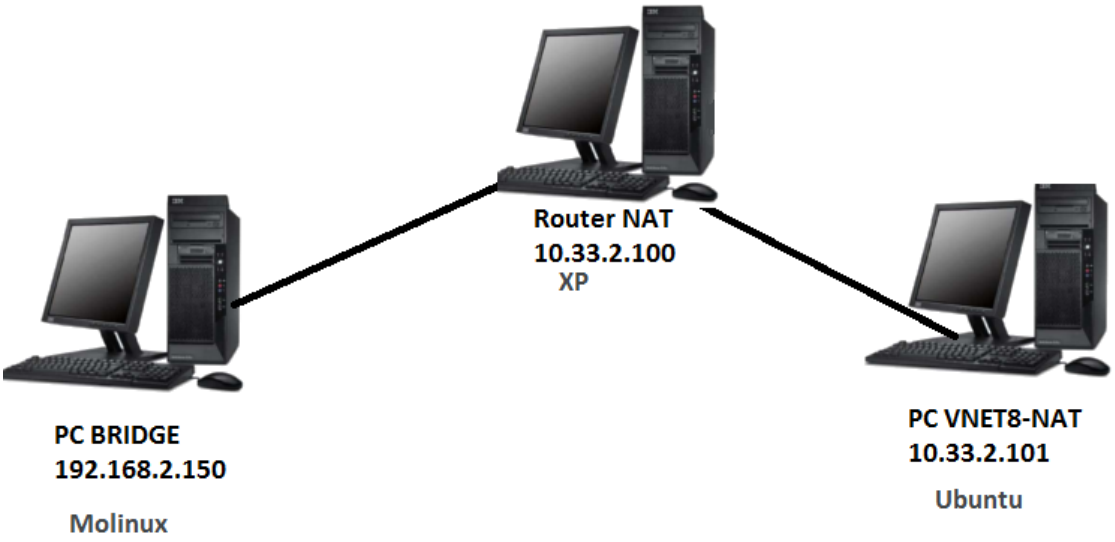
UD 3: “Implantación de técnicas de seguridad remoto. Seguridad perimetral.”

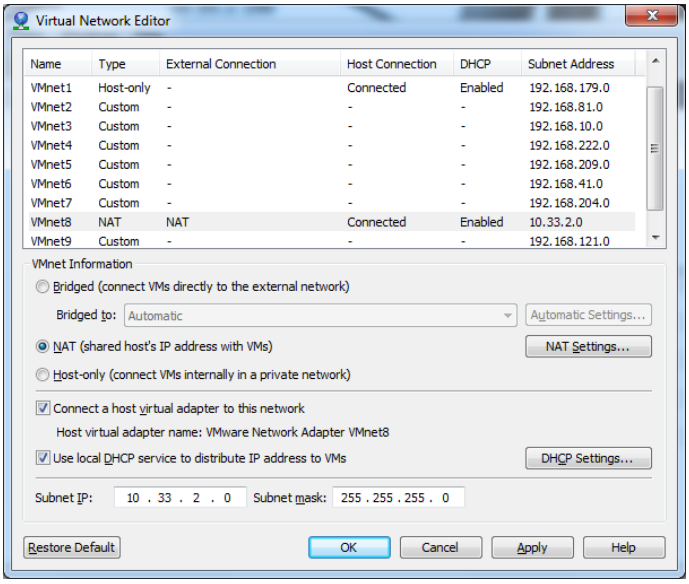
SEGURIDAD PERIMETRAL:

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

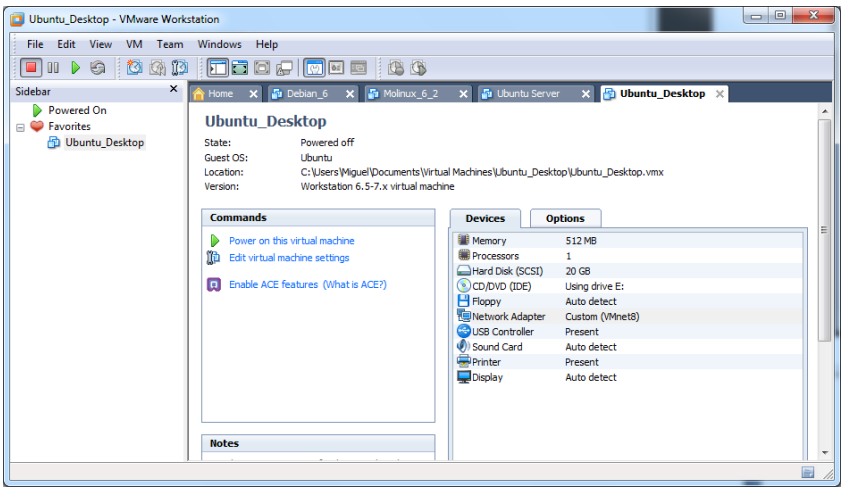
Escenario:



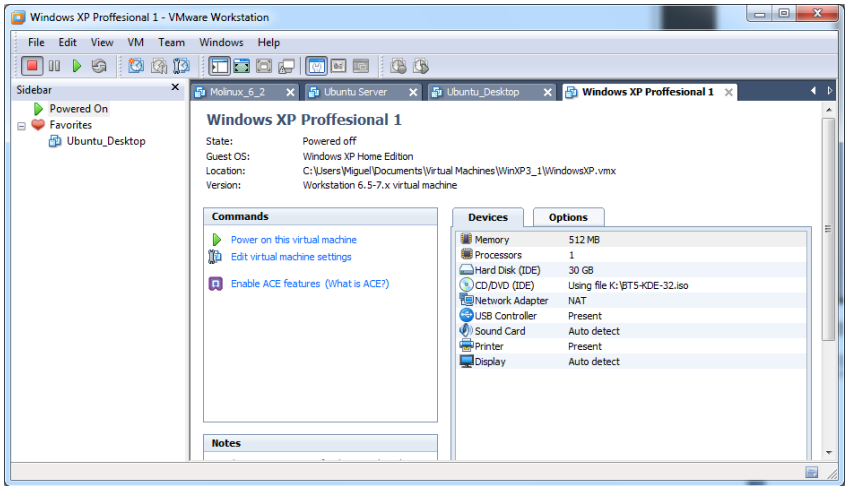
Configuramos el vnet8-NAT, para la red “**10.33.2.0**”



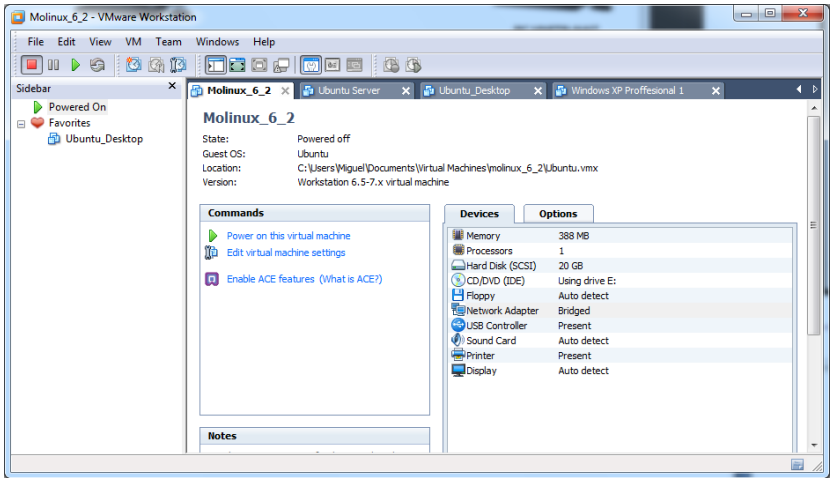
En el equipo Ubuntu elegimos el tipo **VNET8-NAT**



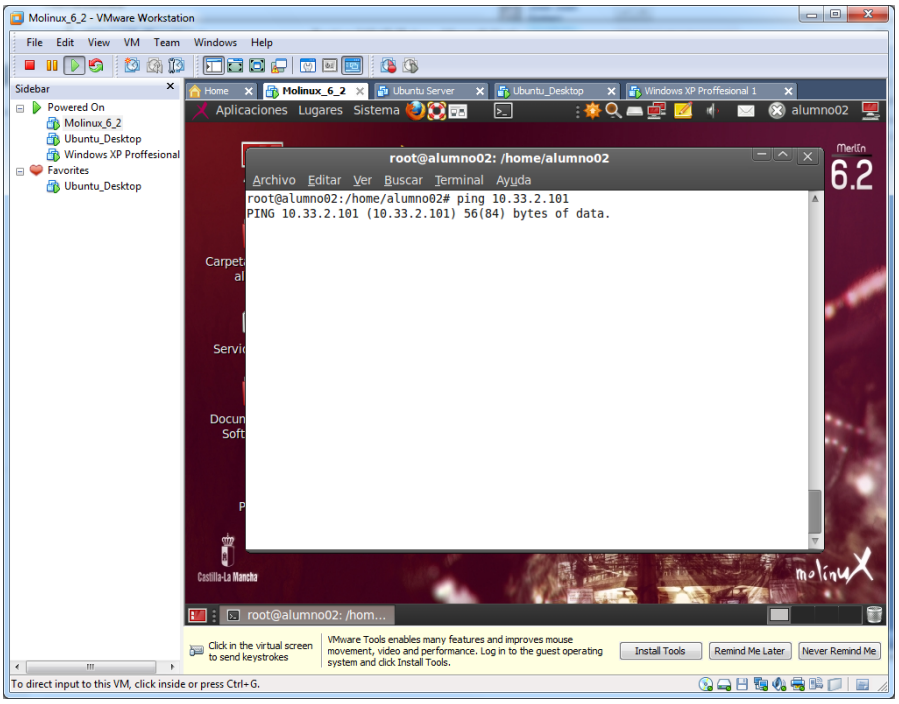
En el equipo XP elegimos el tipo **NAT**



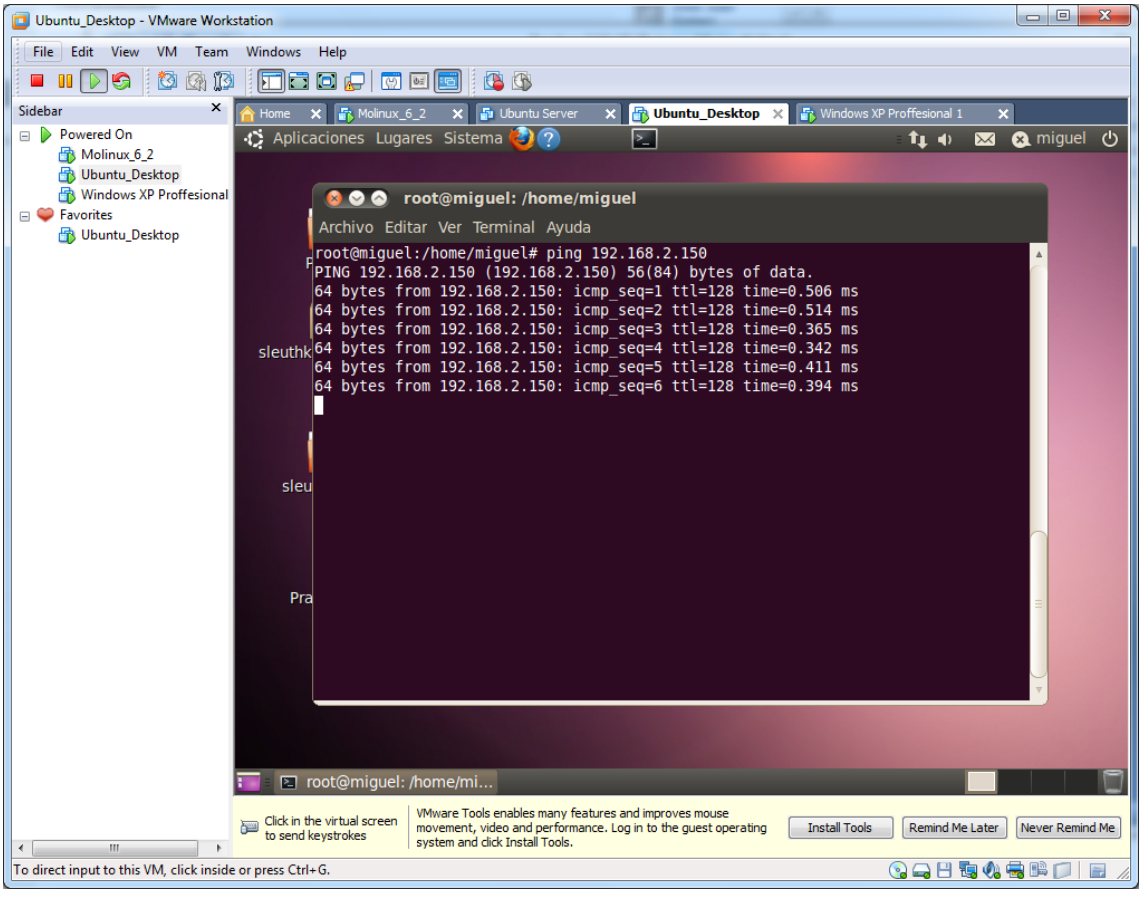
En el equipo Molinux elegimos el tipo **BRIDGED**



Comprobamos que el cliente Molinux no puede acceder a la dirección "**10.33.2.101**"



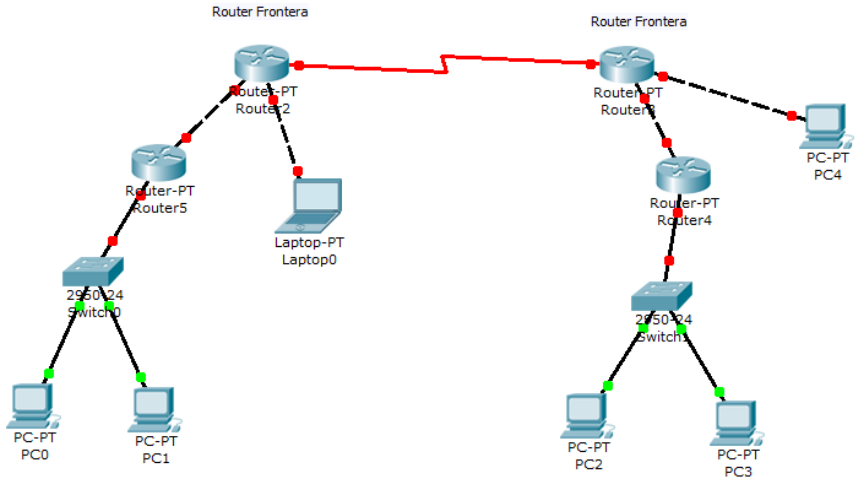
Mientras que el Cliente Ubuntu sí que puede acceder a la dirección **"192.168.2.150".**



2. Router frontera:

a) Planteamiento escenario CISCO Packet Tracert: esquema.

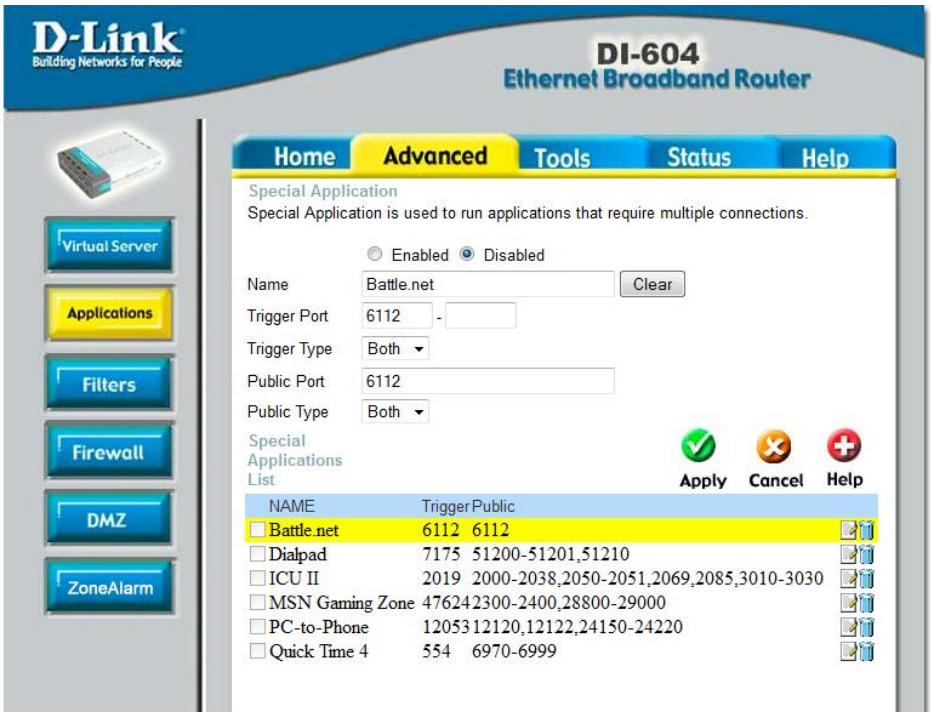
Tenemos 2 router frontera que unen dos empresas en zonas geográficas diferentes.



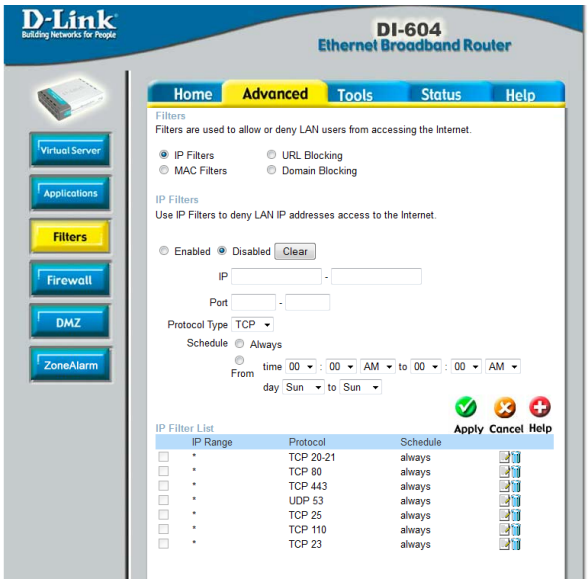
b) Realiza una comparativa entre los routers frontera atendiendo a las opciones de seguridad perimetral (NAT,Firewall,DMZ,…etc)

Router DLINK:

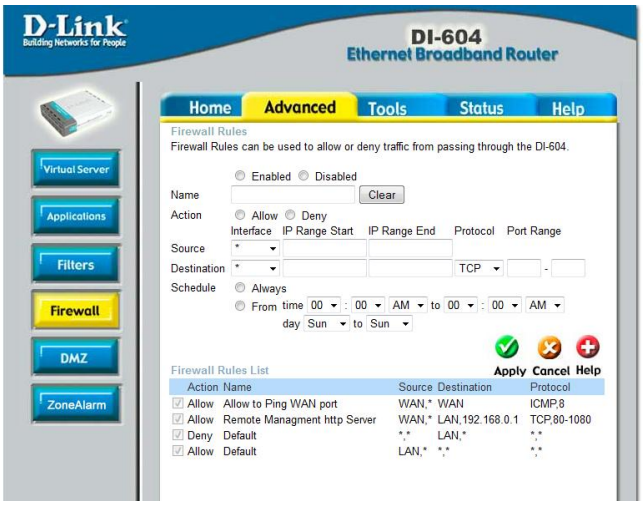
Podemos editar y eliminar diferentes aplicaciones que usan más de un puerto



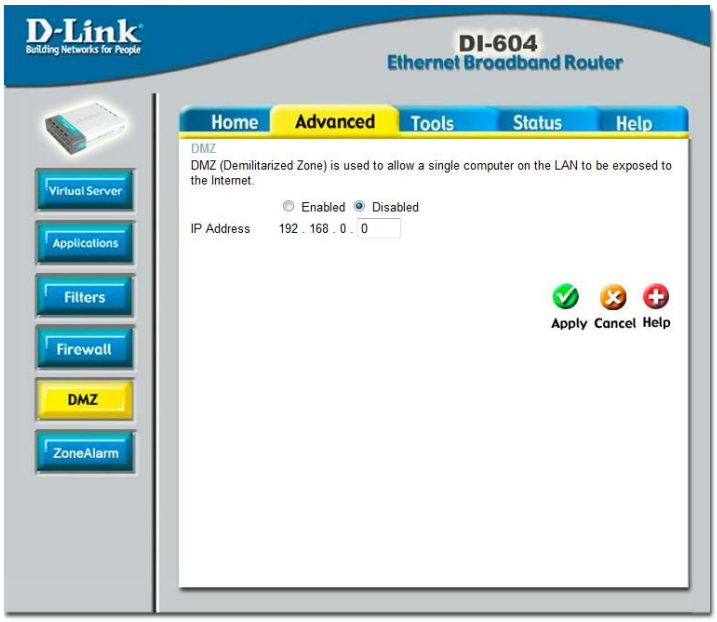
Podemos hacer filtrados de ip, mac y puertos configurando si queremos la fecha y hora.



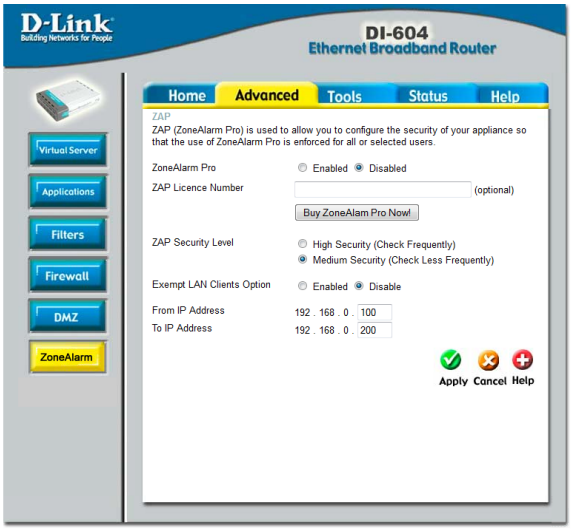
Podemos configurar en el firewall, diversos filtros para controlar la entrada a diferentes nombres y direcciones.



En esta pestaña podemos configurar la zona desmilitarizada.

