

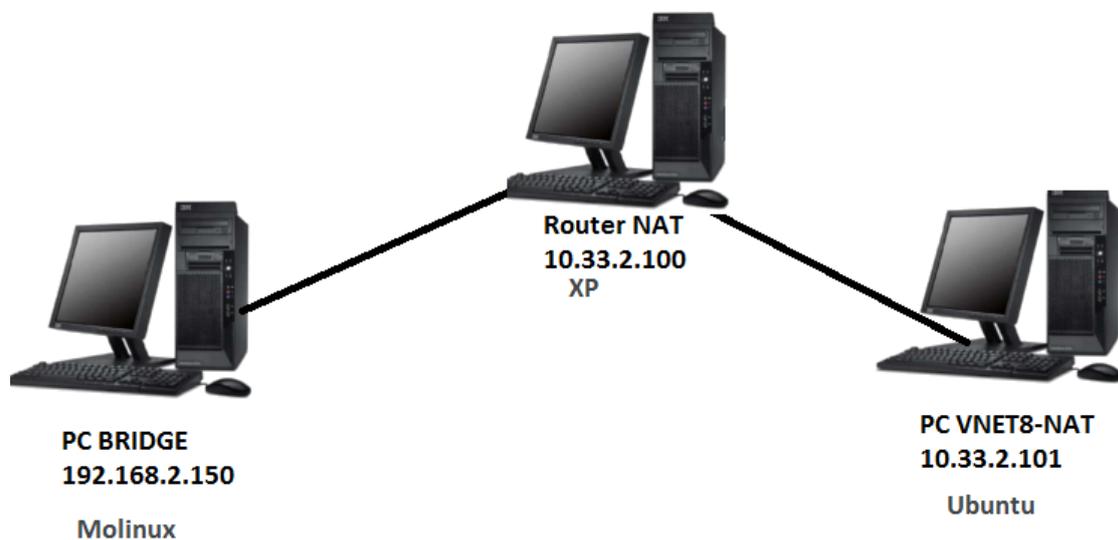
UD 3: “Implantación de técnicas de seguridad remoto. Seguridad perimetral.”

SEGURIDAD PERIMETRAL:

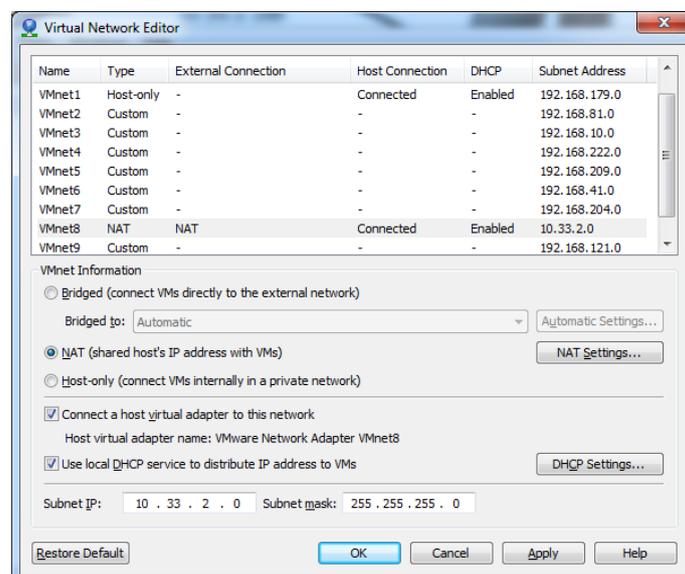
1. NAT:

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

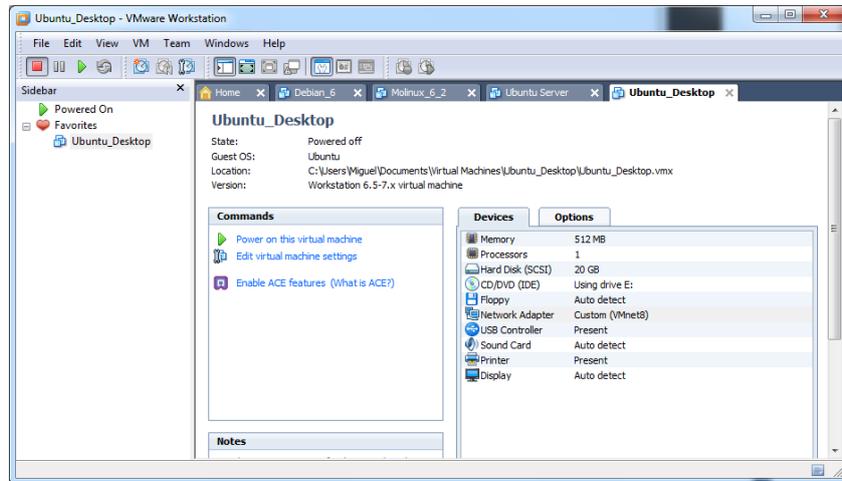
Escenario:



Configuramos el vnet8-NAT, para la red “10.33.2.0”



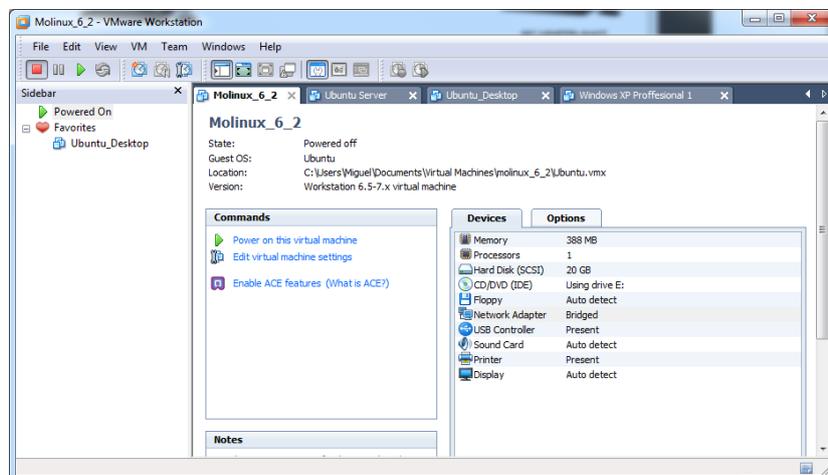
En el equipo Ubuntu elegimos el tipo **VNET8-NAT**



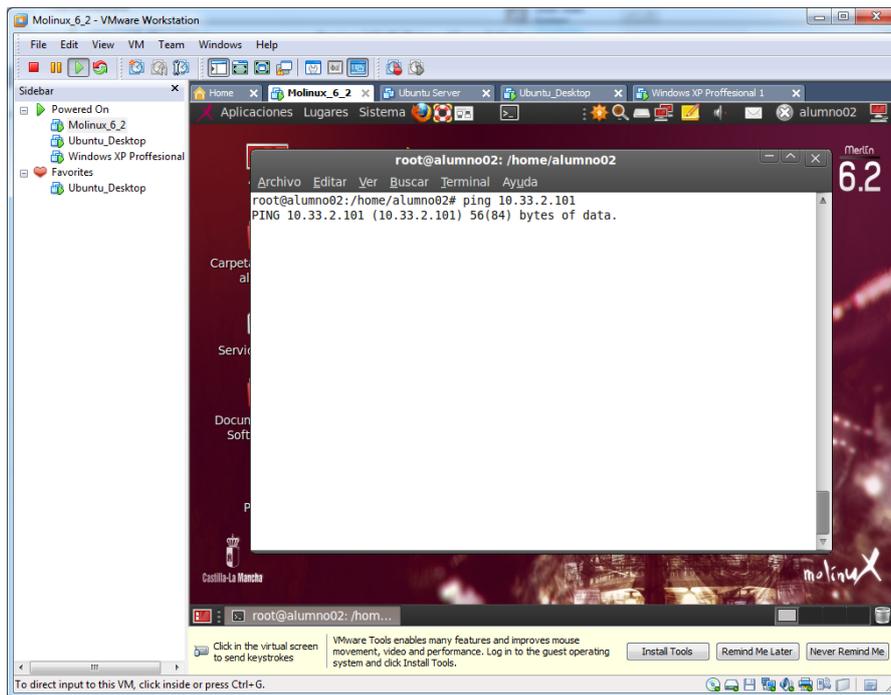
En el equipo XP elegimos el tipo **NAT**



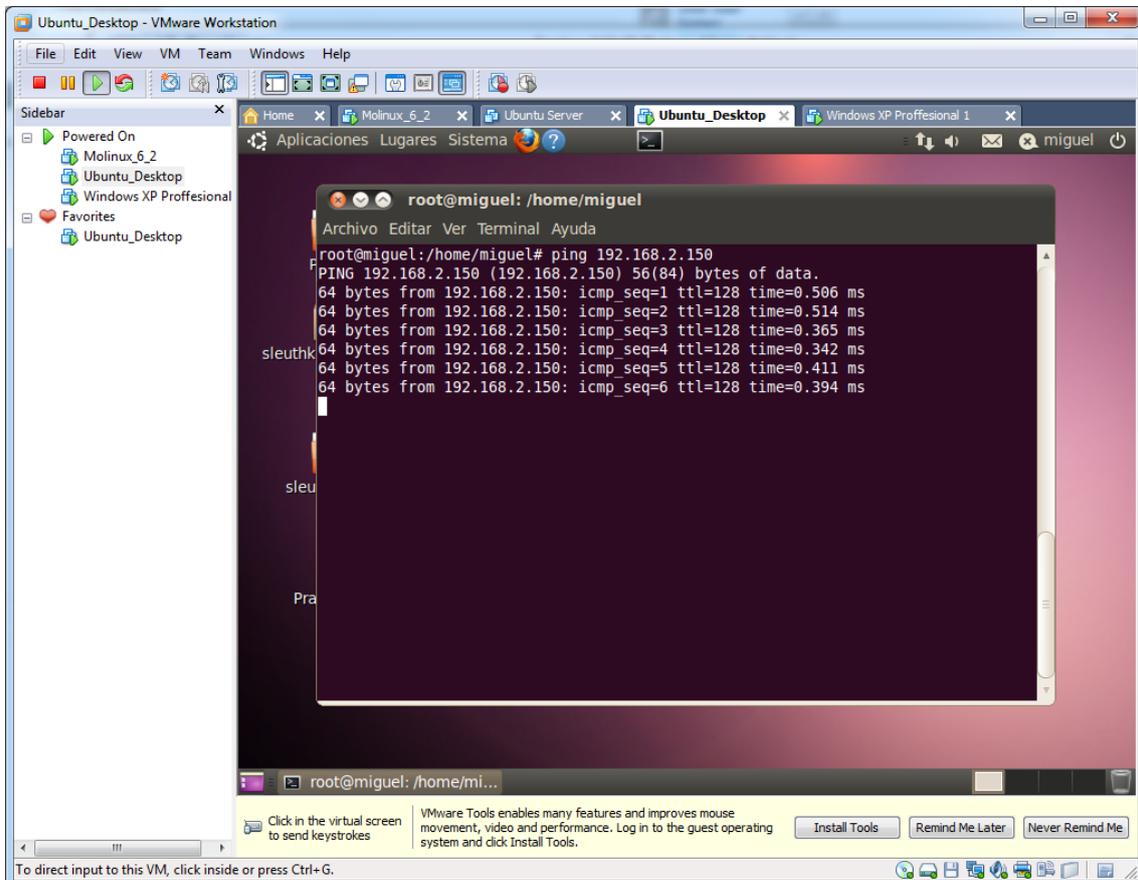
En el equipo Molinux elegimos el tipo **BRIDGED**



Comprobamos que el cliente Molinux no puede acceder a la dirección “10.33.2.101”



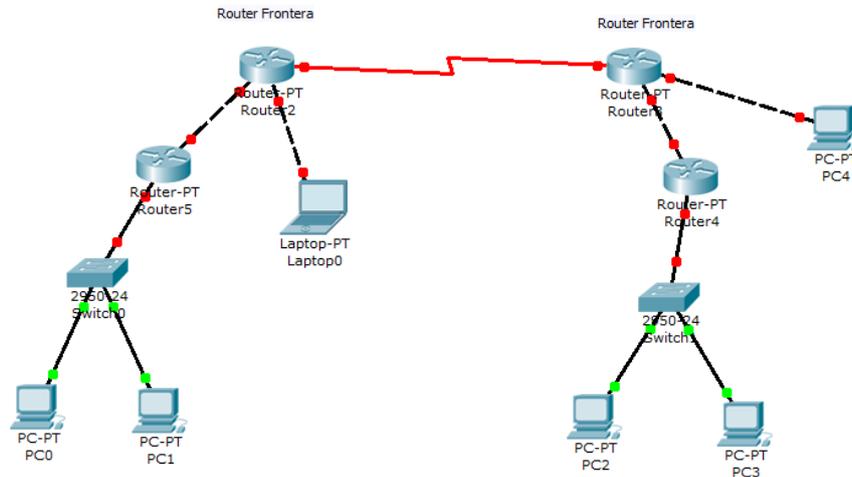
Mientras que el Cliente Ubuntu sí que puede acceder a la dirección “192.168.2.150”.



2. Router frontera:

a) Planteamiento escenario CISCO Packet Tracer: esquema.

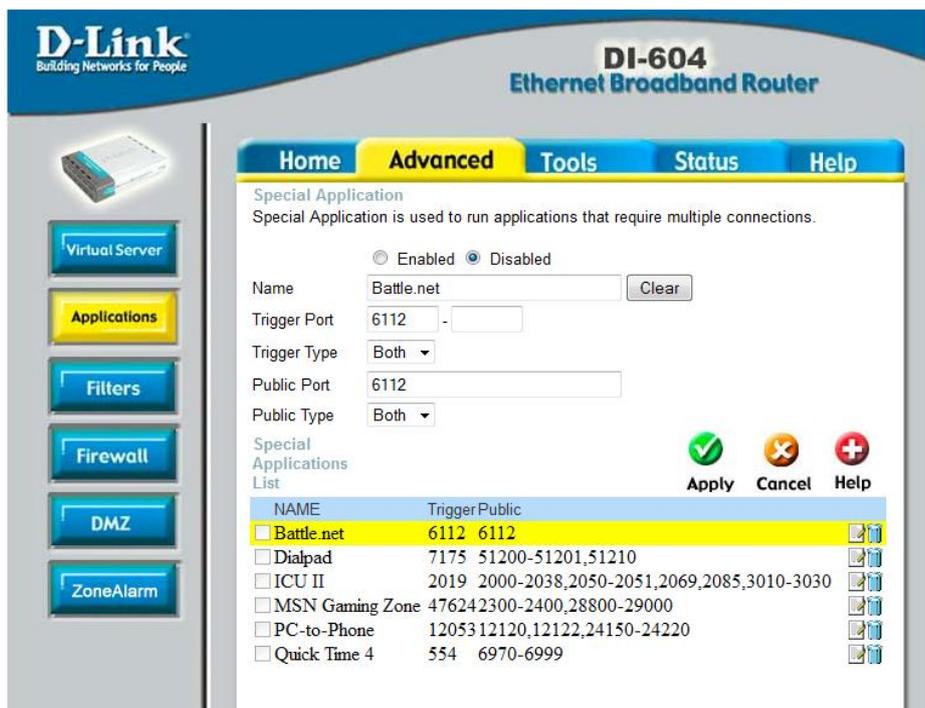
Tenemos 2 router frontera que unen dos empresas en zonas geográficas diferentes.



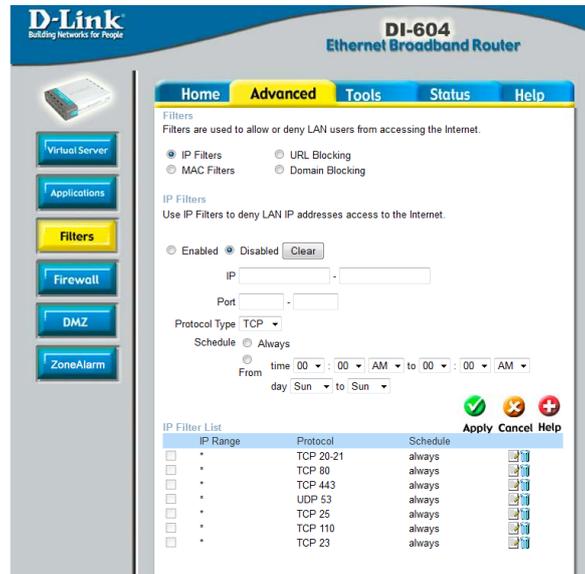
b) Realiza una comparativa entre los routers frontera atendiendo a las opciones de seguridad perimetral (NAT, Firewall, DMZ, ...etc)

Router DLINK:

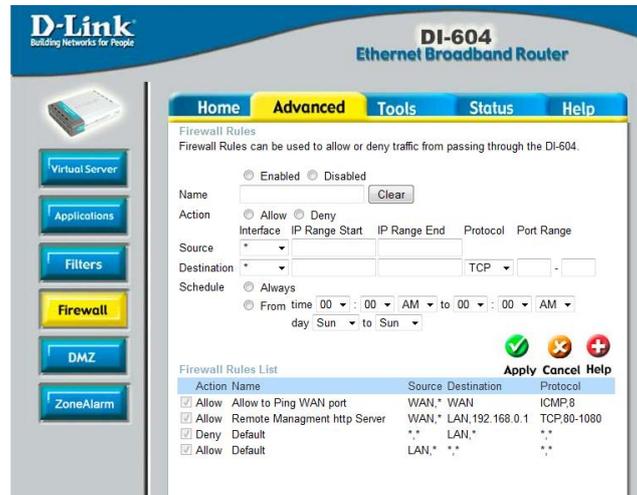
Podemos editar y eliminar diferentes aplicaciones que usan más de un puerto



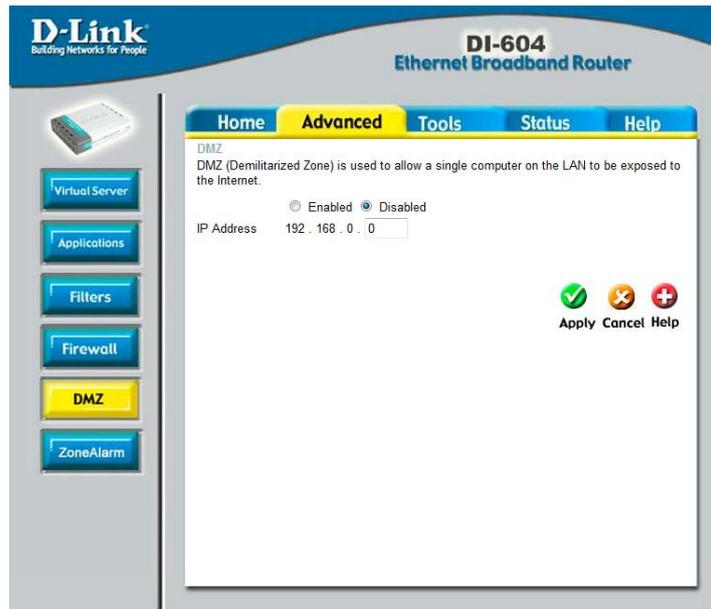
Podemos hacer filtrados de ip, mac y puertos configurando si queremos la fecha y hora.



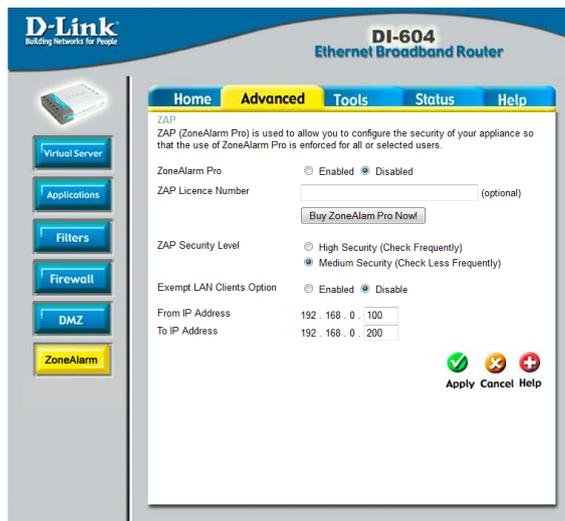
Podemos configurar en el firewall, diversos filtros para controlar la entrada a diferentes nombres y direcciones.



En esta pestaña podemos configurar la zona desmilitarizada.

