y la palabra secreta:

```
  GNU nano 2.2.6      Archivo: /etc/freeradius/clients.conf

#client fe80::/16 {
#       secret          = testing123
#       shortname       = localhost
#}

#client some.host.org {
#       secret          = testing123
#       shortname       = localhost
#}

#
#  You can now specify one secret for a network of clients.
#  When a client request comes in, the BEST match is chosen.
#  i.e. The entry from the smallest possible network.
#
client 192.168.2.100/24 {
        secret          = inves
        shortname       = asir
}
```

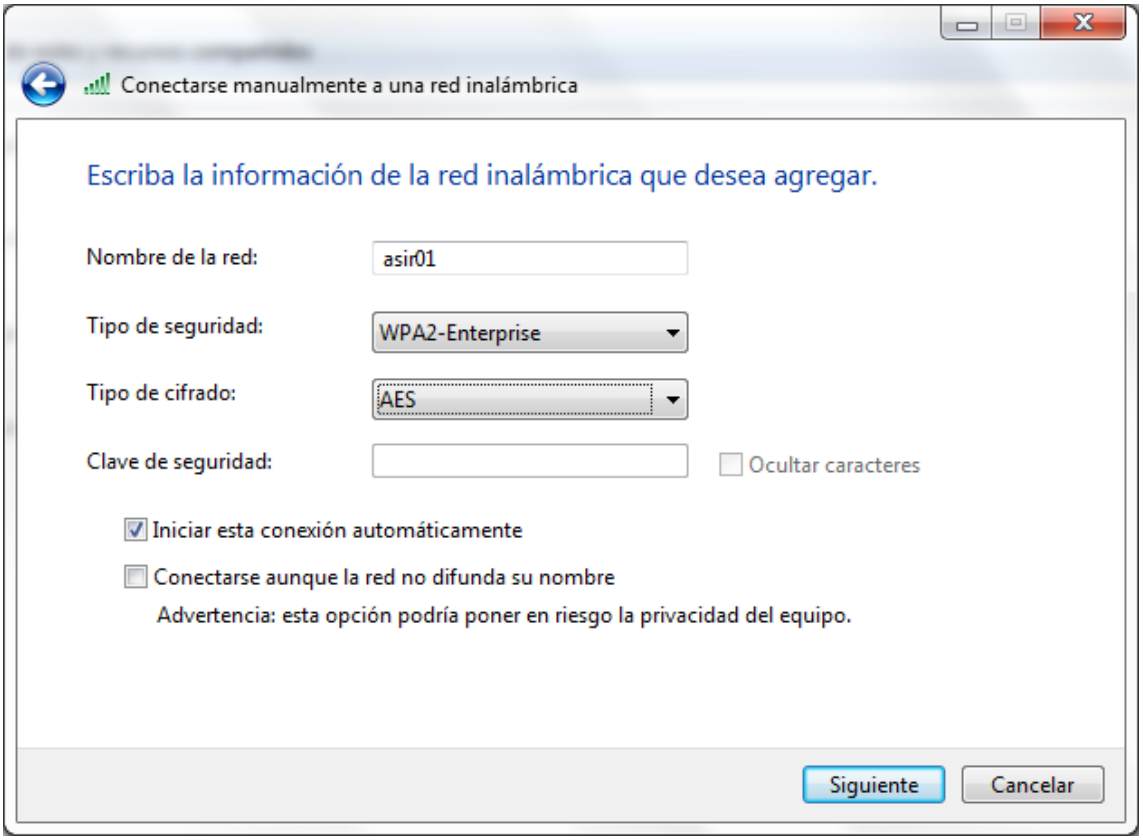
Configuramos la red inalámbrica del Router:



Modo WPA2 Enterprise, indicamos la IP del servidor RADIUS, y la contraseña:



Configuración manual de un cliente w7, para una autenticación RADIUS:



3.- Instalación de un servidor Radius bajo Windows para autenticar conexiones que provienen de un router de acceso Linksys WRT54GL. *Comprobación en un escenario real.*

4.- Busca información sobre EDUROAM y elabora un breve informe sobre dicha infraestructura. http://www.eduroam.es/

¿Qué es eduroam?

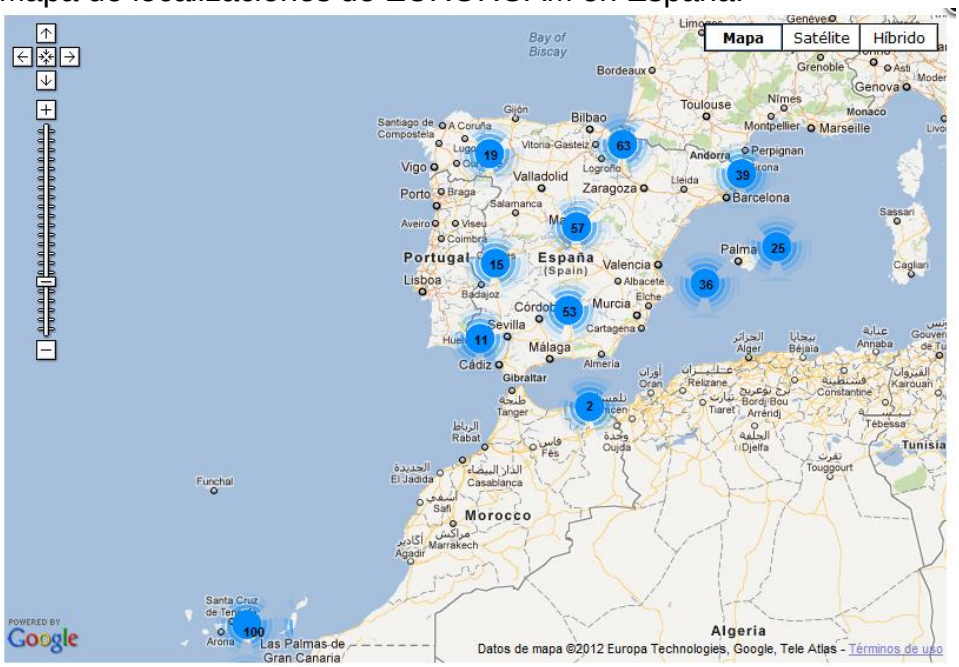
eduroam (contracción de **edu**cation **roam**ing) es el servicio mundial de movilidad segura desarrollado para la comunidad académica y de investigación. eduroam persigue el lema *"abre tu portátil y estás conectado"*.

El servicio permite que estudiantes, investigadores y personal de las intituciones participantes tengan conectividad Internet a través de su propio campus y cuando visitan otras instituciones participantes.

eduroam ES es una iniciativa englobada en el proyecto RedIRISque se encarga de coordinar a nivel nacional los esfuerzos de instituciones académicas con el fin de conseguir un espacio único de movilidad. En este espacio de movilidad participa un amplio grupo deorganizaciones que en base a una política de uso y una serie de requerimientos tecnológicos y funcionales, permiten que sus usuarios puedan desplazarse entre ellas disponiendo en todo momento de conectividad.

Por otro lado, eduroam ES forma parte de la iniciativa eduroam a nivel internacional, financiada a trav&ecute;s de GEANT 3, y operada por varias redes académicas europeas y TERENA. Esta iniciativa amplía el espacio de movilidad al ámbito académico europeo, a través de eduroam Europa, y tiende puentes con eduroam Canadá,eduroam US, y eduroam APAN (Asia y Pacífico).