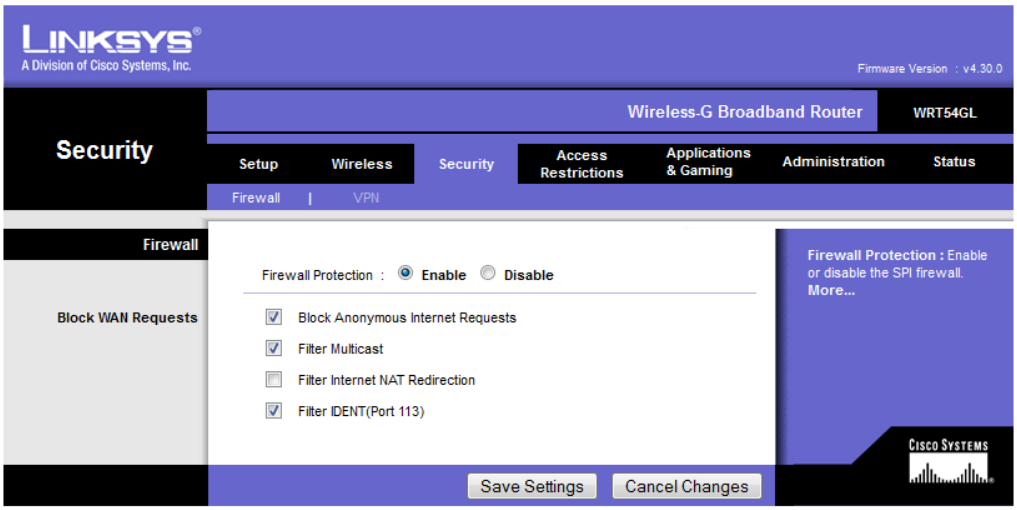


Podemos además configurar una zona de alarma

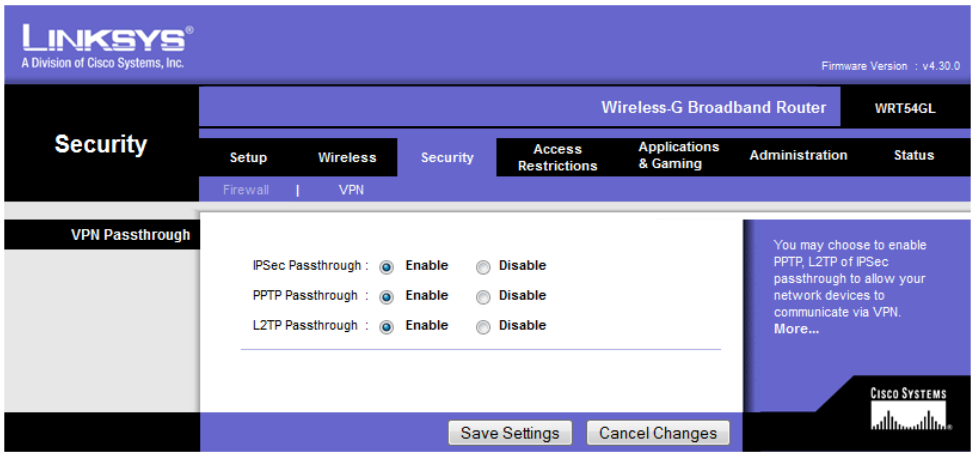


Router LINKSYS:

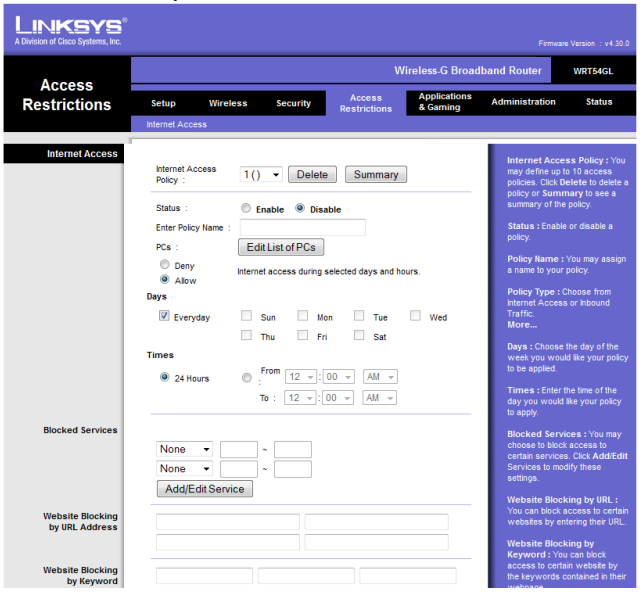
Este router es más avanzado que el anterior, algunas de las opciones de seguridad que podemos encontrar son, el cortafuegos, con sus distintas opciones.



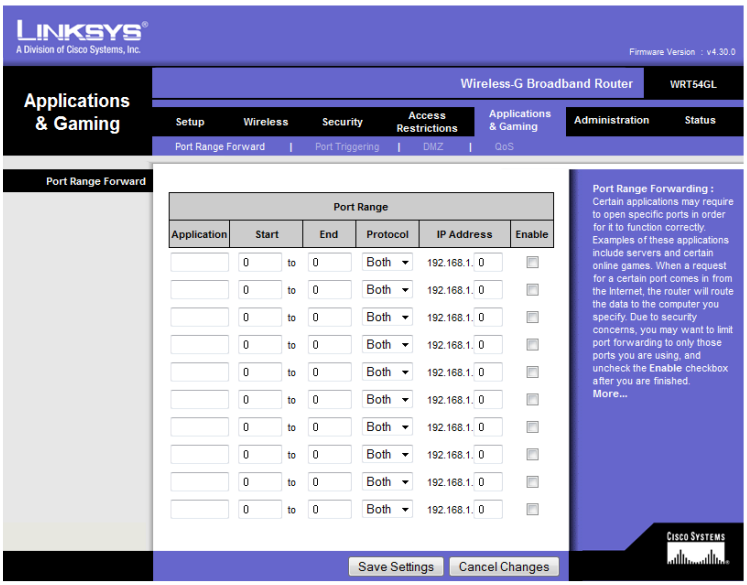
Podemos habilitar opciones VPN.



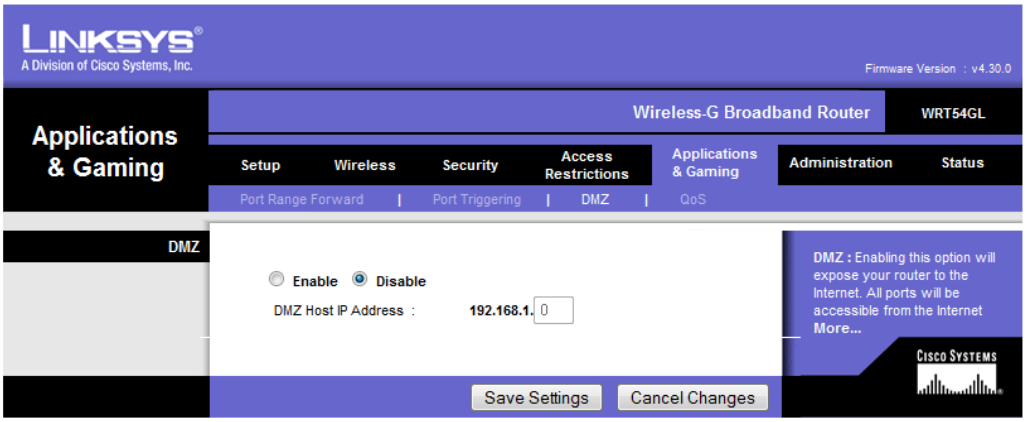
Podemos configurar diferentes parámetros de restricción, direcciones, fechas etc.



Podemos configurar los puertos



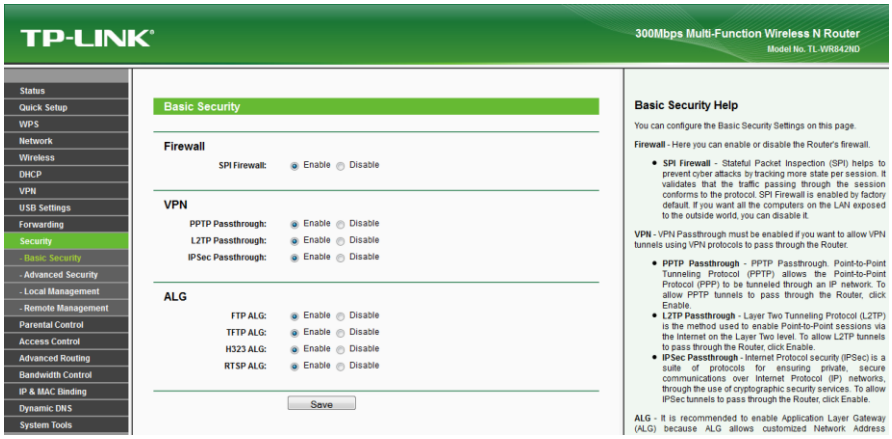
Podemos hacer configuraciones para la zona desmilitarizada



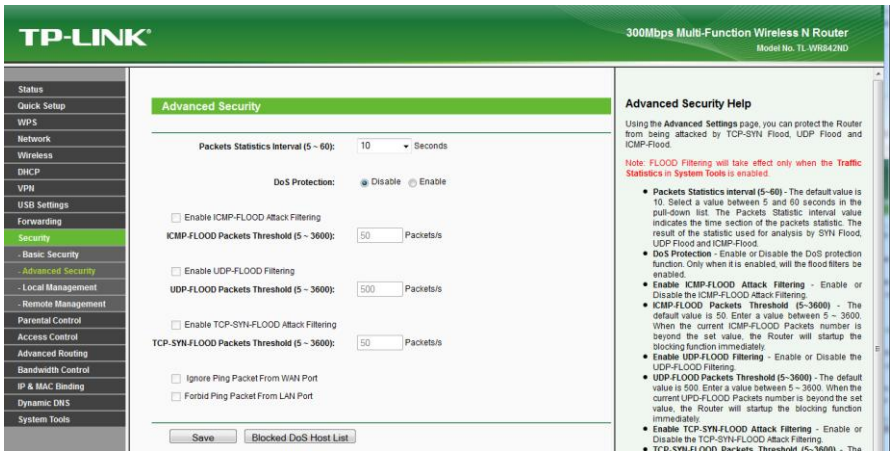
Podemos protegernos acerca de los paquetes QoS.

Router TP-LINK:

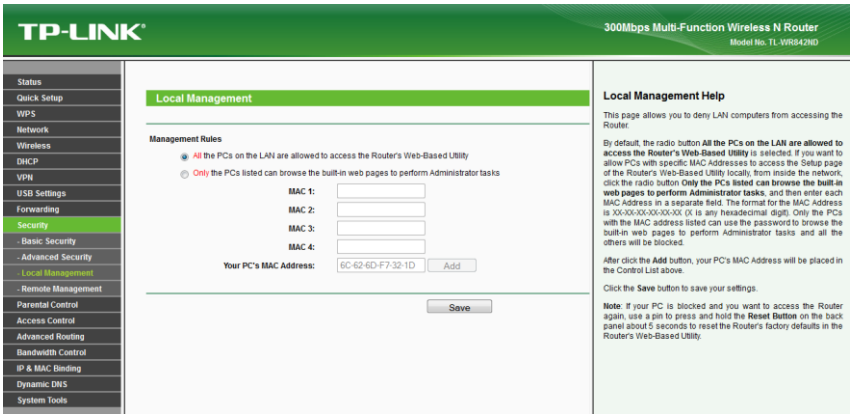
Podemos configurar opciones VPN, ALG activar firewall y habilitar-deshabilitar diferentes protocolos.



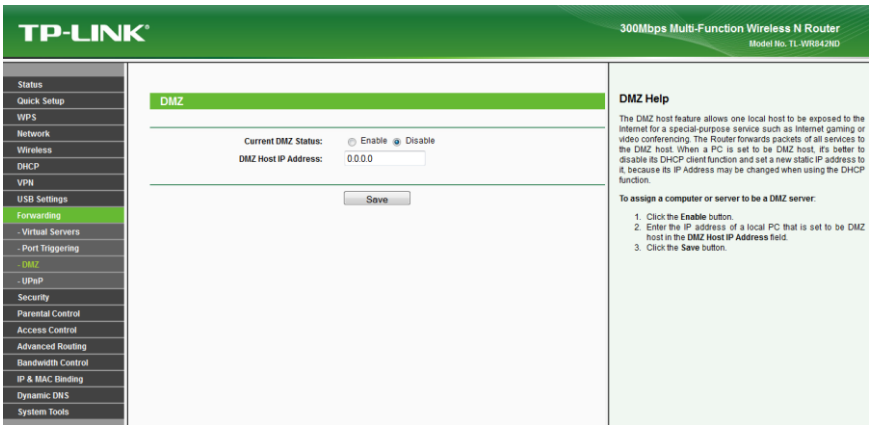
Podemos habilitar el ICMP y otros protocolos.



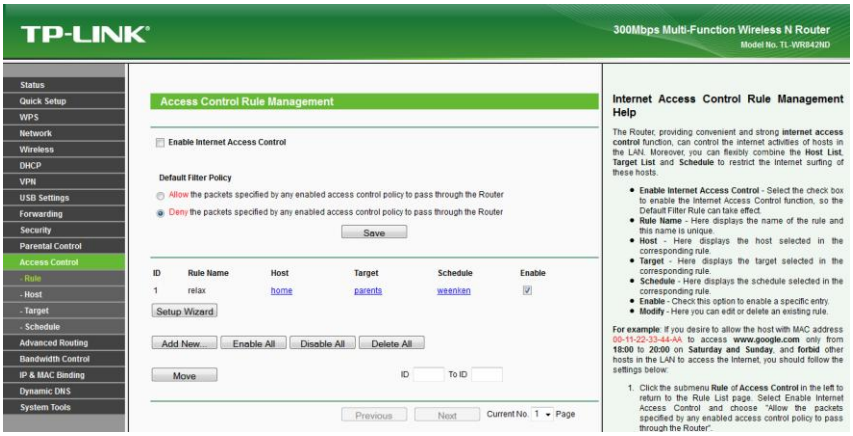
Podemos hacer un filtrado de MAC.



Podemos configurar la zona desmilitarizada.



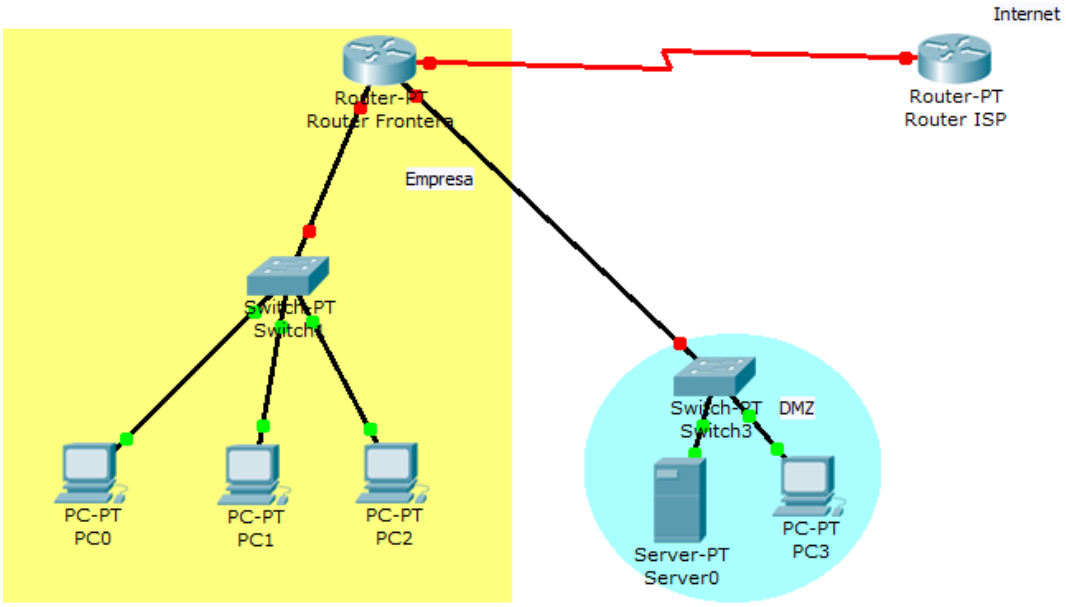
Podemos configurar listas de control de acceso.



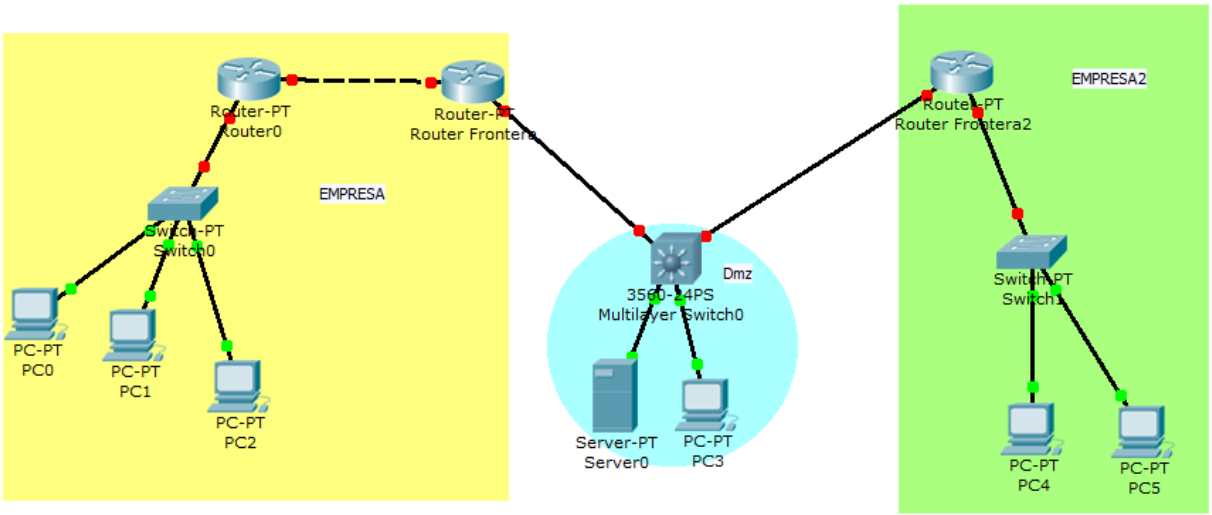
3. DMZ:

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

Un es quema 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.

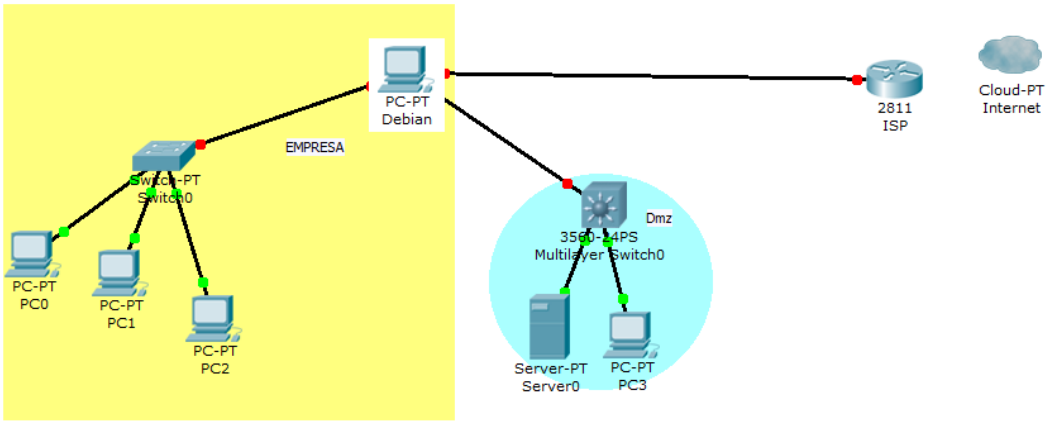


Un esquema complejo de DMZ es el siguiente.
Dos empresas empresa con sus redes, quieren acceder a los datos de la otra, para ello se implanta un DMZ para acceder a los archivos desde allí.

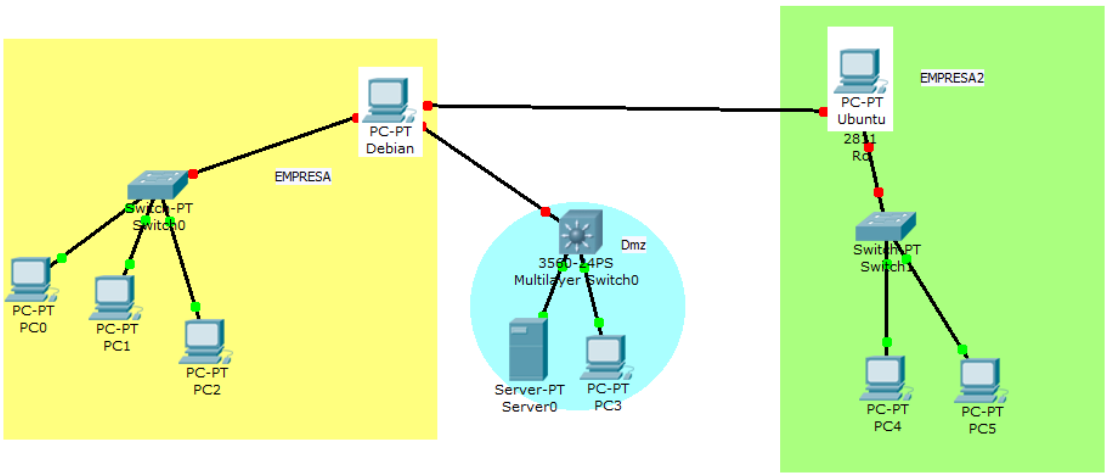


b) Planteamiento de escenarios DMZ en Linux (laboratorio virtual): esquemas.

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.

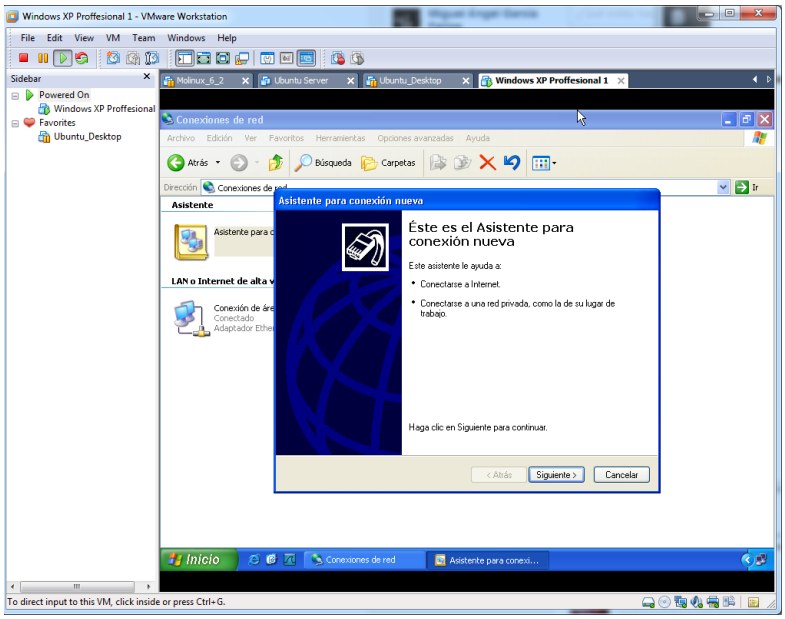


REDES PRIVADAS VIRTUALES (VPN)

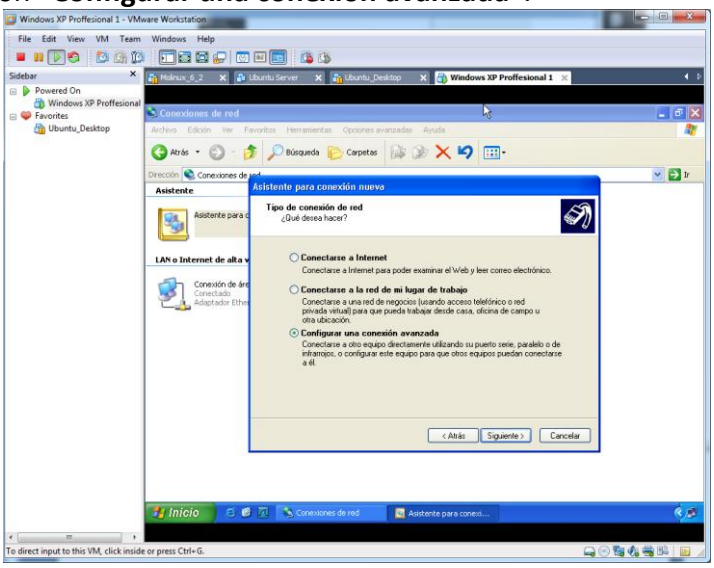
4. VPN sobre red local

a) Instalación de un servidor VPN en Windows XP.

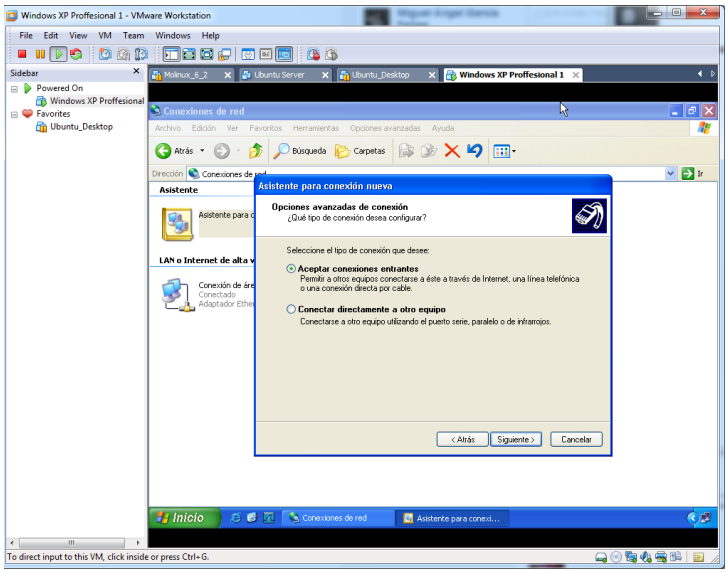
Nos situamos en conexiones de red. Seleccionamos el asistente para la conexión nueva, debe aparecer algo así.