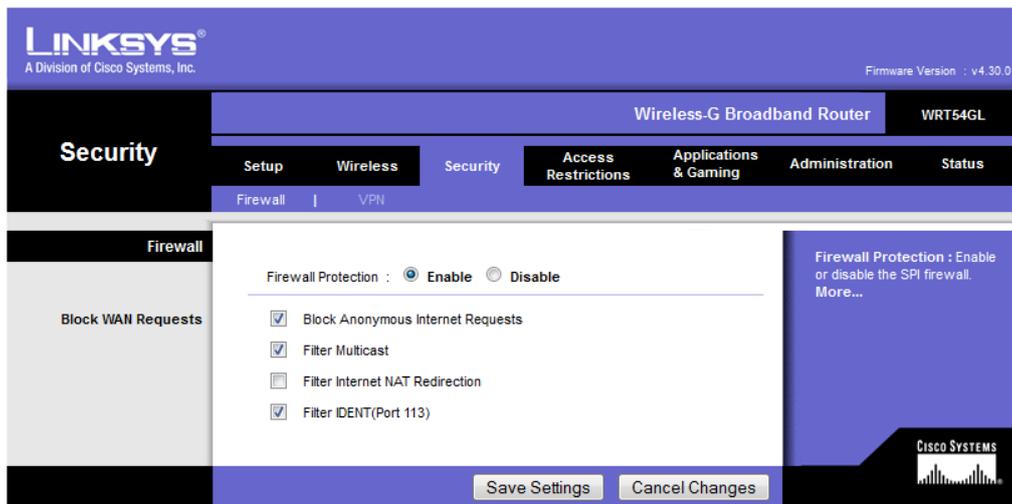


Podemos además configurar una zona de alarma

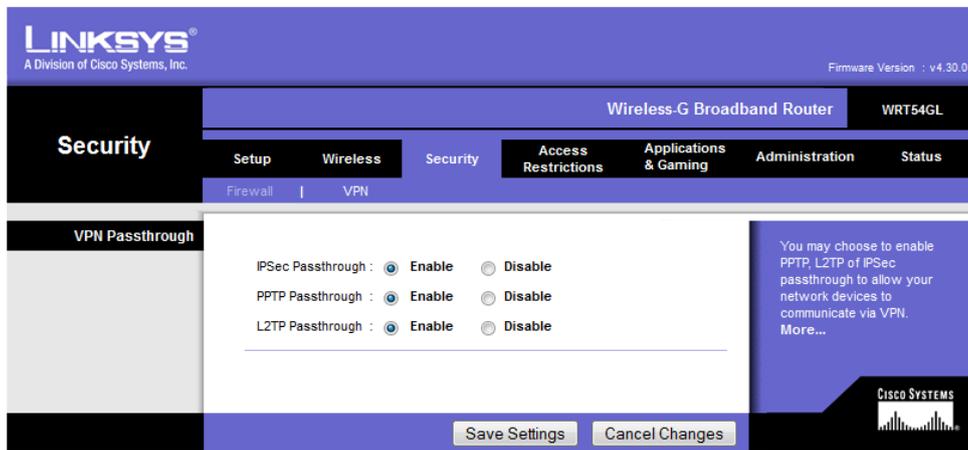


Router LINKSYS:

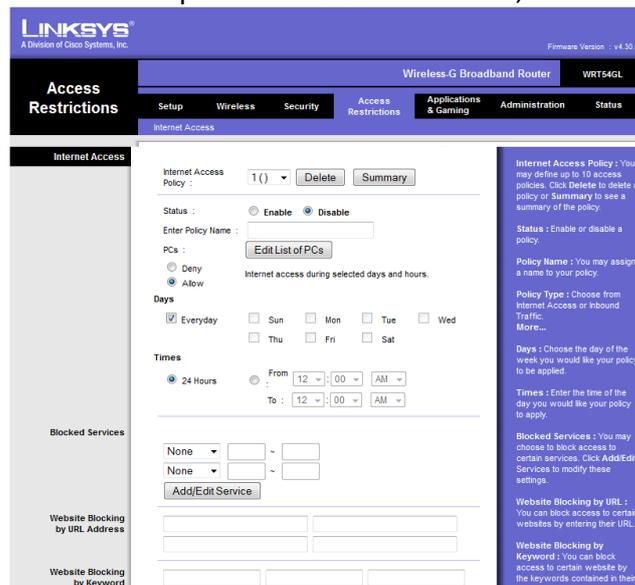
Este router es más avanzado que el anterior, algunas de las opciones de seguridad que podemos encontrar son, el cortafuegos, con sus distintas opciones.



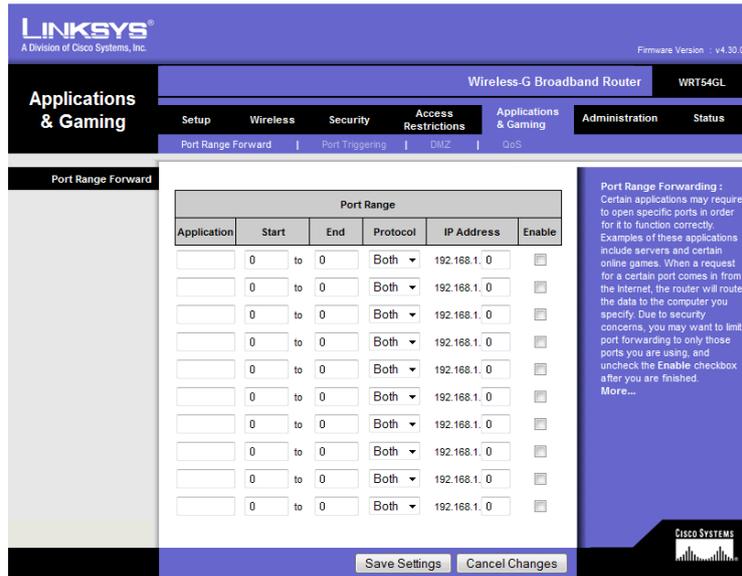
Podemos habilitar opciones VPN.



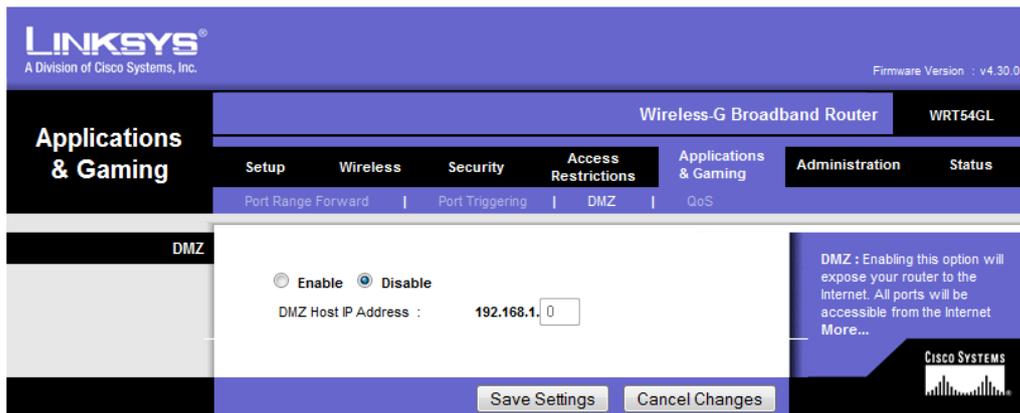
Podemos configurar diferentes parámetros de restricción, direcciones, fechas etc.



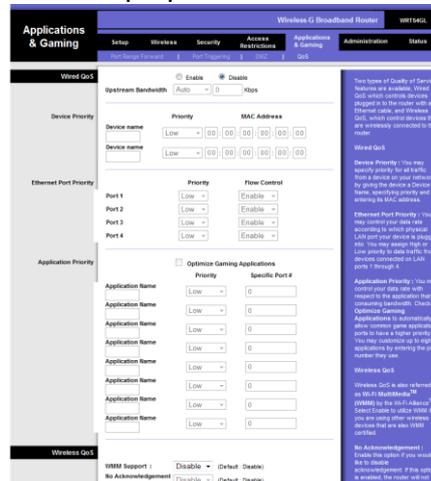
Podemos configurar los puertos



Podemos hacer configuraciones para la zona desmilitarizada



Podemos protegernos acerca de los paquetes QoS.



Router TP-LINK:

Podemos configurar opciones VPN, ALG activar firewall y habilitar-deshabilitar diferentes protocolos.

TP-LINK 300Mbps Multi-Function Wireless N Router Model No. TL-WR842ND

Basic Security

Firewall
SPI Firewall: Enable Disable

VPN
PPTP Passthrough: Enable Disable
L2TP Passthrough: Enable Disable
IPSec Passthrough: Enable Disable

ALG
FTP ALG: Enable Disable
TFTP ALG: Enable Disable
H323 ALG: Enable Disable
RTSP ALG: Enable Disable

Basic Security Help
You can configure the Basic Security Settings on this page.
Firewall - Here you can enable or disable the Router's firewall.
• **SPI Firewall** - Stateful Packet Inspection (SPI) helps to prevent cyber attacks by tracing more state per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by factory default. If you want all the computers on the LAN exposed to the outside world, you can disable it.
VPN - VPN Passthrough must be enabled if you want to allow VPN tunnels using VPN protocols to pass through the Router.
• **PPTP Passthrough** - PPTP Passthrough Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, click Enable.
• **L2TP Passthrough** - Layer Two Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the Internet on the Layer Two level. To allow L2TP tunnels to pass through the Router, click Enable.
• **IPSec Passthrough** - Internet Protocol security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the Router, click Enable.
ALG - It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address

Podemos habilitar el ICMP y otros protocolos.

TP-LINK 300Mbps Multi-Function Wireless N Router Model No. TL-WR842ND

Advanced Security

Packets Statistics Interval (5 - 60): 10 Seconds

DoS Protection: Disable Enable

Enable ICMP-FLOOD Attack Filtering
ICMP-FLOOD Packets Threshold (5 - 3600): 50 Packets/s

Enable UDP-FLOOD Filtering
UDP-FLOOD Packets Threshold (5 - 3600): 500 Packets/s

Enable TCP-SYN-FLOOD Attack Filtering
TCP-SYN-FLOOD Packets Threshold (5 - 3600): 50 Packets/s

Ignore Ping Packet From WAN Port
 Forbid Ping Packet From LAN Port

Advanced Security Help
Using the Advanced Settings page you can protect the Router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood.
Note: FLOOD Filtering will take effect only when the Traffic Statistics in System Tools is enabled.
• **Packets Statistics Interval (5-60)** - The default value is 10. Selected a value between 5 and 60 seconds in the pull-down list. The Packets Statistics interval value indicates the time section of the packets statistic. The result of the statistic used for analysis by SYN Flood, UDP Flood and ICMP-Flood.
• **DoS Protection** - Enable or Disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.
• **Enable ICMP-FLOOD Attack Filtering** - Enable or Disable the ICMP-FLOOD Attack Filtering.
• **ICMP-FLOOD Packets Threshold (5-3600)** - The default value is 50. Enter a value between 5 - 3600. When the current ICMP-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.
• **Enable UDP-FLOOD Filtering** - Enable or Disable the UDP-FLOOD Filtering.
• **UDP-FLOOD Packets Threshold (5-3600)** - The default value is 500. Enter a value between 5 - 3600. When the current UDP-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.
• **Enable TCP-SYN-FLOOD Attack Filtering** - Enable or Disable the TCP-SYN-FLOOD Attack Filtering.
• **TCP-SYN-FLOOD Packets Threshold (5-3600)** - The

Podemos hacer un filtrado de MAC.

TP-LINK 300Mbps Multi-Function Wireless N Router Model No. TL-WR842ND

Local Management

Management Rules
 All the PCs on the LAN are allowed to access the Router's Web-Based Utility.
 Only the PCs listed can browse the built-in web pages to perform Administrator tasks

MAC 1:
MAC 2:
MAC 3:
MAC 4:

Your PC's MAC Address: EC:62:6D:F7:32:1D

Local Management Help
This page allows you to deny LAN computers from accessing the Router.
By default, the radio button **All the PCs on the LAN are allowed to access the Router's Web-Based Utility** is selected. If you want to allow PCs with specific MAC Addresses to access the Setup page of the Router's Web-Based Utility locally, from inside the network, click the radio button **Only the PCs listed can browse the built-in web pages to perform Administrator tasks**, and then enter each MAC Address in a separate field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). Only the PCs with the MAC address listed can use the password to browse the built-in web pages to perform Administrator tasks and all the others will be blocked.
After click the **Add** button, your PC's MAC Address will be placed in the Control List above.
Click the **Save** button to save your settings.
Note: If your PC is blocked and you want to access the Router again, use a pin to press and hold the **Reset** Button on the back panel about 5 seconds to reset the Router's factory defaults in the Router's Web-Based Utility.

Podemos configurar la zona desmilitarizada.

The screenshot shows the DMZ configuration page on a TP-Link 300Mbps Multi-Function Wireless N Router. The left sidebar contains a navigation menu with options like Status, Quick Setup, WPS, Network, Wireless, DHCP, VPN, USB Settings, Forwarding, and Access Control. The main content area is titled 'DMZ' and includes a 'Current DMZ Status' section with radio buttons for 'Enable' and 'Disable'. Below this is a 'DMZ Host IP Address' field with the value '0.0.0.0' and a 'Save' button. A 'DMZ Help' section on the right explains the feature and provides a list of steps to assign a computer or server to be a DMZ server.

Podemos configurar listas de control de acceso.

The screenshot shows the Internet Access Control Rule Management page on a TP-Link 300Mbps Multi-Function Wireless N Router. The left sidebar is similar to the previous screenshot, with 'Access Control' selected. The main content area is titled 'Access Control Rule Management' and features a 'Default Filter Policy' section with radio buttons for 'Allow' and 'Deny'. Below this is a table with columns for ID, Rule Name, Host, Target, Schedule, and Enable. A single rule is listed with ID '1', Rule Name 'relax', Host 'home', Target 'parents', Schedule 'weekend', and an 'Enable' checkbox checked. Below the table are buttons for 'Add New', 'Enable All', 'Disable All', and 'Delete All', along with a 'Move' button and a 'Setup Wizard' link. A 'Previous' and 'Next' button are at the bottom. A 'Help' section on the right explains the function and provides an example of a rule configuration.

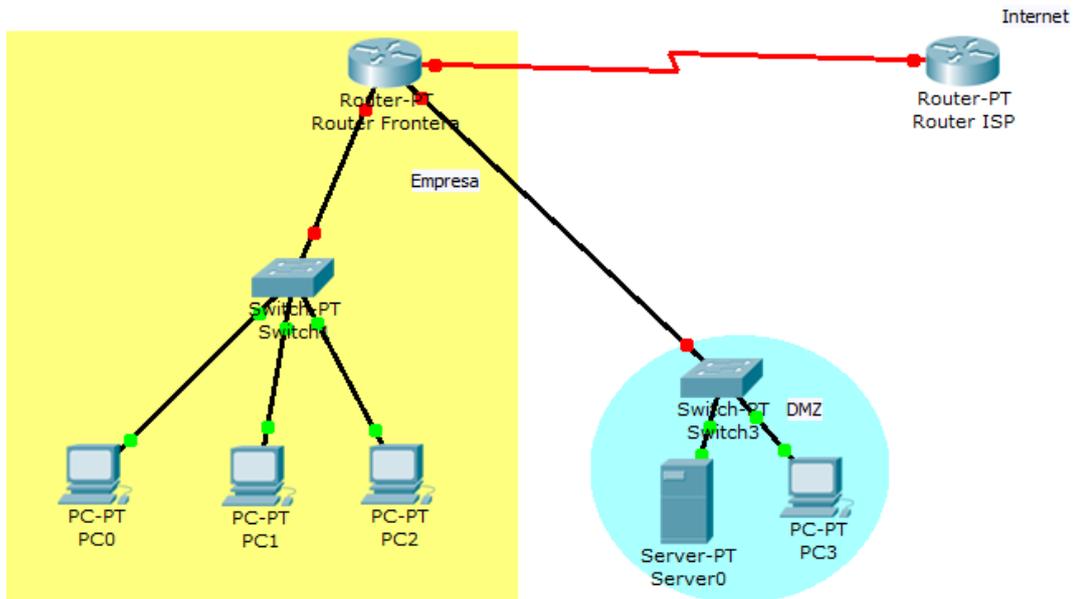
ID	Rule Name	Host	Target	Schedule	Enable
1	relax	home	parents	weekend	<input checked="" type="checkbox"/>

3. DMZ:

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

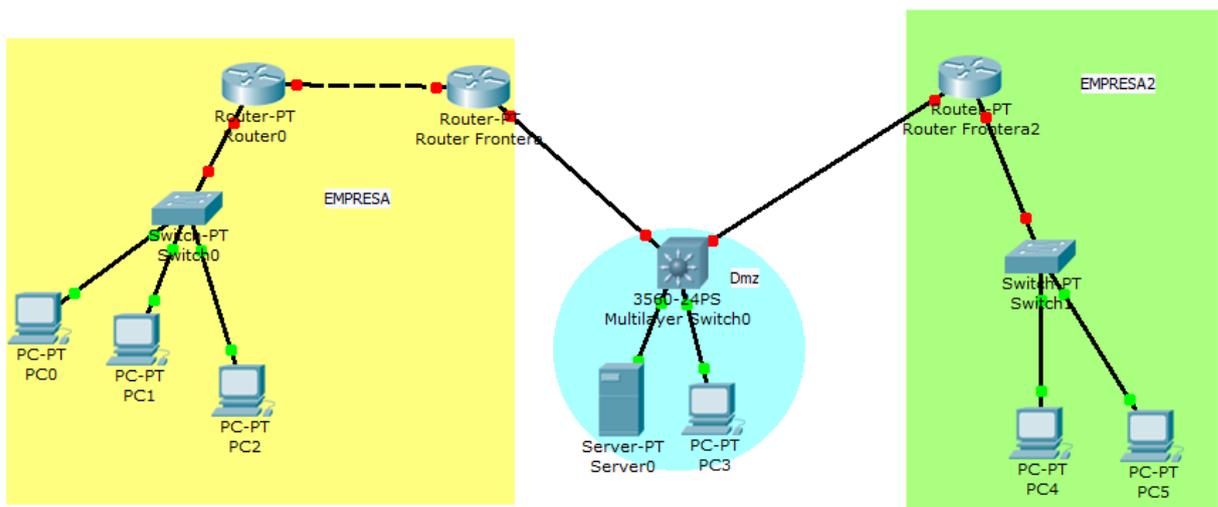
Un esquema básico de DMZ es el siguiente.

Una empresa con su red, una zona de internet o ISP y por último una DMZ donde se puede conectar con los elementos que la componen.



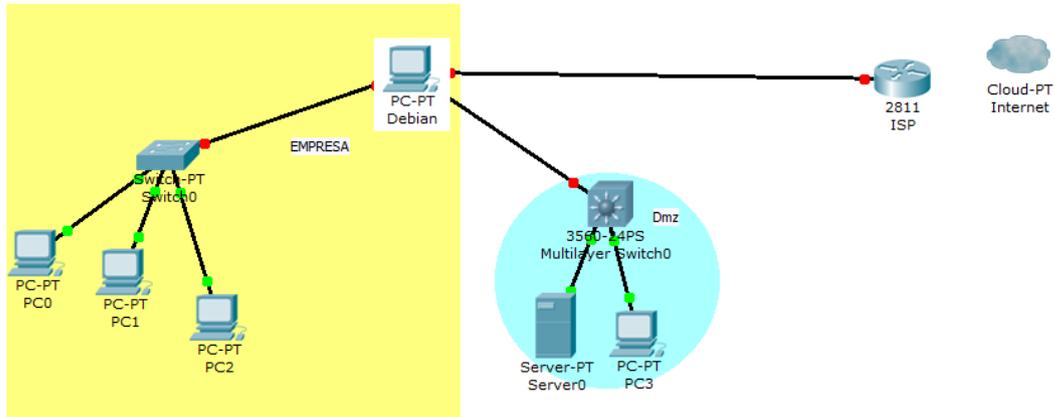
Un esquema complejo de DMZ es el siguiente.

Dos empresas empresa con sus redes, quieren acceder a los datos de la otra, para ello se implanta un DMZ para acceder a los archivos desde allí.

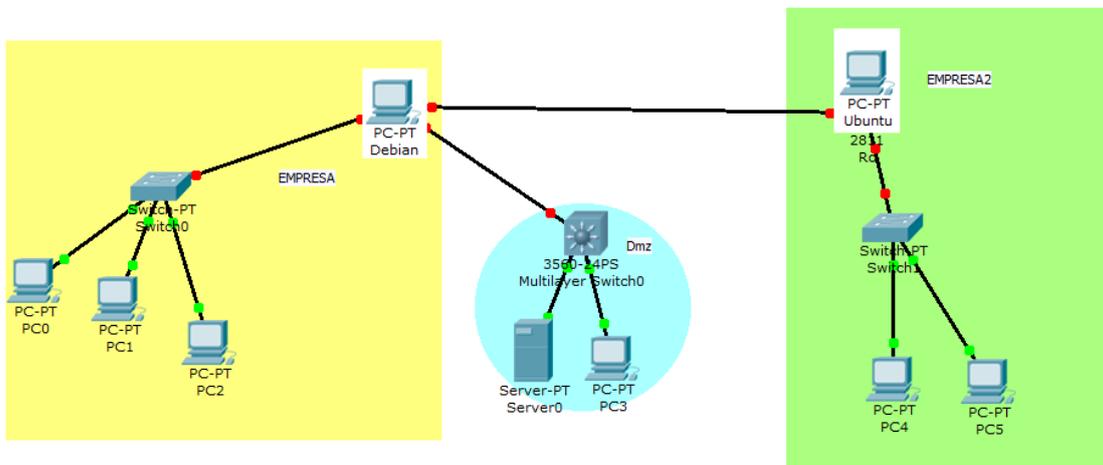


b) Planteamiento de escenarios DMZ en Linux (laboratorio virtual): esquemas.

En este esquema podemos observar una empresa, que permite el acceso de internet a archivos a través de DMZ, usando un equipo debian, con varias tarjetas de red.



En este esquema podemos ver dos empresas con sus redes, usando dos equipos Linux como fronteras, si quieren acceder a los datos de la otra, para ello se implanta un DMZ para acceder a los archivos desde allí.

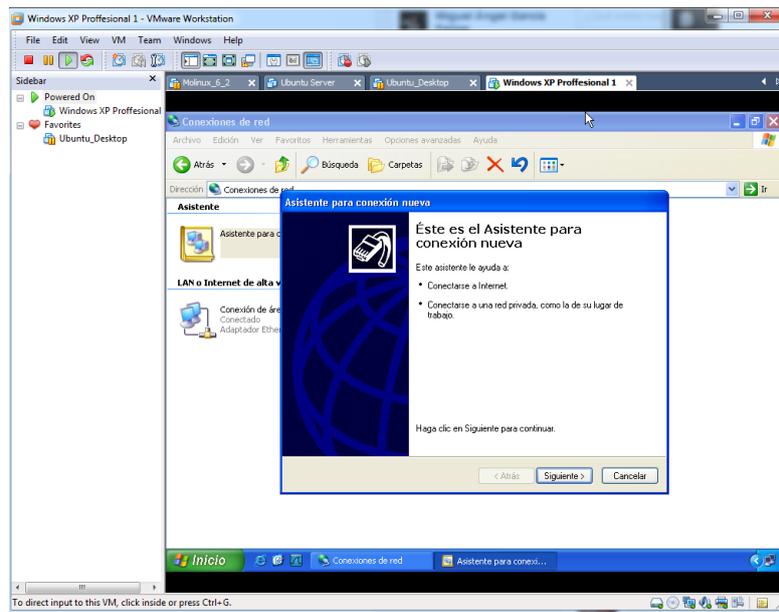


REDES PRIVADAS VIRTUALES (VPN)

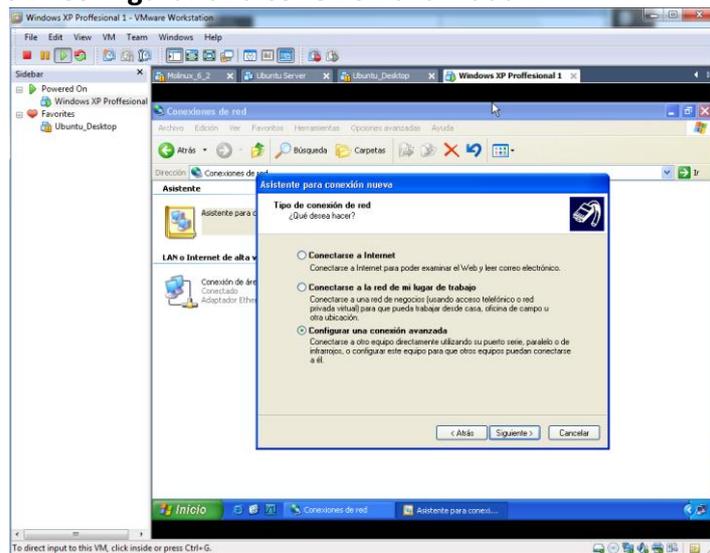
4. VPN sobre red local

a) Instalación de un servidor VPN en Windows XP.

