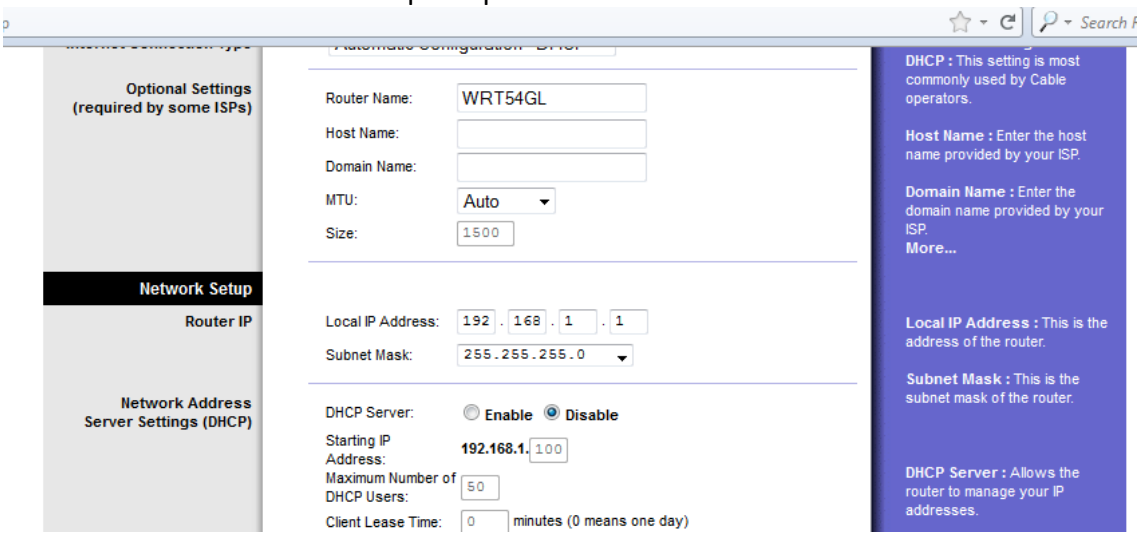
ACTIVIDAD 9 – TEMA 3 – SAD

Servidores de autenticación
a) REDES INALÁMBRICAS: WPA Personal
- Configurar router inalámbrico Linksys WRT54GL en modo seguro:
(Cambia el SSID por defecto y desactivar el broadcasting SSID, deshabilitar DHCP, cambiar nombre de usuario y contraseña, activar el filtrado de MAC, WPA2, cifrado TKIP+AES).