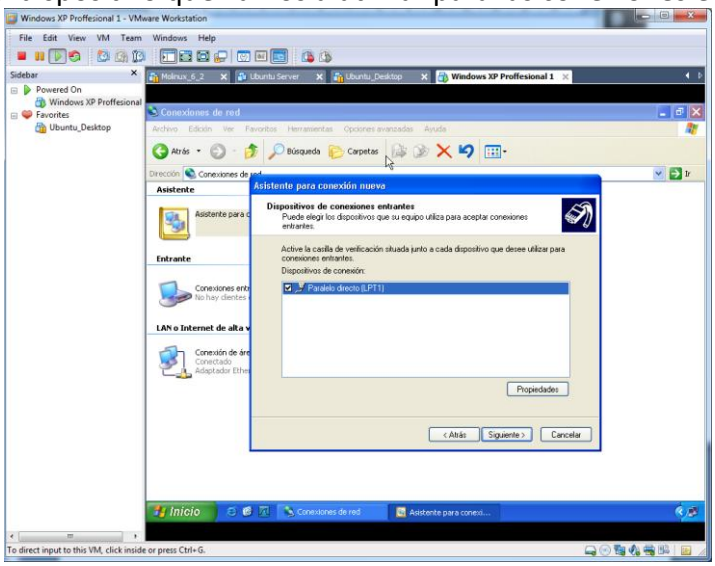
Elegimos la opción "**Configurar una conexión avanzada**".



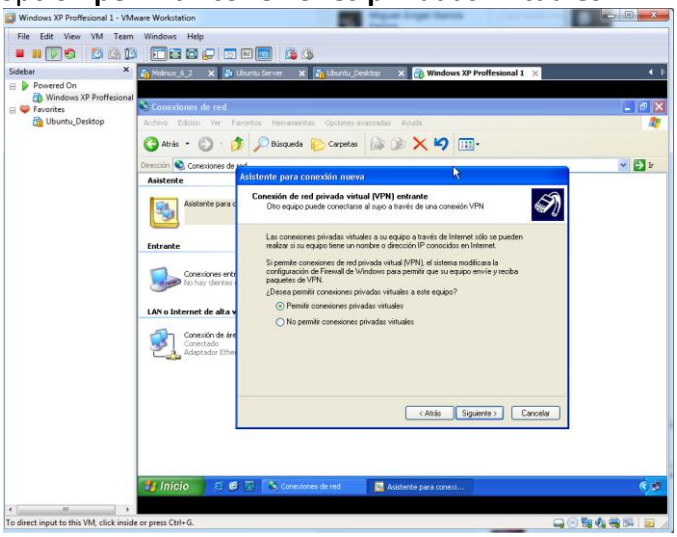
Pulsamos la opción "**Aceptar conexiones entrantes**" para permitir a otros clientes conectarse a éste a través de internet.



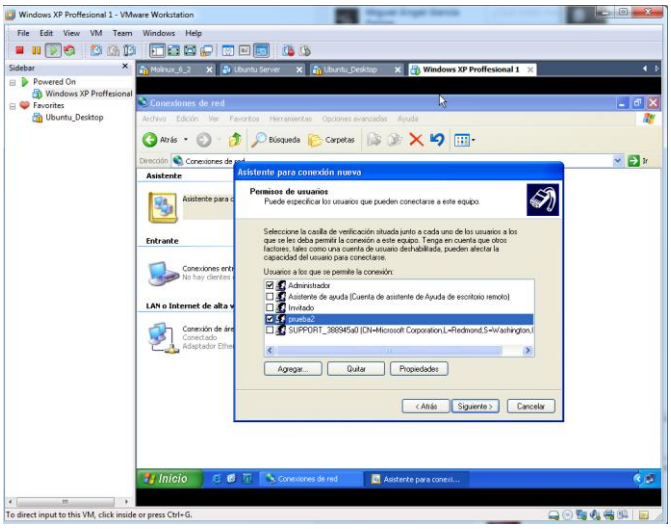
Seleccionamos el dispositivo que vamos a utilizar para las conexiones entrantes.



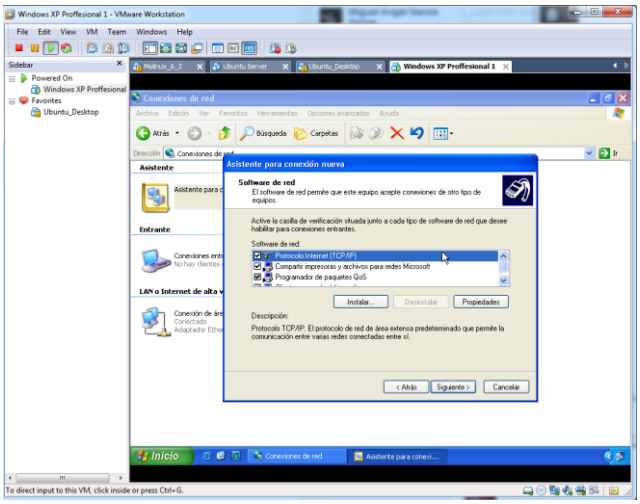
Seleccionamos la opción **permitir conexiones privadas virtuales**.



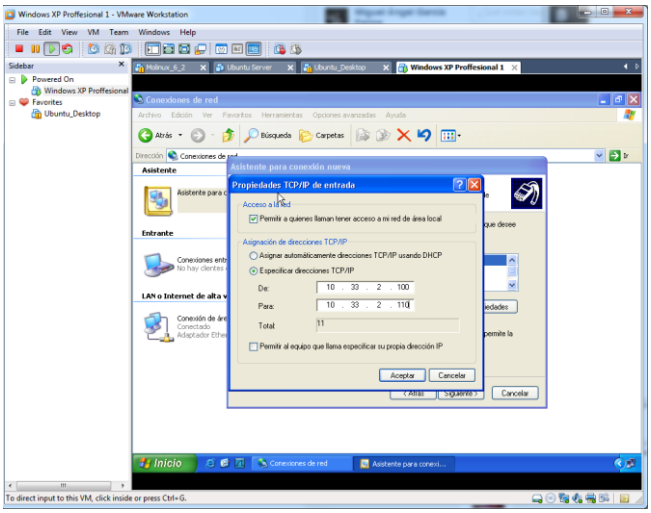
Elegimos los usuarios que pueden acceder, en nuestro caso “**Administrador y prueba2**”



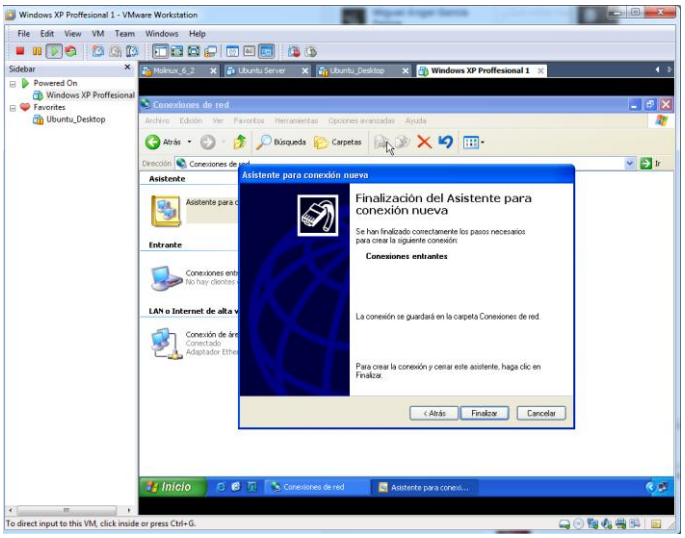
Elegimos las siguientes opciones.



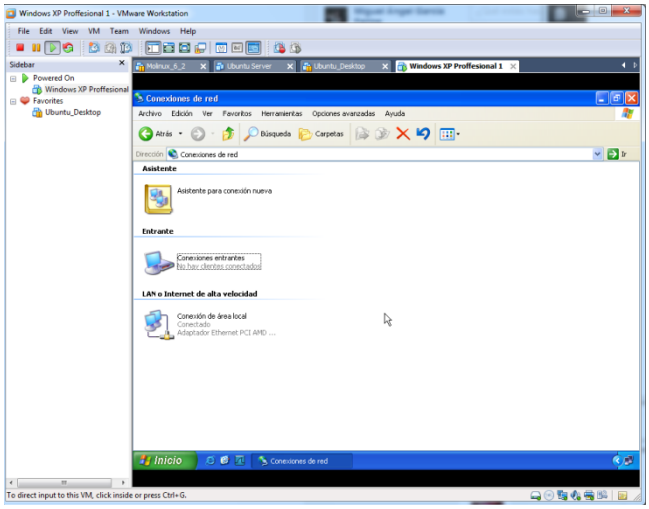
Indicamos el rango de IPS que vamos a permitir.



Finalizamos el asistente.



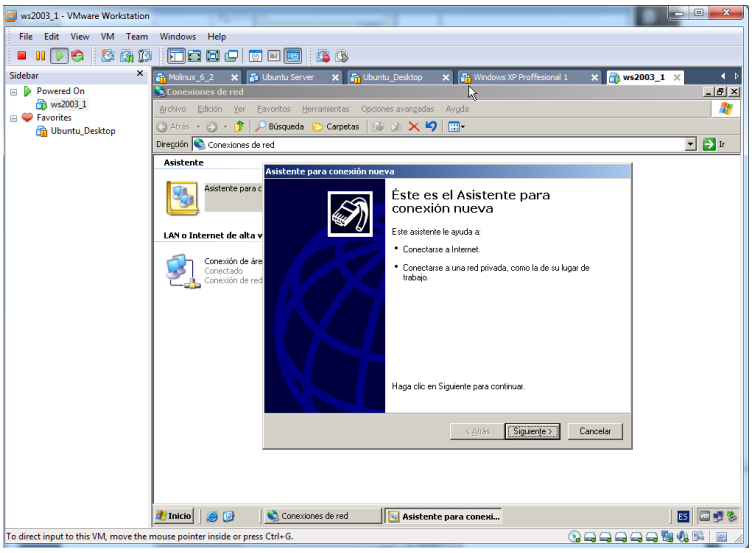
Podemos observar en las conexiones de red que nos ha creado la VPN nueva.



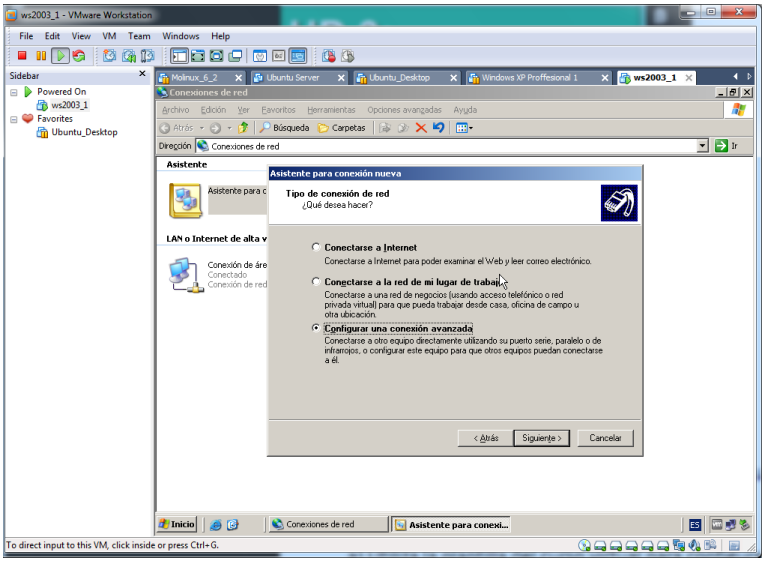
b) Instalación de un servidor VPN en Windows 2003/2008.

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

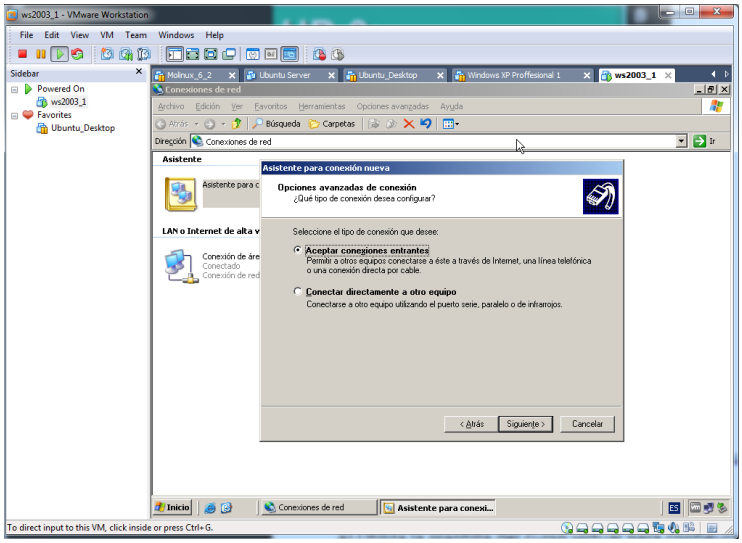
Creamos una nueva conexión a través del asistente para nuevas conexiones.



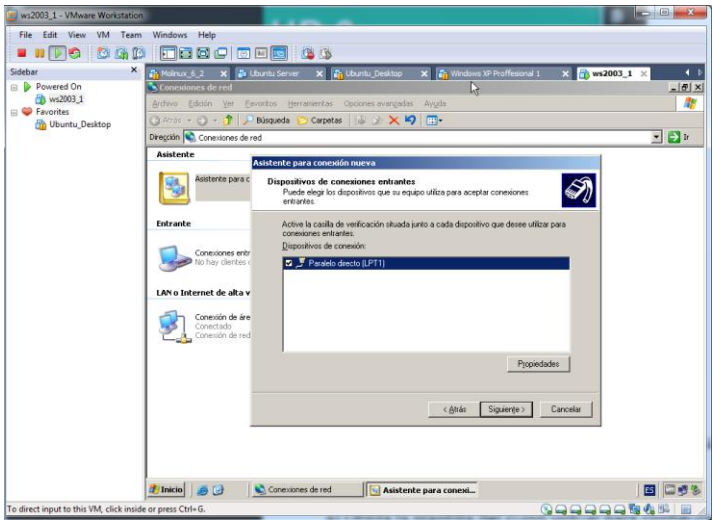
Elegimos la opción “**Configurar una conexión avanzada**”.



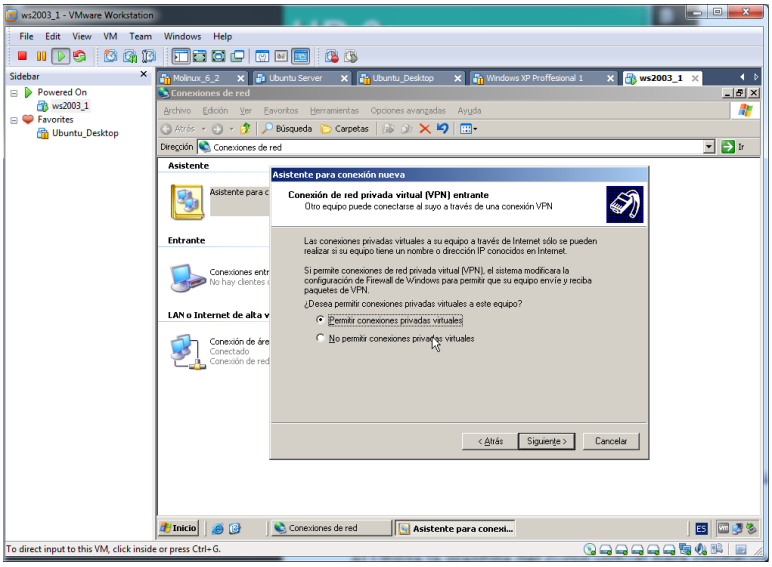
Aceptamos las “**Conexiones entrantes**”



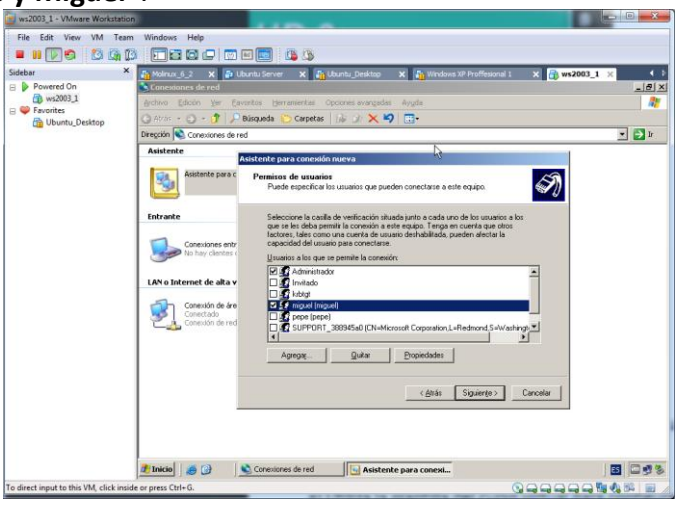
Elegimos el tipo de dispositivos entrantes que vamos a utilizar en la conexión.



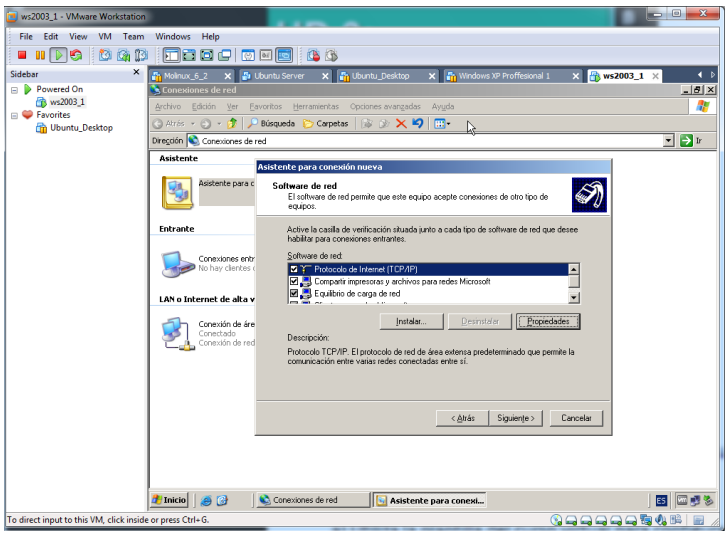
Elegimos la opción “**Permitir conexiones privadas virtuales**” para poder utilizar VPN.



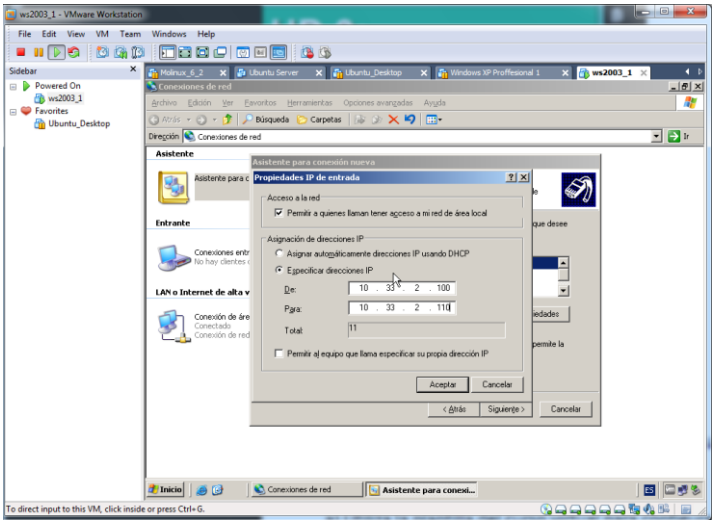
Elegimos los usuarios que podrán conectarse a este equipo, en mi caso “**Administradores y Miguel**”.



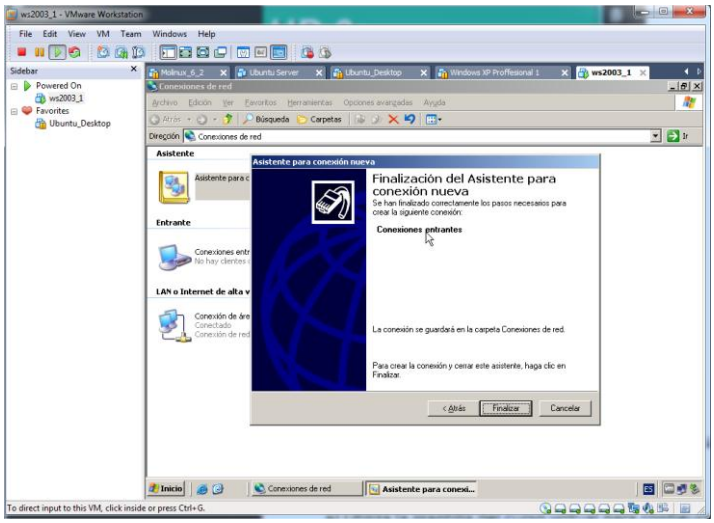
Configuramos esta ventana de la siguiente manera.



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

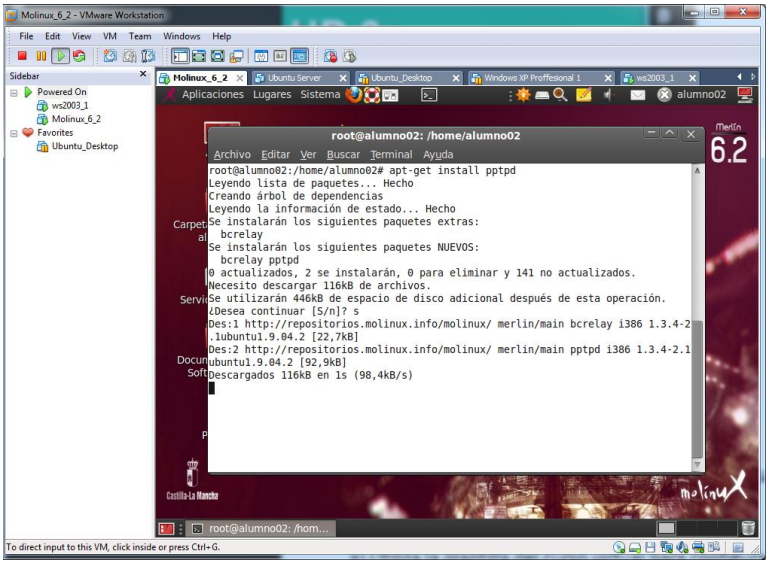


Finalizamos el asistente de configuración.



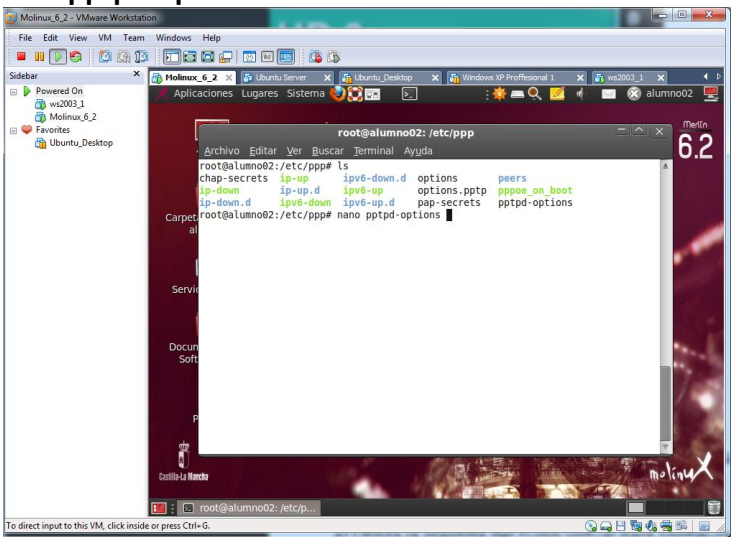
c) Instalación de un servidor VPN en GNU/Linux

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

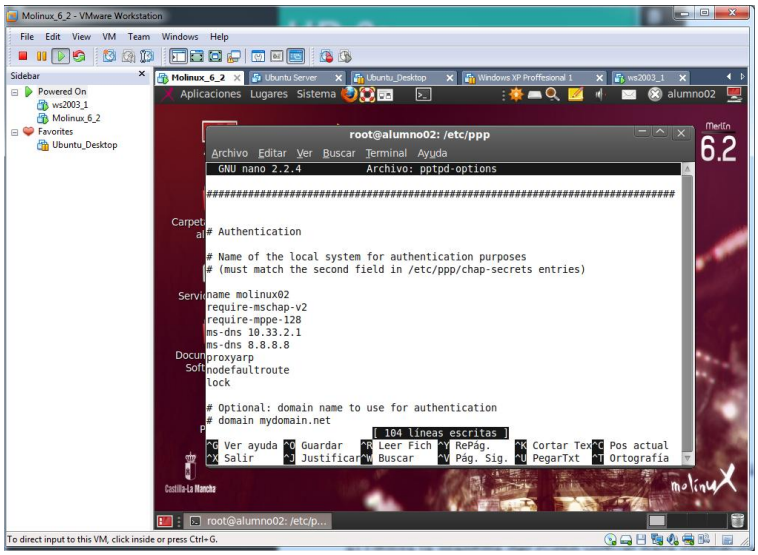


Una vez se haya completado la instalación, nos situaremos en el directorio "**/etc/ppp**", listamos los ficheros y directorios que lo contienen.