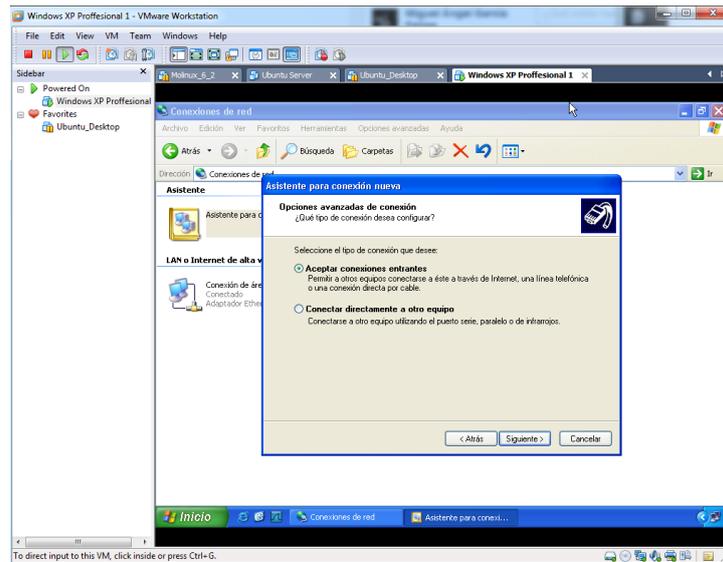
Nos situamos en conexiones de red. Seleccionamos el asistente para la conexión nueva, debe aparecer algo así.



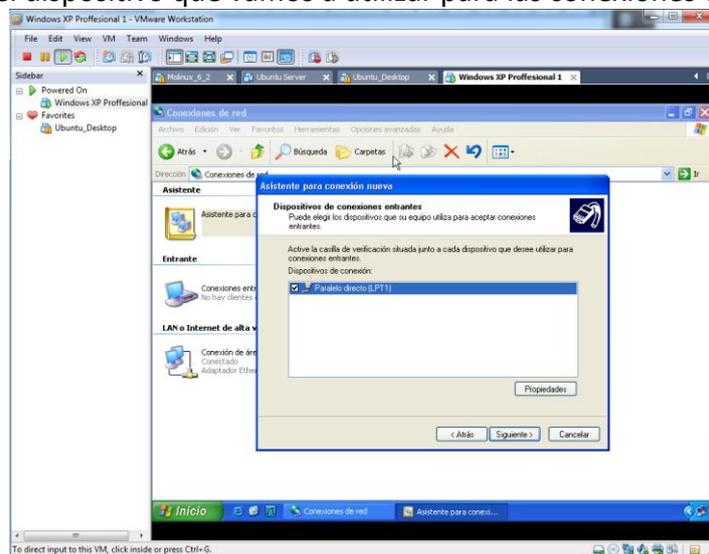
Elegimos la opción **“Configurar una conexión avanzada”**.



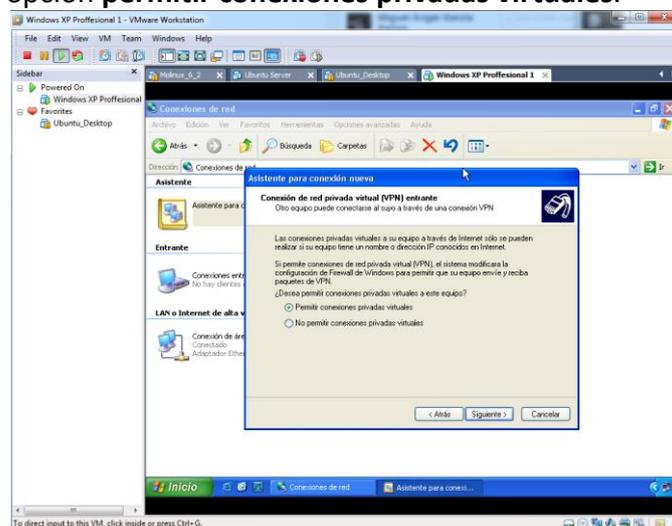
Pulsamos la opción **“Aceptar conexiones entrantes”** para permitir a otros clientes conectarse a éste a través de internet.



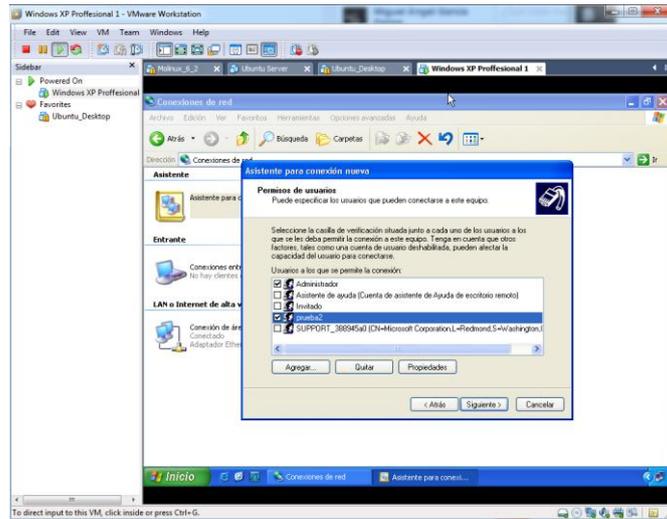
Seleccionamos el dispositivo que vamos a utilizar para las conexiones entrantes.



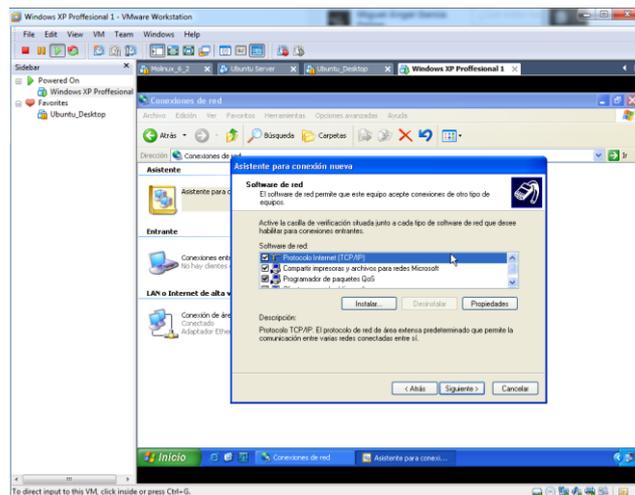
Seleccionamos la opción **permitir conexiones privadas virtuales**.



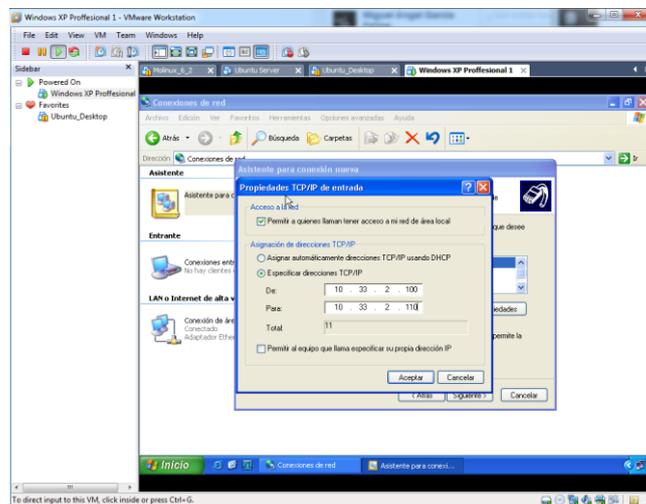
Elegimos los usuarios que pueden acceder, en nuestro caso “Administrador y prueba2”



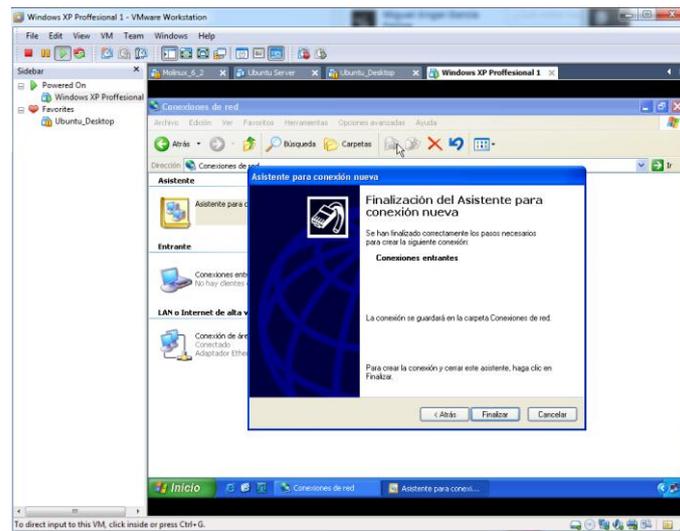
Elegimos las siguientes opciones.



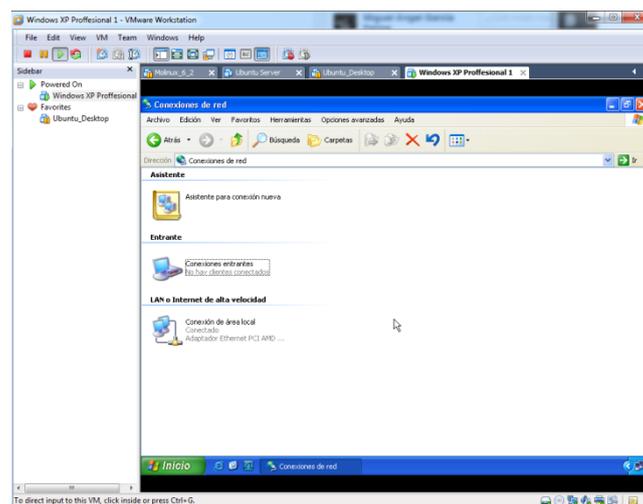
Indicamos el rango de IPS que vamos a permitir.



Finalizamos el asistente.



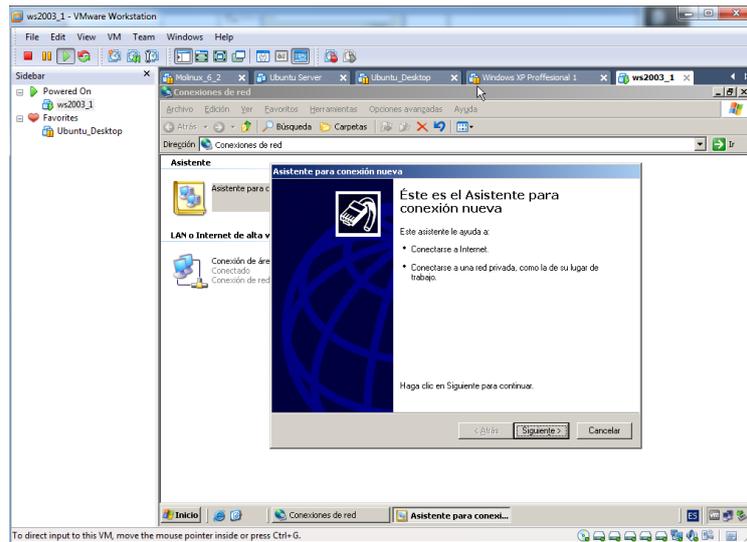
Podemos observar en las conexiones de red que nos ha creado la VPN nueva.



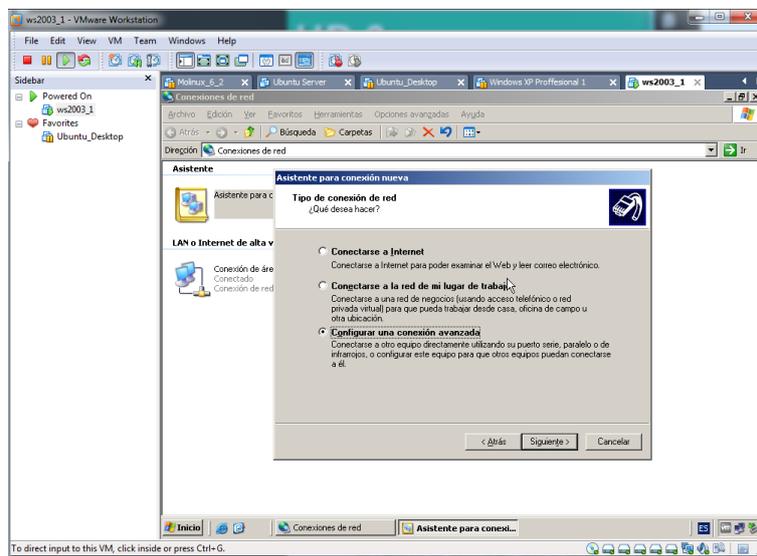
b) Instalación de un servidor VPN en Windows 2003/2008.

Nos dirigimos a las conexiones de red de nuestro Windows 2003 server.

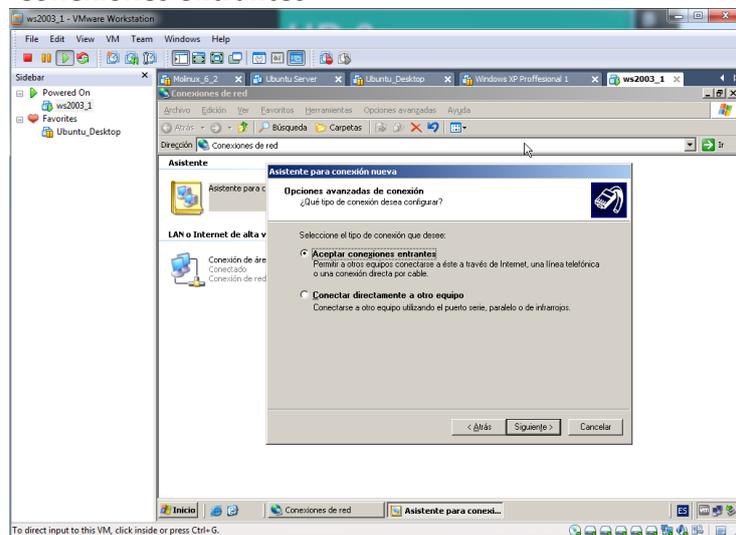
Creamos una nueva conexión a través del asistente para nuevas conexiones.



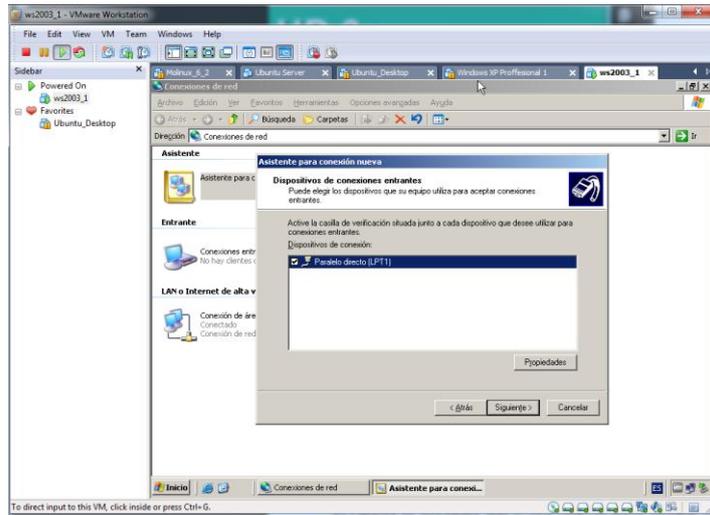
Elegimos la opción **“Configurar una conexión avanzada”**.



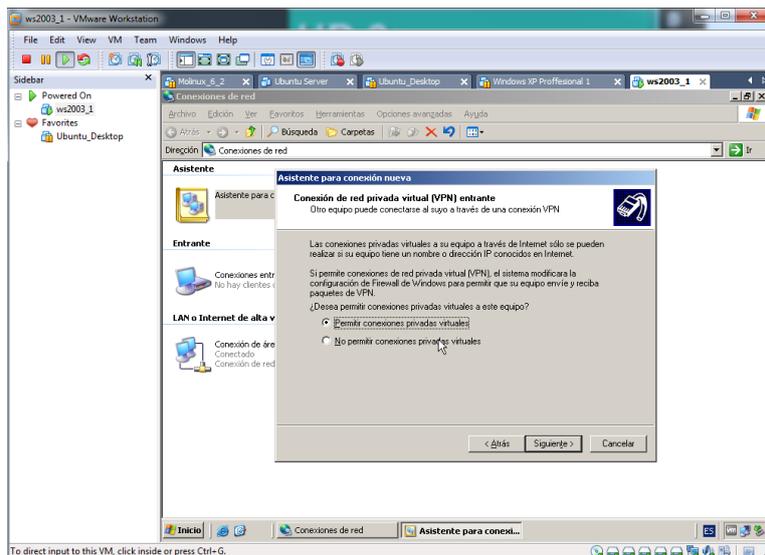
Aceptamos las **“Conexiones entrantes”**



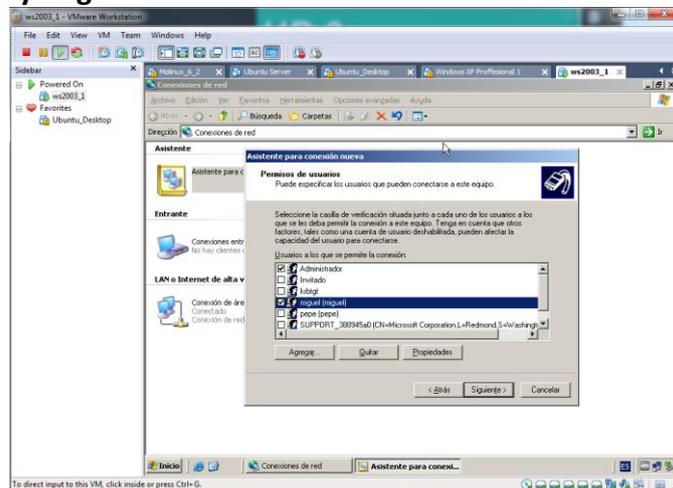
Elegimos el tipo de dispositivos entrantes que vamos a utilizar en la conexión.



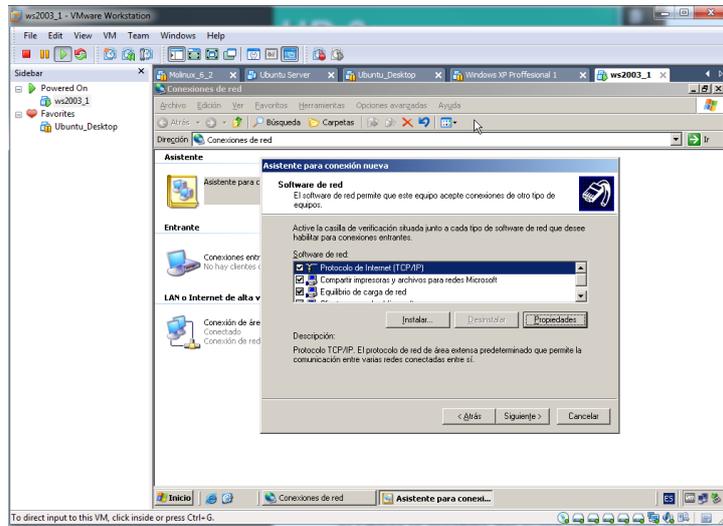
Elegimos la opción "Permitir conexiones privadas virtuales" para poder utilizar VPN.



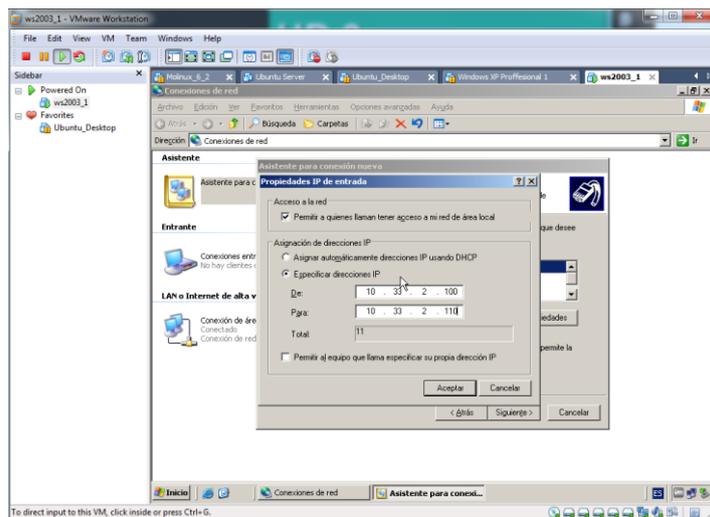
Elegimos los usuarios que podrán conectarse a este equipo, en mi caso "Administradores y Miguel".



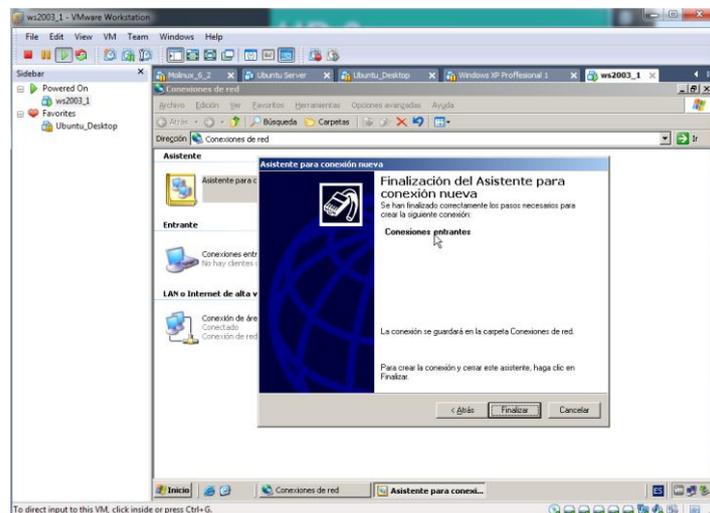
Configuramos esta ventana de la siguiente manera.