Mapa de localizaciones de EUROROAM en España:



Instituciones y centros participantes en eduroam ES

Aquí puede encontrar un listado de todas las instituciones y centros participantes en la iniciativa eduroam ES, ordenado por orden alfabético. En total suman **116** instituciones y centros del CSIC conectados hasta la fecha.

c) SERVIDOR LDAP:

1.- Instalación de un servidor OpenLDAP GNU/LINUX (OpenLDAP).

http://www.openldap.org/

En primer lugar instalaremos openldap:

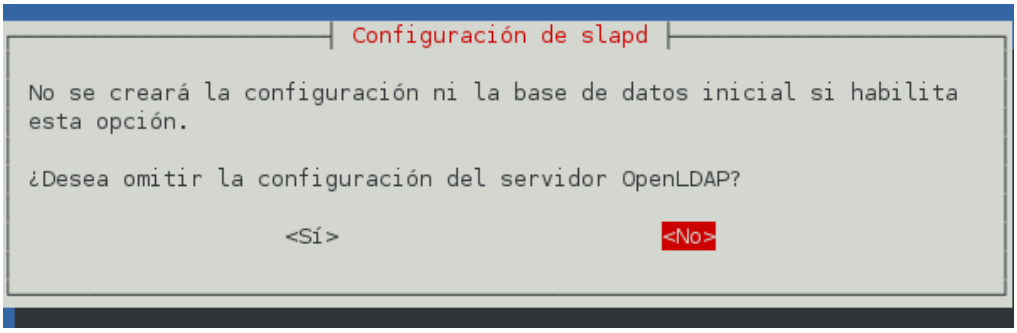
```
root@alvaroniko:/home/alvaroniko# apt-get install slapd ldap-utils
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  odbcinst odbcinst1debian2 unixodbc
Paquetes sugeridos:
  libmyodbc odbc-postgresql tdsodbc unixodbc-bin
Se instalarán los siguientes paquetes NUEVOS:
  ldap-utils odbcinst odbcinst1debian2 slapd unixodbc
0 actualizados, 5 se instalarán, 0 para eliminar y 108 no actualizados.
Se necesita descargar 1495 kB/2150 kB de archivos.
Se utilizarán 5652 kB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]? s
```

Durante el proceso de instalación nos pedirá una contraseña para el usuario administrador del ldap, en nuestro caso introduciremos inves.

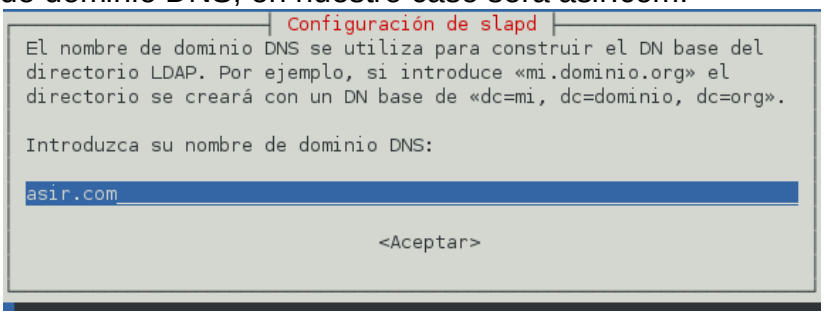
Una vez instalado reconfiguraremos el ldap para así configurar ajustes como el nombre del dominio DNS, el nombre de la organización…Para ello ejecutamos el comando que aparece en la imagen:

```
root@alvaroniko:/home# dpkg-reconfigure slapd
```

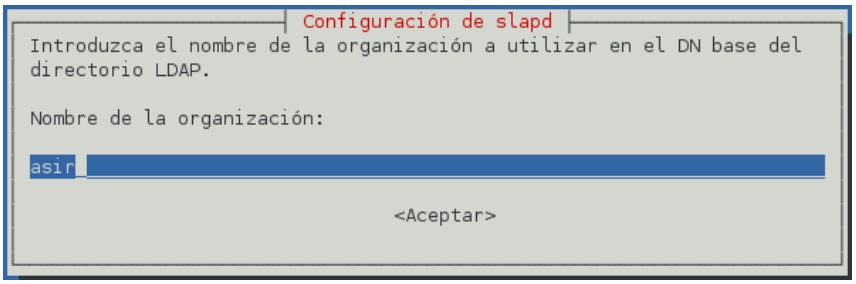
Ahora elegiremos la opcion no a la pregunta de la segunda pantalla para asi poder configurar nuestro servidor ldap:



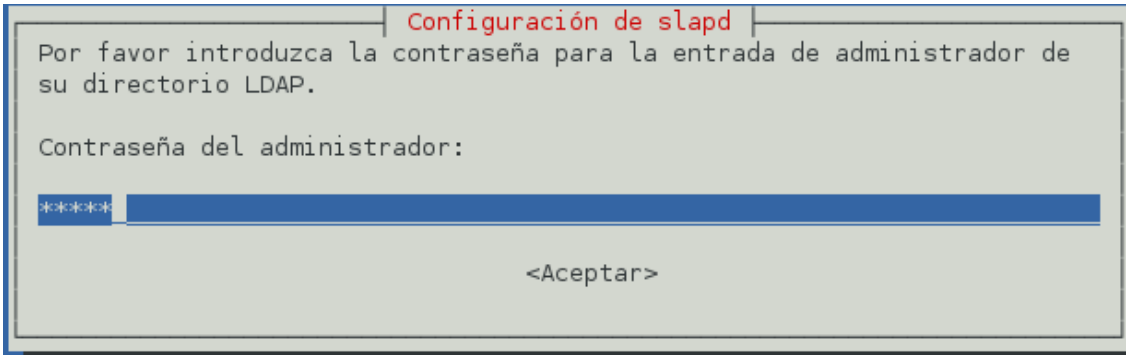
La segunda pantalla que nos aparece es la que nos permite cambiar el nombre de dominio DNS, en nuestro caso será asir.com:



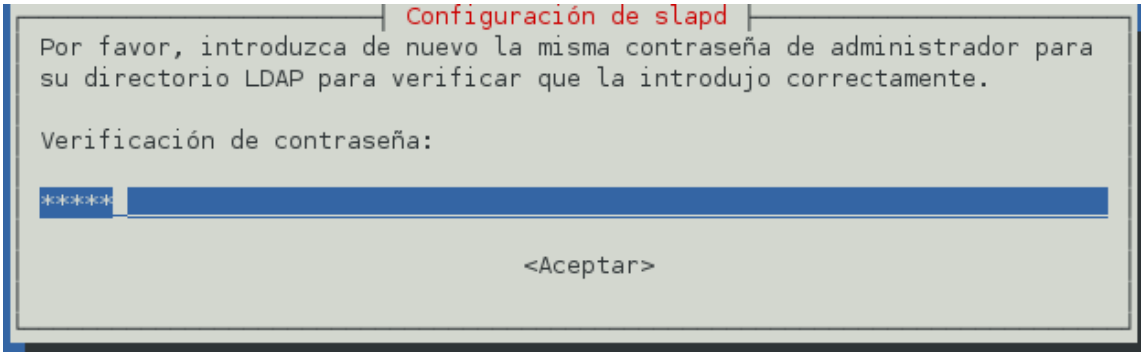
Ahora introducimos el nombre de nuestra compañía, en nuestro caso asir:



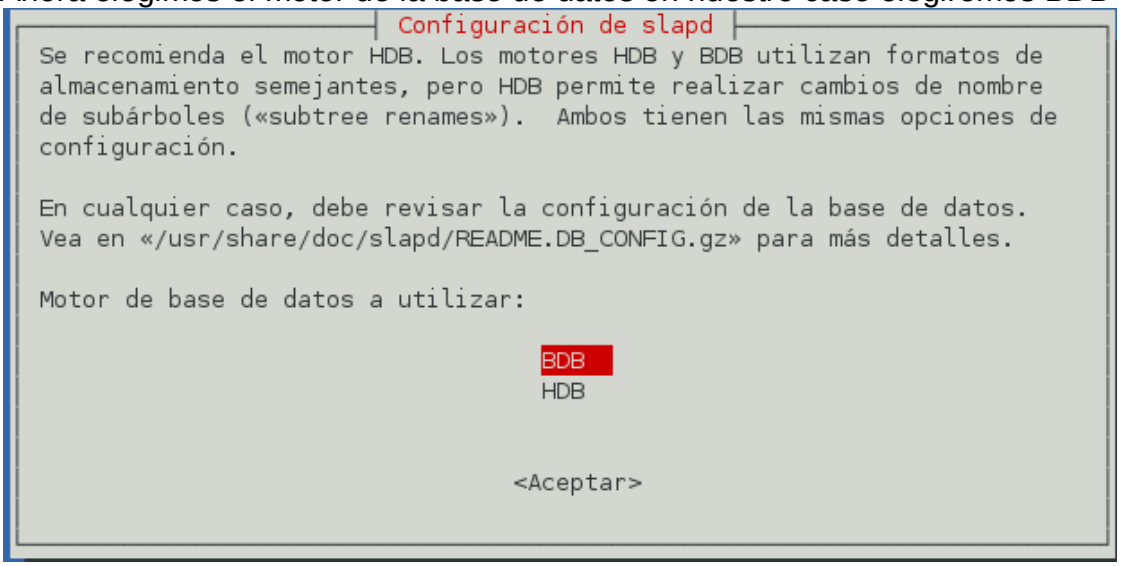
La siguiente pantalla que nos aparecerá será para para cambiar la contraseña del administrador:



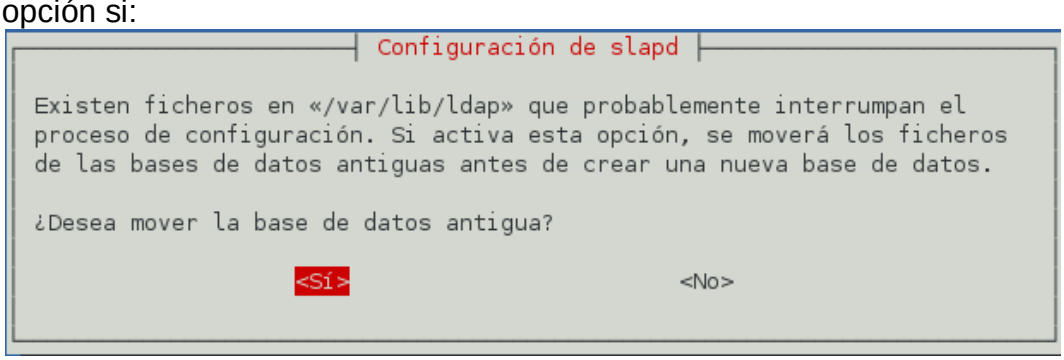
Deberemos de volver a introducir la contraseña:



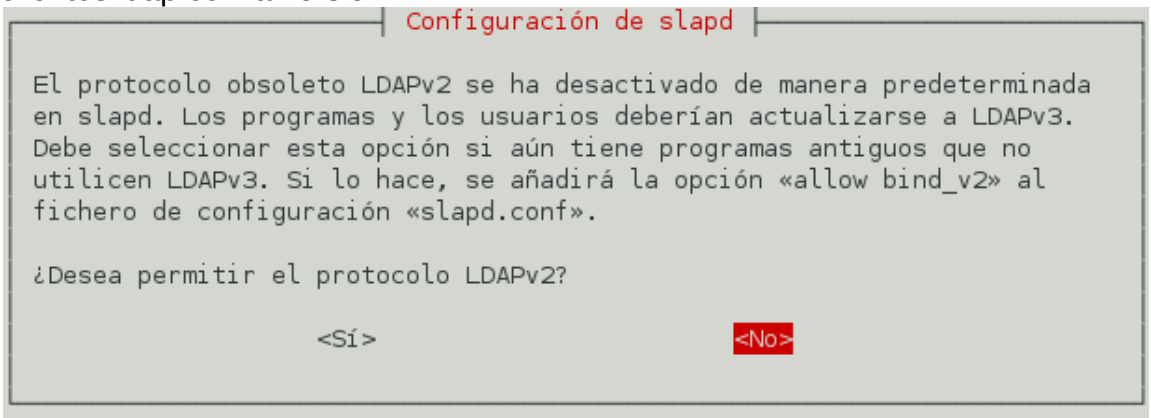
Ahora elegimos el motor de la base de datos en nuestro caso elegiremos BDB



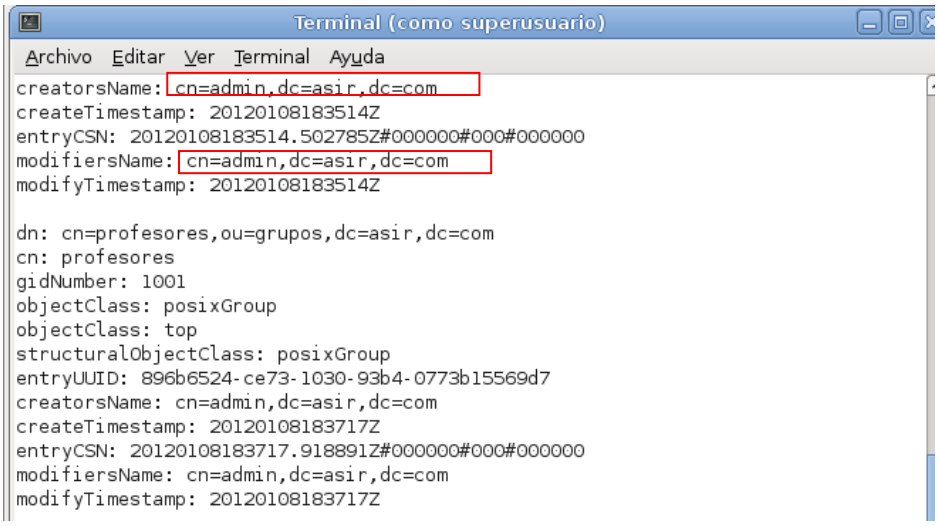
Ahora en la pantalla que nos permite borrar la base de datos elegimos la opción si:



Por último deberemos de elegir la opción no a la pregunta de si usaremos clientes ldap con la versión 2:



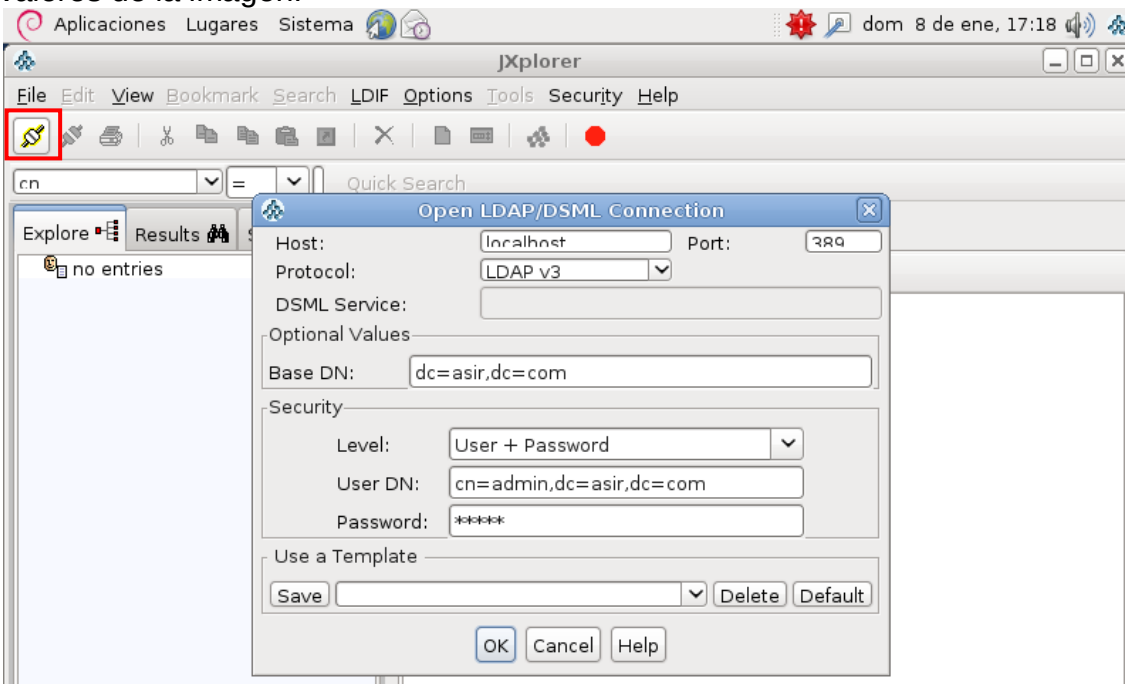
Una vez configurado el ldap ejecutamos un slapcat para comprobar que los cambios se han realizado de una forma satisfactoria:



Una vez comprobados que la configuración se ha aplicado instalaremos jxplorer que es una aplicación que nos permitirá crear usaurios y unidades organizativas en open ldap de forma grafica:

```
root@alvaroniko:/home/alvaroniko# apt-get install jxplorer
```