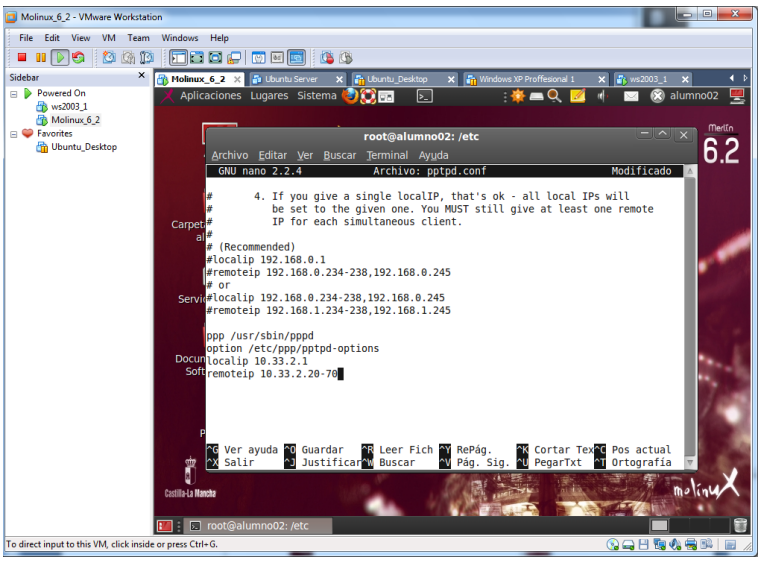
Editamos el fichero "**pptpd-options**" con el comando nano.



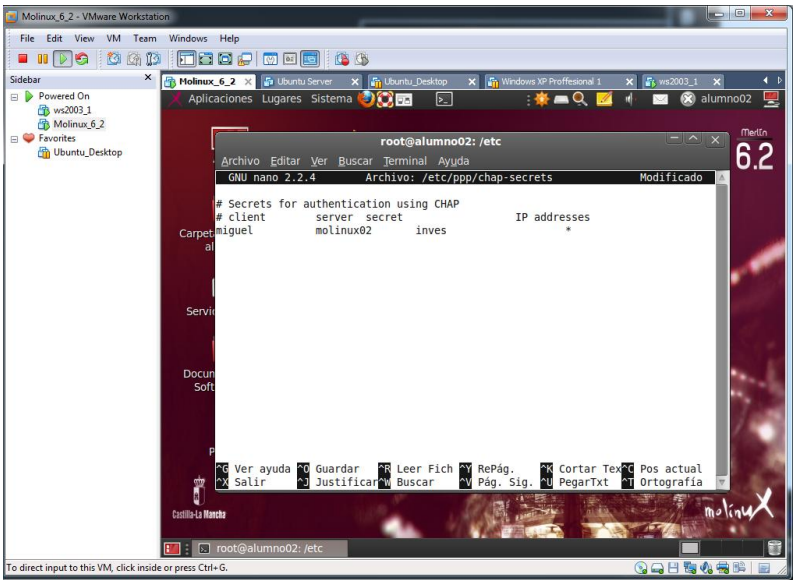
Configuramos el fichero con los siguientes parámetros.



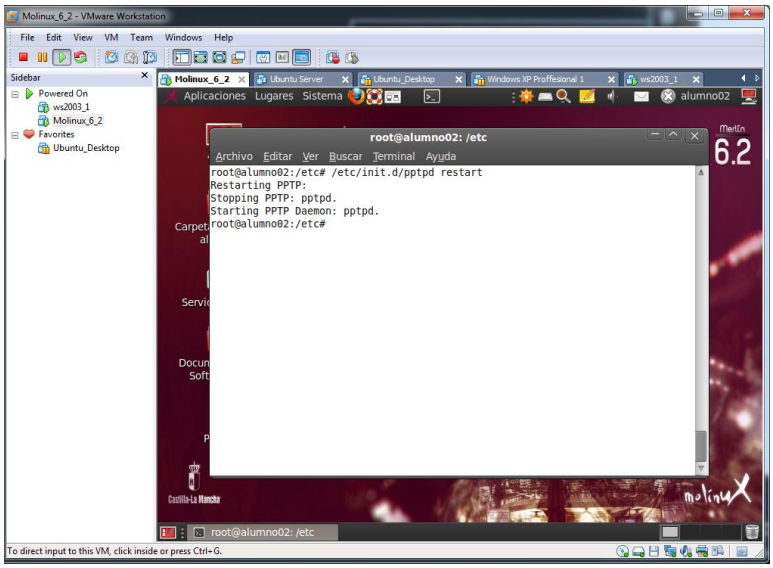
Ahora, nos situamos en el fichero "**pptpd.conf**" del directorio "**/etc**", y hacemos las siguientes configuraciones.



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



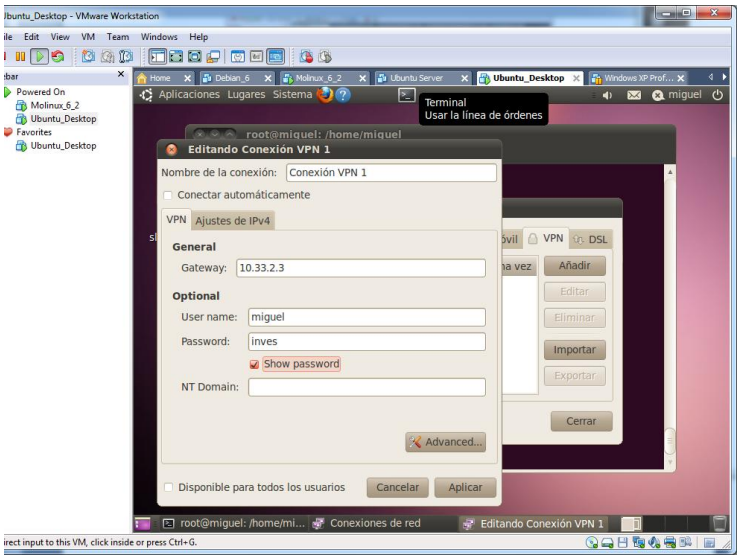
Una vez configurado todos los ficheros anteriores, reiniciamos el servicio, con el comando "**/etc/init.d/pptpd restart**"



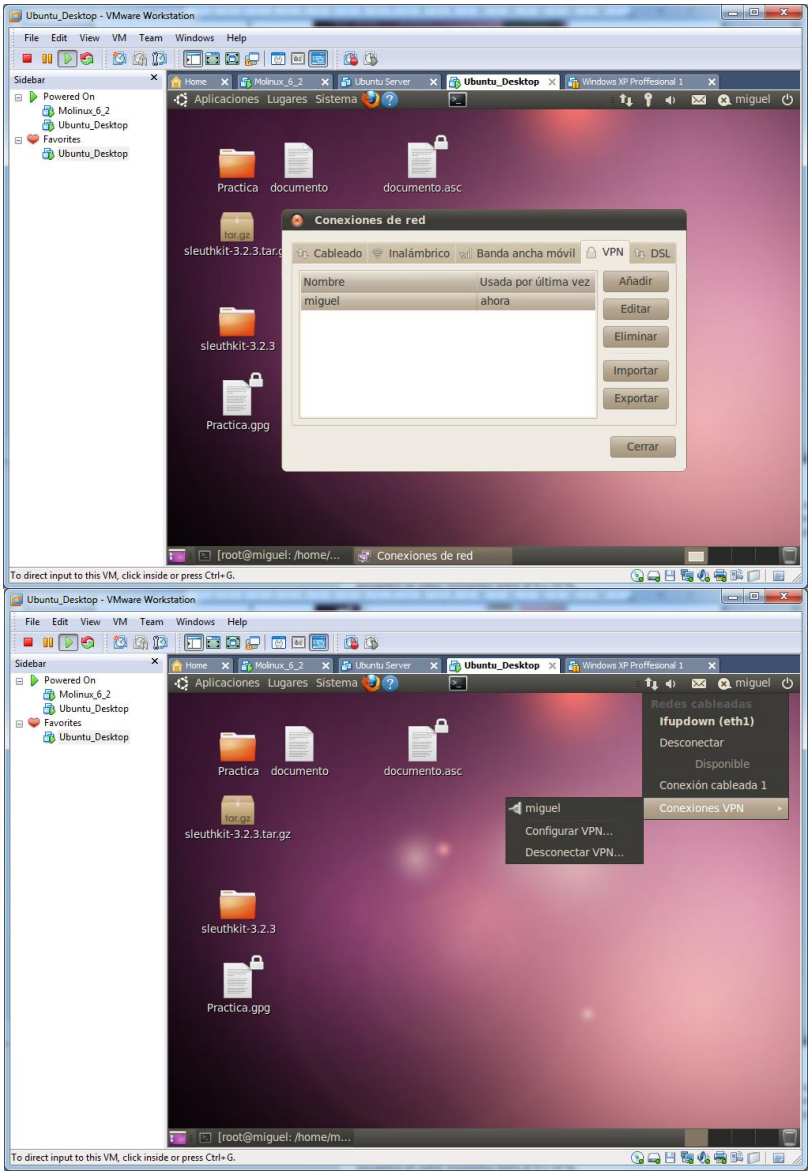
Abrimos un cliente Ubuntu, y configuramos el cliente VPN.

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.

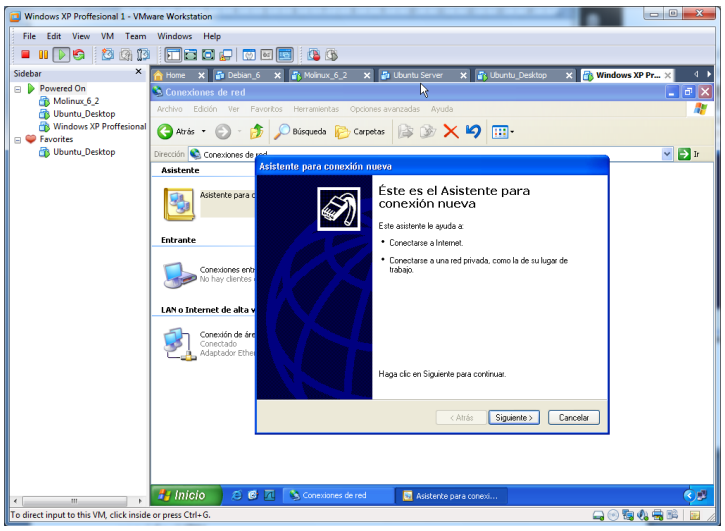


Una vez aplicado los cambios, arrancamos la conexión.

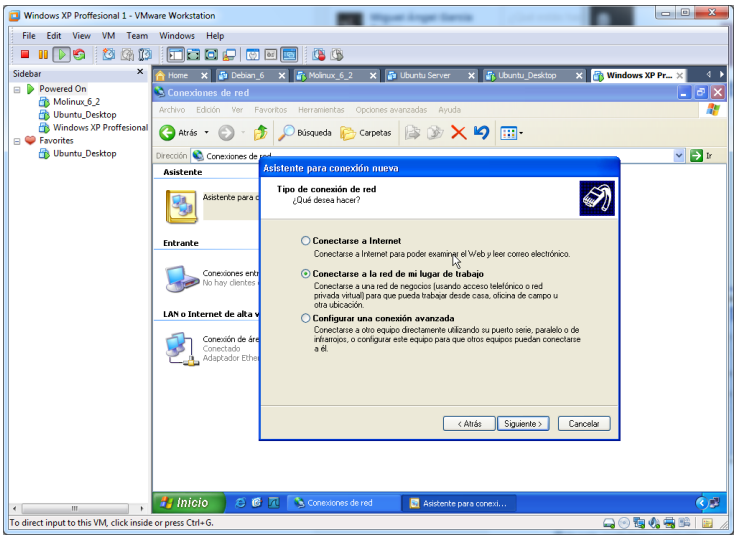


d) Conexión desde un cliente Windows y GNU/Linux VPN a un servidor VPN.

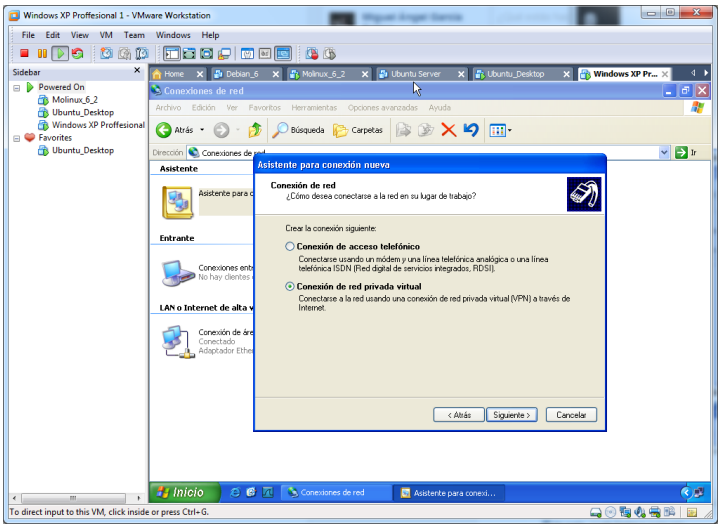
En conexiones de red de un XP, creamos una nueva conexión con el asistente de conexión nueva.



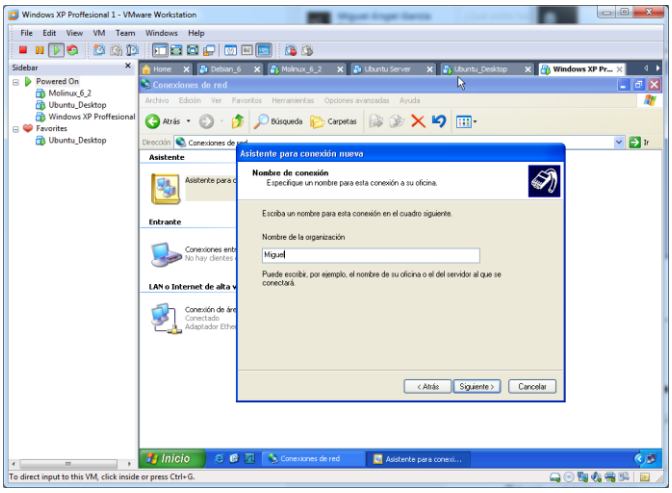
Elegimos la opción "**Conectarse a la red de mi lugar de trabajo**"



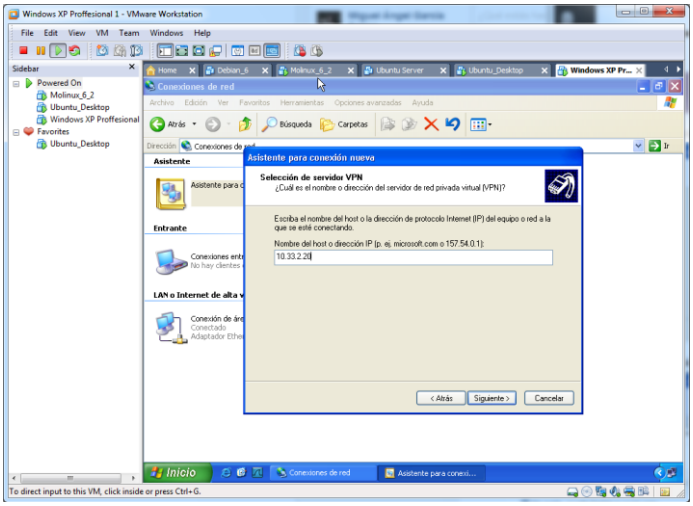
Seguidamente elegimos la opción "**Conexión de red privada virtual**" para conectarse a la red usando VPN a través de Internet.



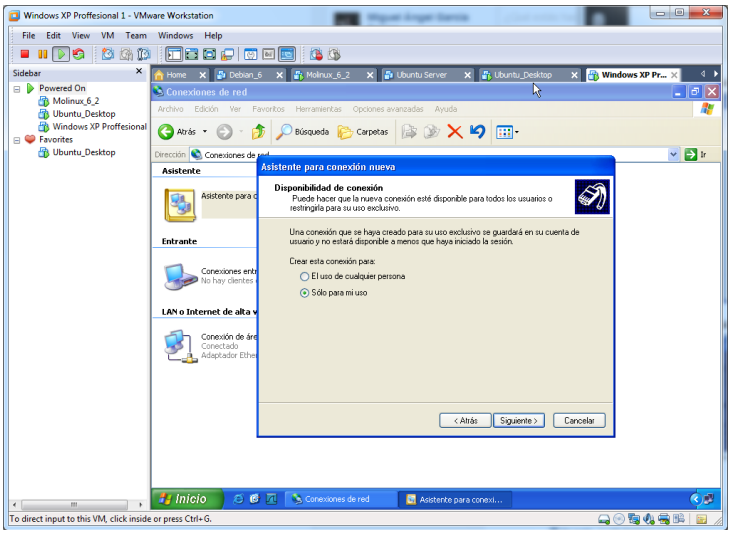
Pulsamos siguiente, y nos desplegara la siguiente ventana. Escribimos un nombre de organización para la conexión.



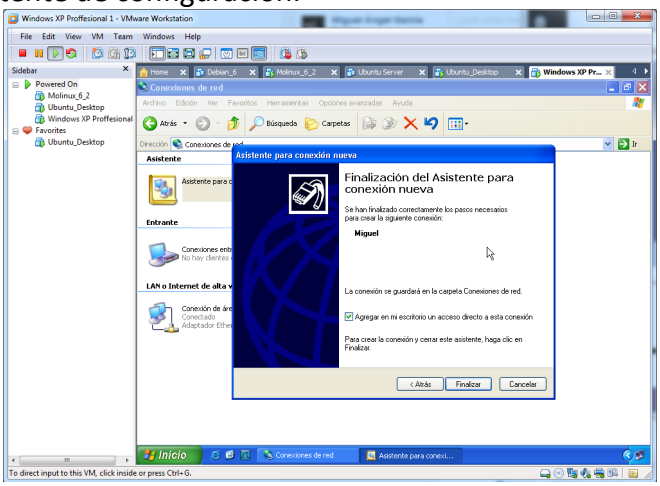
Escribimos la dirección IP del host al que nos vamos a conectar.



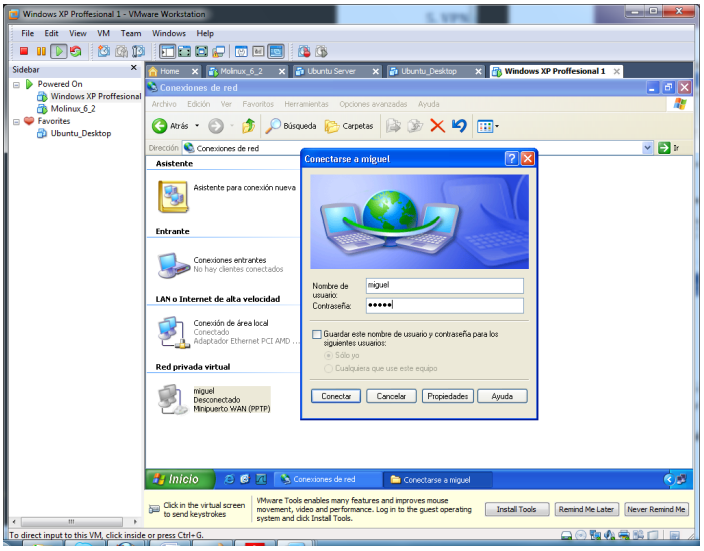
Elegimos la segunda opción, “**Sólo para mi uso**”



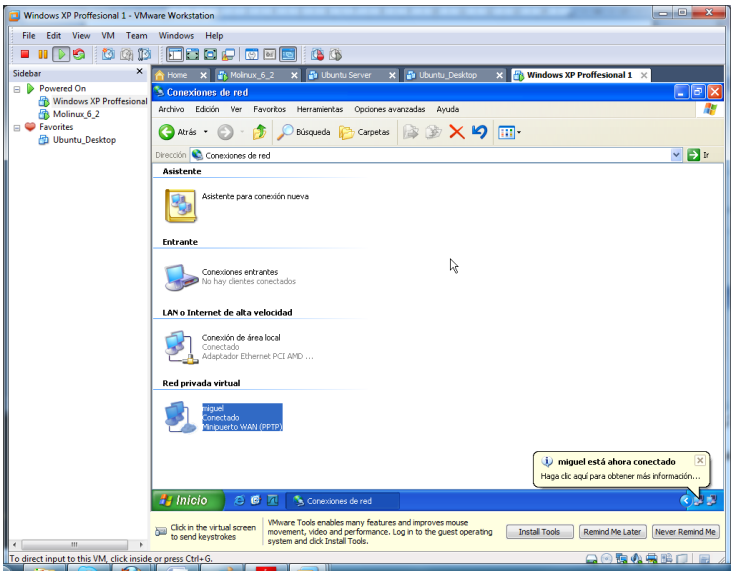
Finalizamos el asistente de configuración.



Establecemos el usuario y la contraseña



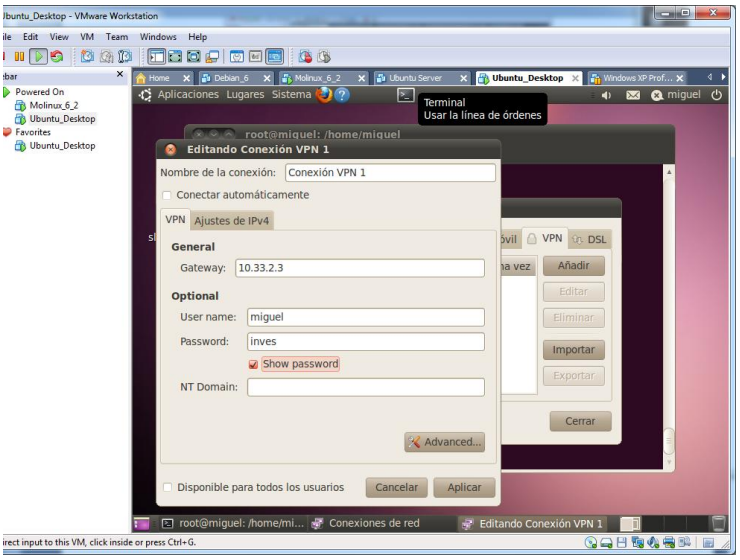
Comprobamos que se ha establecido la conexión con éxito.



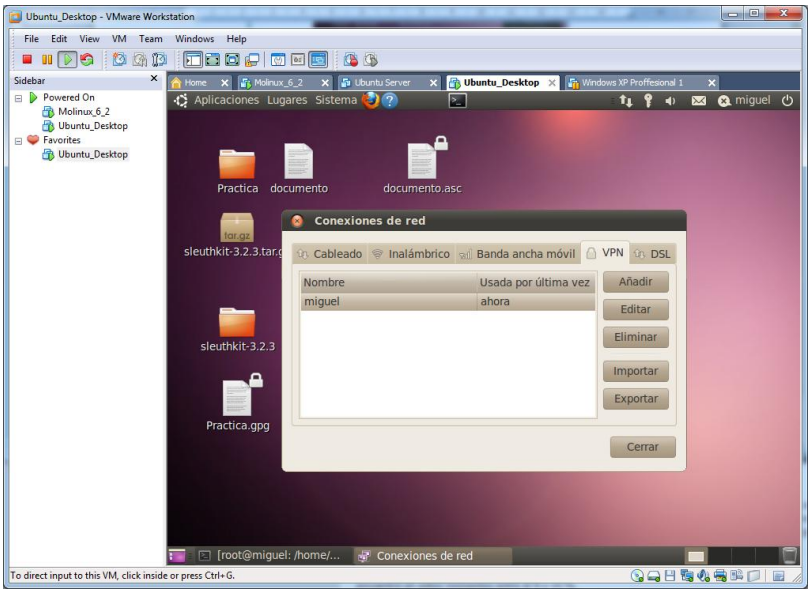
Abrimos un cliente Ubuntu, y configuramos el cliente VPN.