En propiedades, elegimos el rango de puertos que se usarán.



Finalizamos el asistente de configuración.



c) Instalación de un servidor VPN en GNU/Linux

Vamos a instalar el servidor VPN mediante el comando “**apt-get install pptpd**”.

```

root@alumno02: /home/alumno02
root@alumno02:/home/alumno02# 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 141 no actualizados.
Necesito descargar 116kB de archivos.
Se utilizarán 446kB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]? s
Des:1 http://repositorios.molinux.info/molinux/ merlin/main bcrelay 1386 1.3.4-2
     1ubuntu1.9.04.2 [22,7kB]
Des:2 http://repositorios.molinux.info/molinux/ merlin/main pptpd 1386 1.3.4-2.1
Documubuntu1.9.04.2 [92,9kB]
SoftDescargados 116kB en 1s (98,4kB/s)
    
```

Una vez se haya completado la instalación, nos situaremos en el directorio “**/etc/ppp**”, listamos los ficheros y directorios que lo contienen.

Editamos el fichero “**pptpd-options**” con el comando nano.

```

root@alumno02: /etc/ppp
root@alumno02:/etc/ppp# ls
chap-secrets  ip-up  ipv6-down.d  options  peers
ip-down      ip-up.d  ipv6-up      options.ppt  pppoe_on_boot
ip-down.d    ipv6-down  ipv6-up.d    pap-secrets  pptpd-options
    
```

Configuramos el fichero con los siguientes parámetros.

```

root@alumno02: /etc/ppp
Archivo  Editor  Ver  Buscar  Terminal  Ayuda
GNU nano 2.2.4 Archivo: pptpd-options

#####

Carpet
al# Authentication
# Name of the local system for authentication purposes
# (must match the second field in /etc/ppp/chap-secrets entries)

Servicio molinux02
require-mschap-v2
require-mppe-128
ms-dns 10.33.2.1
ms-dns 0.0.0.0

Documen proxyarp
Softwode defaultroute
lock

# Optional: domain name to use for authentication
# domain mydomain.net

F Ver ayuda Guardar Leer Fich RePág Cortar Tex Pos actual
X Salir Justificar Buscar Pág. Sig PegarTxt Ortografía

104 líneas escritas

```

Ahora, nos situamos en el fichero “**pptpd.conf**” del directorio “**/etc**”, y hacemos las siguientes configuraciones.

```

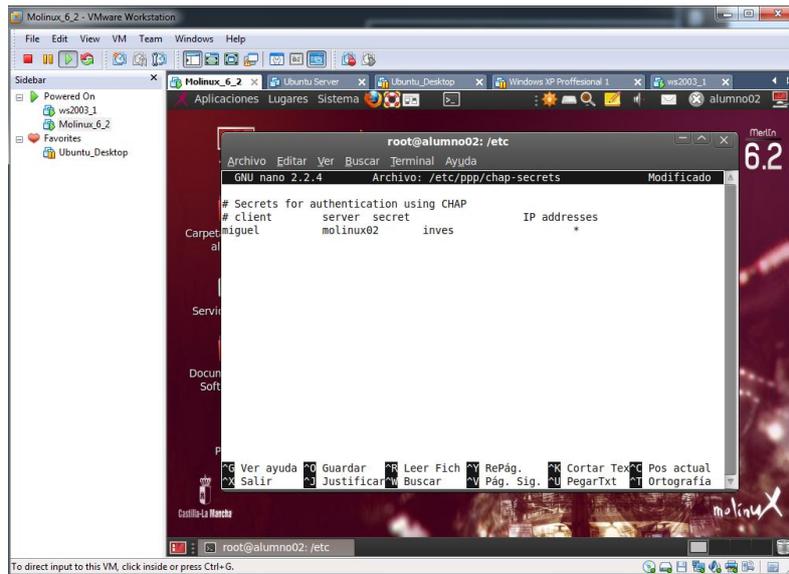
root@alumno02: /etc
Archivo  Editor  Ver  Buscar  Terminal  Ayuda
GNU nano 2.2.4 Archivo: pptpd.conf Modificado

#
# 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

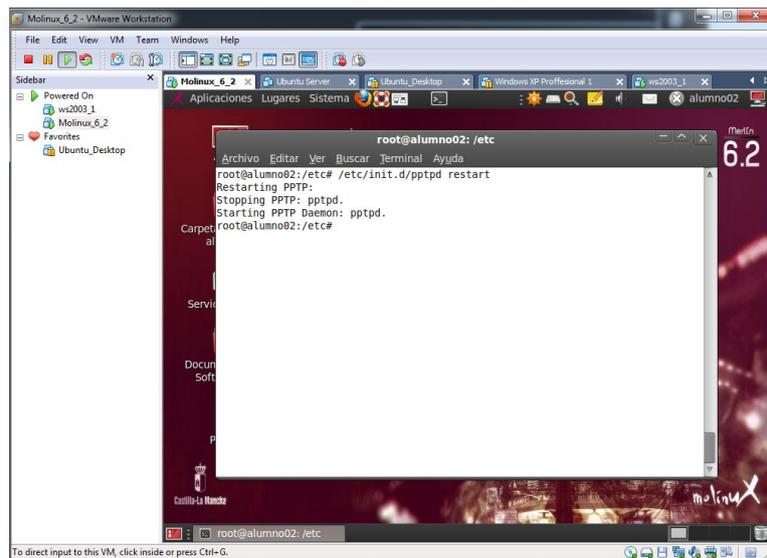
ppp /usr/sbin/pppd
option /etc/ppp/pptpd-options
localip 10.33.2.1
remoteip 10.33.2.20-70

```

Nos cambiamos al directorio “**/etc/ppp**” y editamos el fichero “**chap-secrets**”, dónde le asignamos un nombre de usuario, nombre de máquina y contraseña.



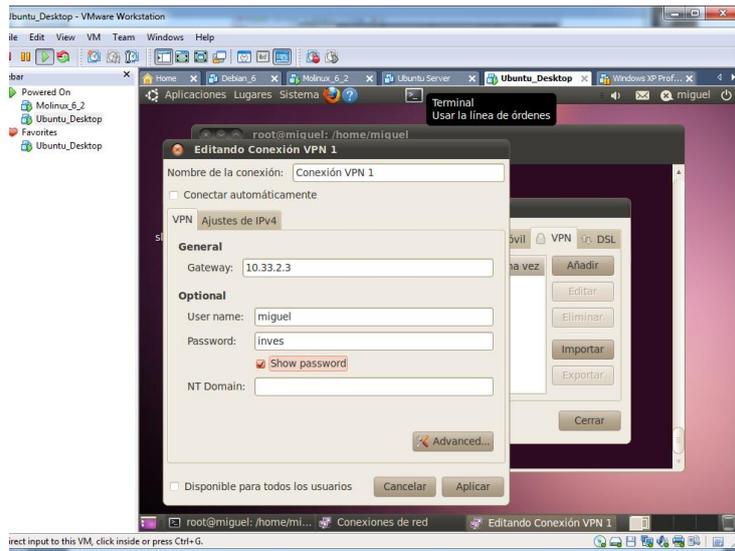
Una vez configurado todos los ficheros anteriores, reiniciamos el servicio, con el comando **“/etc/init.d/pppd restart”**



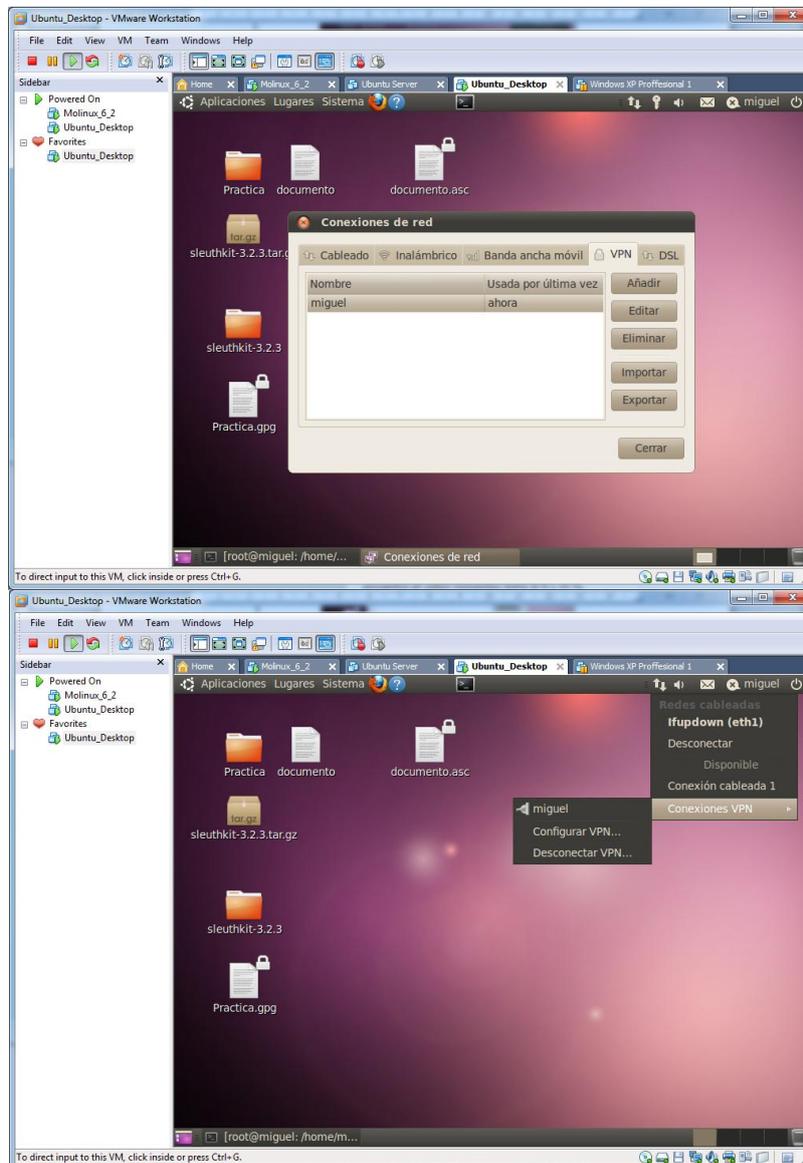
Abrimos un cliente Ubuntu, y configuramos el cliente VPN.

Elegimos el tipo de conexión VPN (**PPTP**)

Editamos las conexiones VPN, elegimos la puerta de enlace a la que nos vamos a conectar con su respectivo usuario y contraseña.

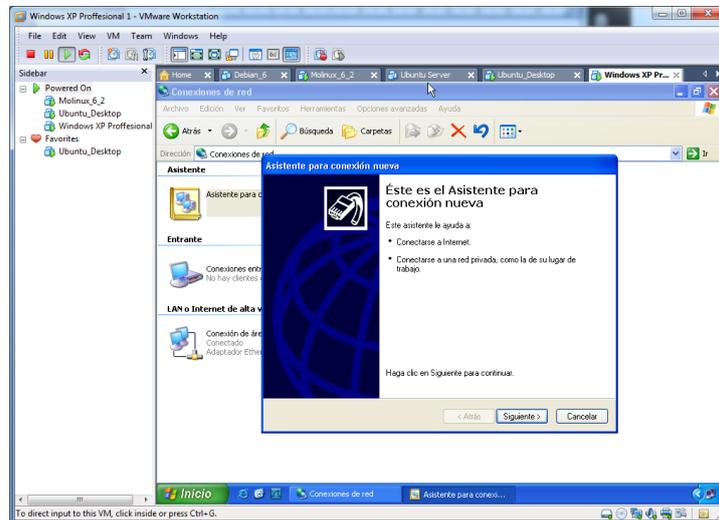


Una vez aplicado los cambios, arrancamos la conexión.

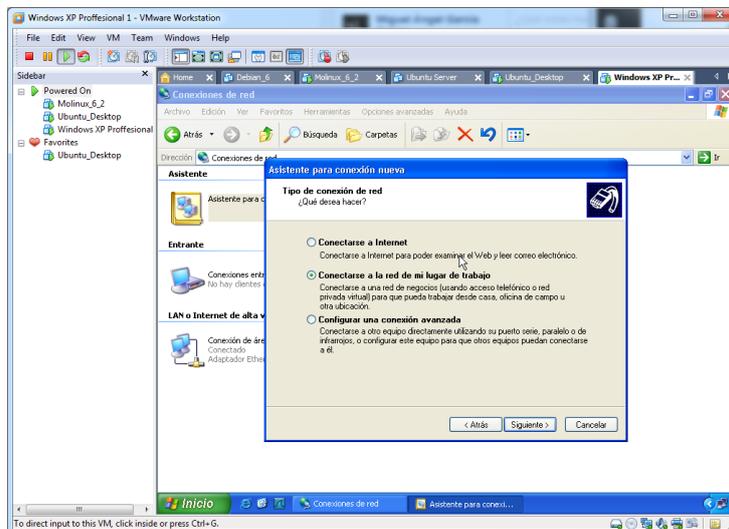


d) Conexión desde un cliente Windows y GNU/Linux VPN a un servidor VPN.

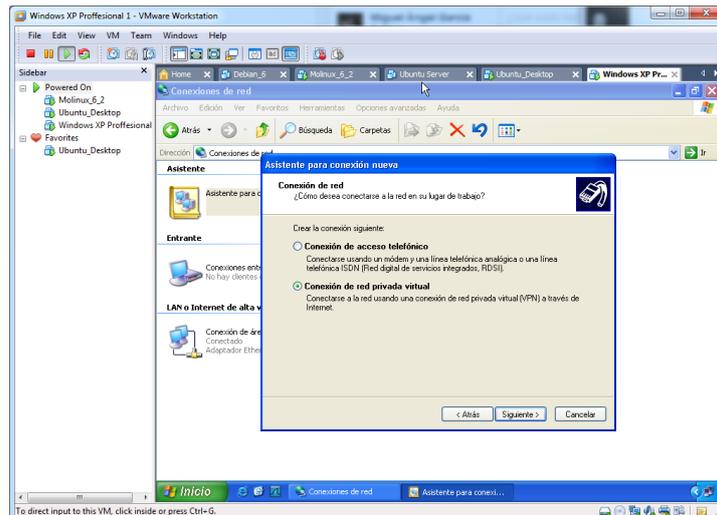
En conexiones de red de un XP, creamos una nueva conexión con el asistente de conexión nueva.



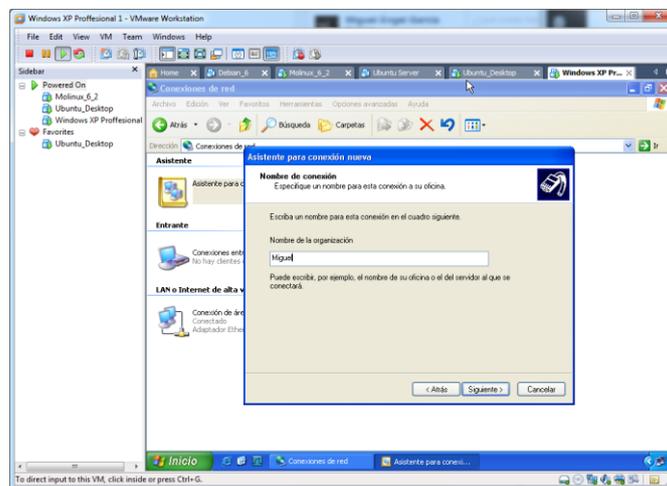
Elegimos la opción “Conectarse a la red de mi lugar de trabajo”



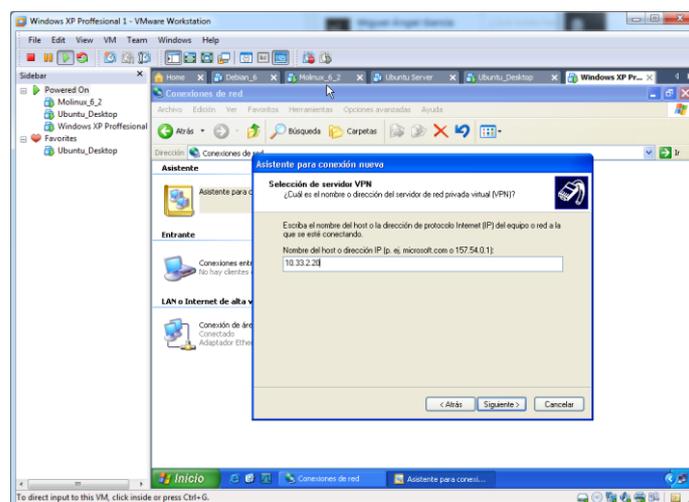
Seguidamente elegimos la opción “Conexión de red privada virtual” para conectarse a la red usando VPN a través de Internet.



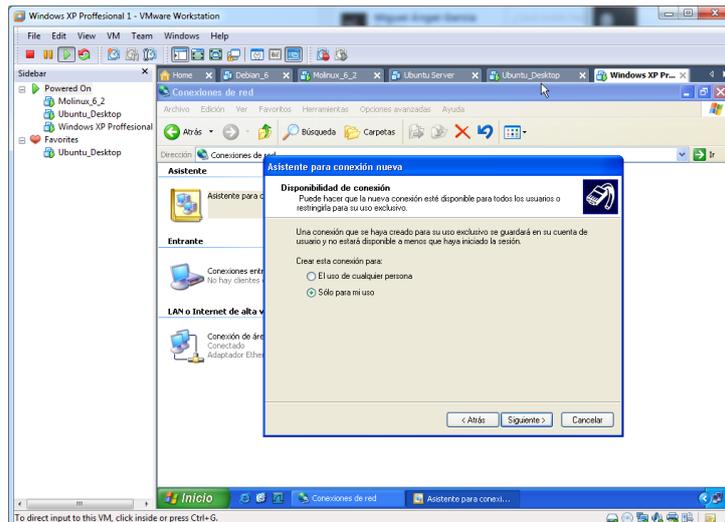
Pulsamos siguiente, y nos desplegará la siguiente ventana. Escribimos un nombre de organización para la conexión.



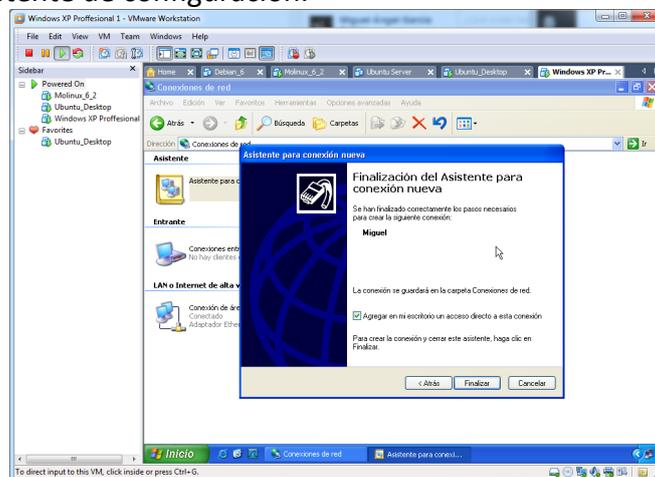
Escribimos la dirección IP del host al que nos vamos a conectar.



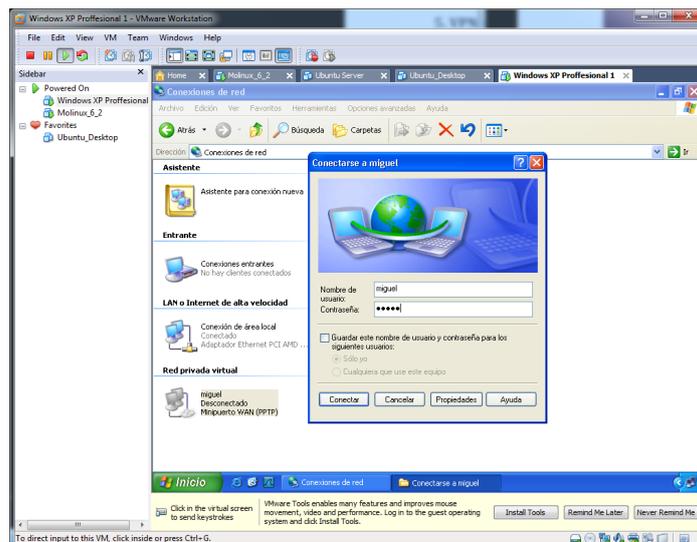
Elegimos la segunda opción, “Sólo para mi uso”



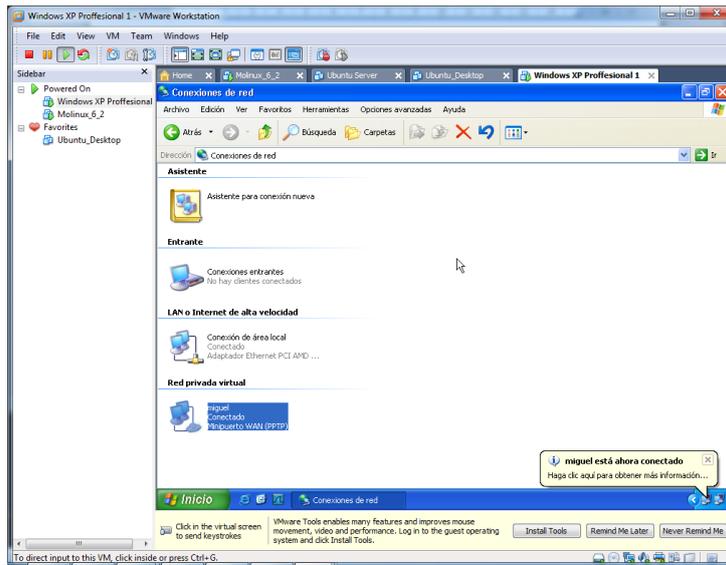
Finalizamos el asistente de configuración.