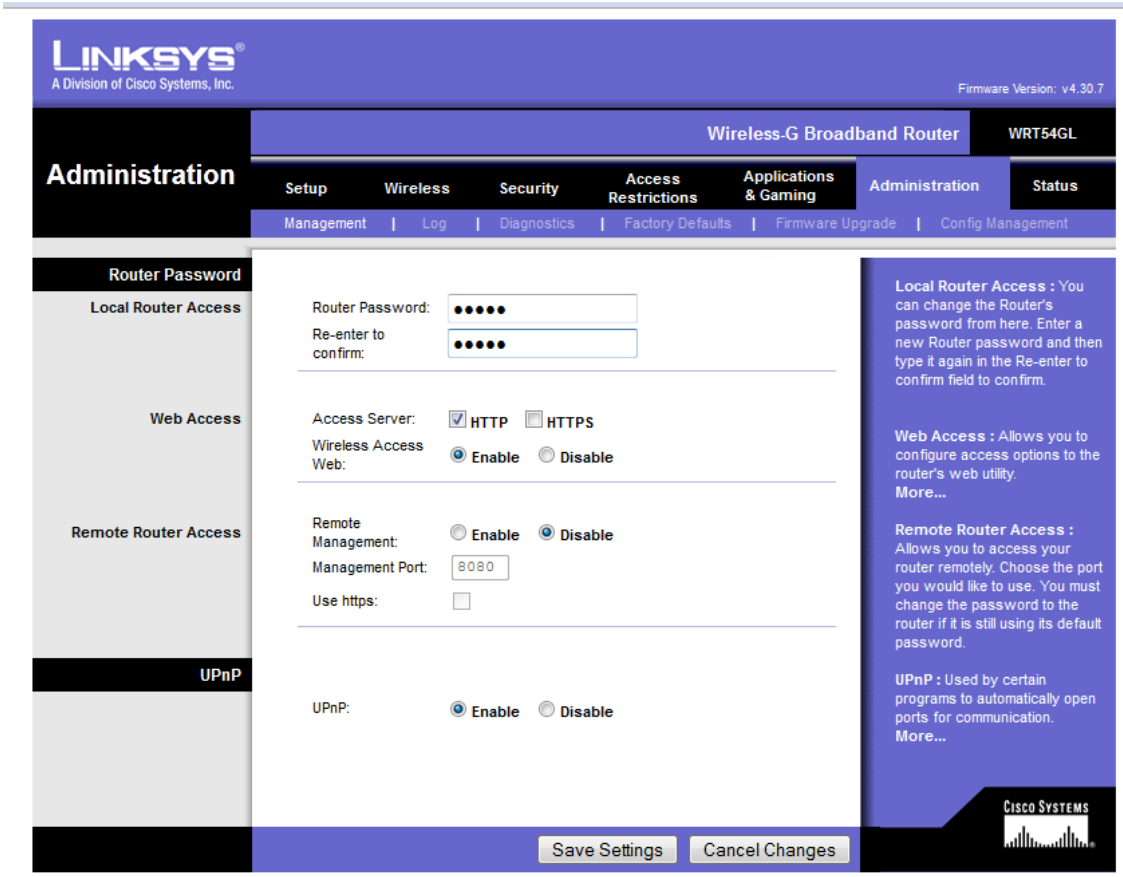
- Configurar la tarjeta de red de un cliente inalámbrico con dichas medidas de seguridad y comprobar la autenticación a dicho router inalámbrico.

Accedemos desde el navegador a nuestro router poniendo la ip por defecto y vamos a cambiar el SSID

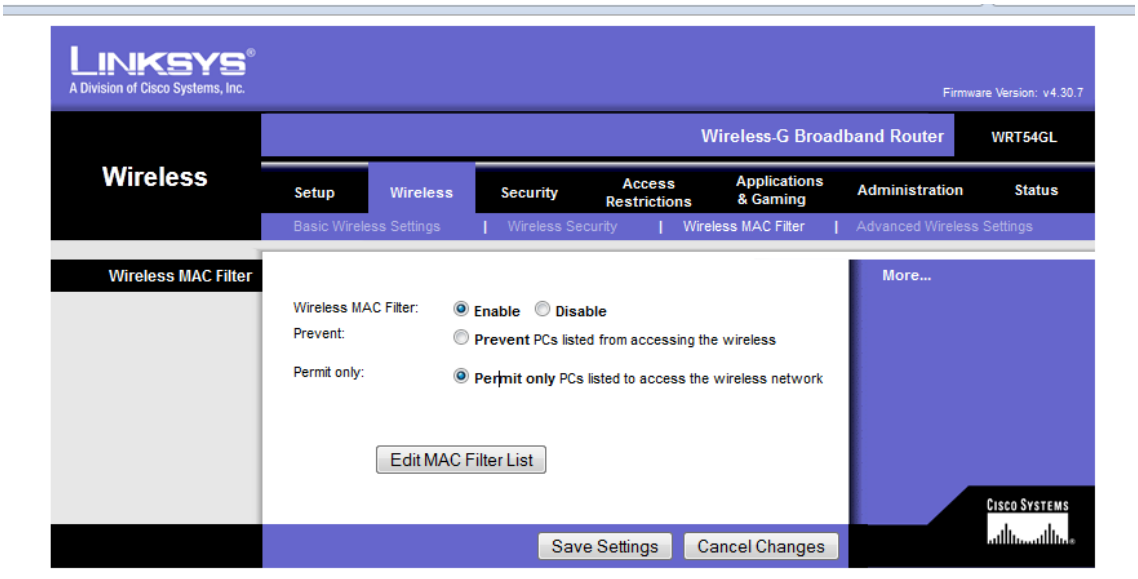
Desactivamos DHCP para que no nos dé una dirección automática