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

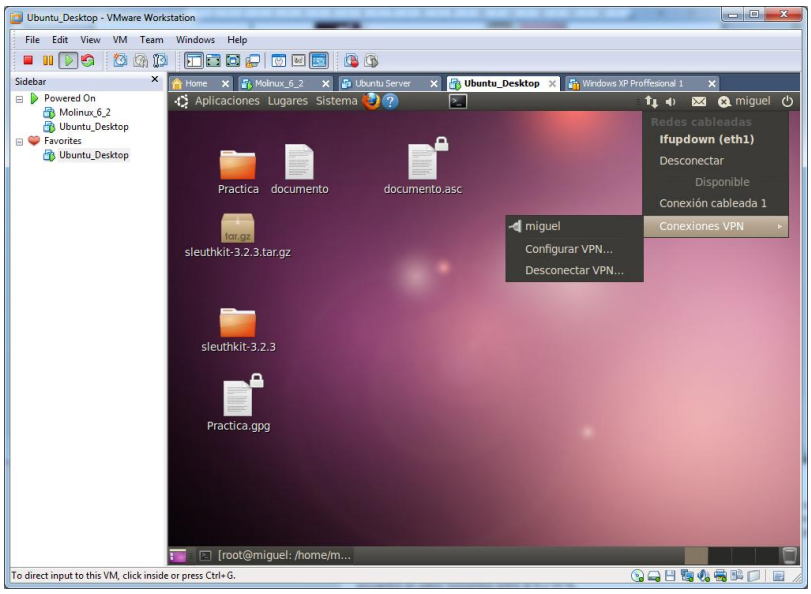
Editamos las conexiones VPN, elegimos la puerta de enlace a la que nos vamos a conectar con su respectivo usuario y contraseña.



Una vez aplicado los cambios, arrancamos la conexión.



Esperamos a que se conecte.

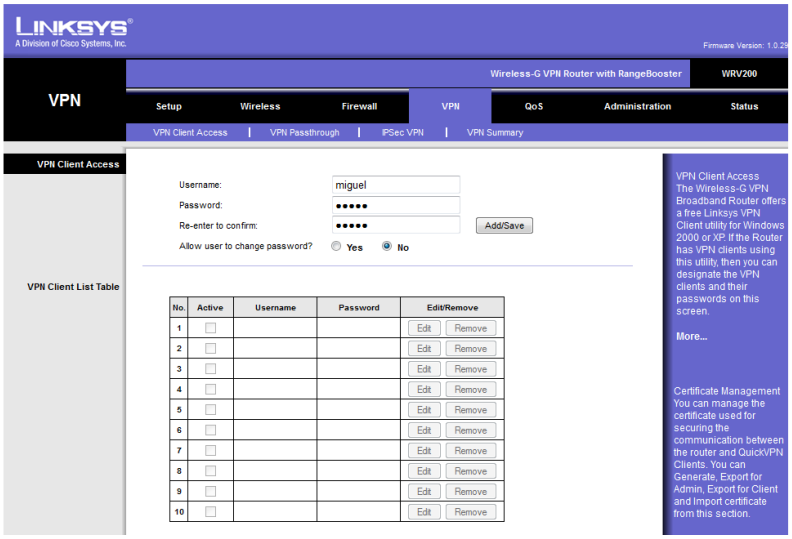


5. VPN de acceso remoto

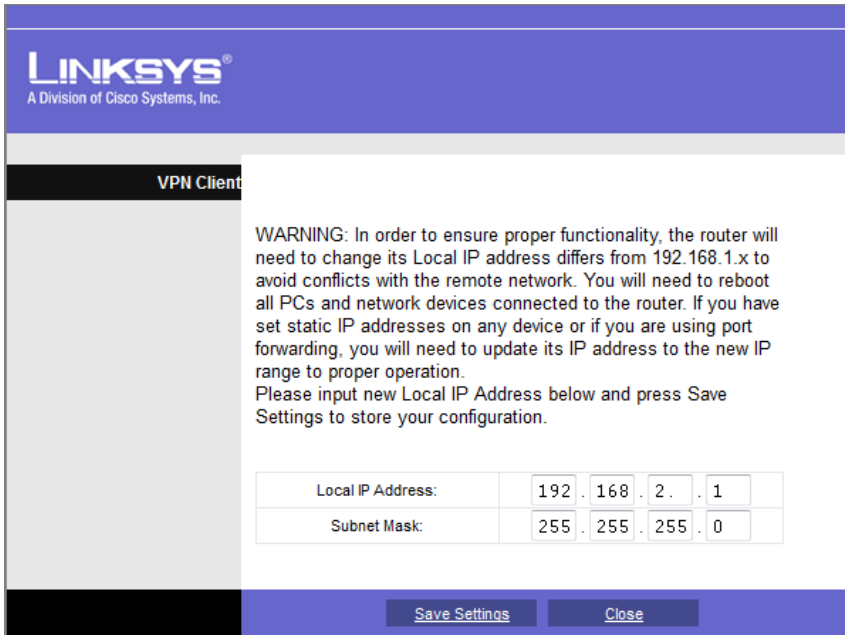
a) Utiliza la plantilla del curso virtual para configurar los parámetros.

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

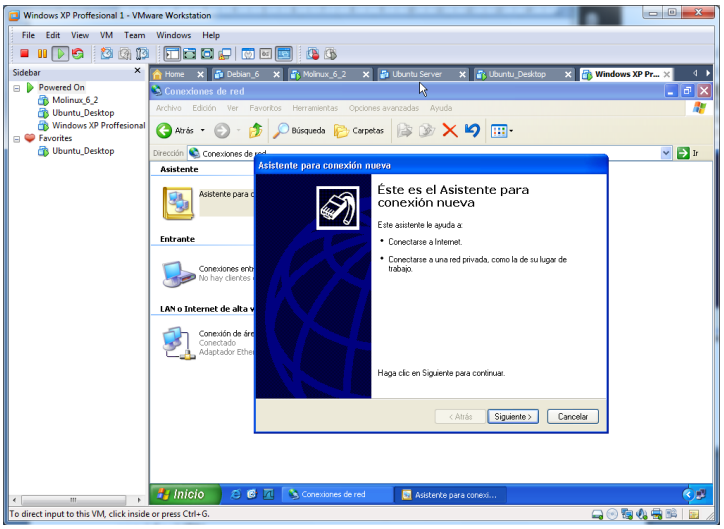


Una vez pulsado el botón "**ADD**" configuramos la IP a través de la siguiente pantalla.

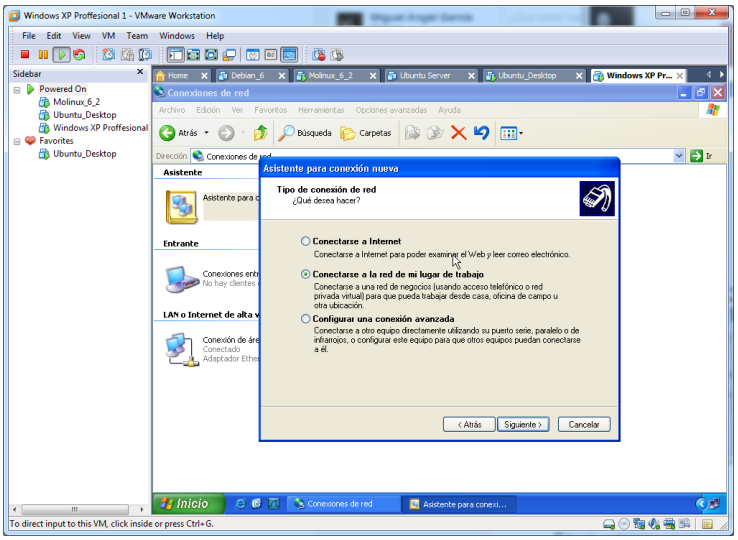


c) Configura tu cliente VPN en Windows.

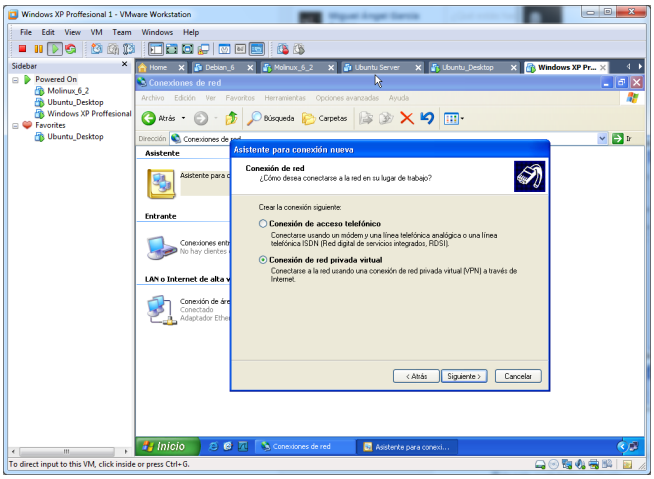
En conexiones de red de un XP, creamos una nueva conexión con el asistente de conexión nueva.



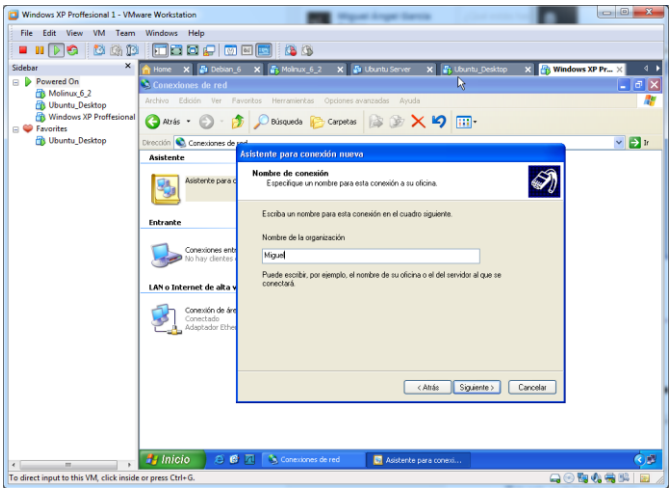
Elegimos la opción “**Conectarse a la red de mi lugar de trabajo**”



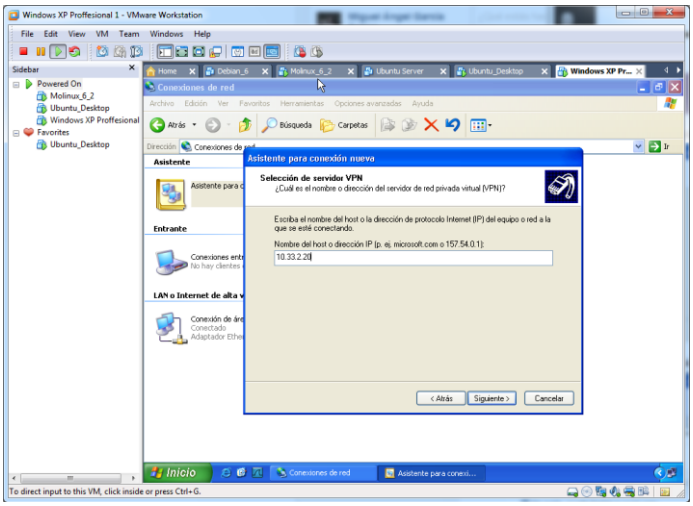
Seguidamente elegimos la opción “**Conexión de red privada virtual**” para conectarse a la red usando VPN a través de Internet.



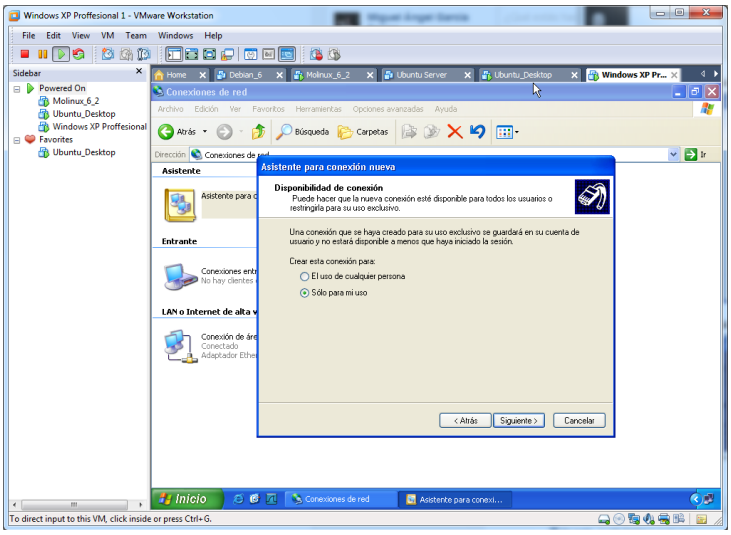
Pulsamos siguiente, y nos desplegara la siguiente ventana. Escribimos un nombre de organización para la conexión.



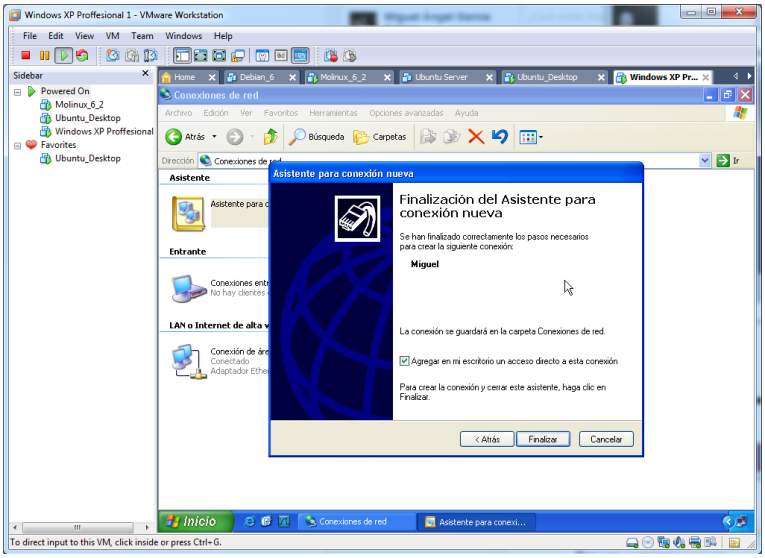
Escribimos la dirección IP del host al que nos vamos a conectar.



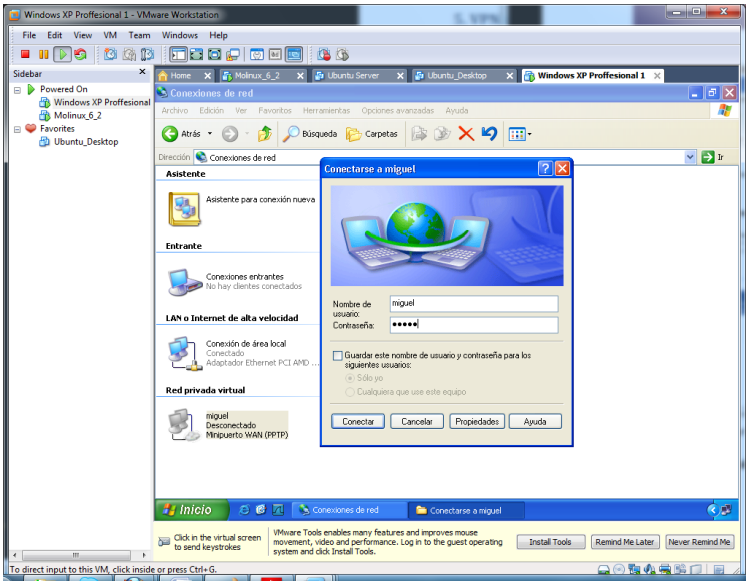
Elegimos la segunda opción, “**Sólo para mi uso**”



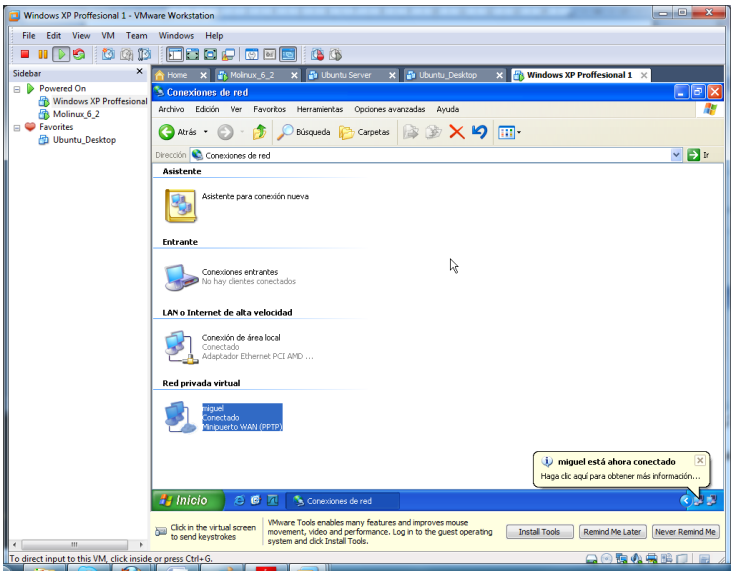
Finalizamos el asistente de configuración.



Establecemos el usuario y la contraseña



Comprobamos que se ha establecido la conexión con éxito.



6. VPN sitio a sitio

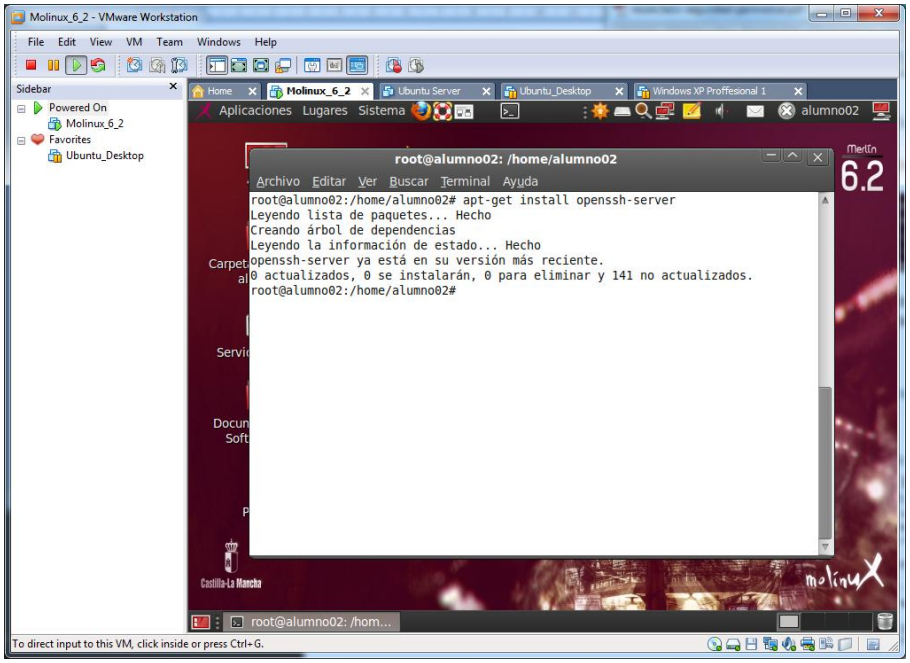
a) Utiliza la plantilla del curso virtual para configurar los parámetros.

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

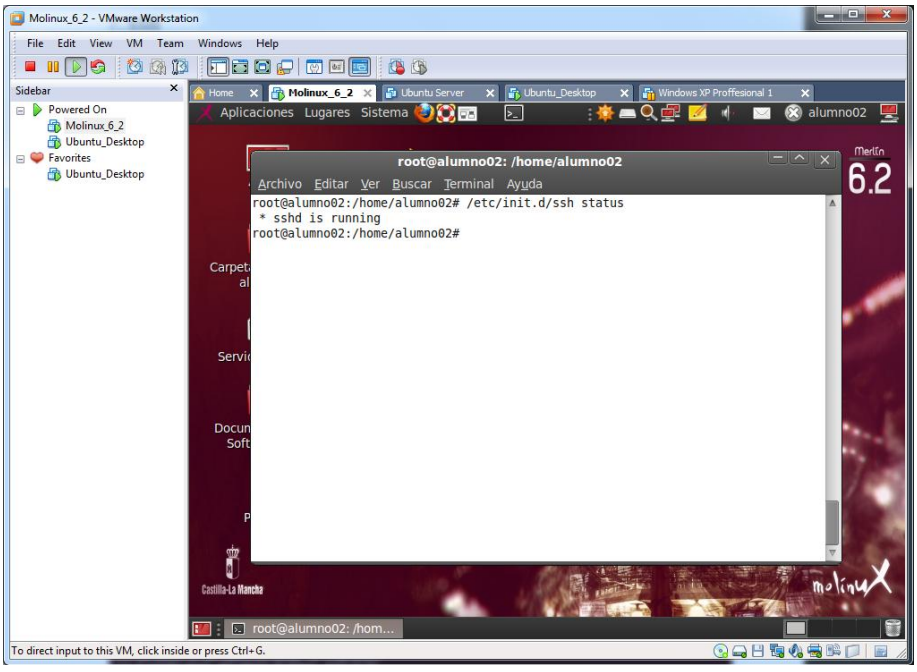
TECNICAS DE CIFRADO: COMUNICACIONES SEGURAS

7. SSH
a) Instalación del servidor SSH en GNU/Linux

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

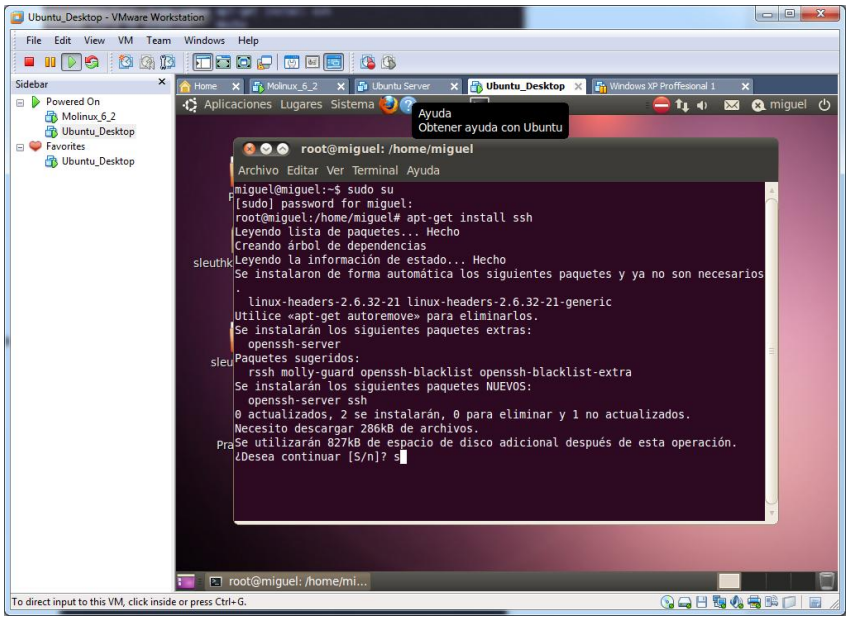


Comprobamos el estado del servidor ssh con el comando "**/etc/init.d/ssh status**"

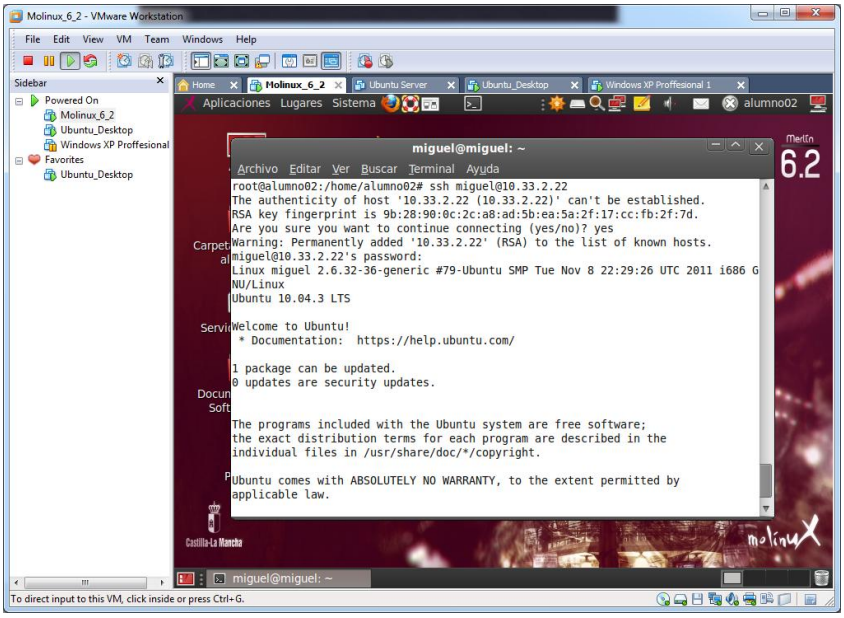


b) Conexión al servidor SSH mediante cliente GNU/Linux y cliente Windows.