Establecemos el usuario y la contraseña



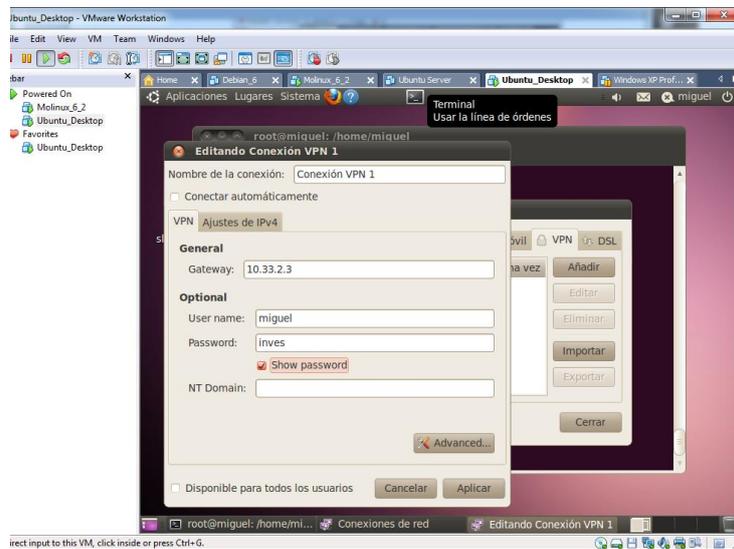
Comprobamos que se ha establecido la conexión con éxito.



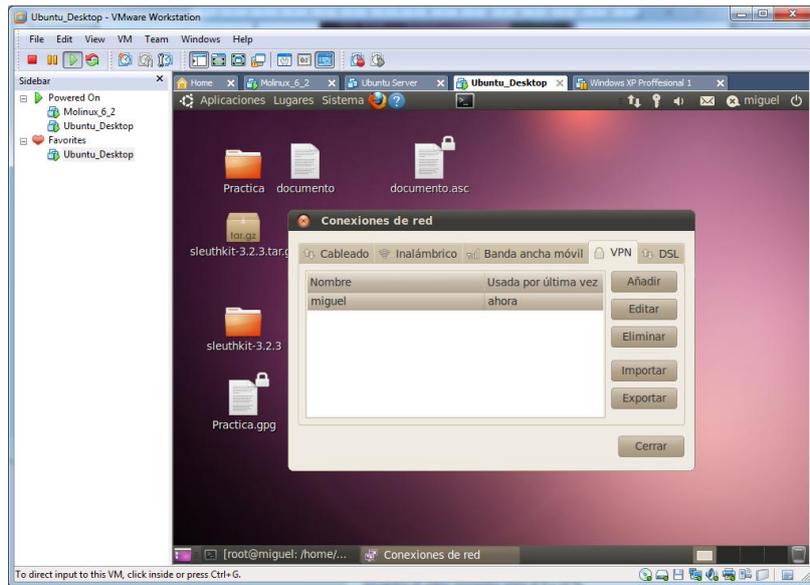
Abrimos un cliente Ubuntu, y configuramos el cliente VPN.

Elegimos el tipo de conexión VPN (**PPTP**)

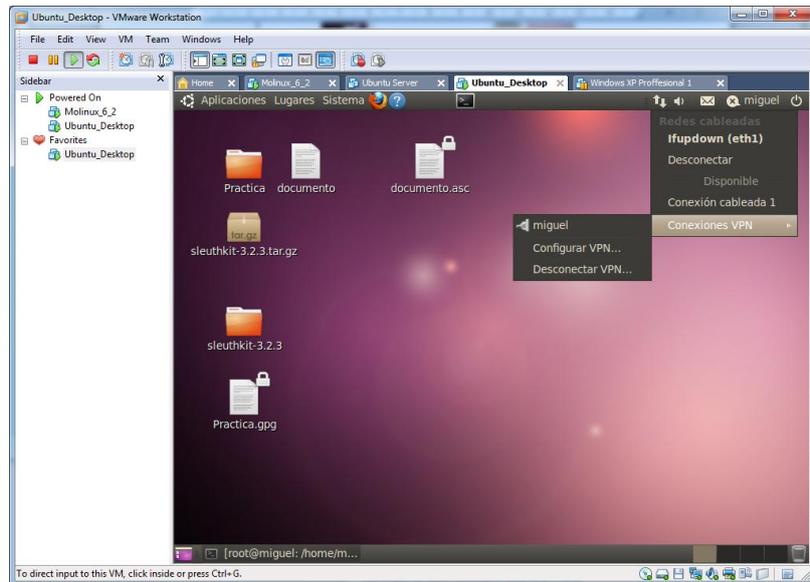
Editamos las conexiones VPN, elegimos la puerta de enlace a la que nos vamos a conectar con su respectivo usuario y contraseña.



Una vez aplicado los cambios, arrancamos la conexión.



Esperamos a que se conecte.

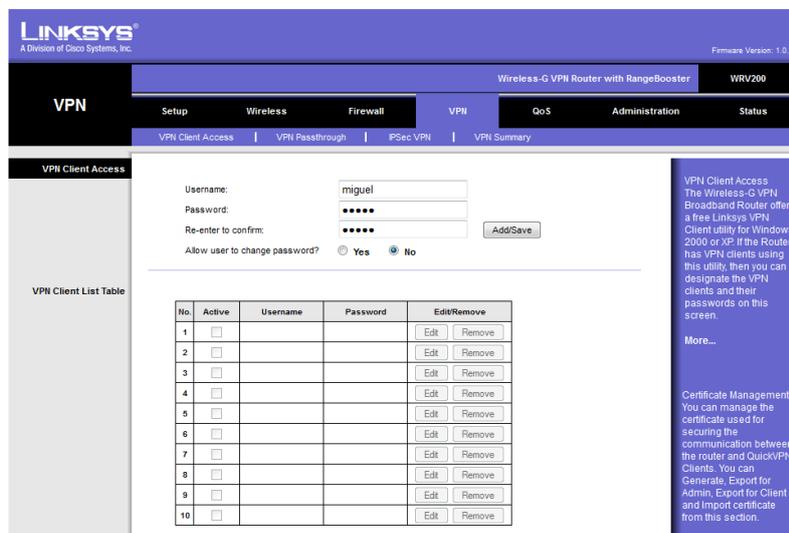


5. VPN de acceso remoto

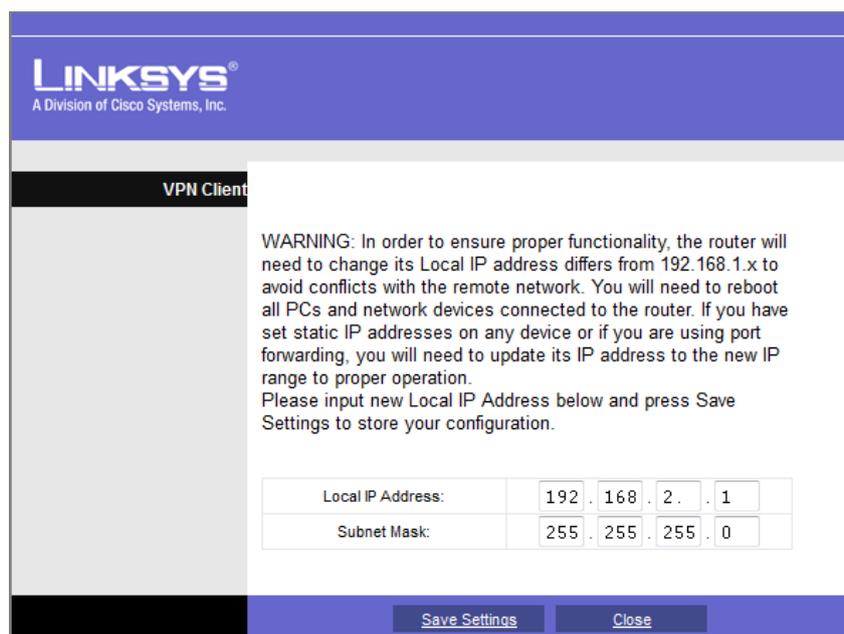
a) Utiliza la plantilla del curso virtual para configurar los parámetros.

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

En la pestaña VPN, cliente de acceso, nos creamos un nombre de usuario con su contraseña

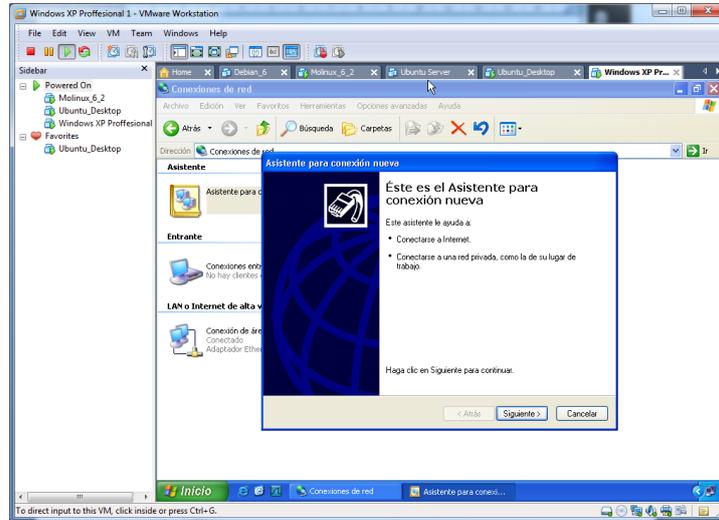


Una vez pulsado el botón “ADD” configuramos la IP a través de la siguiente pantalla.

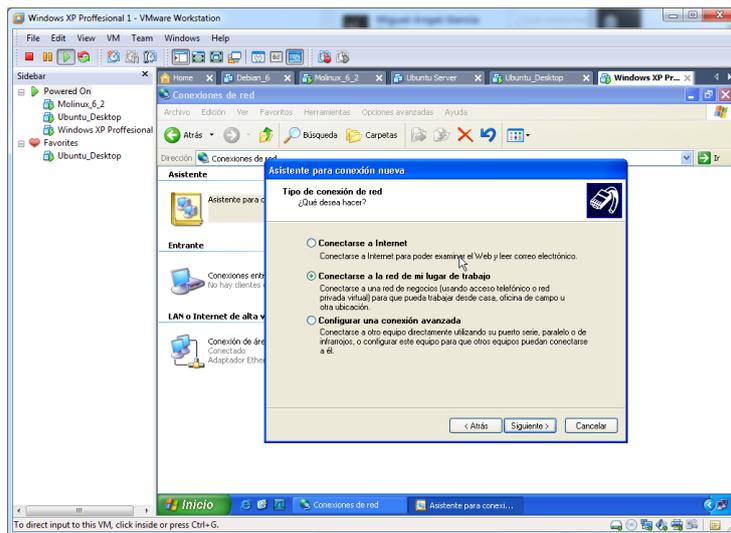


c) Configura tu cliente VPN en Windows.

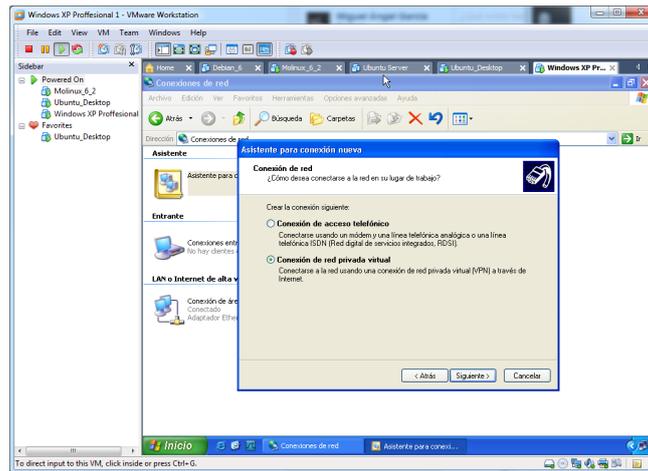
En conexiones de red de un XP, creamos una nueva conexión con el asistente de conexión nueva.



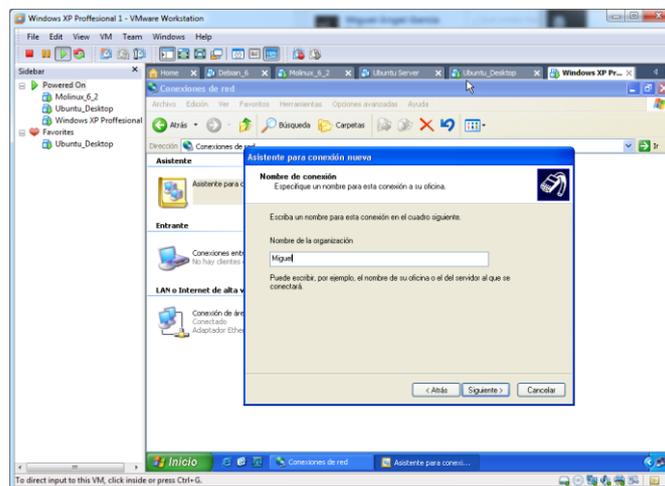
Elegimos la opción **“Conectarse a la red de mi lugar de trabajo”**



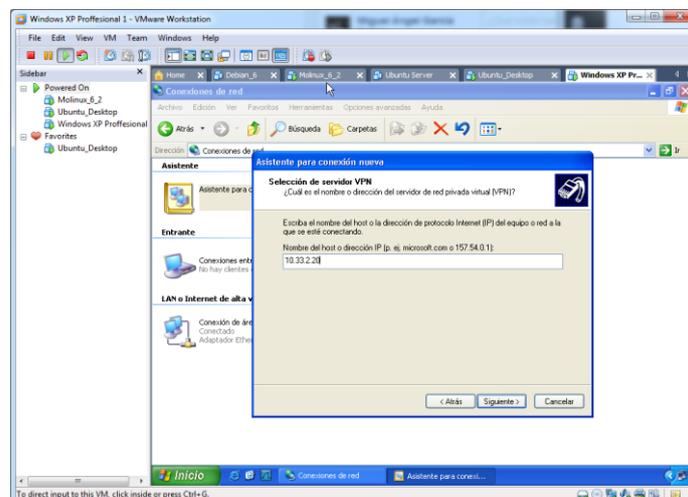
Seguidamente elegimos la opción **“Conexión de red privada virtual”** para conectarse a la red usando VPN a través de Internet.



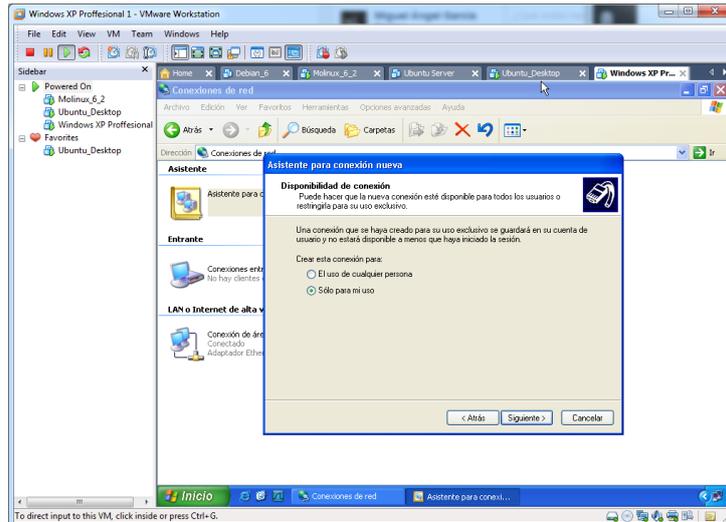
Pulsamos siguiente, y nos desplegará la siguiente ventana. Escribimos un nombre de organización para la conexión.



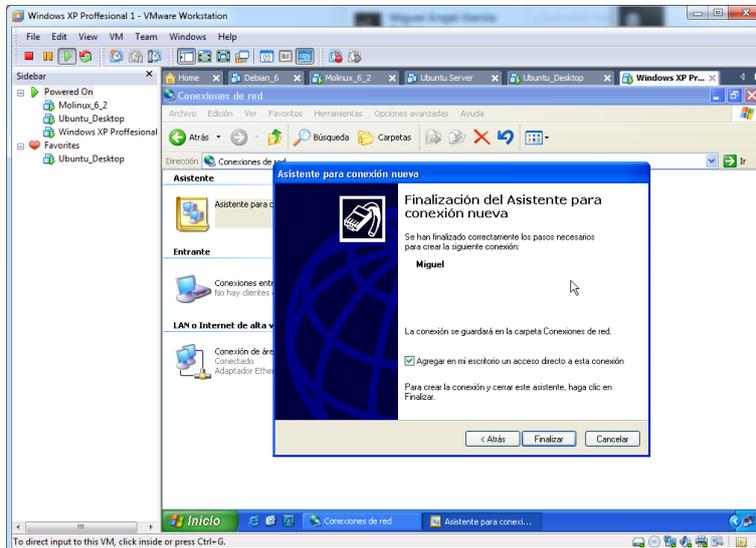
Escribimos la dirección IP del host al que nos vamos a conectar.



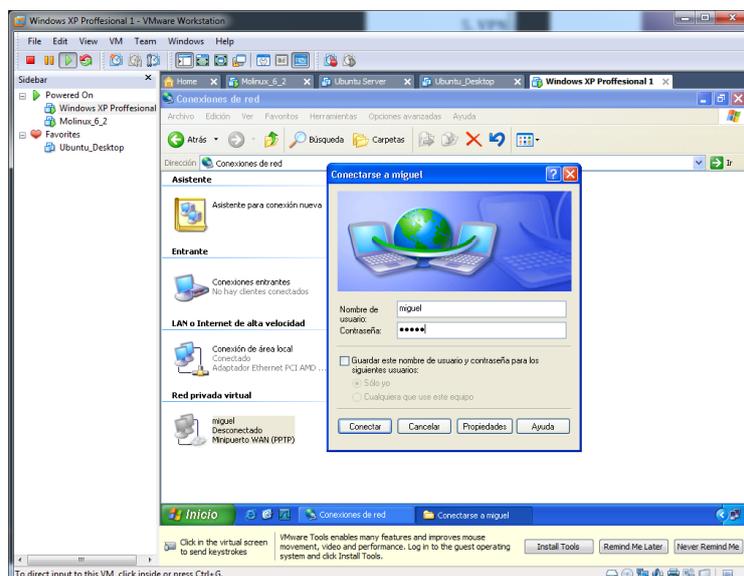
Elegimos la segunda opción, **“Sólo para mi uso”**



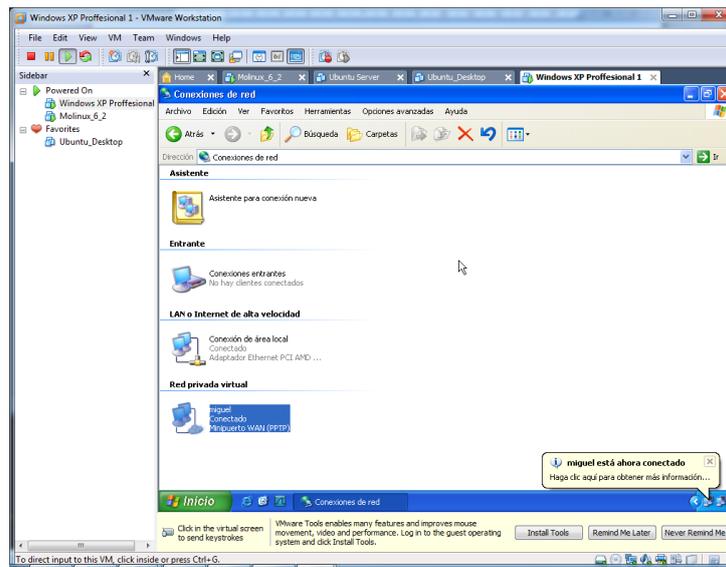
Finalizamos el asistente de configuración.



Establecemos el usuario y la contraseña



Comprobamos que se ha establecido la conexión con éxito.



6. VPN sitio a sitio

a) Utiliza la plantilla del curso virtual para configurar los parámetros.