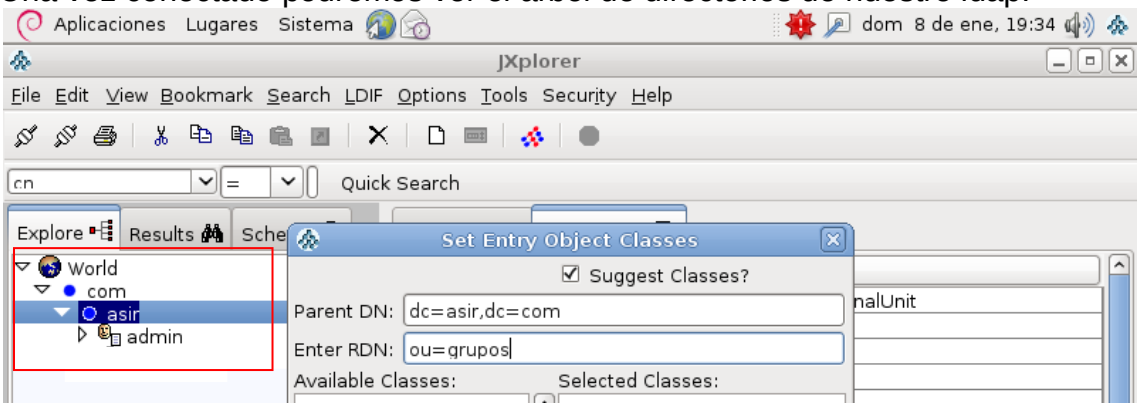
Una vez instalado ejecutamos la aplicación jxplorer:
Una vez ejecutada en primer lugar deberemos de configurar una conexión, para ello pulsamos sobre el icono resaltado en la imagen e introducimos los valores de la imagen:



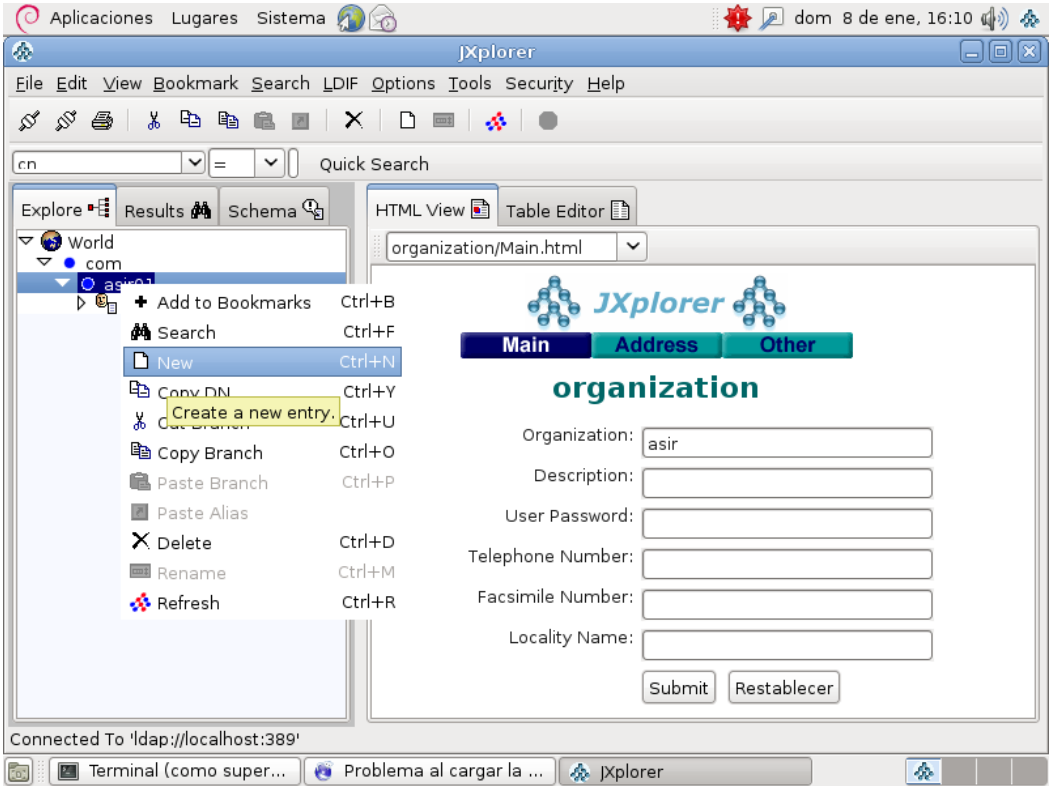
- En host deberemos de indicar localhost puesto que es el equipo en el que se encuentra el servidor ldap.

- En la casilla protocol elegimos LDAP v3 puesto que es la versión que utilizaremos.
- Por último en la sección security deberemos de elegir en la casilla level la opcion User + Password.
- En Base Dn introducimos dc=nombre del dominio, dc=com, es decir el nombre de nuestro dominio. En User DN introducimos cn=admin,dc=asir,dc=com. Y en password la cotraseña de nuestro usuario administrador de ldap.

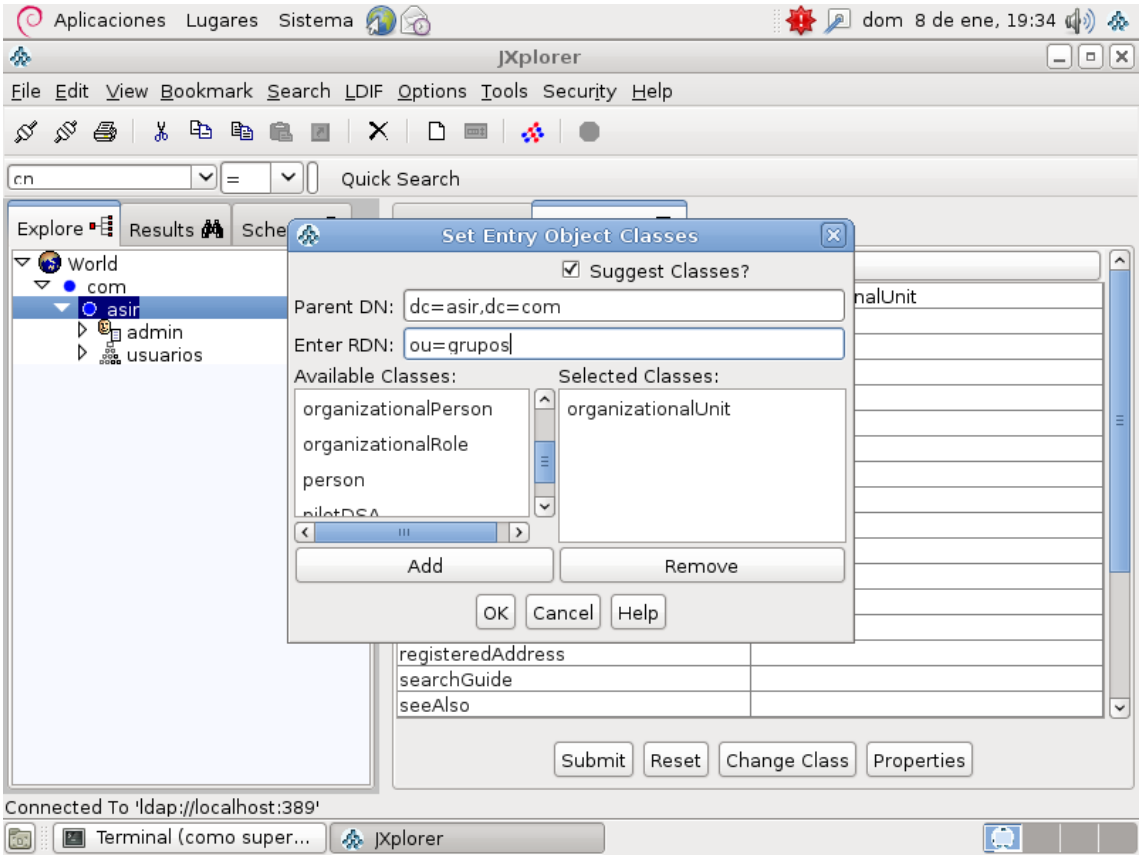
Una vez conectado podremos ver el arbol de directorios de nuestro ldap:



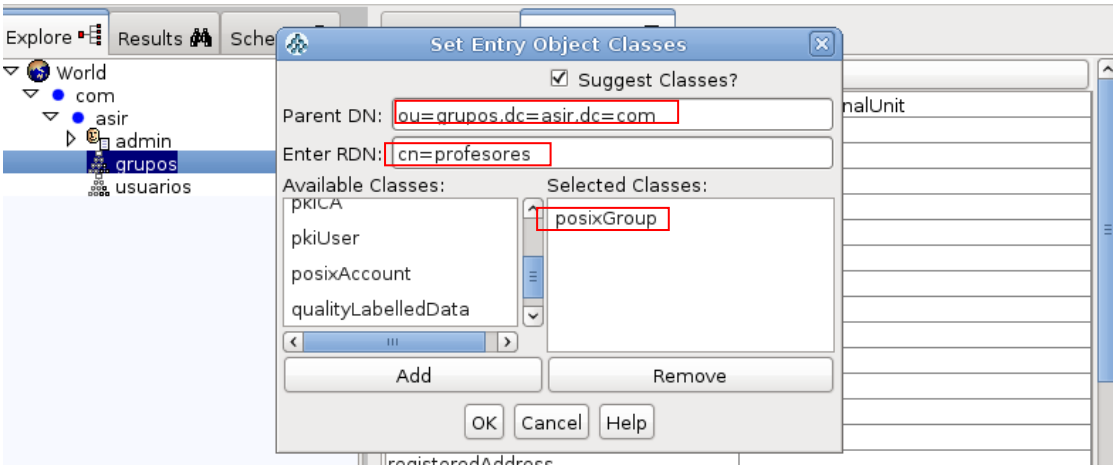
Ahora procederemos a crear una unidad organizativa para los grupos y otra para los usuarios. Para ello en primer lugarnos situaremos sobre el nombre de nuestro dominio en nuestro caso asir y pulsamos botón derecho y pulsamos la opción new:



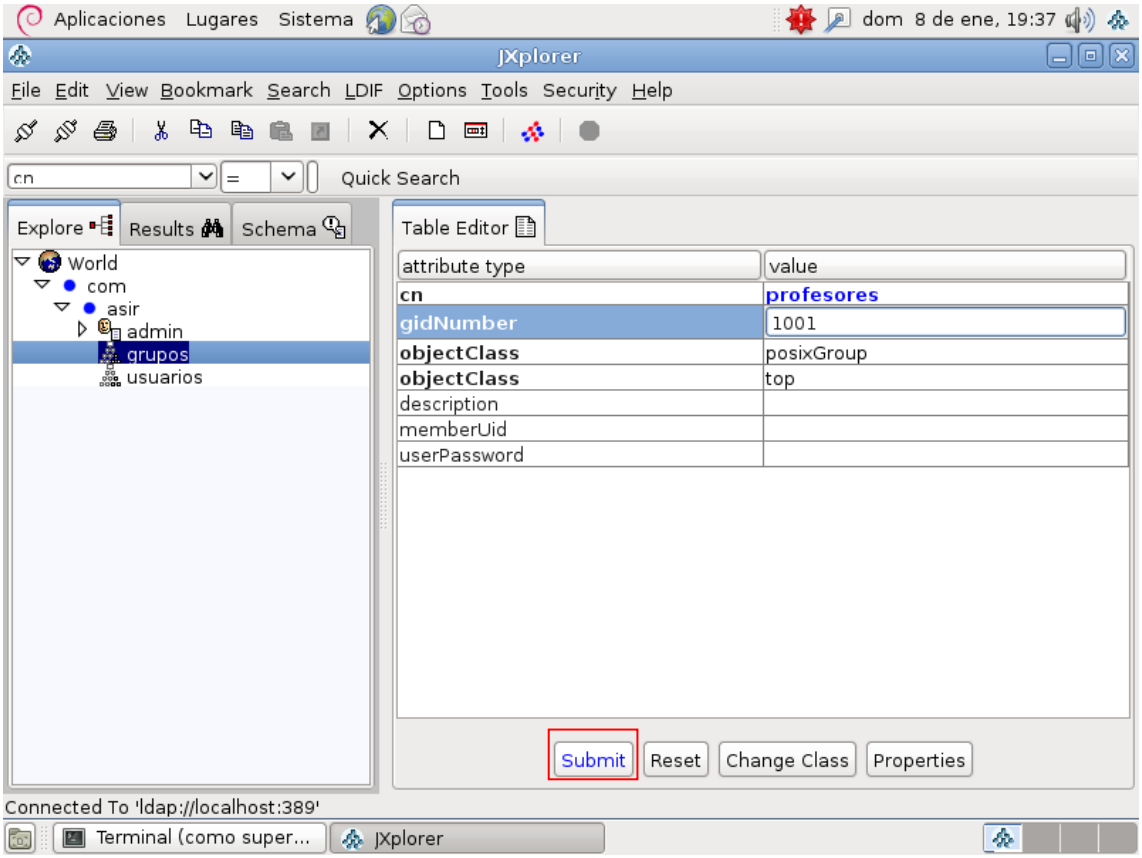
EN la pantalla que nos aparece deberemos de introducir las siguientes configuraciones. En la casilla Parent DN deberemos de introducir el nombre de nuestro dominio, es decir dc=asir,dc=com. Y en enter RDN introduciremos ou=grupos, es decir el nombre de la UO. Por ultimo deberemos de elegir el tipo de clase en nuestro caso OrganizationalUnit:



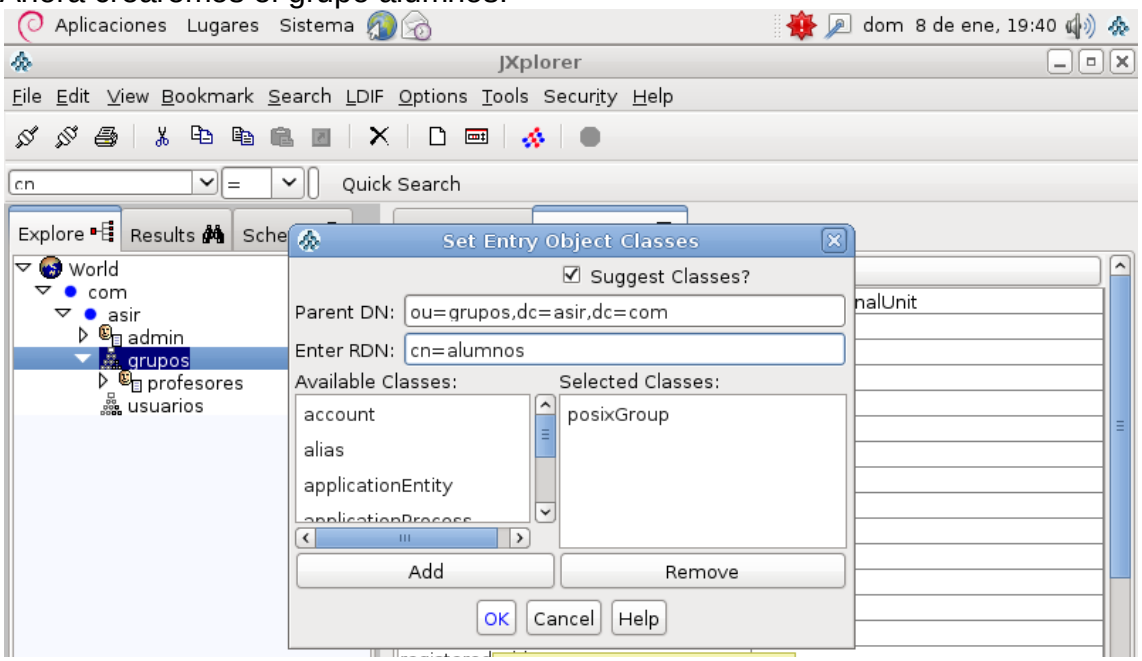
Ahora realizamos los mismos pasos para crear la UO usuarios.
Una vez creada las 2 UO procederemos a la creación del grupo Profesores, para ello nos colocamos sobre la UO grupo/ botón derecho/new. En la pantalla introcucimos los valores que se muestran en la imagen:



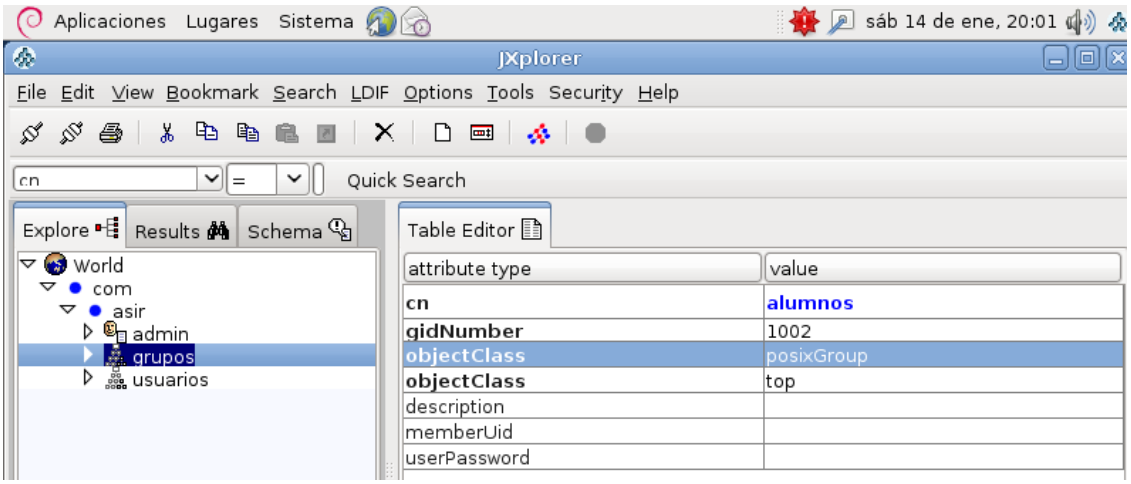
En la siguiente pantalla deberemos de añadir el gidNumber que es el numero del grupo, en nuestro caso será 1001, cuando finalizemos pulsamos submit:



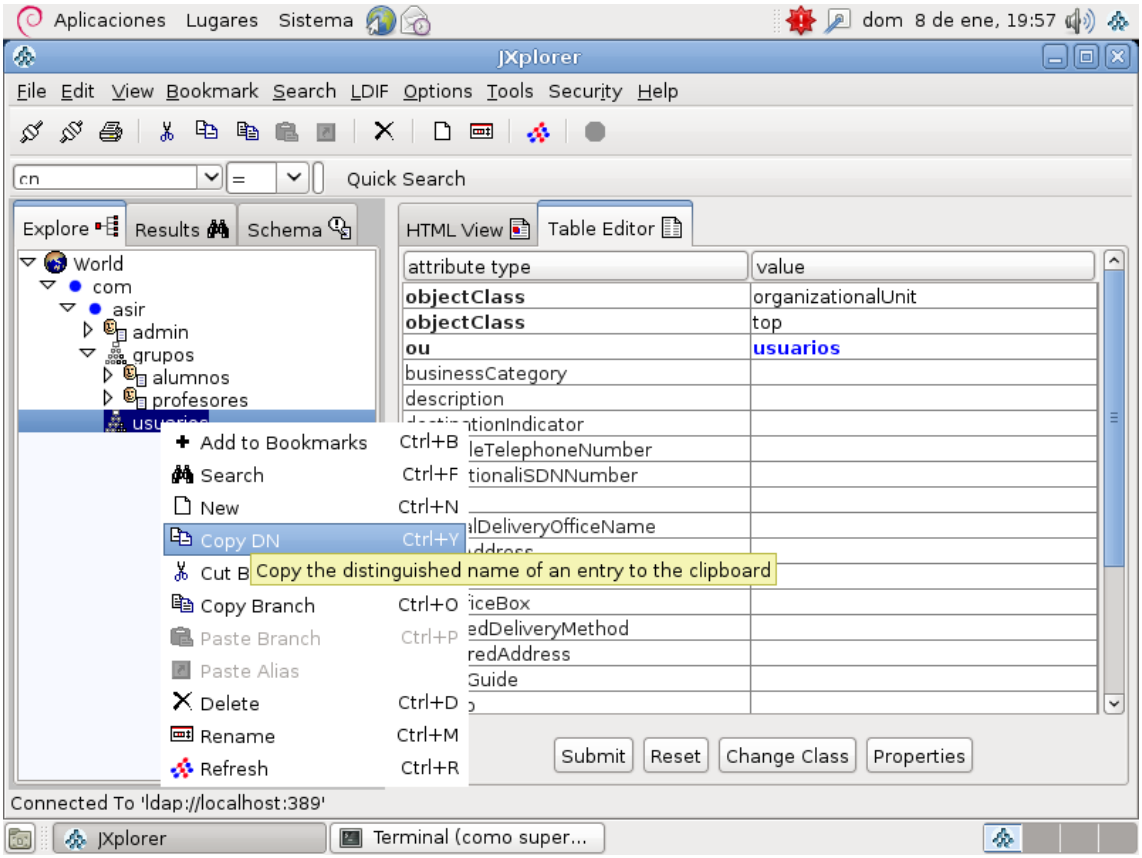
Ahora crearemos el grupo alumnos:



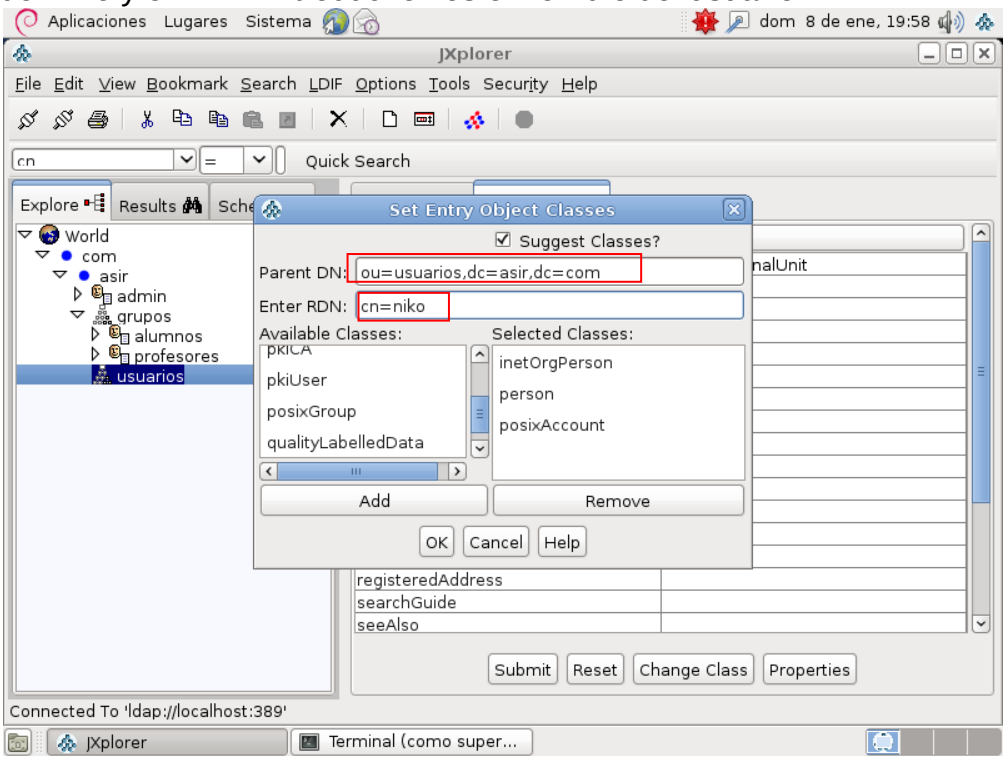
En el grupo alumnos asignaremos el gid 1002:



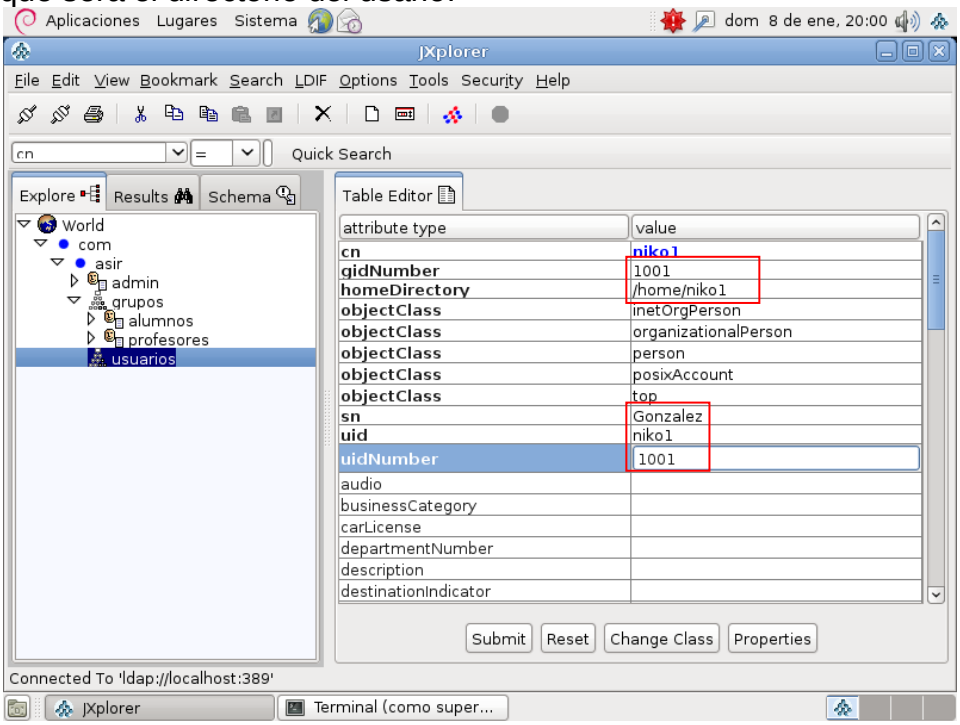
Una vez creado los grupos deberemos de crear usuarios, en el grupo profesores crearemos al usuario niko1 y en el grupo alumnos crearemos al alumno1.
En primer lugar crearemos al usuario niko1, para ello nos situaremos sobre la UO usuarios/botón derecho/new.



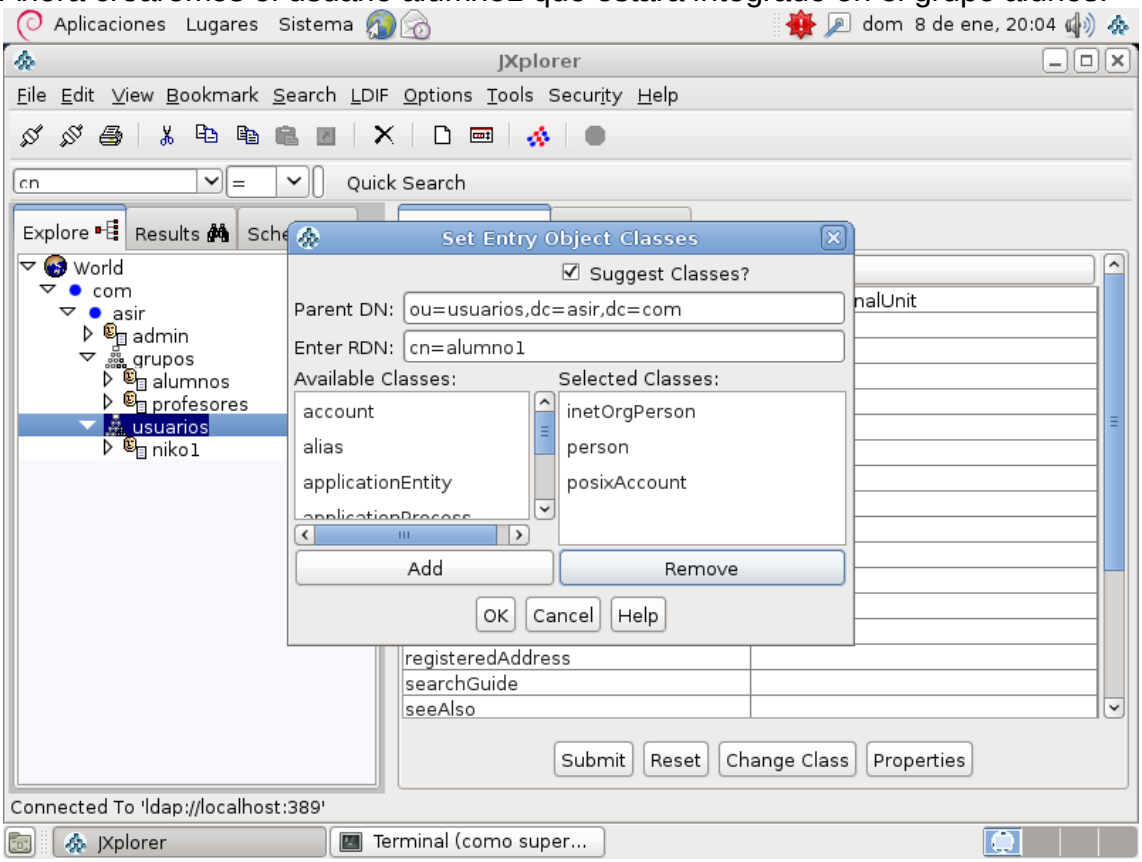
En la pantalla que nos ha aparecido debremos de introducir los siguientes valores. EN Pren DN introduciremos el nombre de la UO y el nombre del dominio y en RDN introduciremos el nombre del usuario:



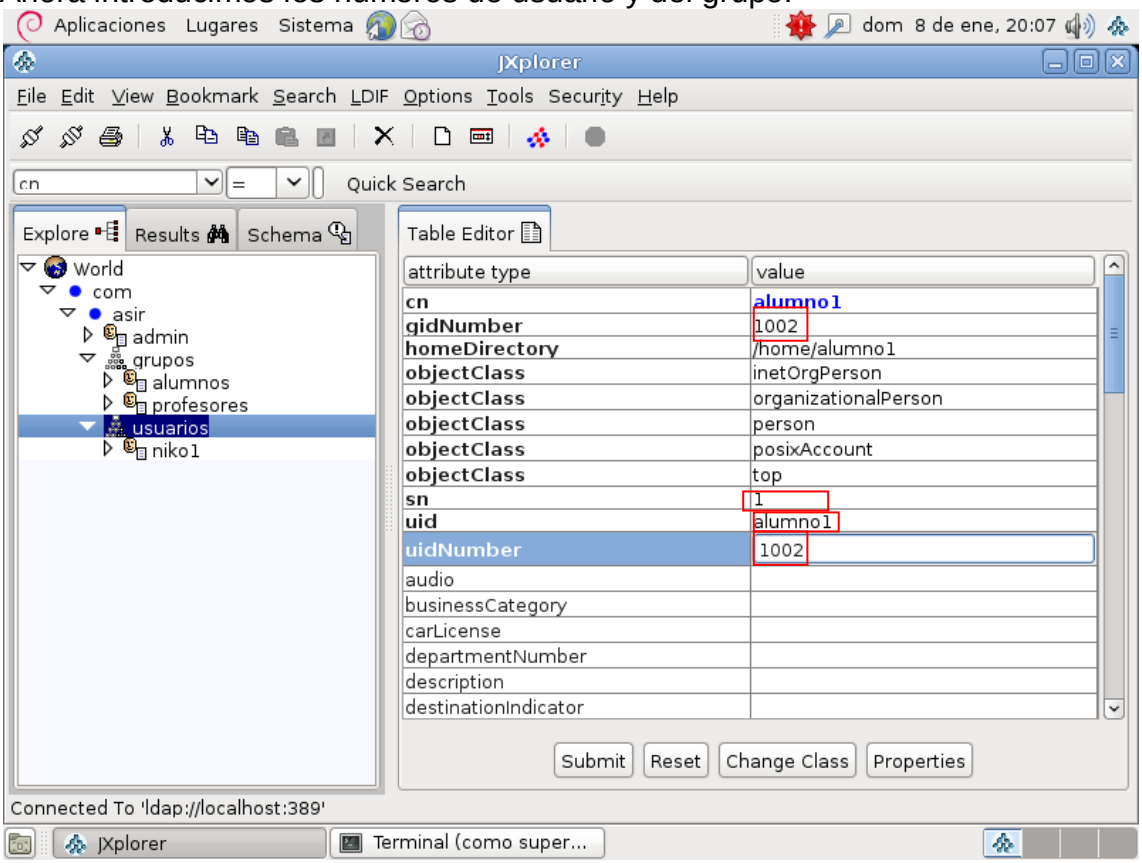
Ahora deberemos de indicar el numero del usuario(uidnumber) y del grupo(gidnumber), ambos valores serán 1001, a su vez el sn y el uid son campos obligatorios a rellenar. Otro campo a rellenar será el homeDirectory que será el directorio del usario:



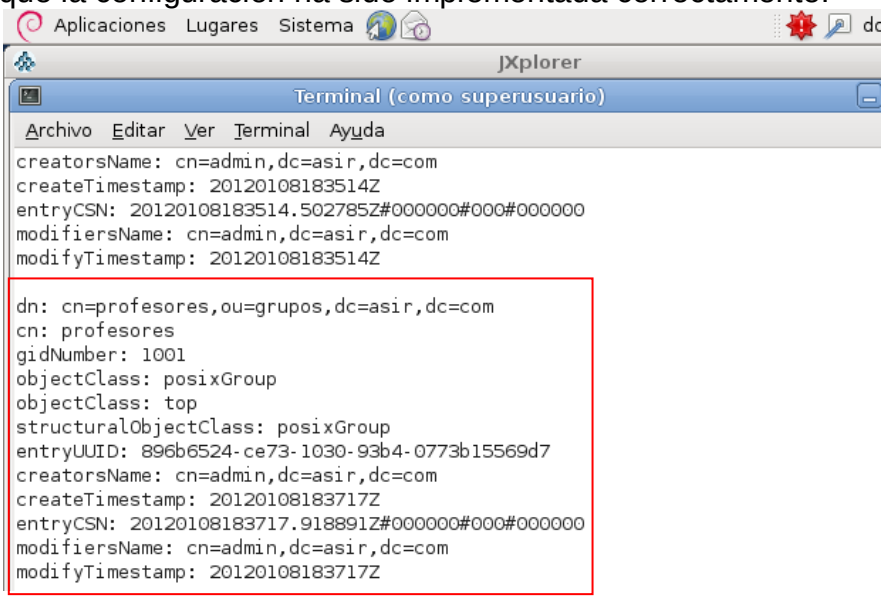
Ahora crearemos el usuario alumno1 que estará integrado en el grupo alunos:



Ahora introducimos los números de usuario y del grupo:



Una vez creados los usuarios y los grupos ejecutaremos uns slapcat para ver que la configuración ha sido implementada correctamente:



Ahora creamos los directorios de conexión de nuestros usuarios:

```
root@alvaroniko:/home/alvaroniko# touch prueba /home/alumno1
root@alvaroniko:/home/alvaroniko# mkdir /home/niko1
```

Por último reiniciaremos el openLdap:

```
root@alvaroniko:/home/alvaroniko# service slapd restart
Stopping OpenLDAP: slapd.
Starting OpenLDAP: slapd.
root@alvaroniko:/home/alvaroniko#
```

Ahora ejecutaremos un ldapsearch para comprobar que los usuarios se han creado satisfactoriamente:

Usuario niko1:

```
root@alvaroniko:/home/alvaroniko# ldapsearch  -x -b 'dc=asir,dc=com' '(cn=niko1)'
# extended LDIF
#
# LDAPv3
# base <dc=asir,dc=com> with scope subtree
# filter: (cn=niko1)
# requesting: ALL
#

# niko1, usuarios, asir.com
dn: cn=niko1,ou=usuarios,dc=asir,dc=com
cn: niko1
gidNumber: 1001
homeDirectory: /home/niko1
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
objectClass: top
sn: Gonzalez
uid: niko1
uidNumber: 1001

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Usuario alumno1:

```
root@alvaroniko:/home/alvaroniko# ldapsearch  -x -b 'dc=asir,dc=com' '(cn=alumno1)'
# extended LDIF
#
# LDAPv3
# base <dc=asir,dc=com> with scope subtree
# filter: (cn=alumno1)
# requesting: ALL
#

# alumno1, usuarios, asir.com
dn: cn=alumno1,ou=usuarios,dc=asir,dc=com
cn: alumno1
gidNumber: 1002
homeDirectory: /home/alumno1
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
objectClass: top
sn: 1
uid: alumno1
uidNumber: 1002

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

2.- Instalación de un cliente LDAP bajo Windows o GNU/Linux para autenticarse.

NO HE DOCUMENTADO ESTA PARTE PORQUE DE MOMENTO NO HE CONSEGUIDO QUE EXISTA CONECTIVIDAD ENTRE LOS CLIENTES LDAP Y EL SERVIDOR LDAP

3.- Busca información sobre LDAP y su implementación en productos comerciales.

Descripción
LDAP (Lightweight Directory Access Protocol, Protocolo Ligero de Acceso a Directorios) **es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.**
LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.
Un directorio es un conjunto de objetos con atributos organizados en una manera lógica y jerárquica. El ejemplo más común es el directorio telefónico, que consiste en una serie de nombres (personas u organizaciones) que están ordenados alfabéticamente, con cada nombre teniendo una dirección y un número de teléfono adjuntos.
Un árbol de directorio LDAP a veces refleja varios límites políticos, geográficos y/o organizacionales, dependiendo del modelo elegido. Los despliegues actuales de LDAP tienden a usar nombres de Sistema de Nombres de Dominio (DNS por sus siglas en inglés) para estructurar los niveles más altos de la jerarquía. Conforme se desciende en el directorio pueden aparecer entradas que representan personas, unidades organizacionales, impresoras, documentos, grupos de personas o cualquier cosa que representa una entrada dada en el árbol (o múltiples entradas).
Habitualmente, almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc).
En síntesis, **LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.**

Un directorio LDAP lo componen:

- Un directorio es un árbol ordenado de entradas
- Una entrada consta de un conjunto de atributos.

- Un atributo tiene un nombre (un tipo de atributo o descripción de atributo) y
- uno o más valores.
- Los atributos son definidos por un esquema
- Cada entrada tiene un identificador único: su Nombre distintivo
- (Distinguished Name, DN).

Usos empresariales

Dadas las características de LDAP sus usos más comunes son:
- **Directorios de información**. Por ejemplo bases de datos de empleados organizados por departamentos (siguiendo la estructura organizativa de la empresa) ó cualquier tipo de páginas amarillas.
- **Sistemas de autenticación/autorización centralizada**. Grandes sistemas donde se guarda gran cantidad de registros y se requiere un uso constante de los mismos. Por ejemplo:
o **Active Directory Server de Microsoft,** para gestionar todas las cuentas de acceso a una red corporativa y mantener centralizada la gestión del acceso a los recursos.
o **Sistemas de autenticación para páginas Web,** algunos de los gestores de contenidos más conocidos disponen de sistemas de autenticación a través de LDAP.
o **Sistemas de control de entradas a edificios, oficinas….**
- **Sistemas de correo electrónico.** Grandes sistemas formados por más de un servidor que accedan a un repositorio de datos común.
- **Sistemas de alojamiento de páginas web y FTP,** con el repositorio de datos de usuario compartido.
- **Grandes sistemas de autenticación basados en RADIUS,** para el control de accesos de los usuarios a una red de conexión o ISP.
- **Servidores de certificados públicos y llaves de seguridad**
- **Autenticación única ó "single sign-on"** para la personalización de aplicaciones.
- Perfiles de usuarios centralizados, para permitir itinerancia ó "roaming"
- Libretas de direcciones compartidas.

Ejemplos de uso de LDAP

Sistema de correo electrónico

Cada usuario se identifica por su dirección de correo electrónico, los atributos que se guardan de cada usuario son su contraseña, su límite de almacenamiento (quota), la ruta del disco duro donde se almacenan los mensajes (buzón) y posiblemente atributos adicionales para activar sistemas anti-spam o anti-virus.
Como se puede ver este sistema LDAP recibirá cientos de consultas cada día (una por cada email recibido y una cada vez que el usuario se conecta mediante POP3 o webmail). No obstante el número de modificaciones diarias

es muy bajo, ya que solo se puede cambiar la contraseña o dar de baja al usuario, operaciones ambas que no se realizan de forma frecuente.

Sistema de autenticación a una red

Cada usuario se identifica por un nombre de usuario y los atributos asignados son la contraseña, los permisos de acceso, los grupos de trabajo a los que pertenece, la fecha de caducidad de la contraseña…
Este sistema recibirá una consulta cada vez que el usuario acceda a la red y una más cada vez que acceda a los recursos del grupo de trabajo (directorios compartidos, impresoras…) para comprobar los permisos del usuario.
Frente a estos cientos de consultas solo unas pocas veces se cambia la contraseña de un usuario o se le incluye en un nuevo grupo de trabajo.