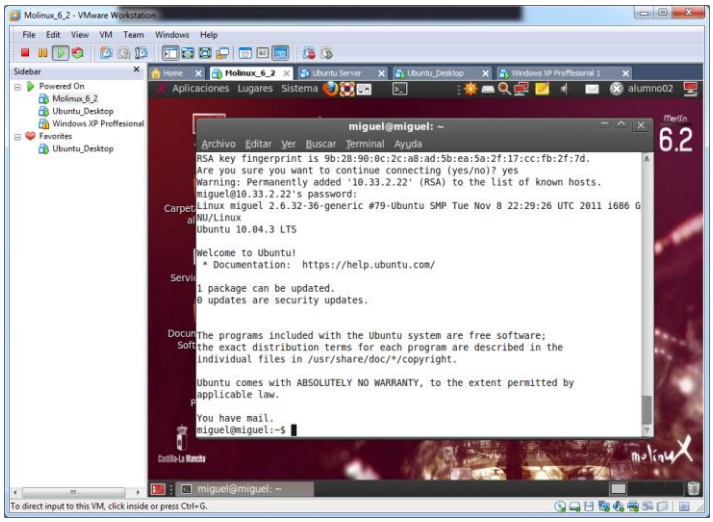
Tenemos instalado el servidor SSH.



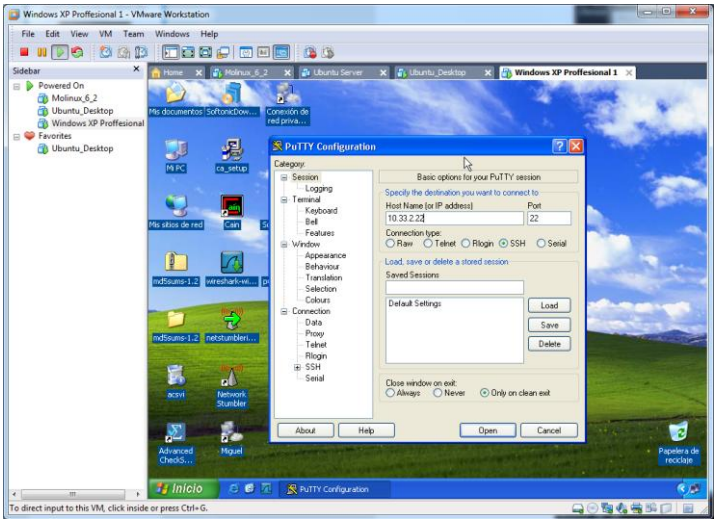
Desde un cliente, ejecutamos **“ssh miguel@10.33.2.22”** esto nos permitirá conectarnos mediante el cliente miguel al pc (10.33.2.22)y así realizar operaciones remotas.



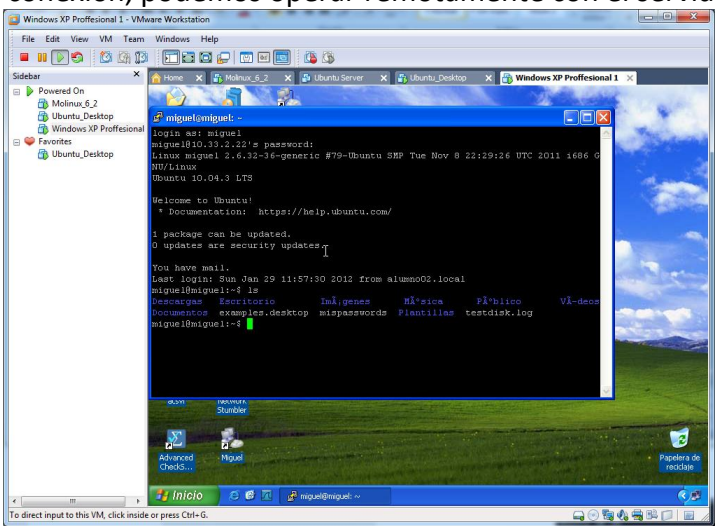
Comprobamos que está conectado.



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.

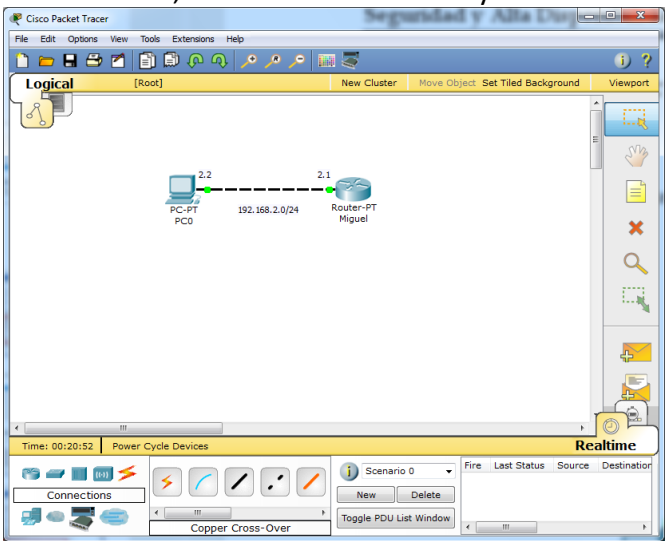


Una vez conectados a la consola, elegimos el usuario, ingresamos la contraseña, y una vez tengamos la conexión, podemos operar remotamente con el servidor.

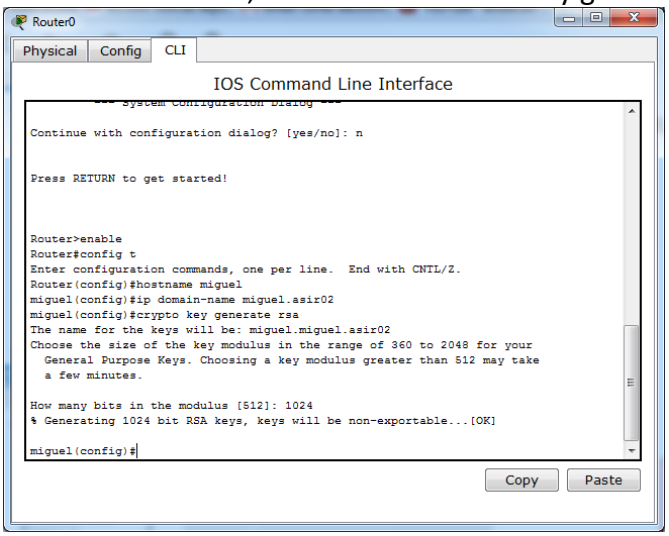


c) Escenario CISCO: Conexión segura a la administración de un router.

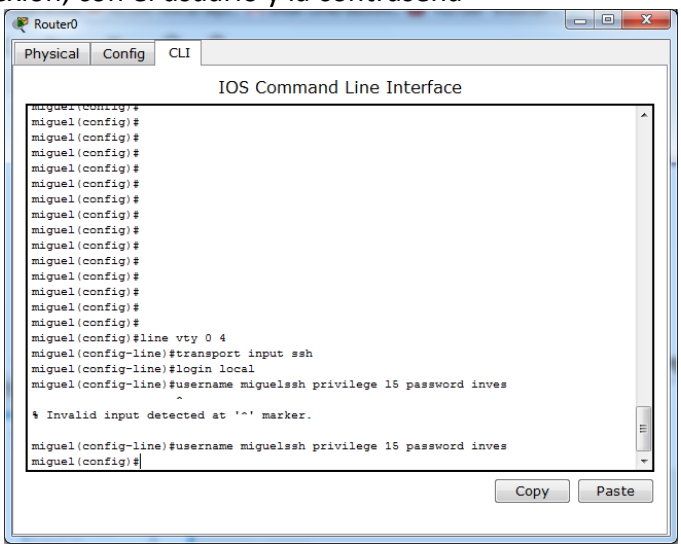
Tenemos el siguiente escenario, con un router con ssh y un cliente.



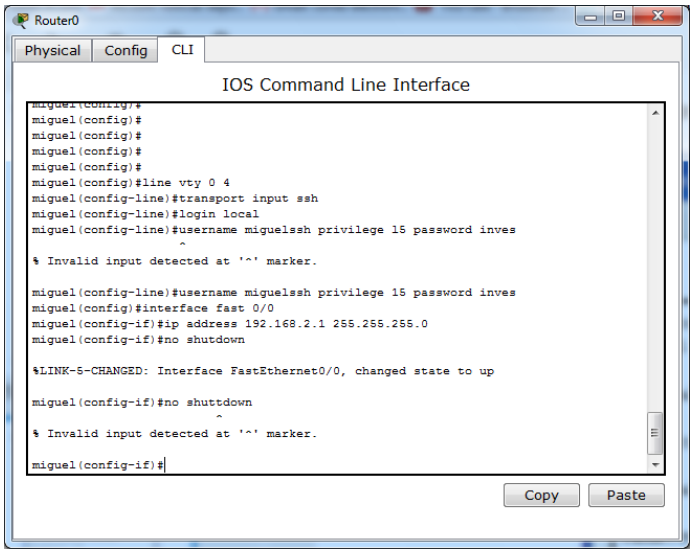
Configuramos el nombre del servidor, el nombre de dominio y generamos una clave.



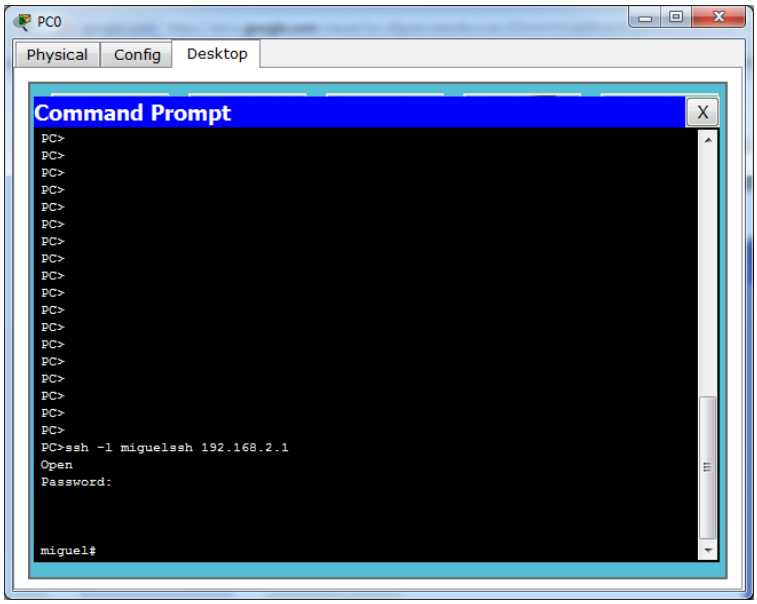
Activamos la conexión, con el usuario y la contraseña



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



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

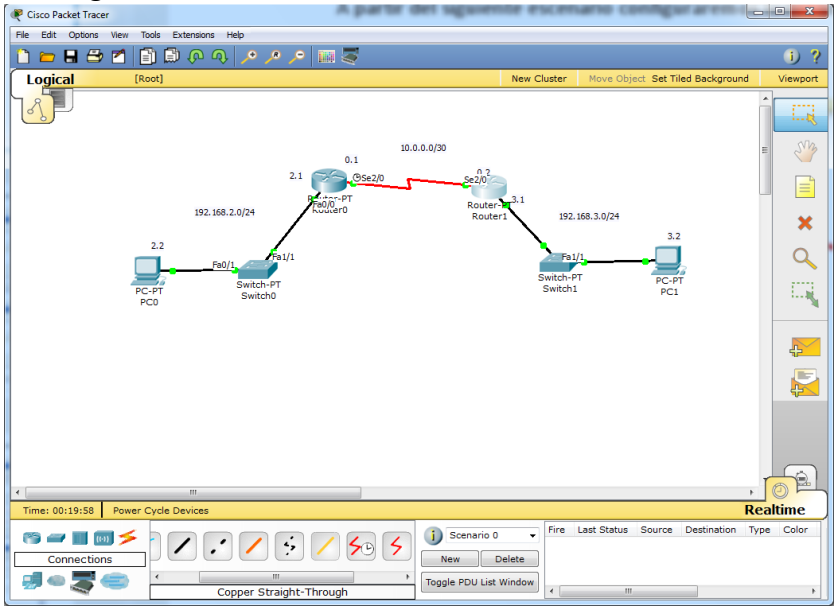


SERVIDORES DE ACCESO REMOTO

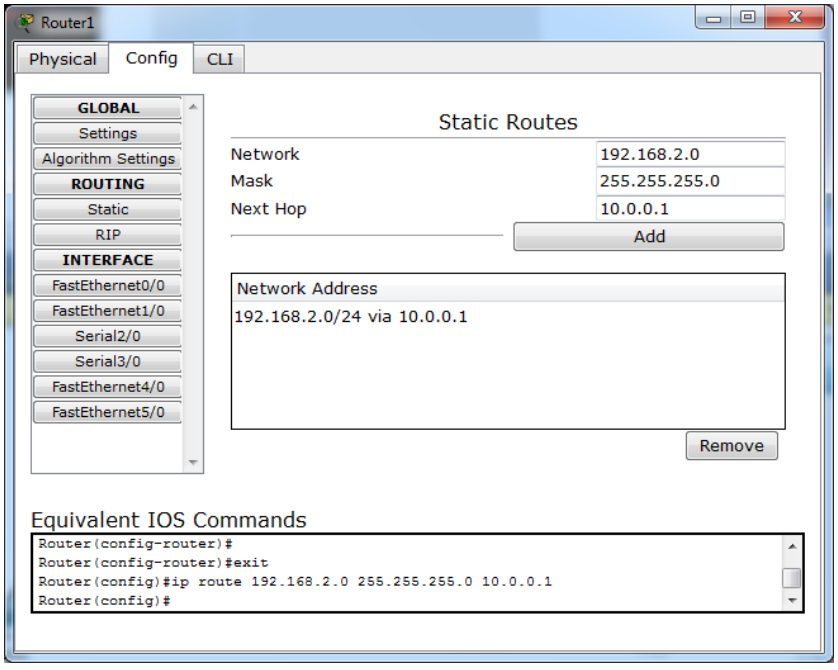
8. Protocolos de autenticación:
a) Escenarios CISCO: Interconexión de redes mediante protocolos PPP, PAP, CHAP

PPP

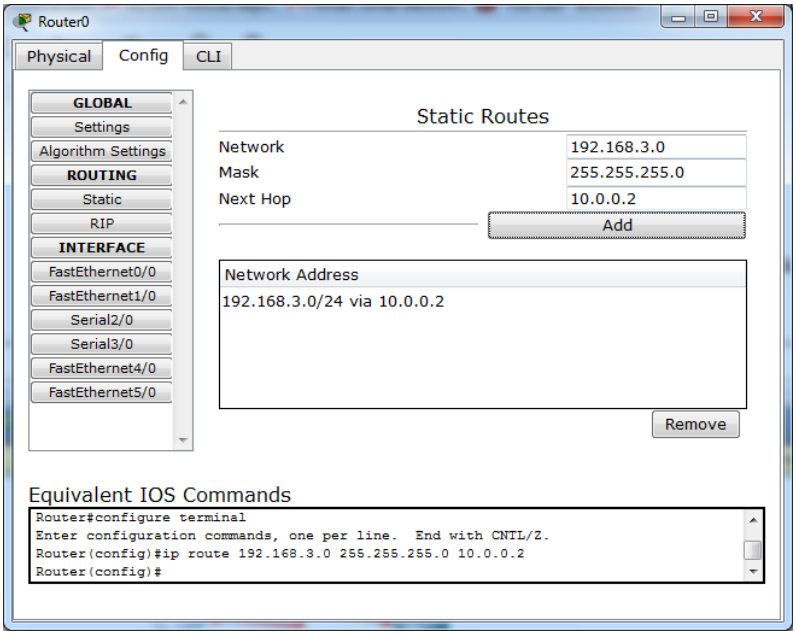
Configuramos el siguiente escenario.



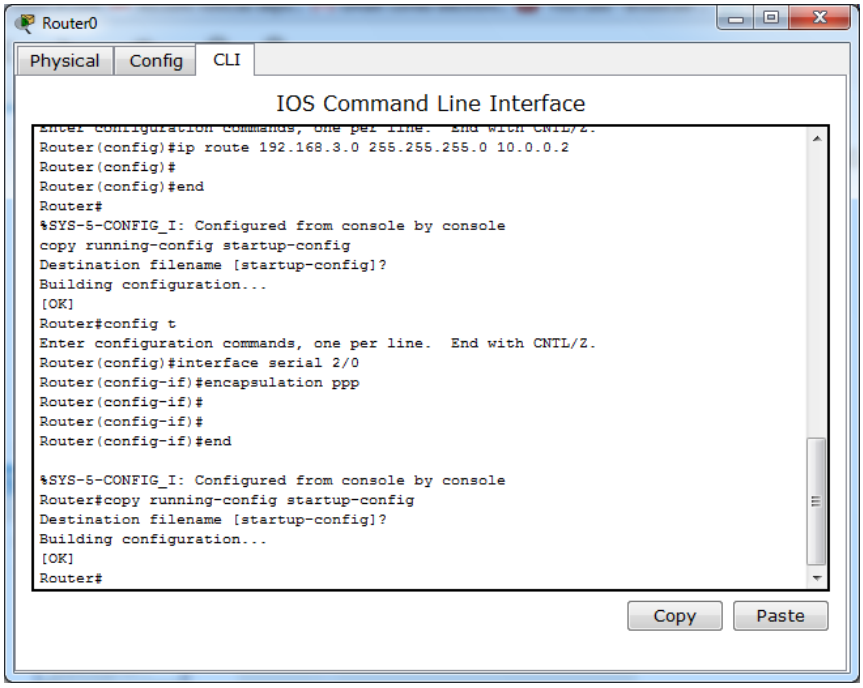
Configuramos el router 1, estableciendo el enrutamiento correcto.



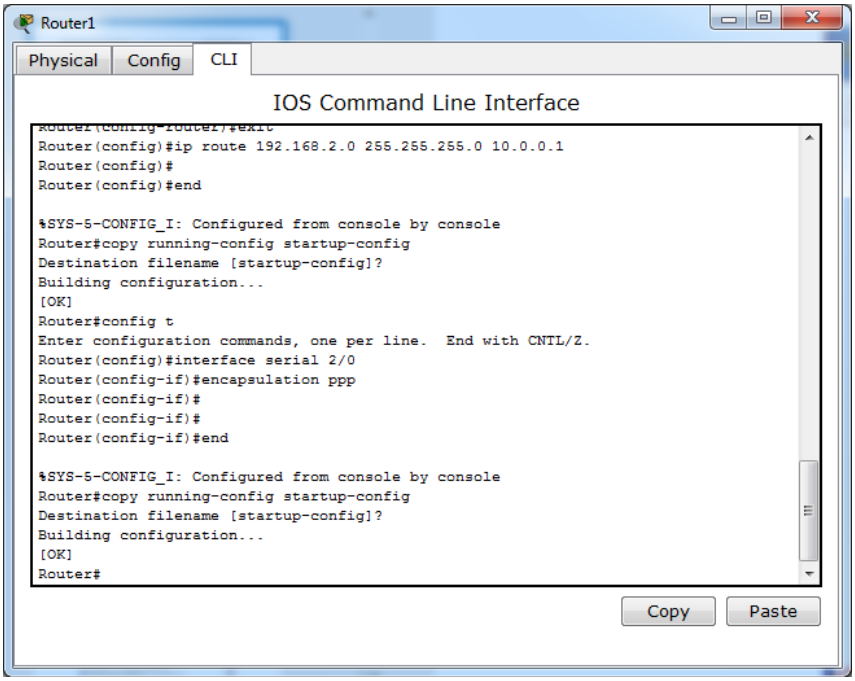
Configuramos el router 0, estableciendo el enrutamiento correcto.