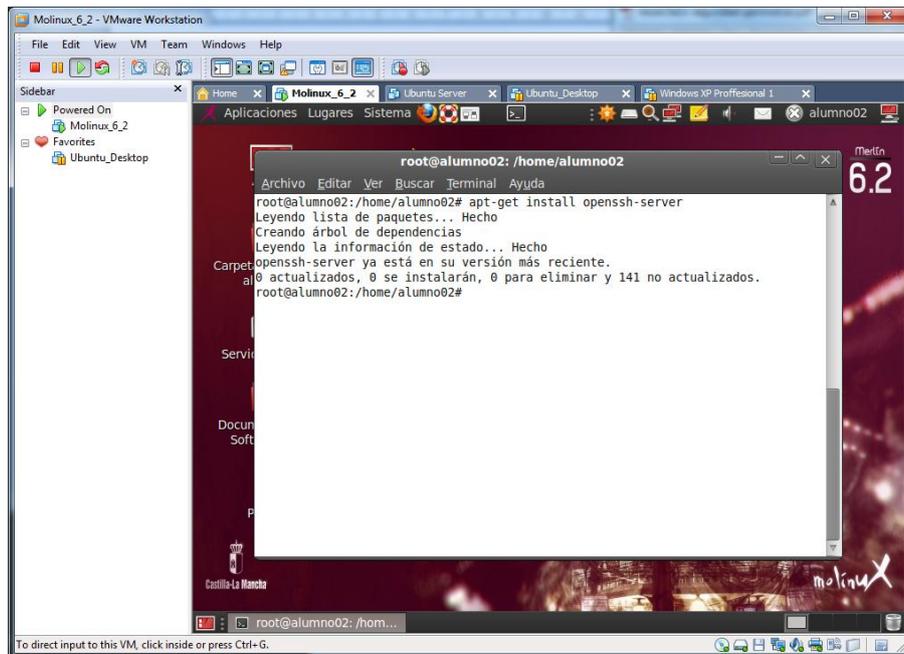
b) En cada sitio existe un router Linksys RV042.
Configurar cada sitio - router Linksys RV042 utilizando el simulador

TECNICAS DE CIFRADO: COMUNICACIONES SEGURAS

7. SSH

a) Instalación del servidor SSH en GNU/Linux

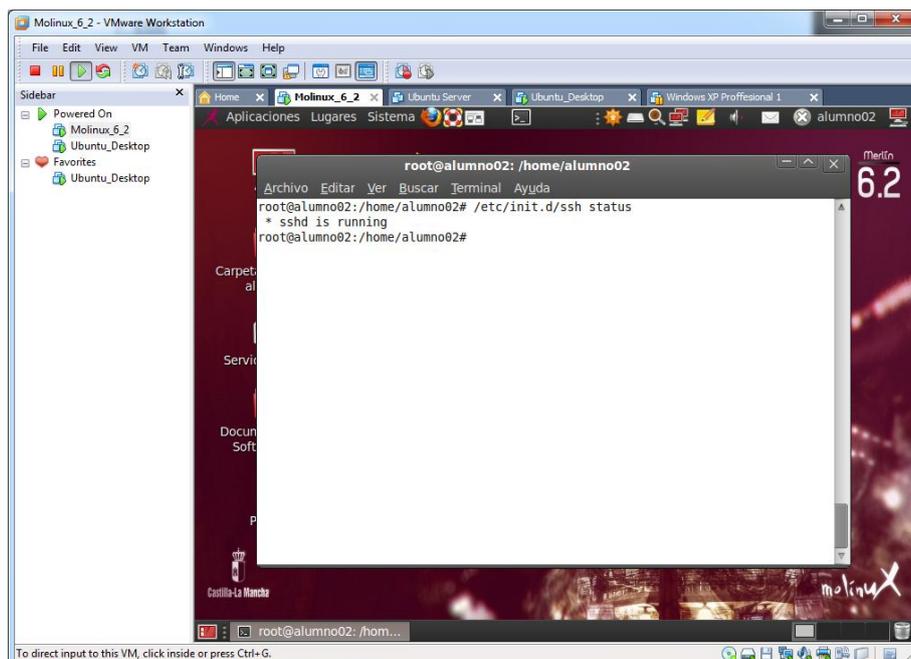
Instalamos el servidor ssh con el comando “**apt-get install openssh-server**”



The screenshot shows a terminal window within a VMware Workstation environment. The terminal prompt is root@alumno02: /home/alumno02. The user enters the command apt-get install openssh-server. The output shows the package list being read, dependencies being created, and the state information being read. The terminal indicates that openssh-server is already installed at its latest version. The terminal output is as follows:

```
root@alumno02: /home/alumno02# apt-get install openssh-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
openssh-server ya está en su versión más reciente.
0 actualizados, 0 se instalarán, 0 para eliminar y 141 no actualizados.
root@alumno02: /home/alumno02#
```

Comprobamos el estado del servidor ssh con el comando “**/etc/init.d/ssh status**”

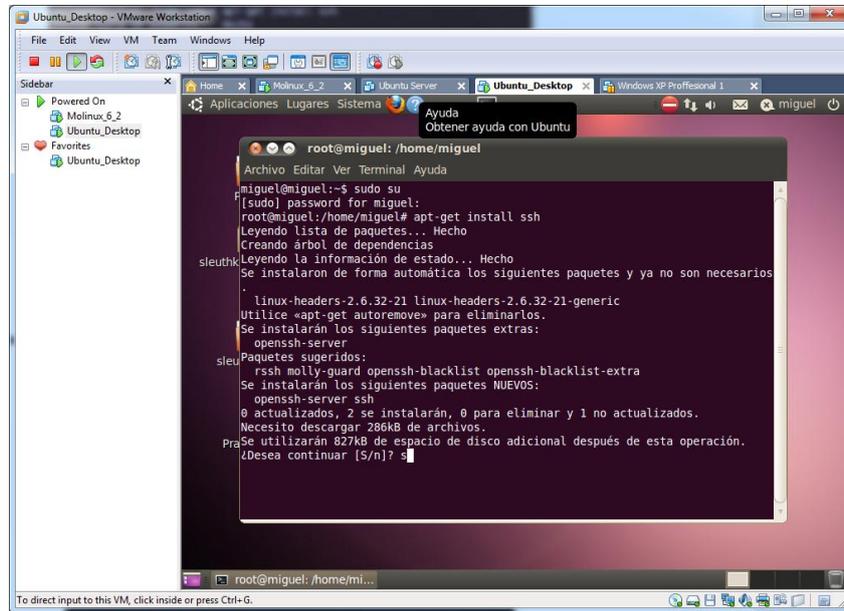


The screenshot shows the same terminal window as above, but now the user has entered the command /etc/init.d/ssh status. The output shows that the sshd service is running. The terminal output is as follows:

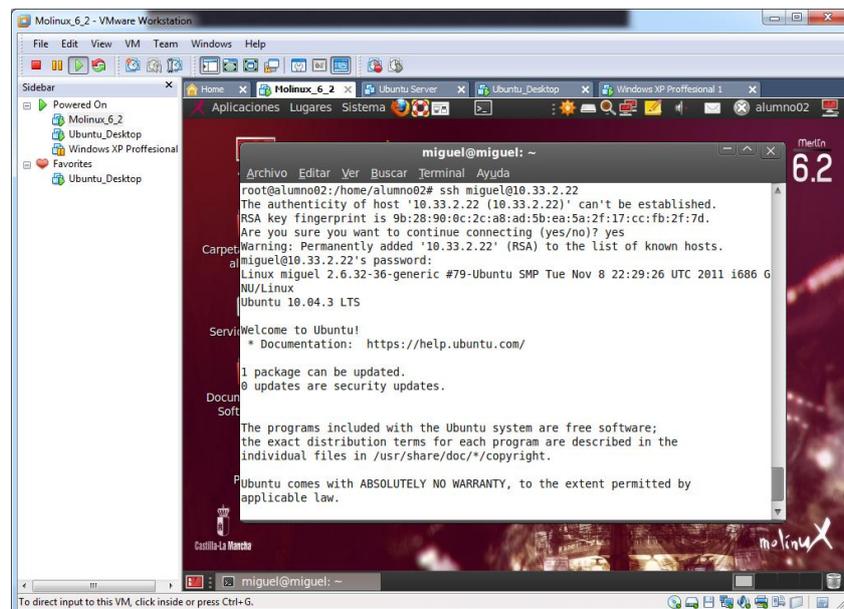
```
root@alumno02: /home/alumno02# /etc/init.d/ssh status
* sshd is running
root@alumno02: /home/alumno02#
```

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

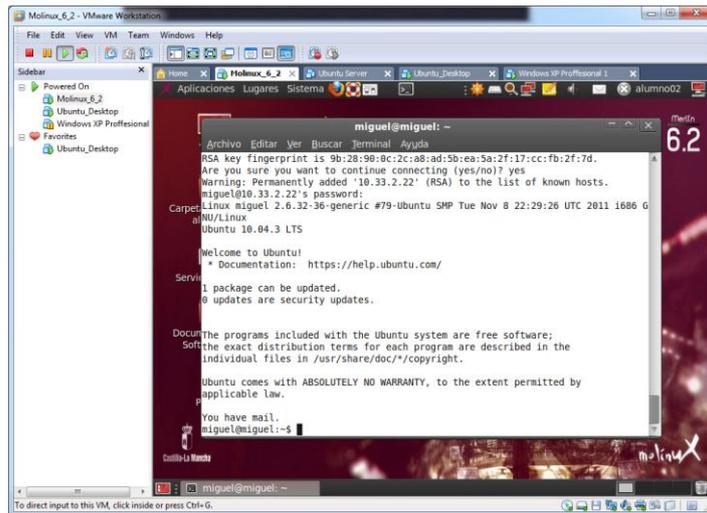
Tenemos instalado el servidor SSH.



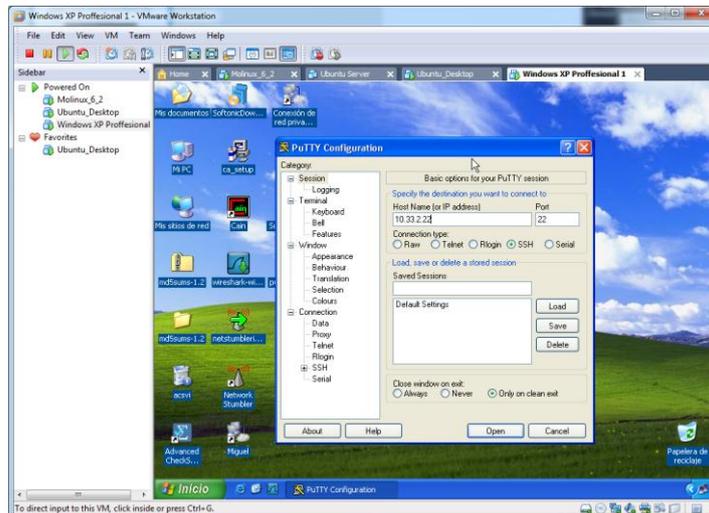
Desde un cliente, ejecutamos “ssh miguel@10.33.2.22” esto nos permitirá conectarnos mediante el cliente miguel al pc (10.33.2.22) y así realizar operaciones remotas.



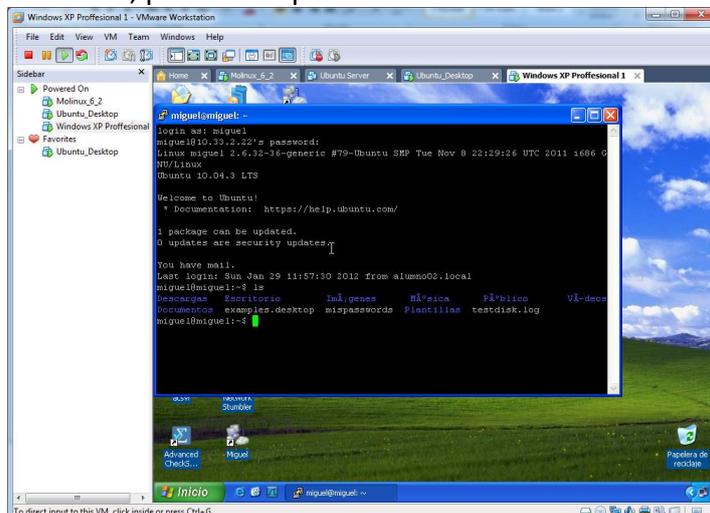
Comprobamos que está conectado.



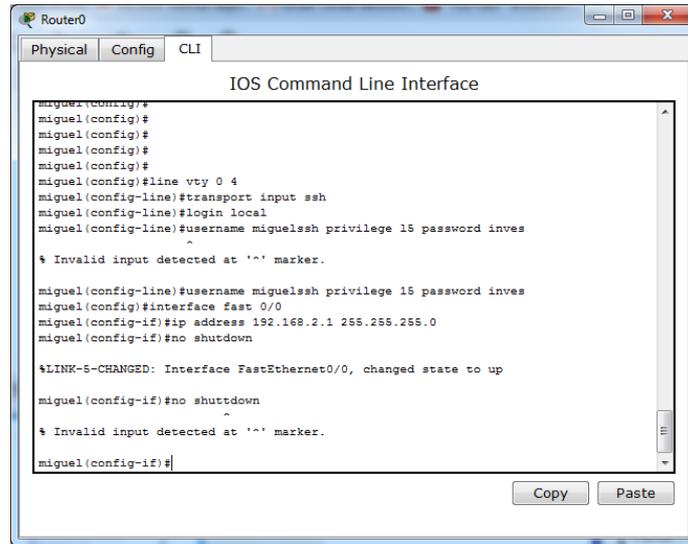
Por el contrario, si queremos conectarnos desde un cliente Windows, debemos instalarnos la aplicación “**putty**” para poder conectarnos al servidor Linux mediante **SSH**. Nos conectamos mediante la IP del servidor usando el puerto 22.



Una vez conectados a la consola, elegimos el usuario, ingresamos la contraseña, y una vez tengamos la conexión, podemos operar remotamente con el servidor.



Establecemos la IP al router, en su correspondiente interfaz. Y guardamos los cambios



The screenshot shows the 'Router0' window with the 'CLI' tab selected. The title bar reads 'IOS Command Line Interface'. The terminal text is as follows:

```
miguel(config)#
miguel(config)#
miguel(config)#
miguel(config)#
miguel(config)#line vty 0 4
miguel(config-line)#transport input ssh
miguel(config-line)#login local
miguel(config-line)#username miguelssh privilege 15 password inves
^
% Invalid input detected at '^' marker.

miguel(config-line)#username miguelssh privilege 15 password inves
miguel(config)#interface fast 0/0
miguel(config-if)#ip address 192.168.2.1 255.255.255.0
miguel(config-if)#no shutdown

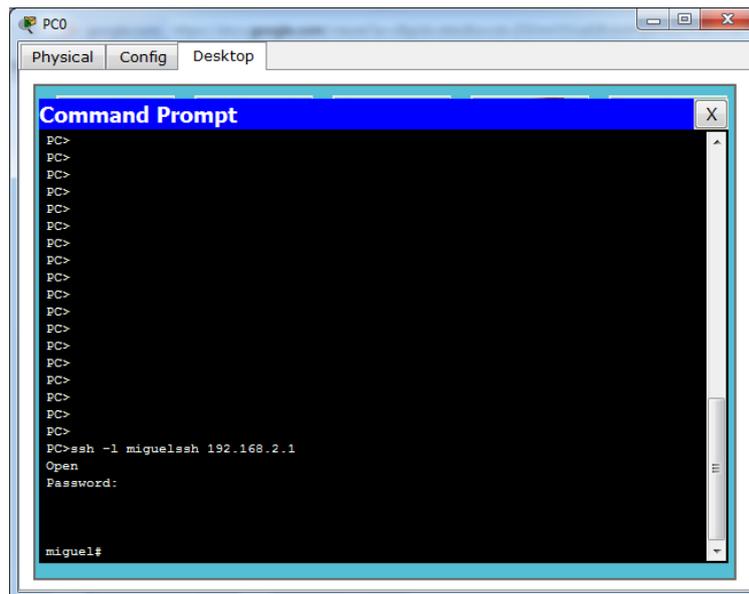
%LINK-6-CHANGED: Interface FastEthernet0/0, changed state to up

miguel(config-if)#no shutdown
^
% Invalid input detected at '^' marker.

miguel(config-if)#
```

Buttons for 'Copy' and 'Paste' are visible at the bottom right of the window.

En el cliente, con la IP ya configurada, abrimos el terminal, y accedemos mediante ssh al router.



The screenshot shows the 'PC0' window with the 'Desktop' tab selected. A 'Command Prompt' window is open, displaying the following text:

```
PC>
PC>ssh -l miguelssh 192.168.2.1
Open
Password:

miguel#
```

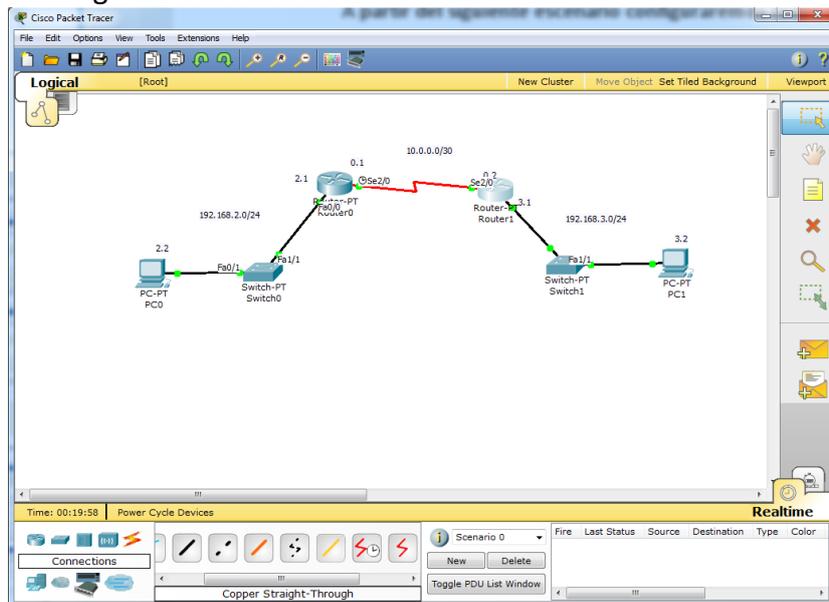
SERVIDORES DE ACCESO REMOTO

8. Protocolos de autenticación:

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

PPP

Configuramos el siguiente escenario.



Configuramos el router 1, estableciendo el enrutamiento correcto.

Static Routes

Network	192.168.2.0
Mask	255.255.255.0
Next Hop	10.0.0.1

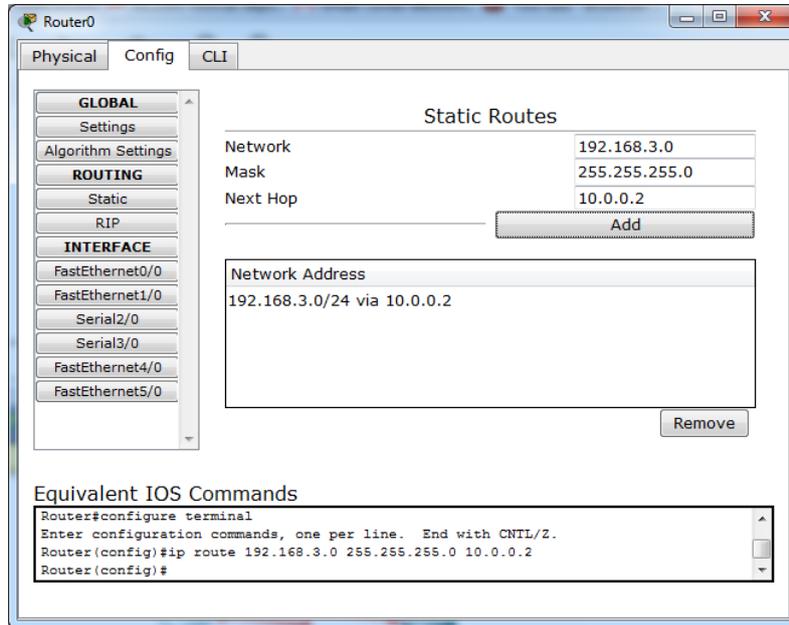
Network Address

192.168.2.0/24 via 10.0.0.1

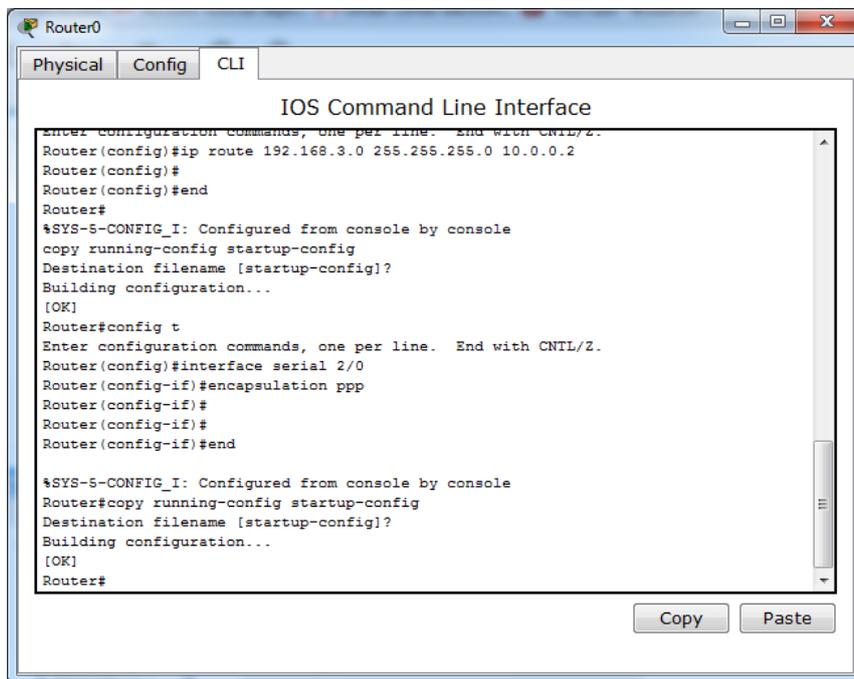
Equivalent IOS Commands

```
Router(config-router)#
Router(config-router)#exit
Router(config)#ip route 192.168.2.0 255.255.255.0 10.0.0.1
Router(config)#
```

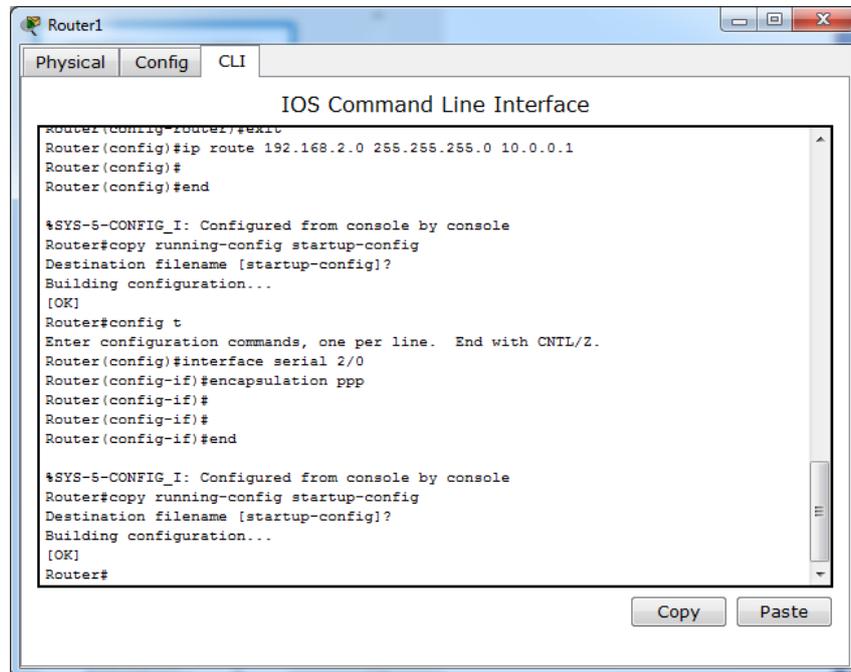
Configuramos el router 0, estableciendo el enrutamiento correcto.



Configuramos el serial 2/0 con el protocolo de encapsulación ppp en el router 0.