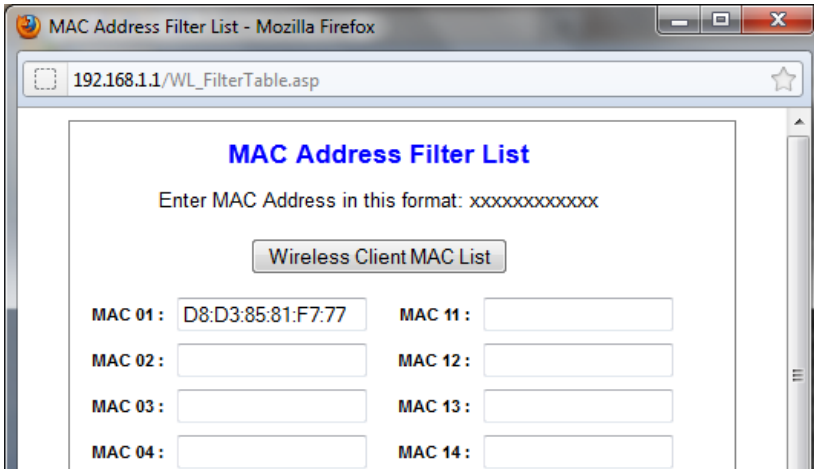


En administración cambiamos la contraseña que nos viene por defecto

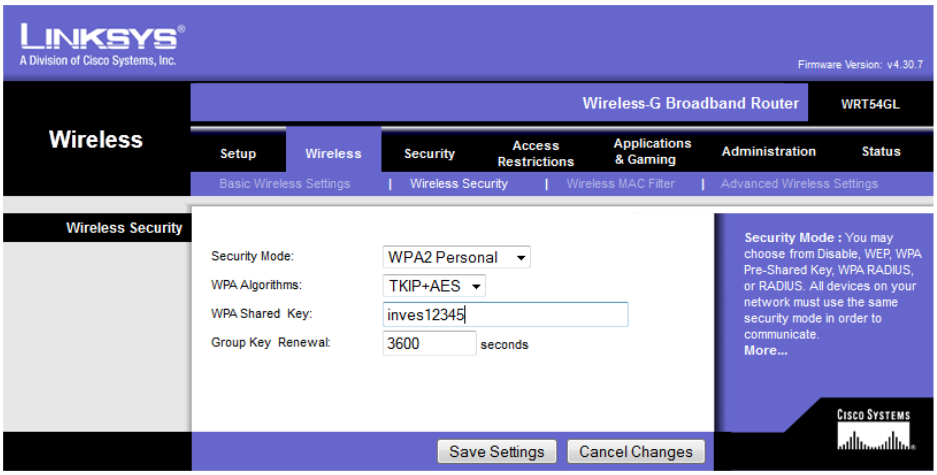


Aquí vamos a incluir la MAC de los equipos que queremos que se conecten al router