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

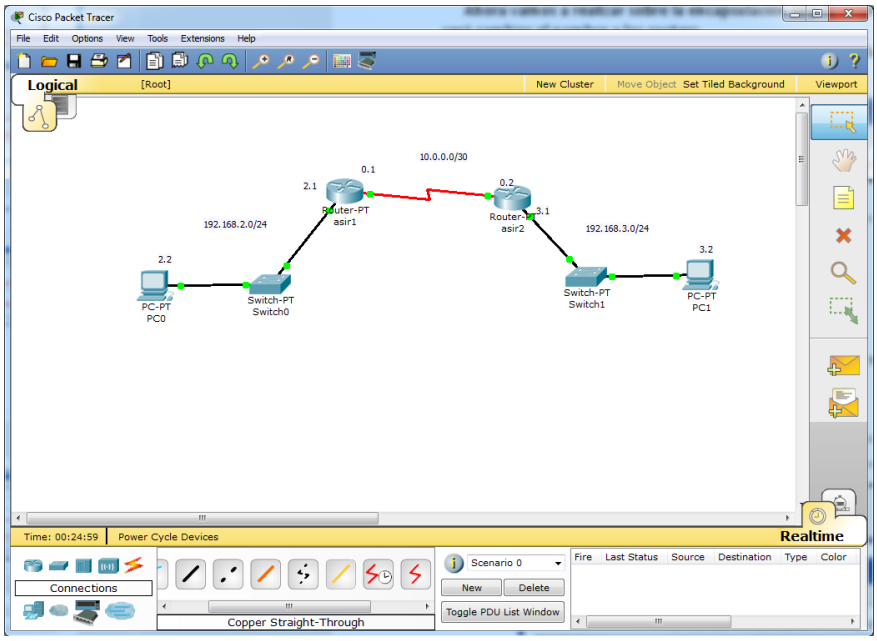


Configuramos el serial **2/0** con el protocolo de encapsulación **ppp en el router 1.**

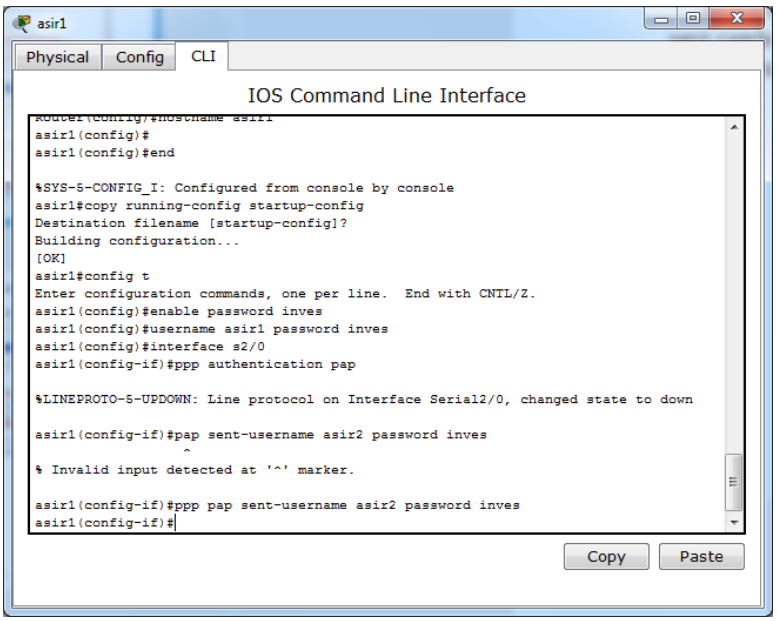


Autenticación PAP

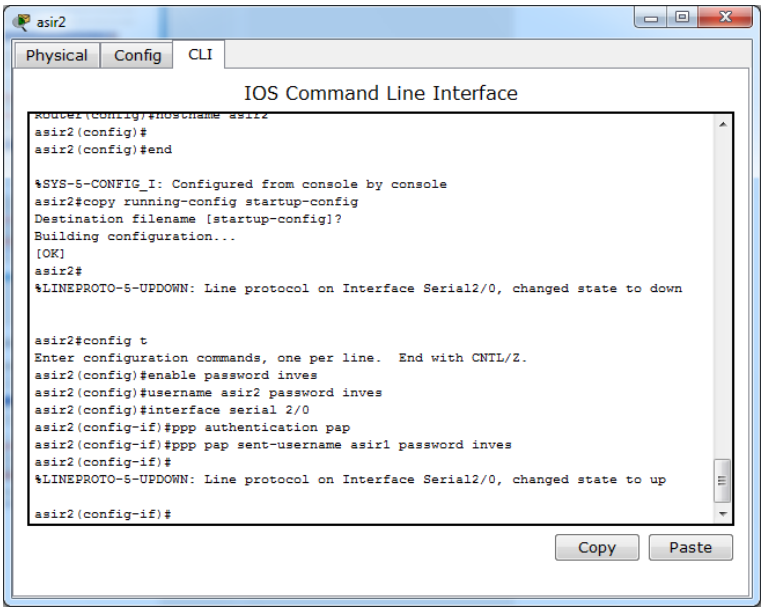
Cambiamos el nombre de los routers (**hostname**)



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



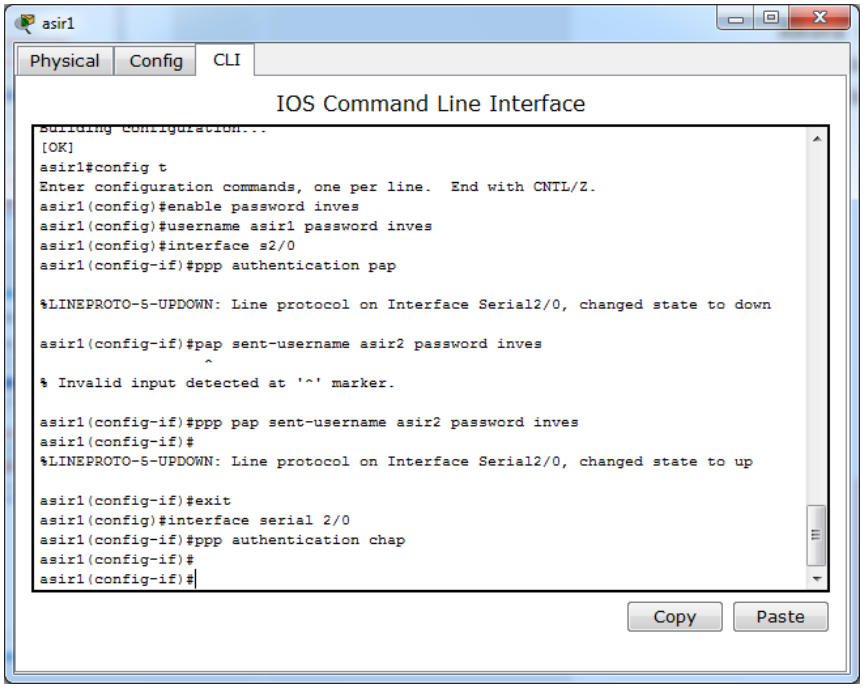
En el router **asir2** habilitamos una contraseña, y un usuario. En la interfaz **serial 2/0** establecemos el protocolo de autenticación pap.



Autenticación CHAP

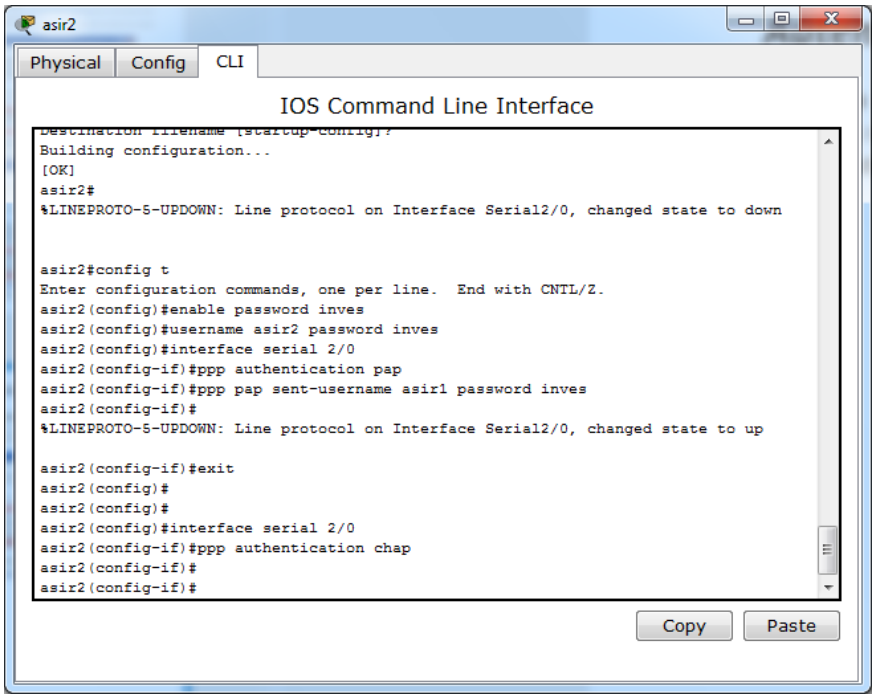
Router asir1

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



Router asir2

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



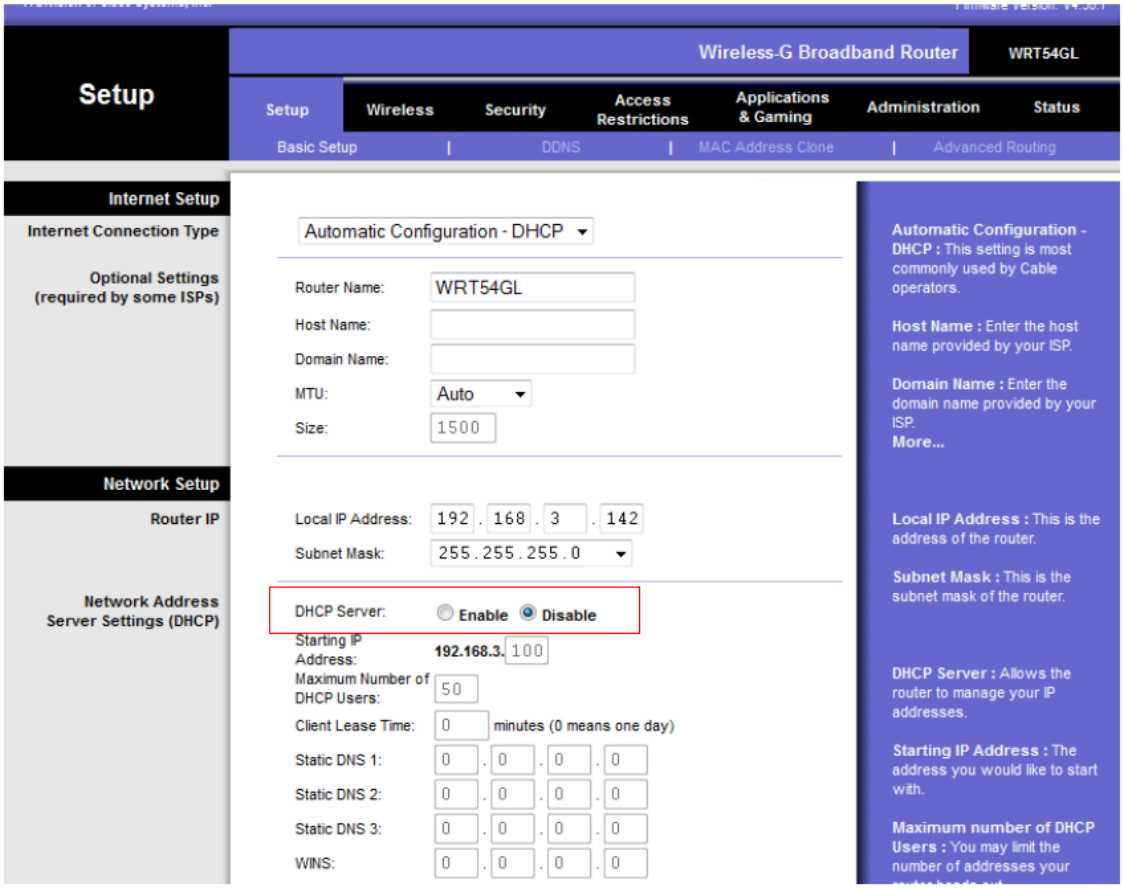
SERVIDORES DE ACCESO REMOTO

9. Servidores de autenticación

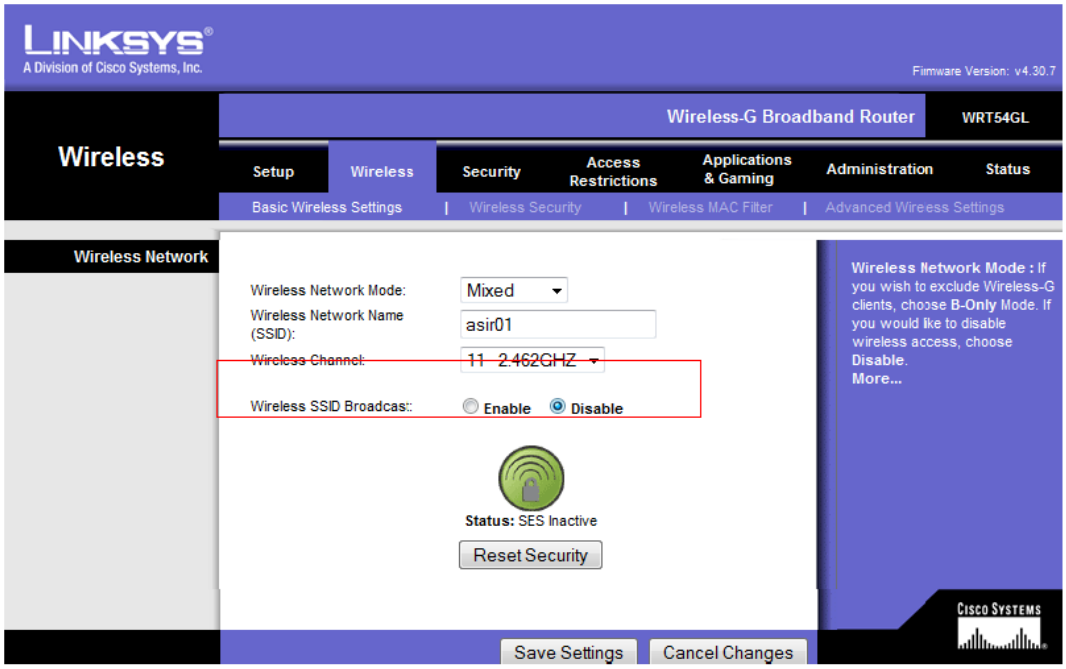
a) REDES INALÁMBRICAS: WPA Personal

- 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).*

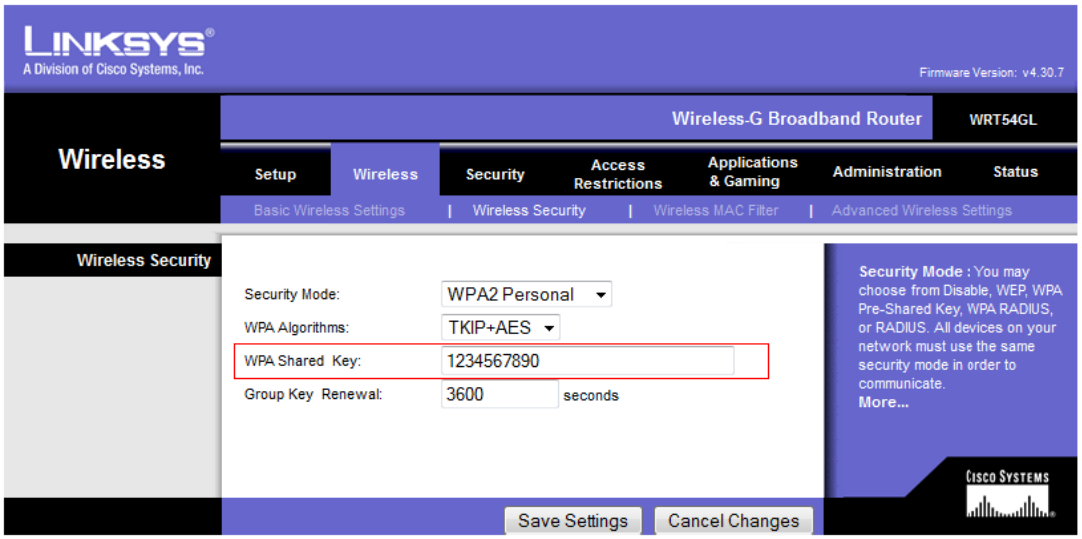
Una vez hemos accedido al router, nos situamos en la pestaña **Setup**, **Basic/Setup**, y deshabilitamos el **servidor DHCP**.



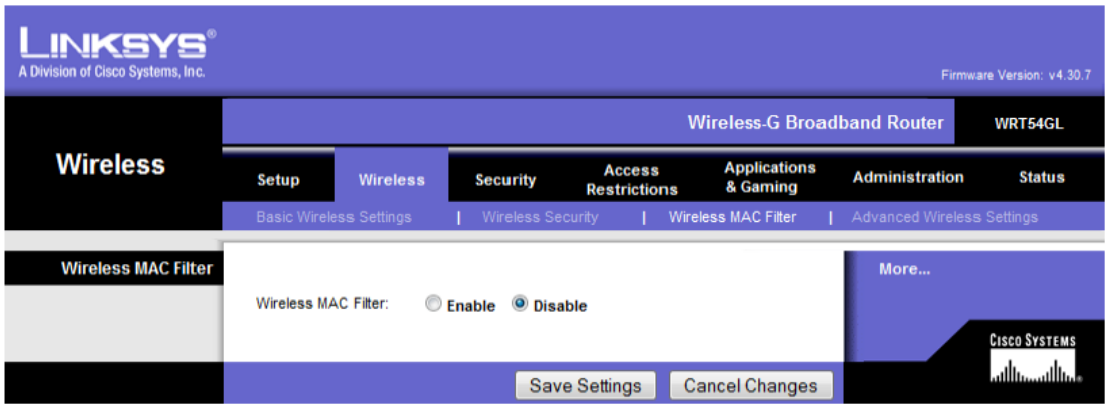
Ahora,en wireless /basic wireless Settings, desactivamos el SSID broadcast, y ponemos el nombre, en nuestro caso asir01.



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

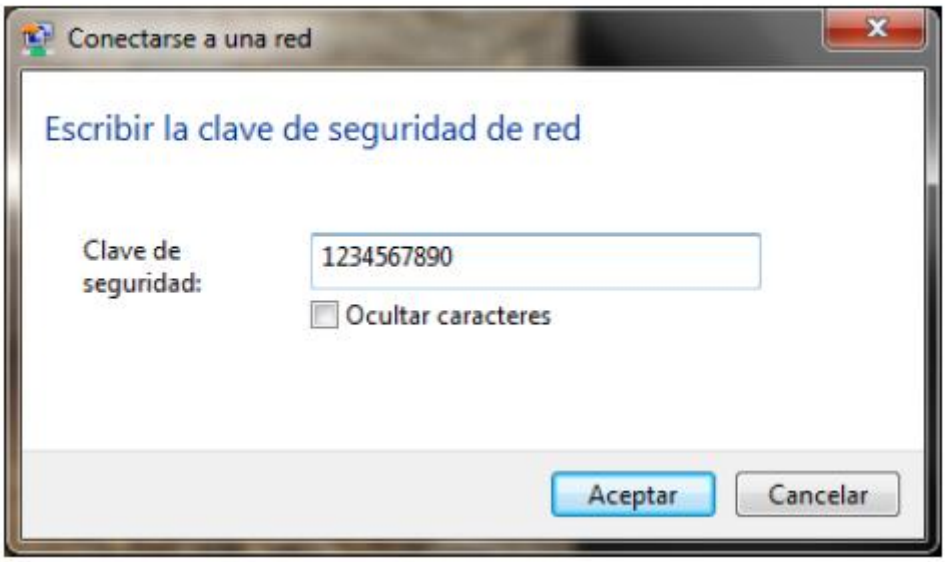


Deshabilitamos el filtro de MAC.



En un cliente, buscamos la red asir01.

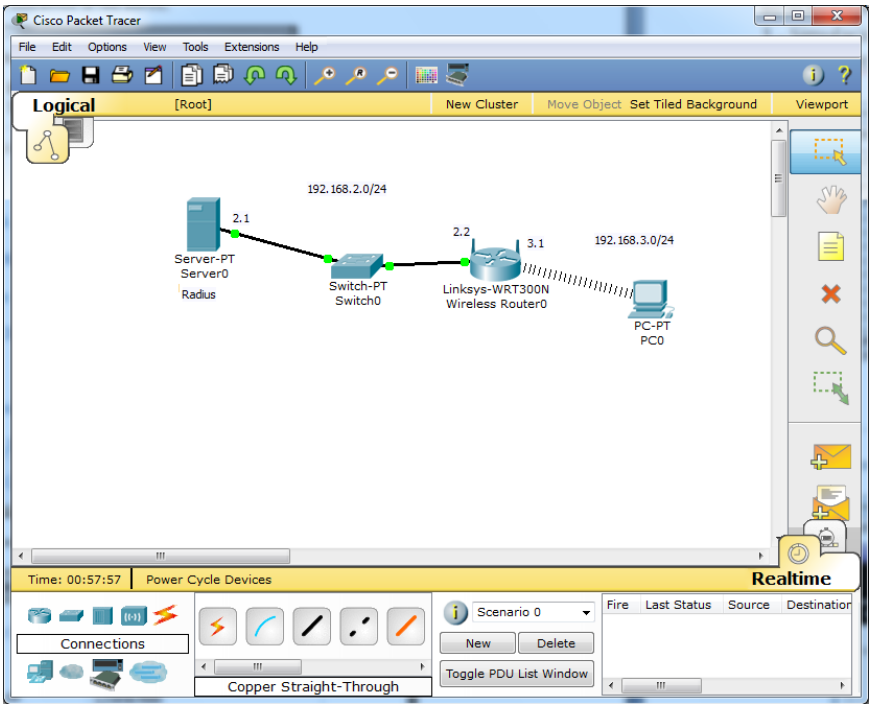
Y le introducimos la contraseña.



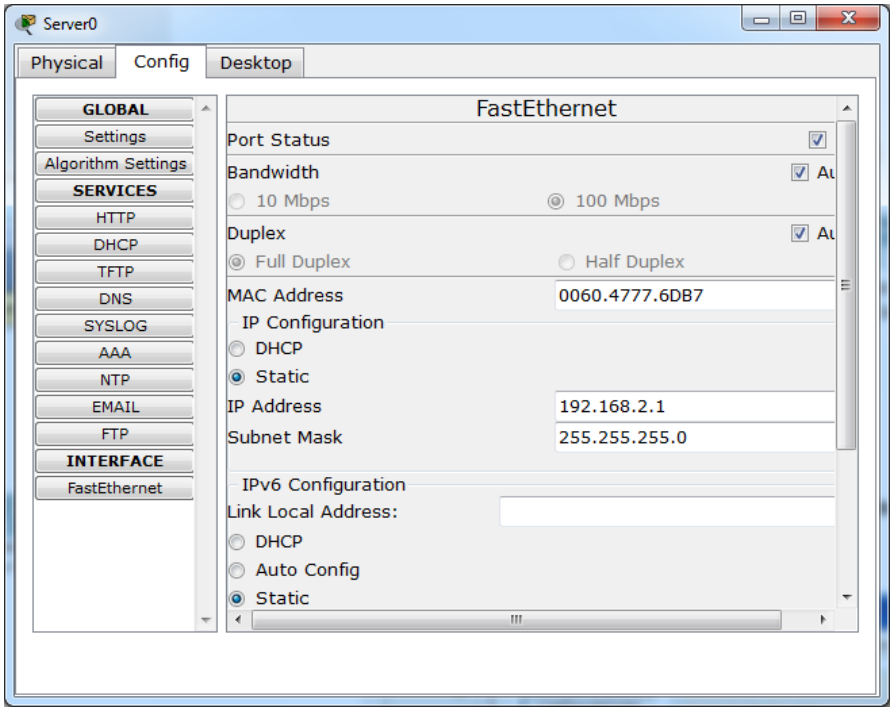
b) SERVIDOR RADIUS:

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

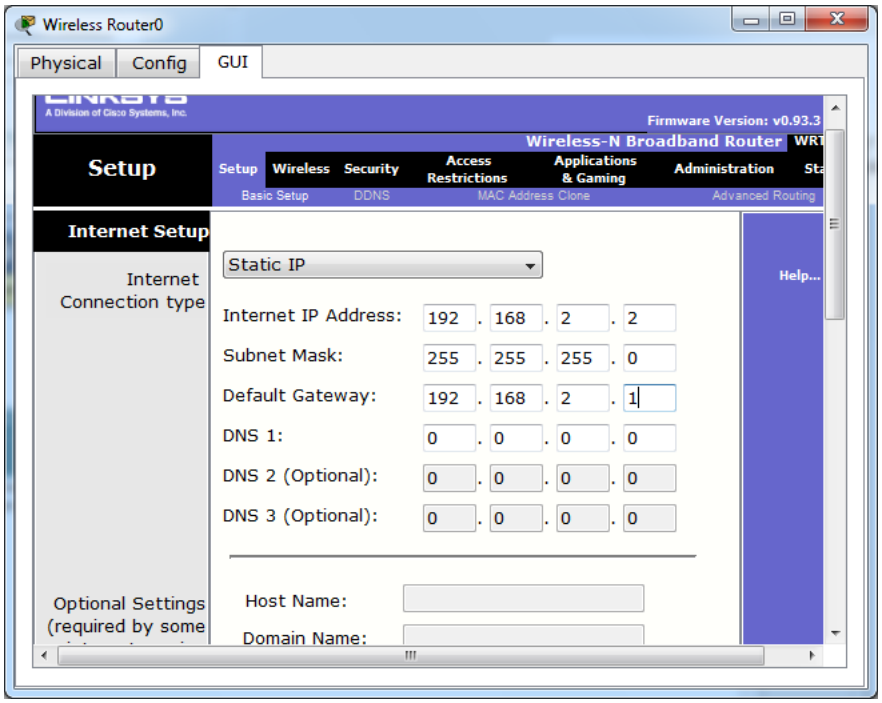
Tenemos planteado el siguiente esquema



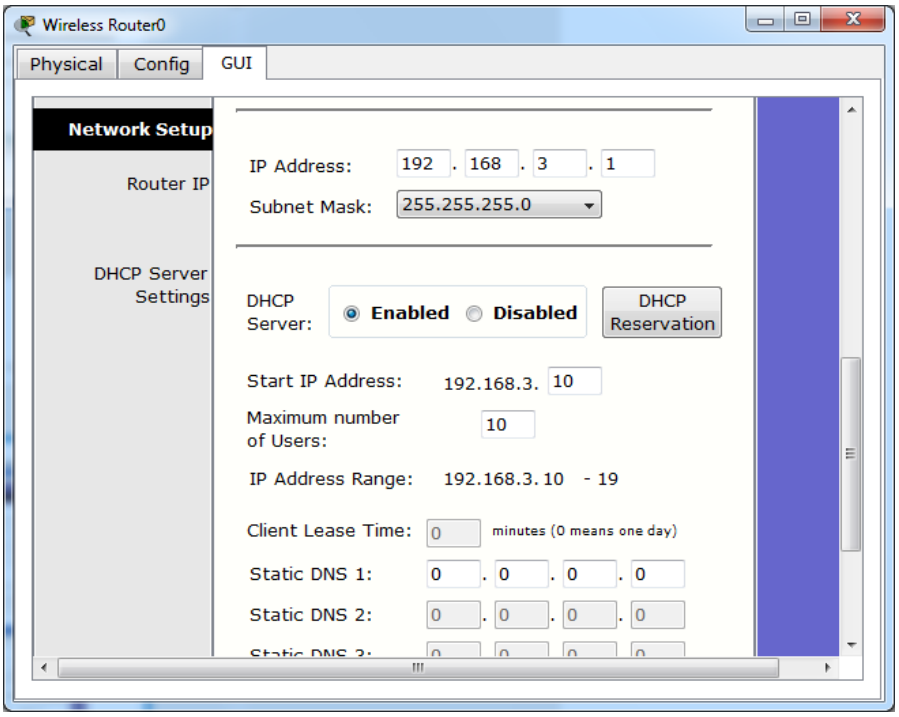
Configuramos la IP de la interfaz FastEthernet de nuestro servidor Radius.