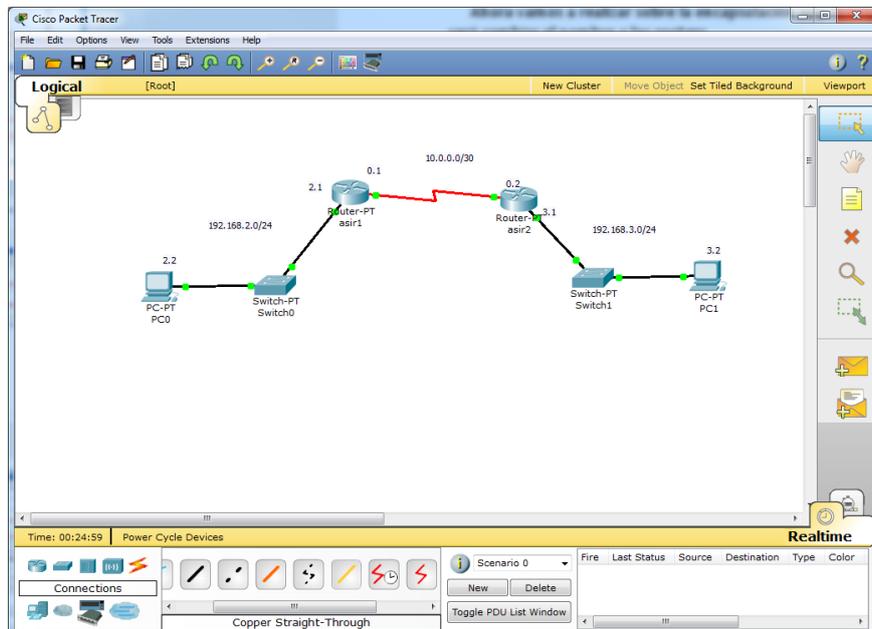


Configuramos el serial **2/0** con el protocolo de encapsulación **ppp** en el **router 1**.

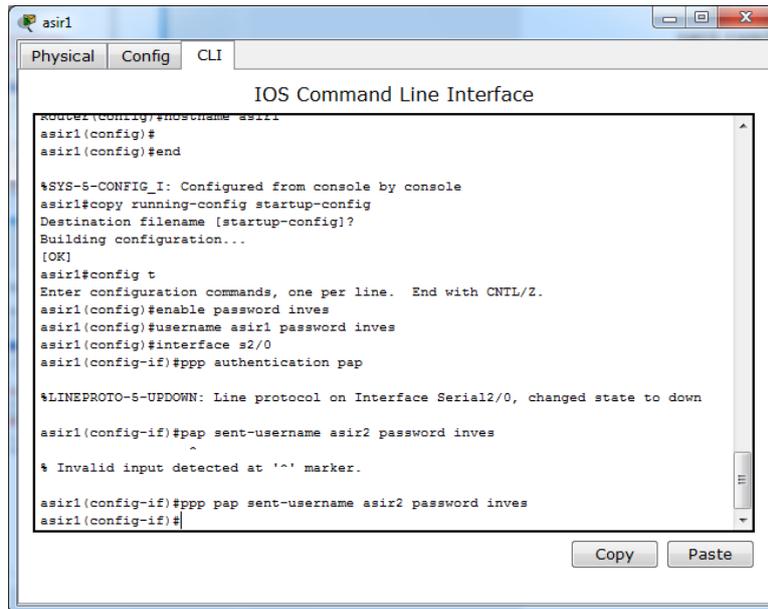


Autenticación PAP

Cambiamos el nombre de los routers (**hostname**)



En el router **asir1** habilitamos una contraseña, y un usuario. En la interfaz **serial 2/0** establecemos el protocolo de autenticación pap.



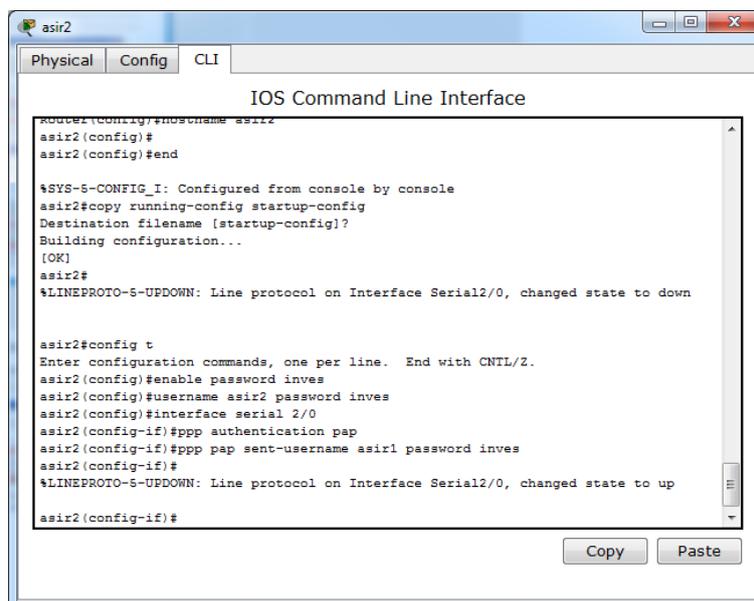
```
asir1
Physical Config CLI
IOS Command Line Interface
Router(config)#hostname asir1
asir1(config)#
asir1(config)#end

%SYS-5-CONFIG_I: Configured from console by console
asir1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
asir1#config t
Enter configuration commands, one per line. End with CNTL/Z.
asir1(config)#enable password inves
asir1(config)#username asir1 password inves
asir1(config)#interface s2/0
asir1(config-if)#ppp authentication pap

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down

asir1(config-if)#pap sent-username asir2 password inves
^
% Invalid input detected at '^' marker.
asir1(config-if)#ppp pap sent-username asir2 password inves
asir1(config-if)#
```

En el router **asir2** habilitamos una contraseña, y un usuario. En la interfaz **serial 2/0** establecemos el protocolo de autenticación pap.



```
asir2
Physical Config CLI
IOS Command Line Interface
Router(config)#hostname asir2
asir2(config)#
asir2(config)#end

%SYS-5-CONFIG_I: Configured from console by console
asir2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
asir2#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down

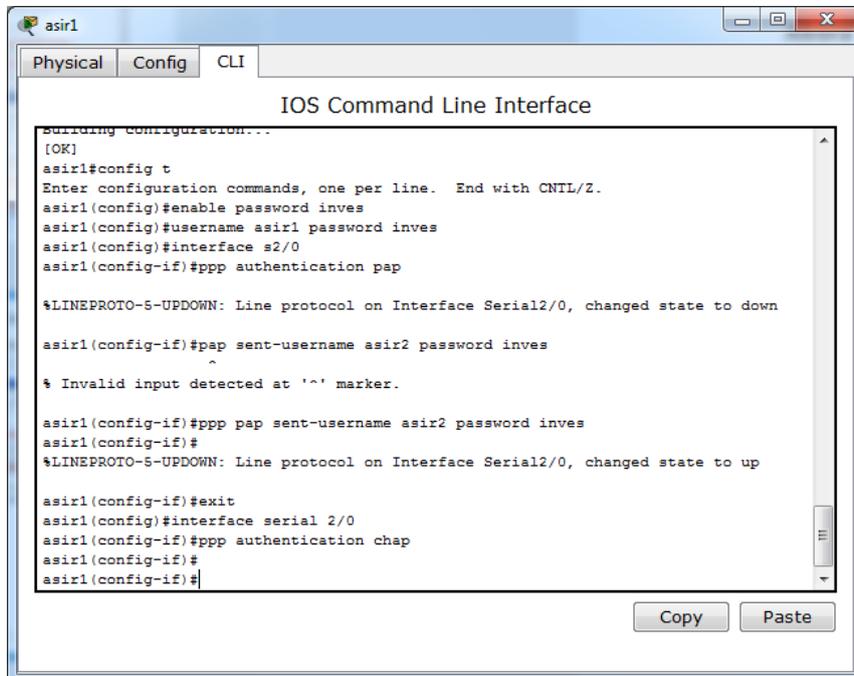
asir2#config t
Enter configuration commands, one per line. End with CNTL/Z.
asir2(config)#enable password inves
asir2(config)#username asir2 password inves
asir2(config)#interface serial 2/0
asir2(config-if)#ppp authentication pap
asir2(config-if)#ppp pap sent-username asir1 password inves
asir2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

asir2(config-if)#
```

Autenticación CHAP

Router asir1

En la interfaz **serial 2/0** establecemos el protocolo de autenticación pap.



```
asir1
Physical Config CLI
IOS Command Line Interface
Building configuration...
[OK]
asir1#config t
Enter configuration commands, one per line. End with CNTL/Z.
asir1(config)#enable password inves
asir1(config)#username asir1 password inves
asir1(config)#interface s2/0
asir1(config-if)#ppp authentication pap

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down

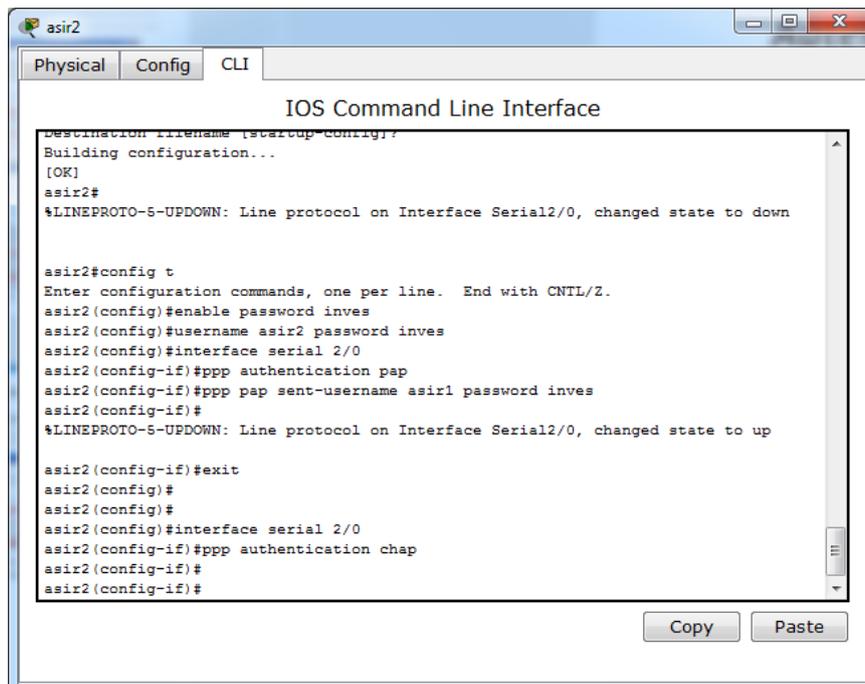
asir1(config-if)#pap sent-username asir2 password inves
^
% Invalid input detected at '^' marker.

asir1(config-if)#ppp pap sent-username asir2 password inves
asir1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

asir1(config-if)#exit
asir1(config)#interface serial 2/0
asir1(config-if)#ppp authentication chap
asir1(config-if)#
asir1(config-if)#
```

Router asir2

En la interfaz **serial 2/0** establecemos el protocolo de autenticación pap.



```
asir2
Physical Config CLI
IOS Command Line Interface
Destination filename [startup-config]:
Building configuration...
[OK]
asir2#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down

asir2#config t
Enter configuration commands, one per line. End with CNTL/Z.
asir2(config)#enable password inves
asir2(config)#username asir2 password inves
asir2(config)#interface serial 2/0
asir2(config-if)#ppp authentication pap
asir2(config-if)#ppp pap sent-username asir1 password inves
asir2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

asir2(config-if)#exit
asir2(config)#
asir2(config)#
asir2(config)#interface serial 2/0
asir2(config-if)#ppp authentication chap
asir2(config-if)#
asir2(config-if)#
```

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).*

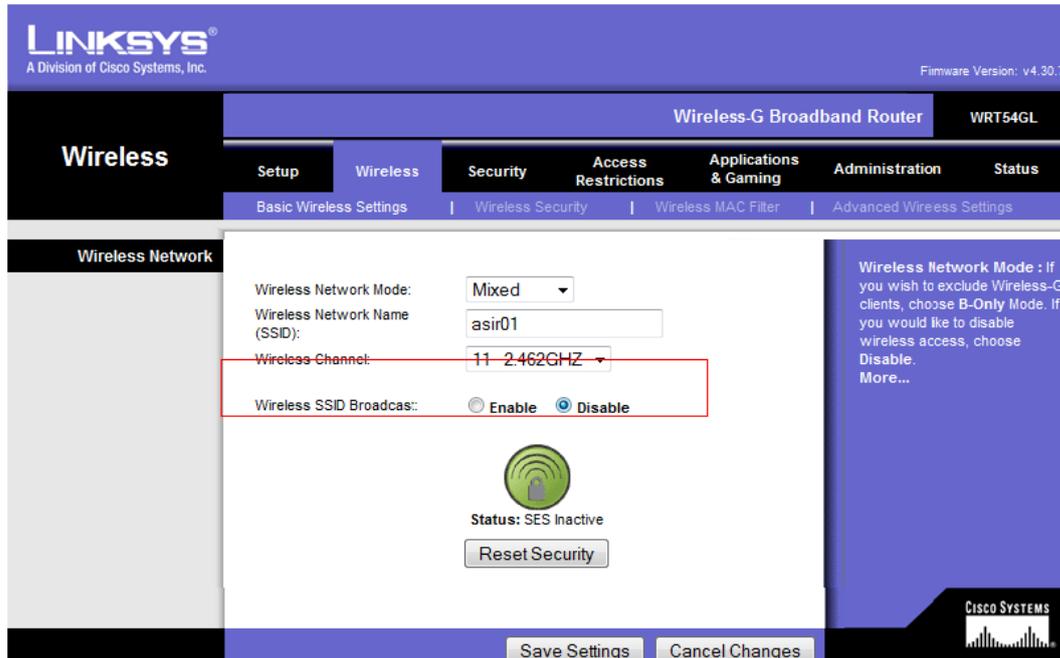
Una vez hemos accedido al router, nos situamos en la pestaña **Setup, Basic/Setup**, y deshabilitamos el **servidor DHCP**.

The screenshot shows the 'Setup' page for a Wireless-G Broadband Router (WRT54GL). The 'Internet Setup' section is active, showing 'Automatic Configuration - DHCP' selected. The 'DHCP Server' section is highlighted with a red box, showing the 'Disable' radio button selected. The 'Starting IP Address' is set to 192.168.3.100, and the 'Maximum Number of DHCP Users' is set to 50. The 'Local IP Address' is 192.168.3.142 and the 'Subnet Mask' is 255.255.255.0. The 'Static DNS' and 'WINS' fields are all set to 0.0.0.0.

Field	Value
Internet Connection Type	Automatic Configuration - DHCP
Router Name	WRT54GL
Host Name	
Domain Name	
MTU	Auto
Size	1500
Local IP Address	192 . 168 . 3 . 142
Subnet Mask	255 . 255 . 255 . 0
DHCP Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Starting IP Address	192.168.3.100
Maximum Number of DHCP Users	50
Client Lease Time	0 minutes (0 means one day)
Static DNS 1	0 . 0 . 0 . 0
Static DNS 2	0 . 0 . 0 . 0
Static DNS 3	0 . 0 . 0 . 0
WINS	0 . 0 . 0 . 0

Automatic Configuration - DHCP : This setting is most commonly used by Cable operators.
Host Name : Enter the host name provided by your ISP.
Domain Name : Enter the domain name provided by your ISP.
More...
Local IP Address : This is the address of the router.
Subnet Mask : This is the subnet mask of the router.
DHCP Server : Allows the router to manage your IP addresses.
Starting IP Address : The address you would like to start with.
Maximum number of DHCP Users : You may limit the number of addresses your

Ahora, en wireless /basic wireless Settings, desactivamos el SSID broadcast, y ponemos el nombre, en nuestro caso asir01.



En la pestaña **Wireless Security** configuramos la contraseña y el tipo de tal.



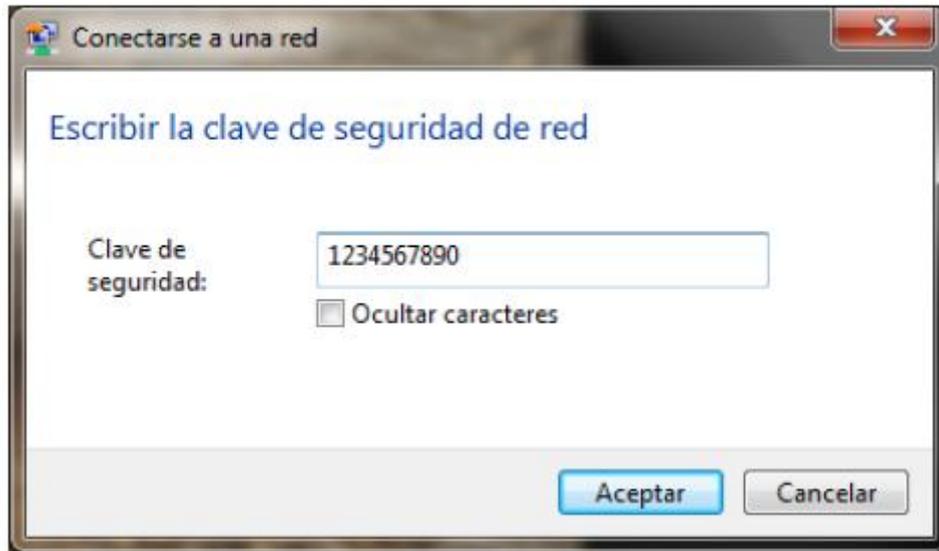
Desactivamos el filtro de MAC.



En un cliente, buscamos la red asir01.



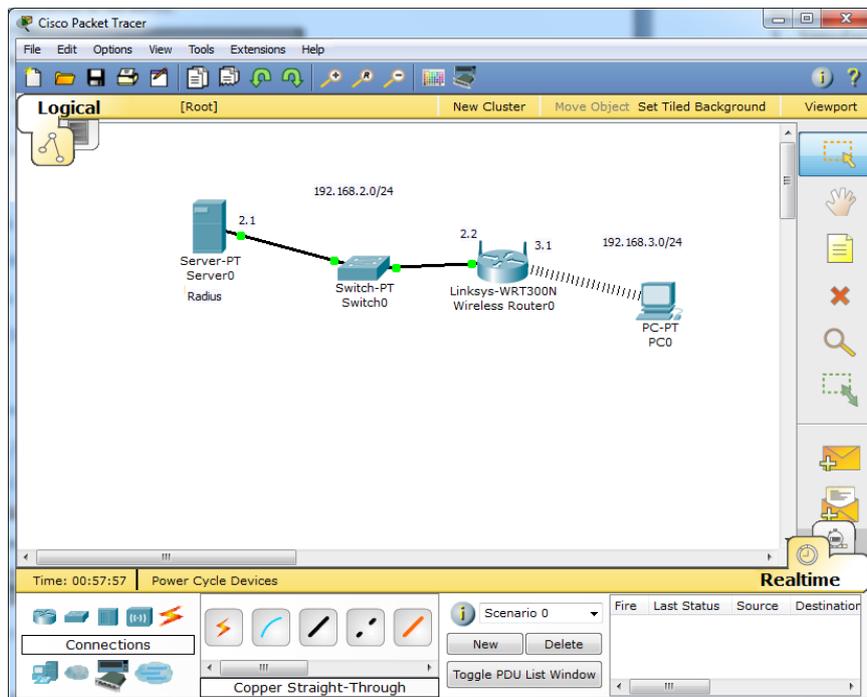
Y le introducimos la contraseña.



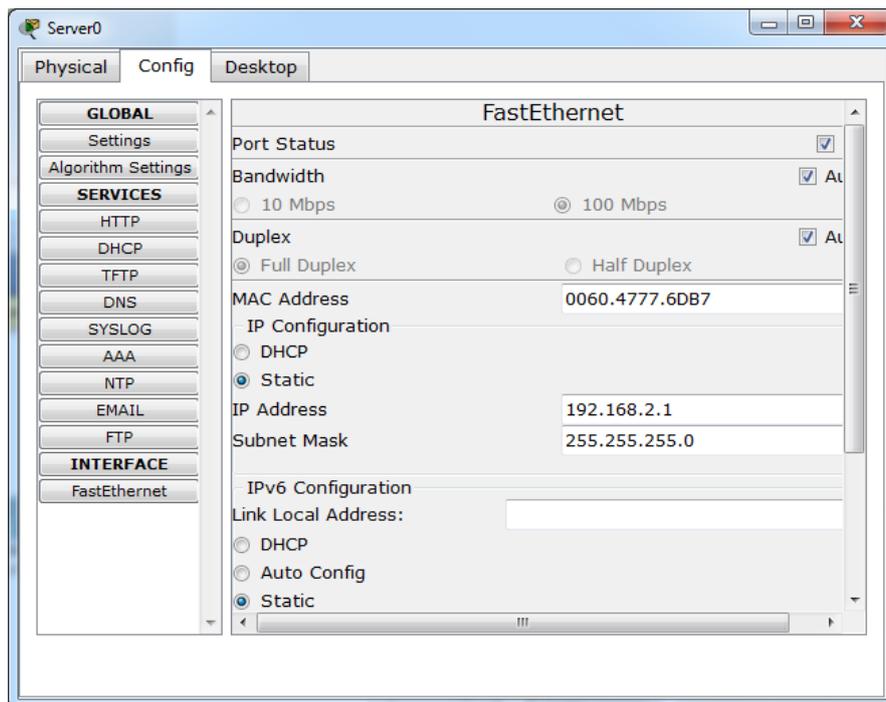
b) SERVIDOR RADIUS:

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

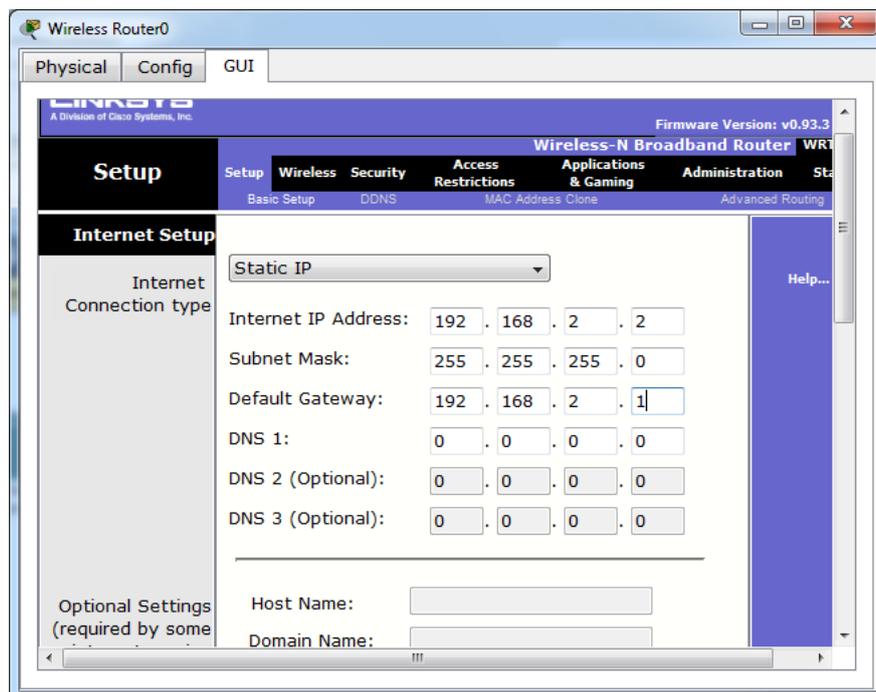
Tenemos planteado el siguiente esquema



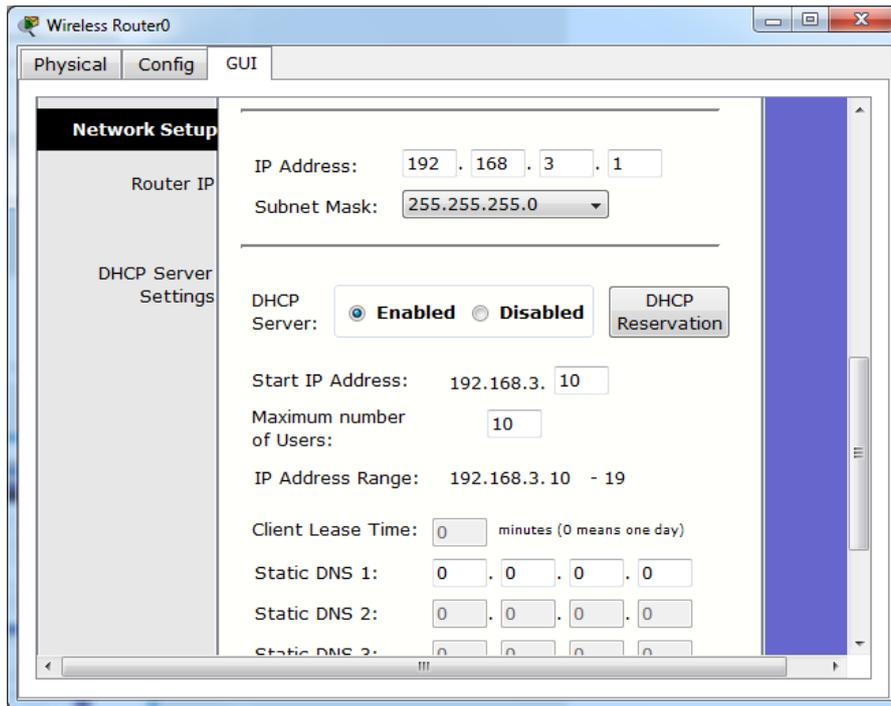
Configuramos la IP de la interfaz FastEthernet de nuestro servidor Radius.