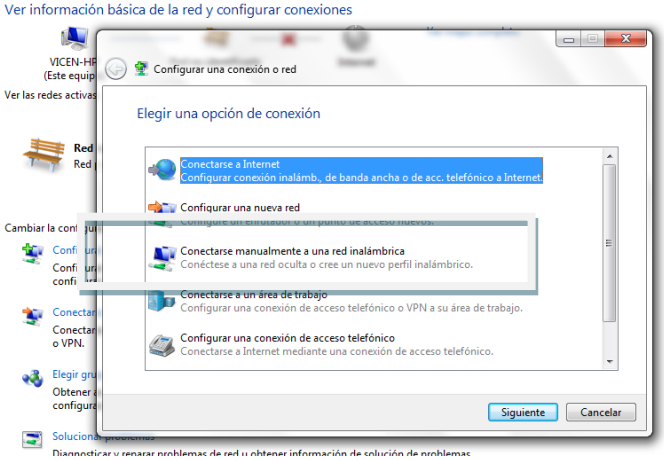




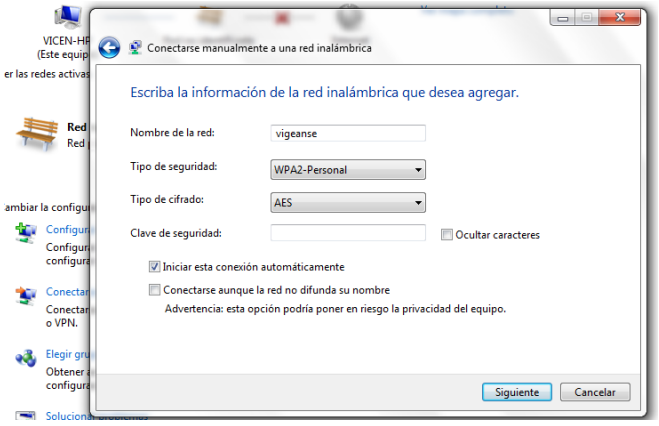
Ahora vamos a poner una contraseña en WPA2Personal y de modo TKIP+AES



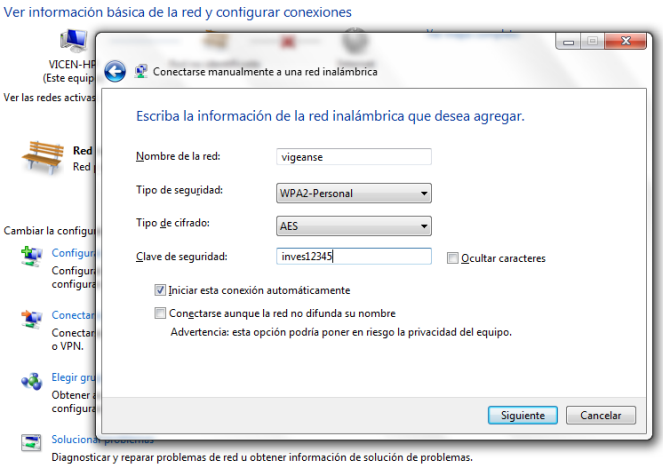
Ahora vamos a acceder desde un equipo al router, debe ser el equipo que pusimos la MAC, le damos a conectarse manualmente a una red inalámbrica