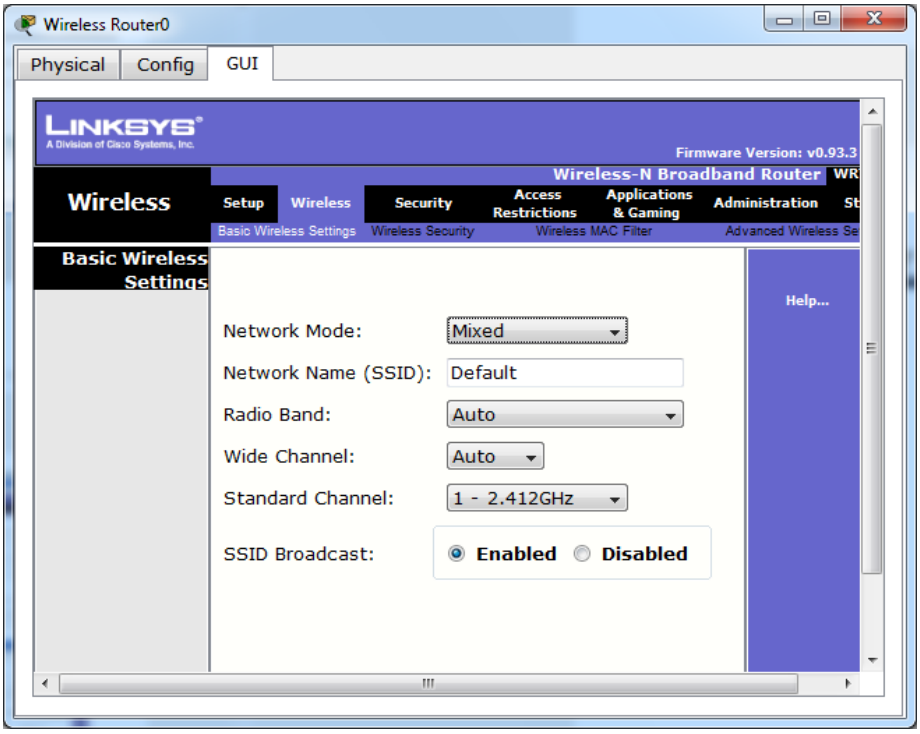
Seguidamente, configuramos la IP del router inalámbrico, estableciendo el servidor Radius como puerta de enlace.



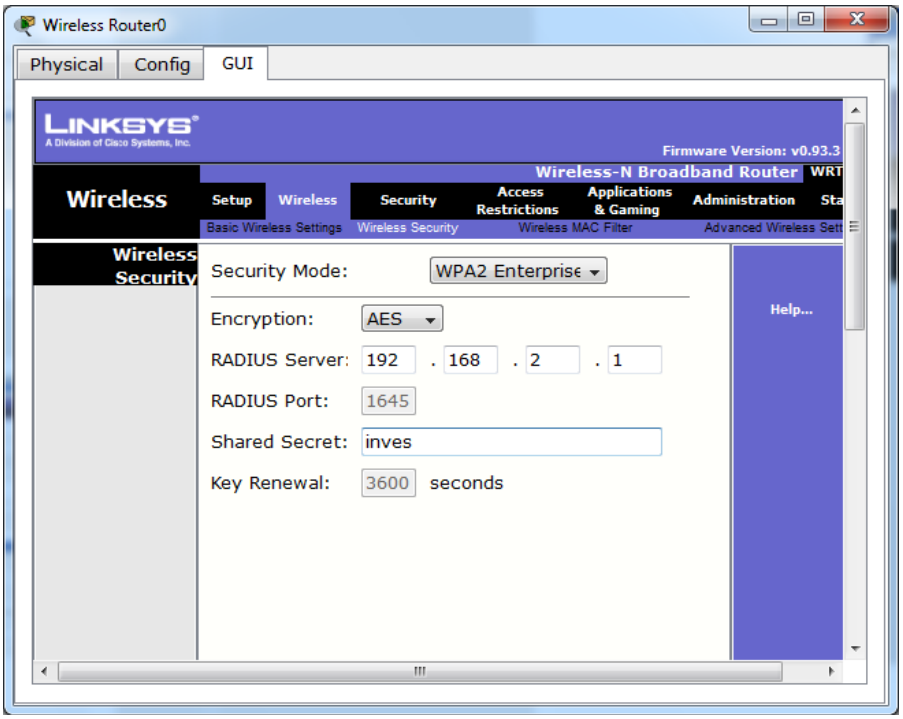
Habilitamos el servicio DHCP para asignar una IP a los equipos que se vayan a conectar al servidor Radius.



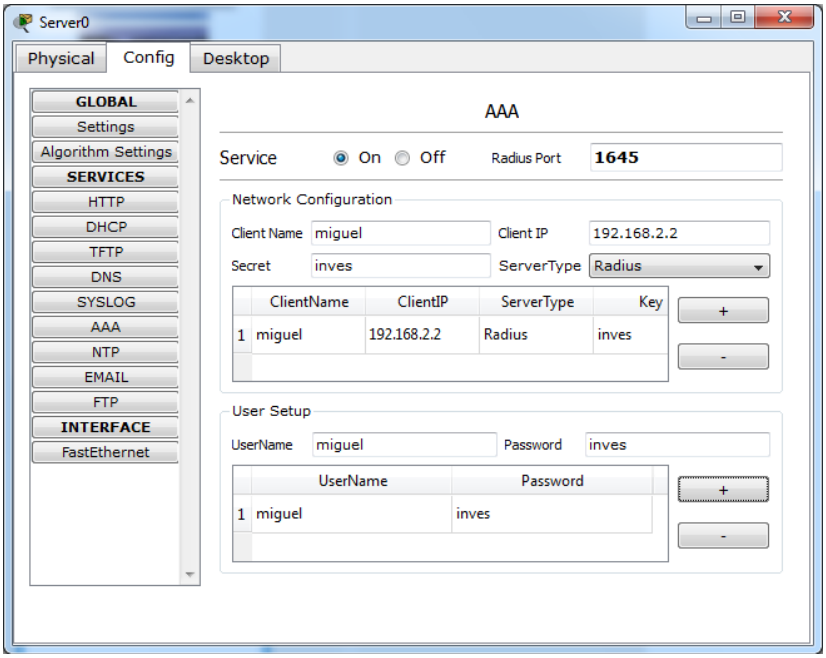
En el router inalámbrico, nos vamos a la pestaña Wireless y configuramos…



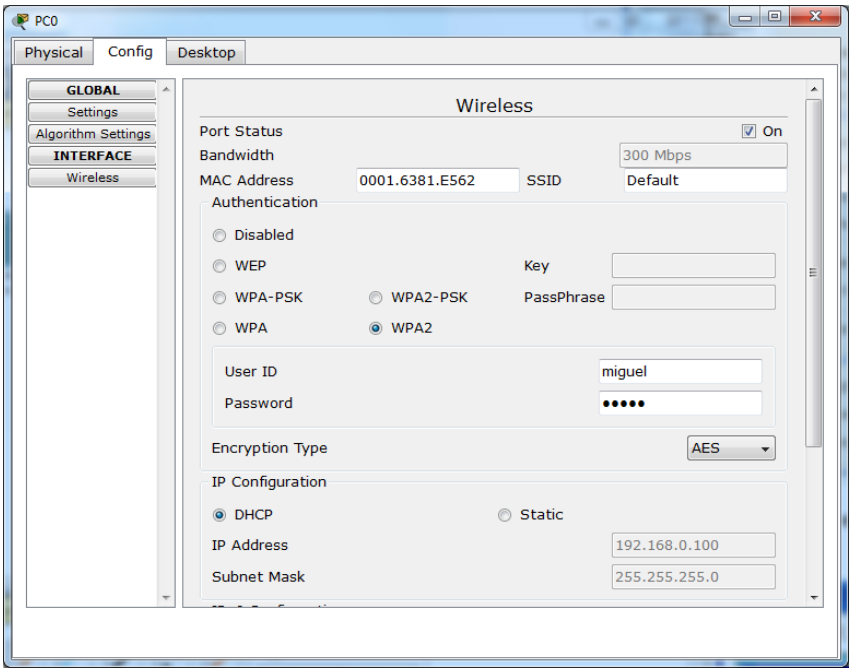
En **Wireless Security** introducimos la IP del servidor y la contraseña que utilizaremos.



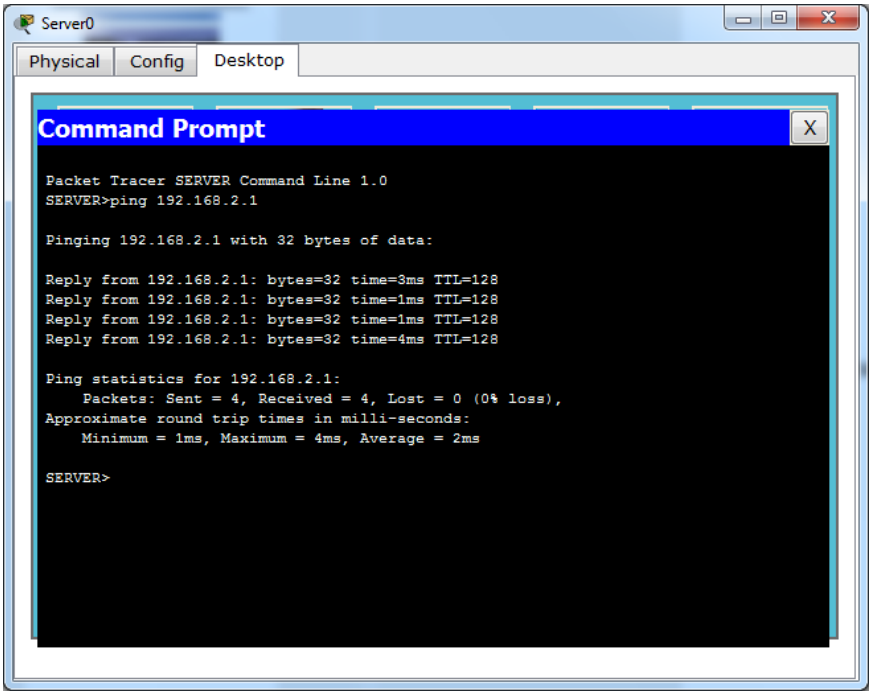
De vuelta en el servidor Radius, en la zona AAA configuramos los clientes Radius con su contraseña.



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

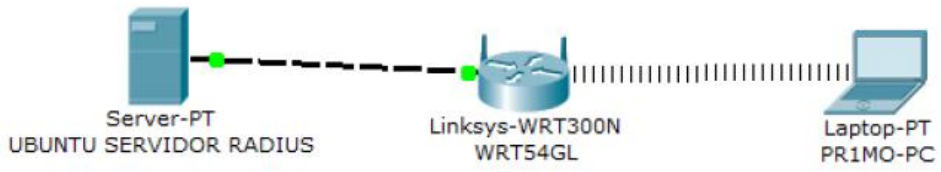


Abrimos el terminal del cliente, y comprobamos la conexión con el servidor Radius.

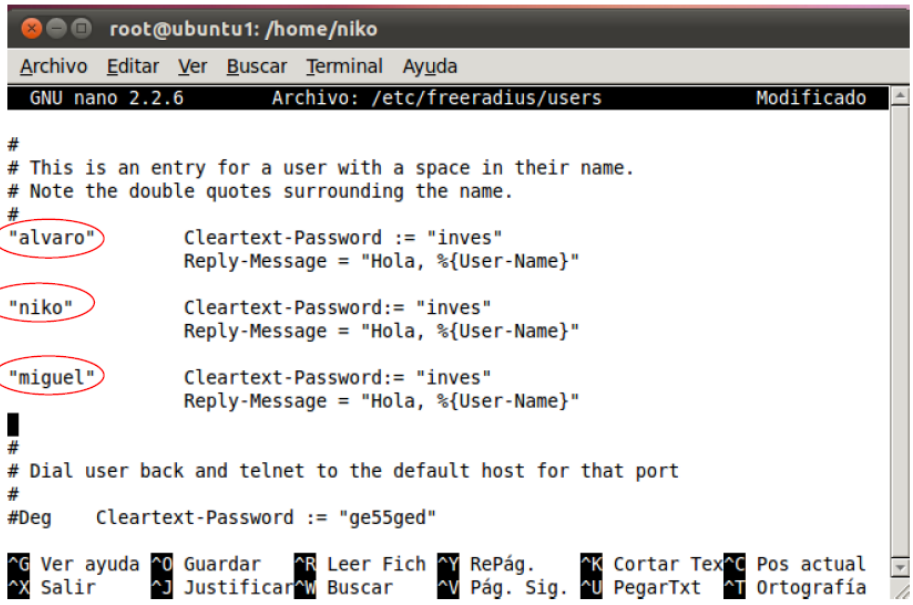


2.- Instalación de un servidor Radius bajo GNU/LINUX (**freeradius),** para autenticar conexiones que provienen de un router de acceso Linksys WRT54GL: WPA Empresarial. *Comprobación en un escenario real.*

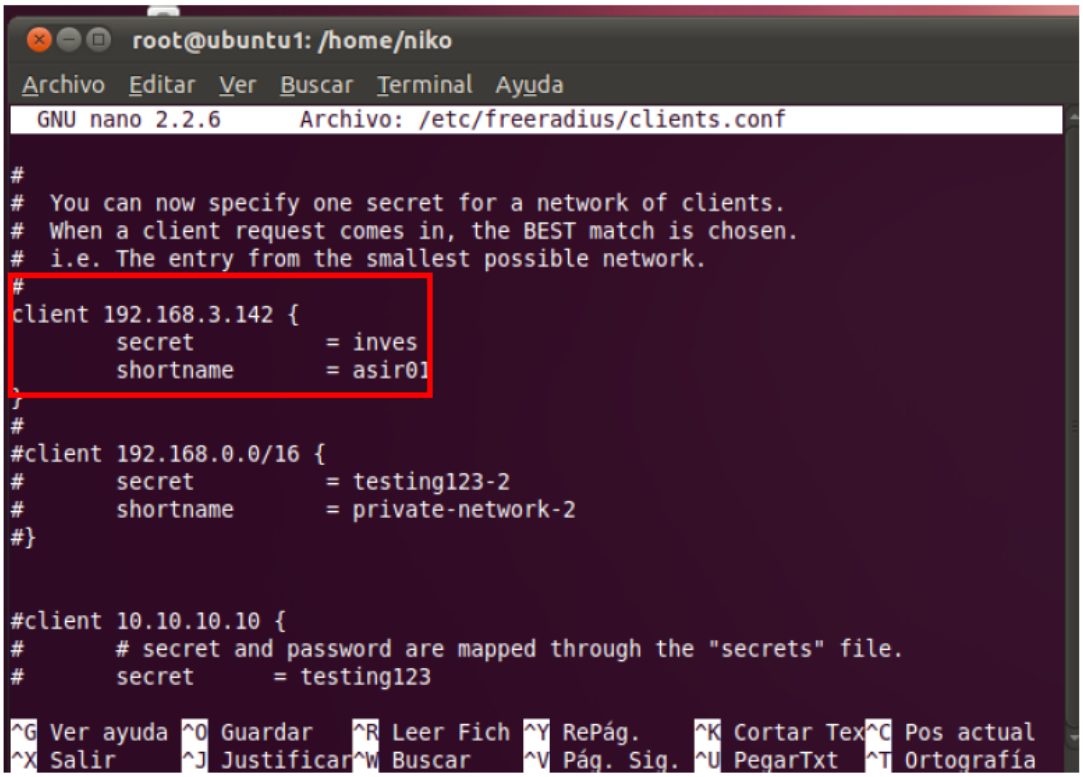
Tenemos el siguiente escenario.



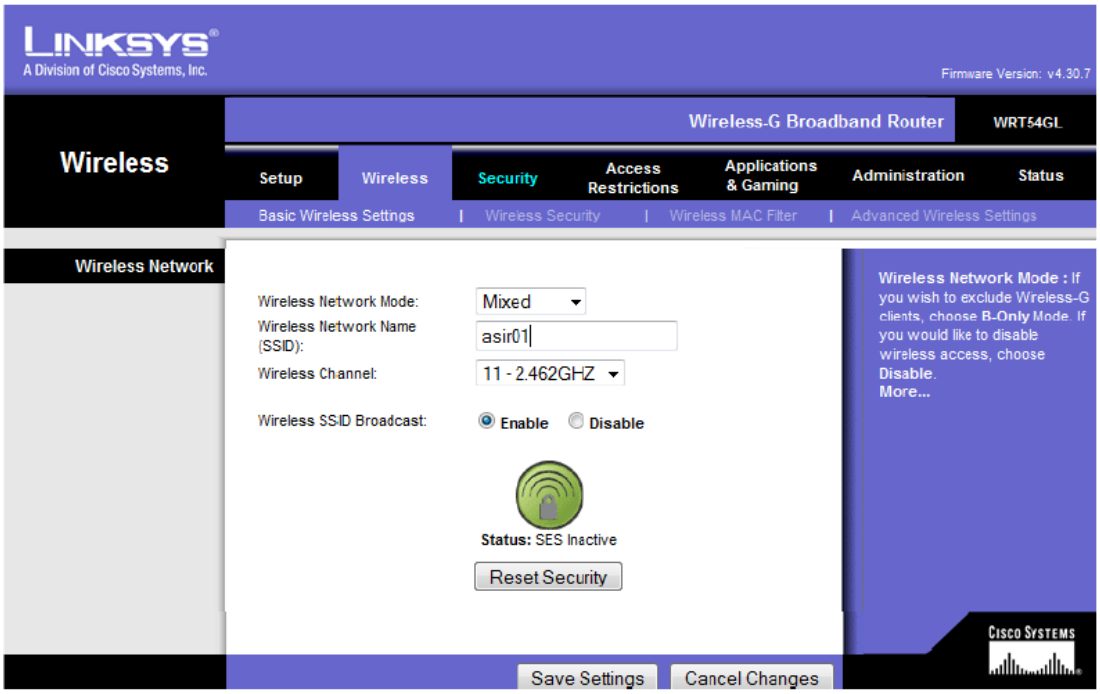
Tenemos un servidor radius con la dirección 192.168.2.150
Instalamos el servidor Radius, en Ubuntu.
Accedemos a configurar los archivos más importantes.
Agregamos usuarios.



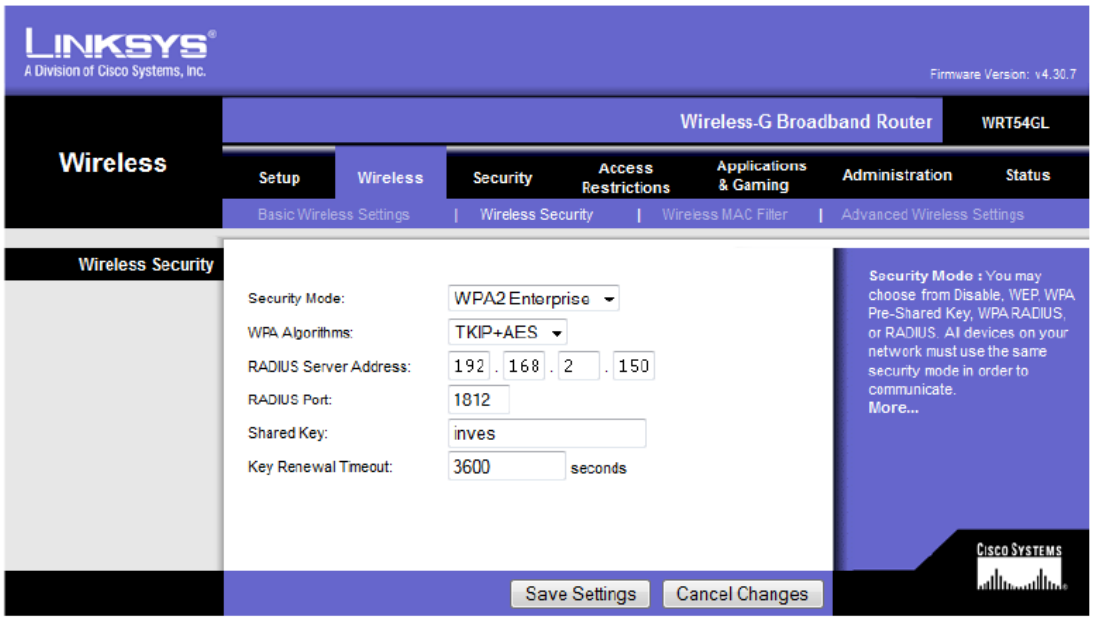
Configuramos los parámetros para el cliente RADIUS, que en nuestro caso es el Router.



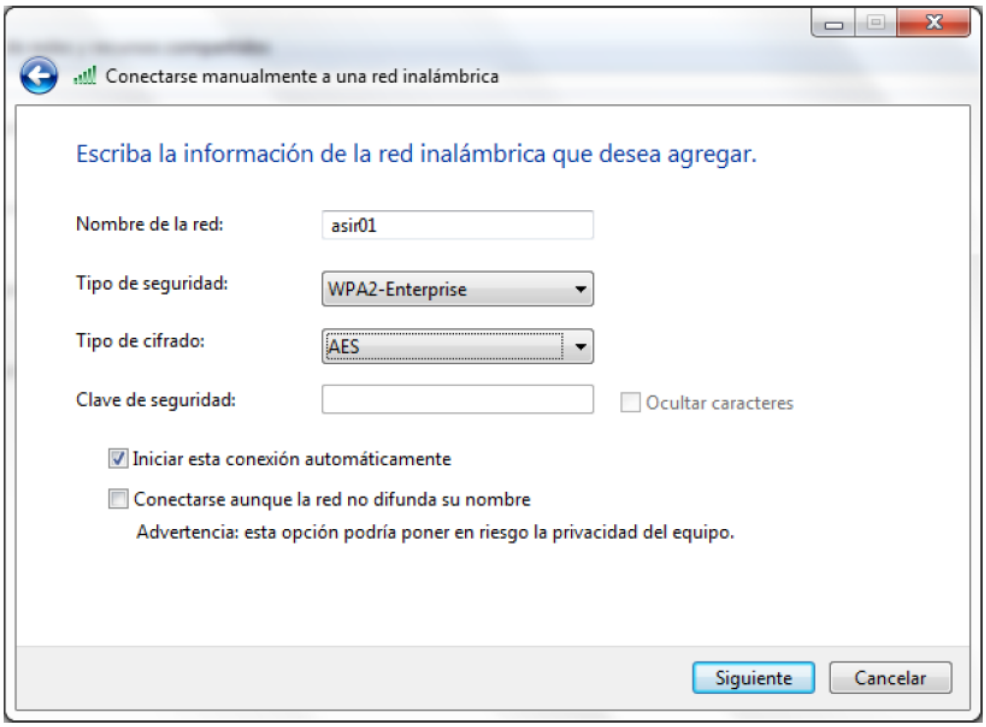
Configuramos el Router inalámbrico.



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 **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 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 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).