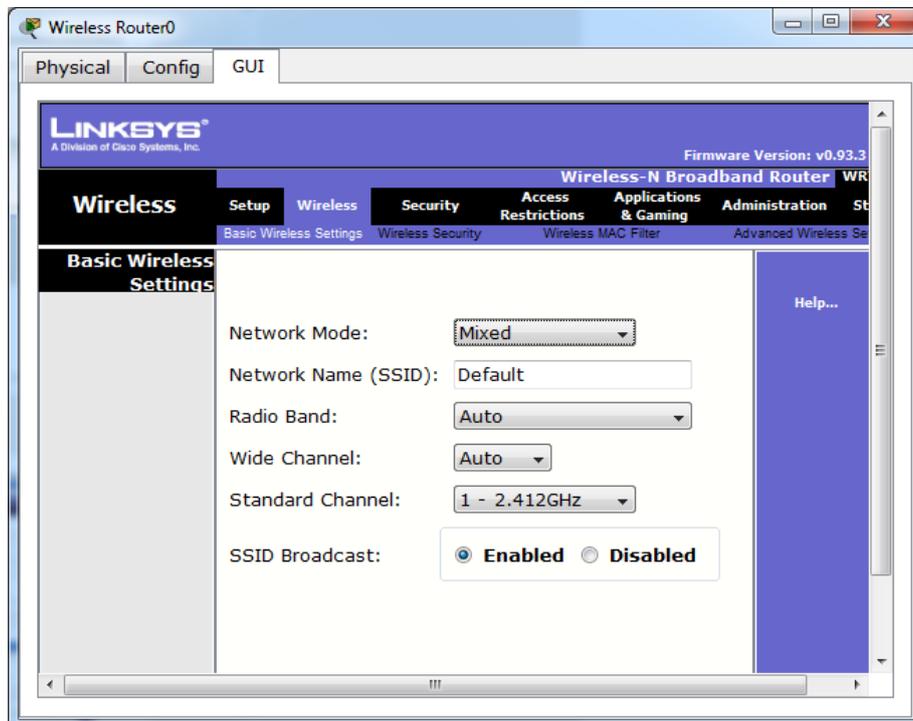
Seguidamente, configuramos la IP del router inalámbrico, estableciendo el servidor Radius como puerta de enlace.



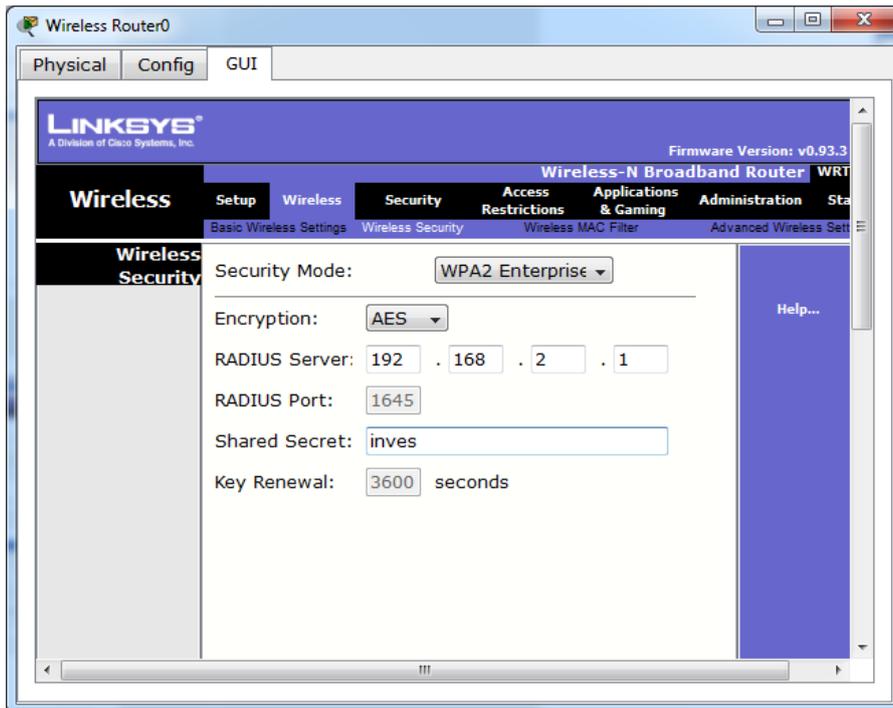
Habilitamos el servicio DHCP para asignar una IP a los equipos que se vayan a conectar al servidor Radius.



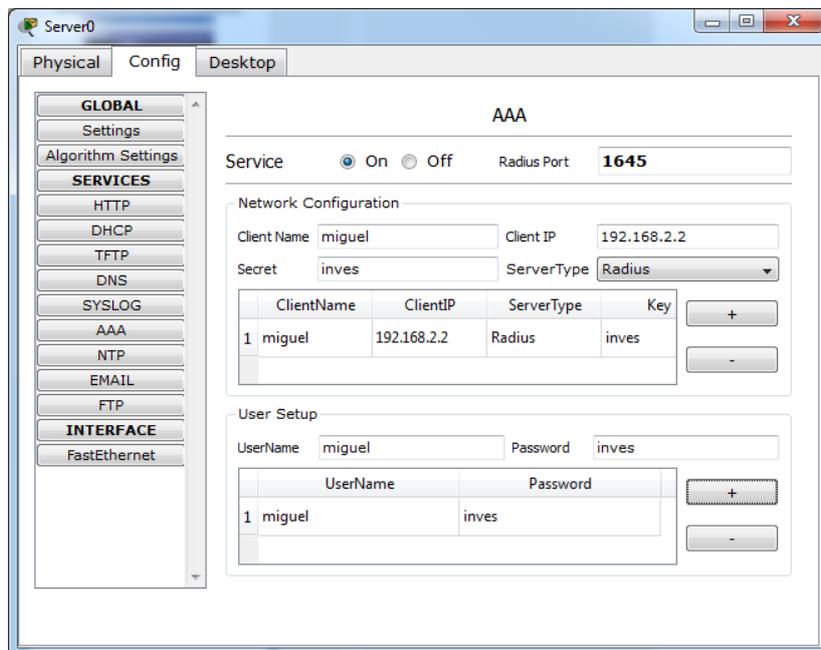
En el router inalámbrico, nos vamos a la pestaña Wireless y configuramos...



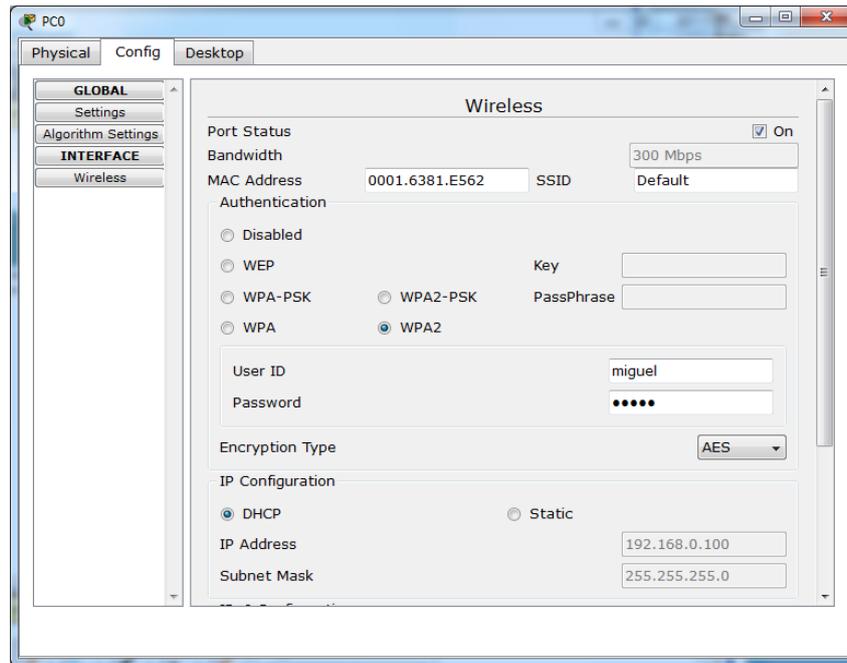
En **Wireless Security** introducimos la IP del servidor y la contraseña que utilizaremos.



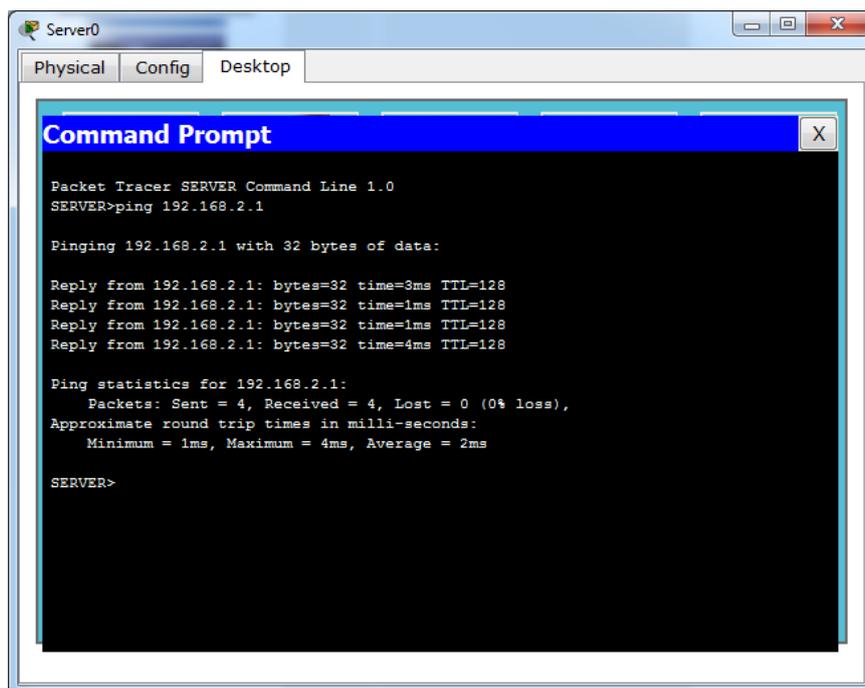
De vuelta en el servidor Radius, en la zona AAA configuramos los clientes Radius con su contraseña.



Nos situamos en el cliente, y en la zona Wireless, ingresamos el usuario y contraseña para la conexión con el servidor Radius.

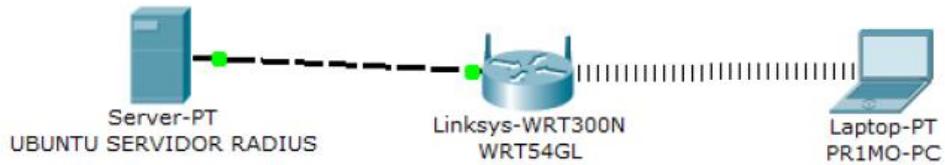


Abrimos el terminal del cliente, y comprobamos la conexión con el servidor Radius.



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.*

Tenemos el siguiente escenario.



Tenemos un servidor radius con la dirección 192.168.2.150
Instalamos el servidor Radius, en Ubuntu.
Accedemos a configurar los archivos más importantes.
Agregamos usuarios.

```
root@ubuntu1: /home/niko
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.2.6 Archivo: /etc/freeradius/users Modificado

#
# This is an entry for a user with a space in their name.
# Note the double quotes surrounding the name.
#
"alvaro"      Cleartext-Password := "inves"
              Reply-Message = "Hola, %{User-Name}"

"niko"       Cleartext-Password:= "inves"
              Reply-Message = "Hola, %{User-Name}"

"miguel"     Cleartext-Password:= "inves"
              Reply-Message = "Hola, %{User-Name}"

#
# Dial user back and telnet to the default host for that port
#
#Deg      Cleartext-Password := "ge55ged"

^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
```

Configuramos los parámetros para el cliente RADIUS, que en nuestro caso es el Router.

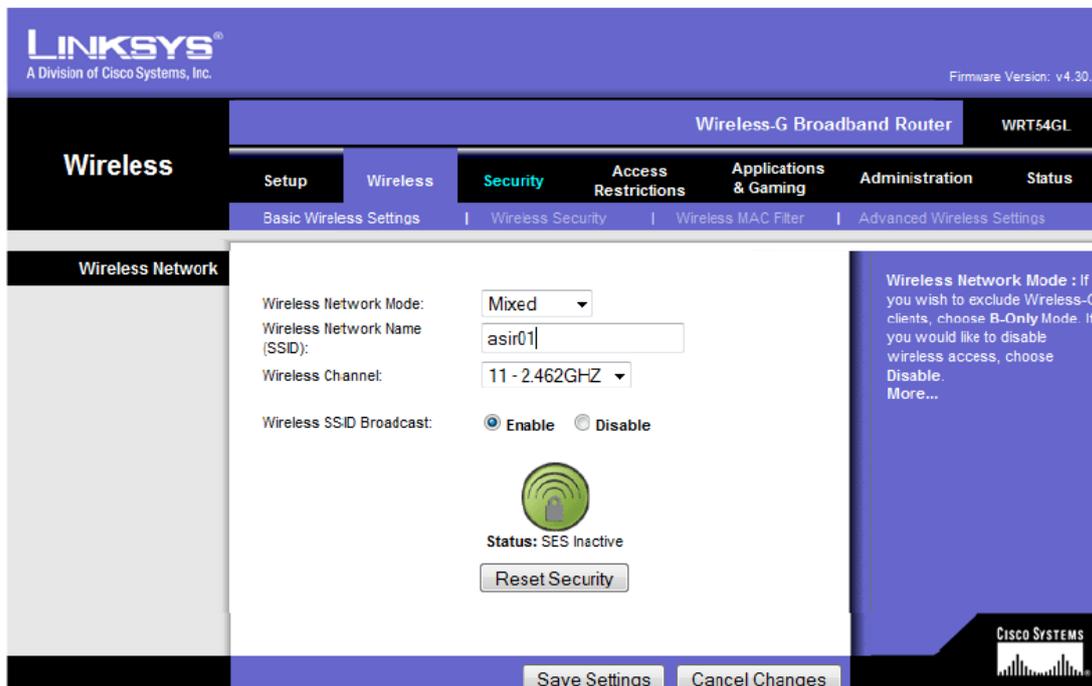
```
root@ubuntu1: /home/niko
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.2.6 Archivo: /etc/freeradius/clients.conf

#
# 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 192.168.3.142 {
    secret = inves
    shortname = asir01
}
#
#client 192.168.0.0/16 {
#    secret = testing123-2
#    shortname = private-network-2
#}

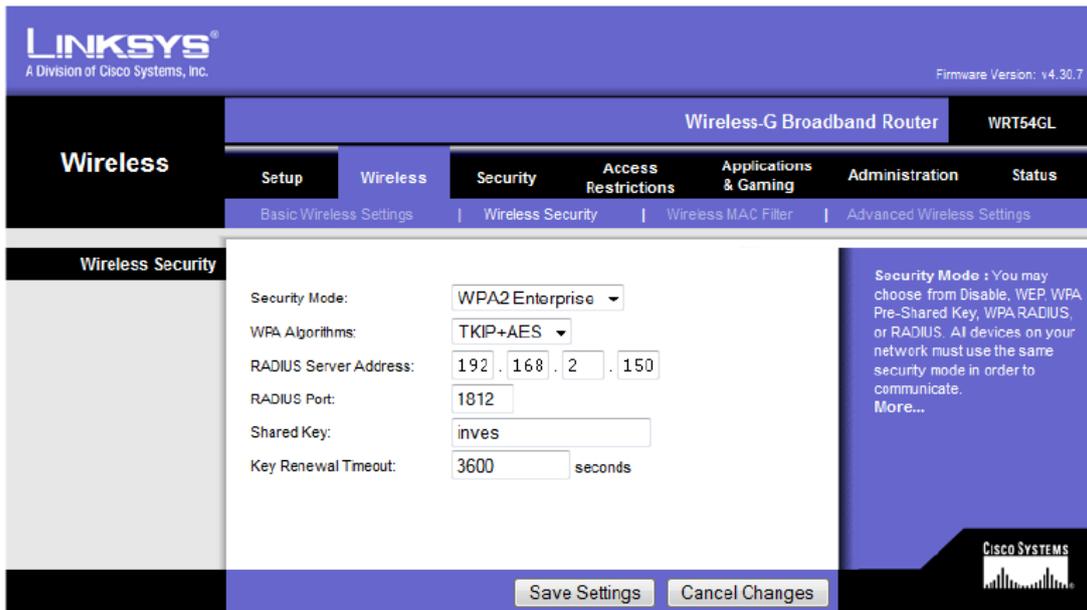
#client 10.10.10.10 {
#    # secret and password are mapped through the "secrets" file.
#    secret = testing123

^G Ver ayuda ^O Guardar ^R Leer Fich ^Y RePág. ^K Cortar Text ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág. Sig. ^U PegarText ^T Ortografía
```

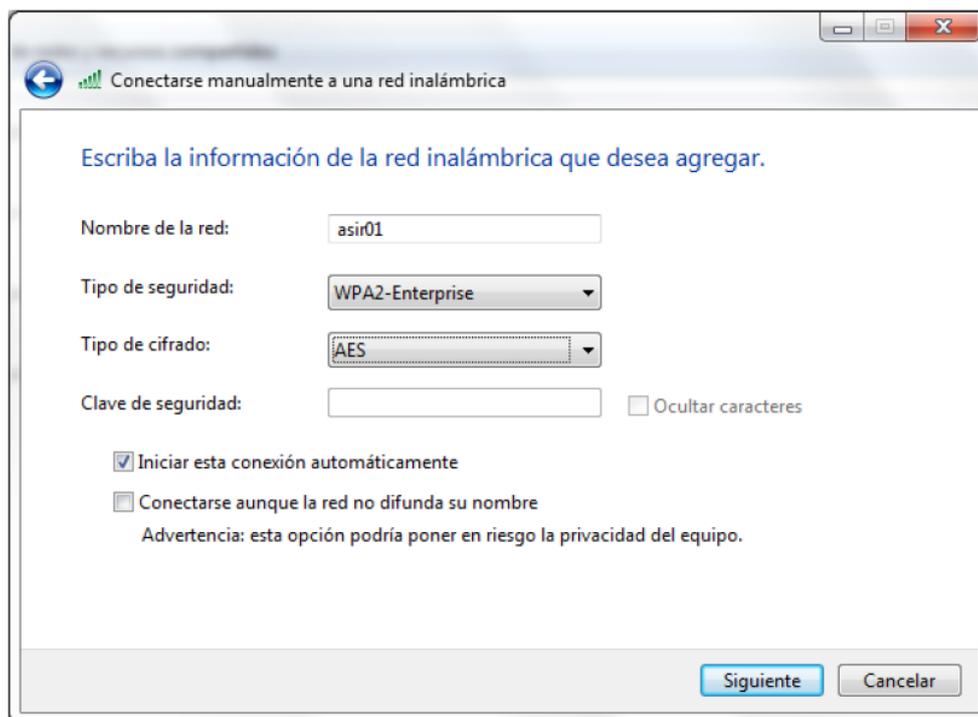
Configuramos el Router inalámbrico.



Indicamos la IP del servidor Radius.



Configuramos un cliente, un W7, para la autenticación con el servidor 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.

¿Qué es eduroam?

Eduroam (contracción de **education roaming**) 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 instituciones 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 RedIRIS que 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 de organizaciones 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 través de GEANT 3, y operada por varias redes académicas

europas 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).