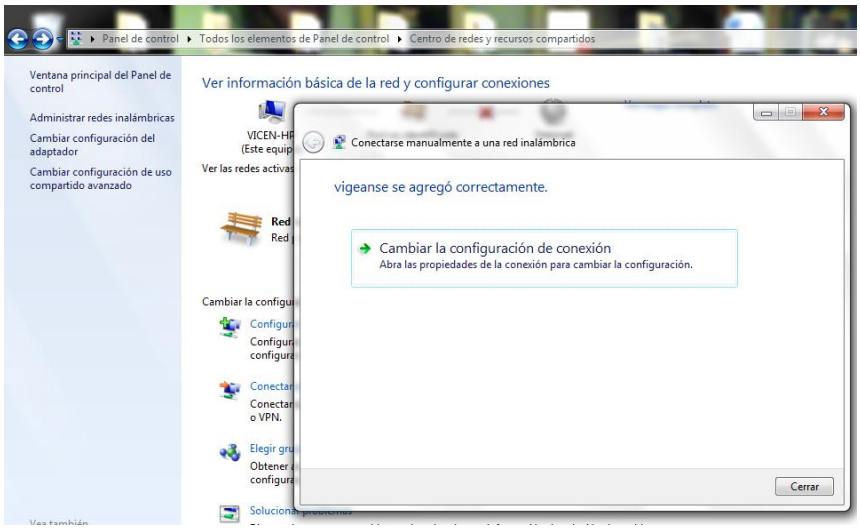
Ponemos el nombre de la red



Y la contraseña



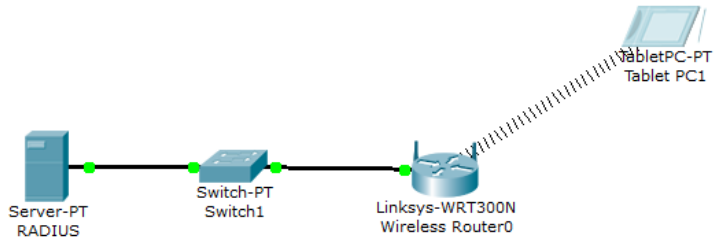
Y ya hemos entrado correctamente



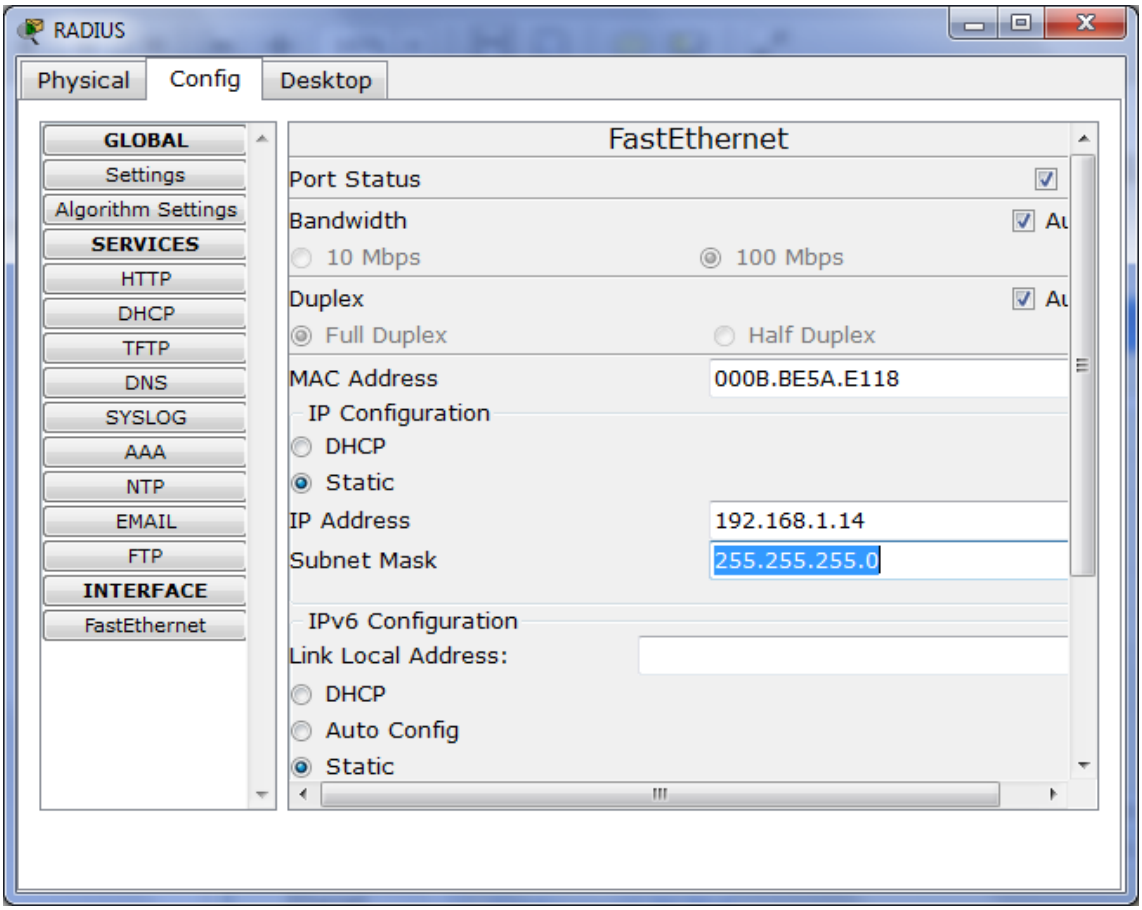
b) SERVIDOR RADIUS:

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

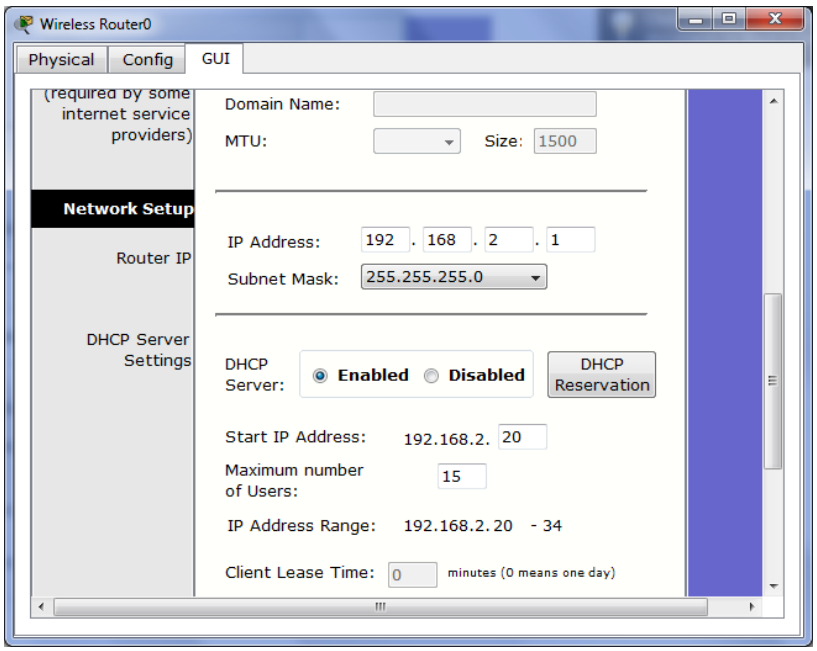
Este es el escenario que vamos a utilizar



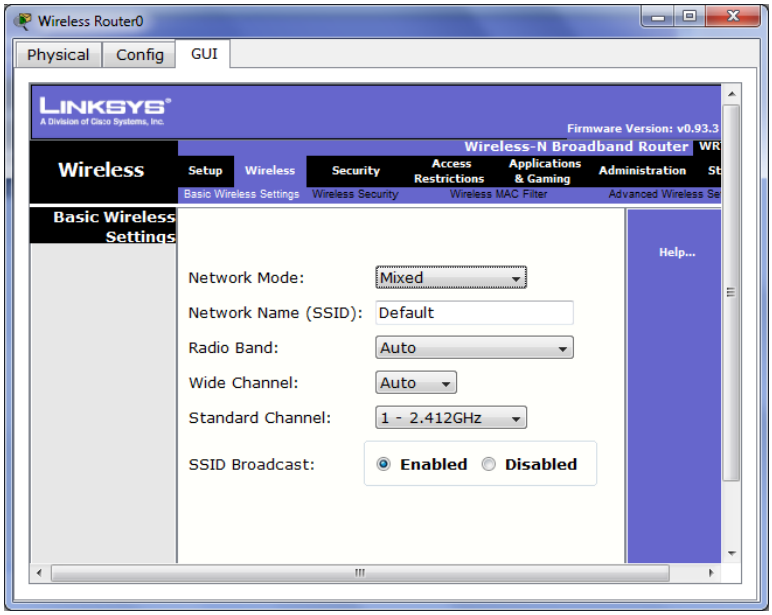
Ponemos la dirección ip en el Radius



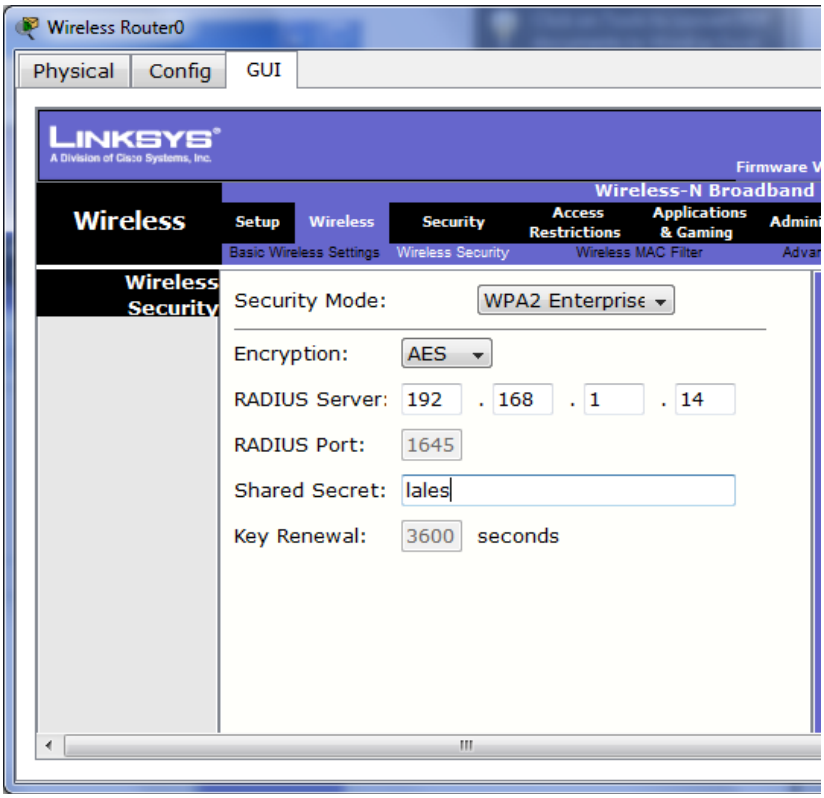
Y ponemos el rango de direcciones en el Router Inalámbrico



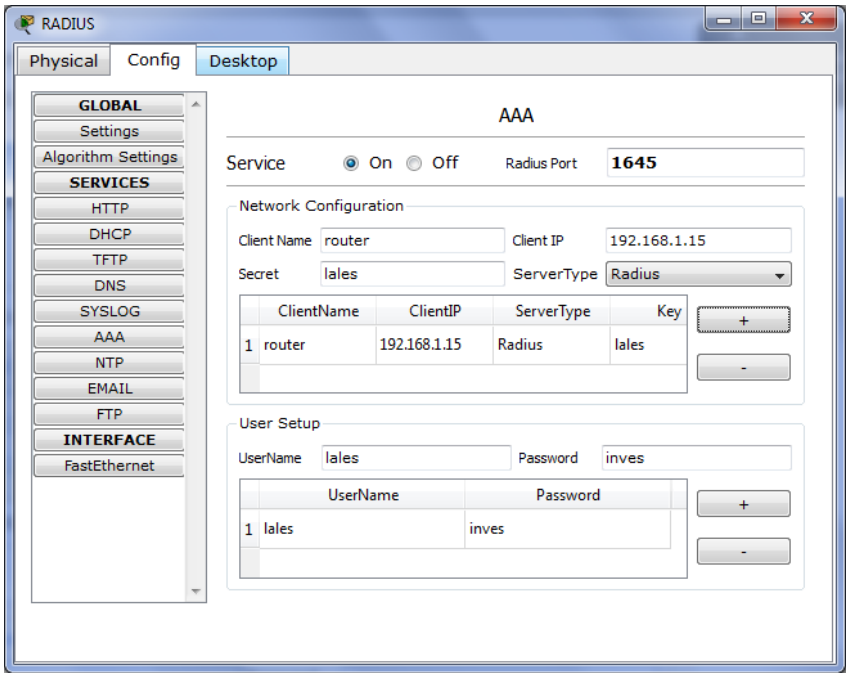
En Wireless Settings dejamos por defecto como viene



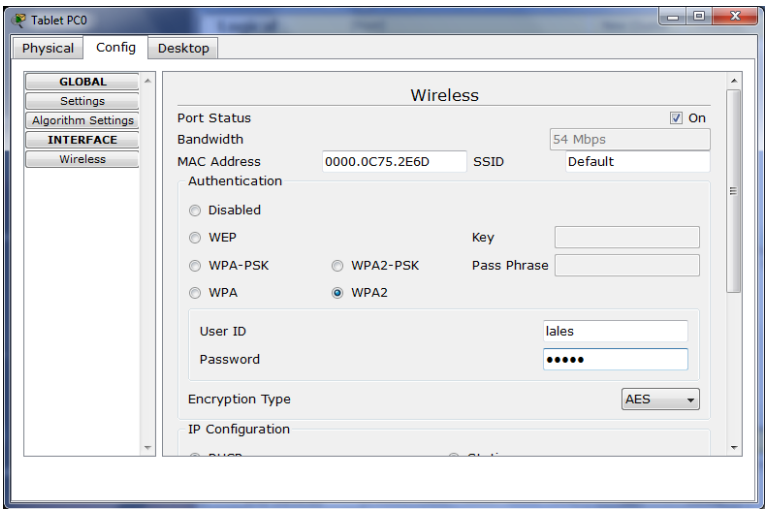
Ponemos la ip y la contraseña



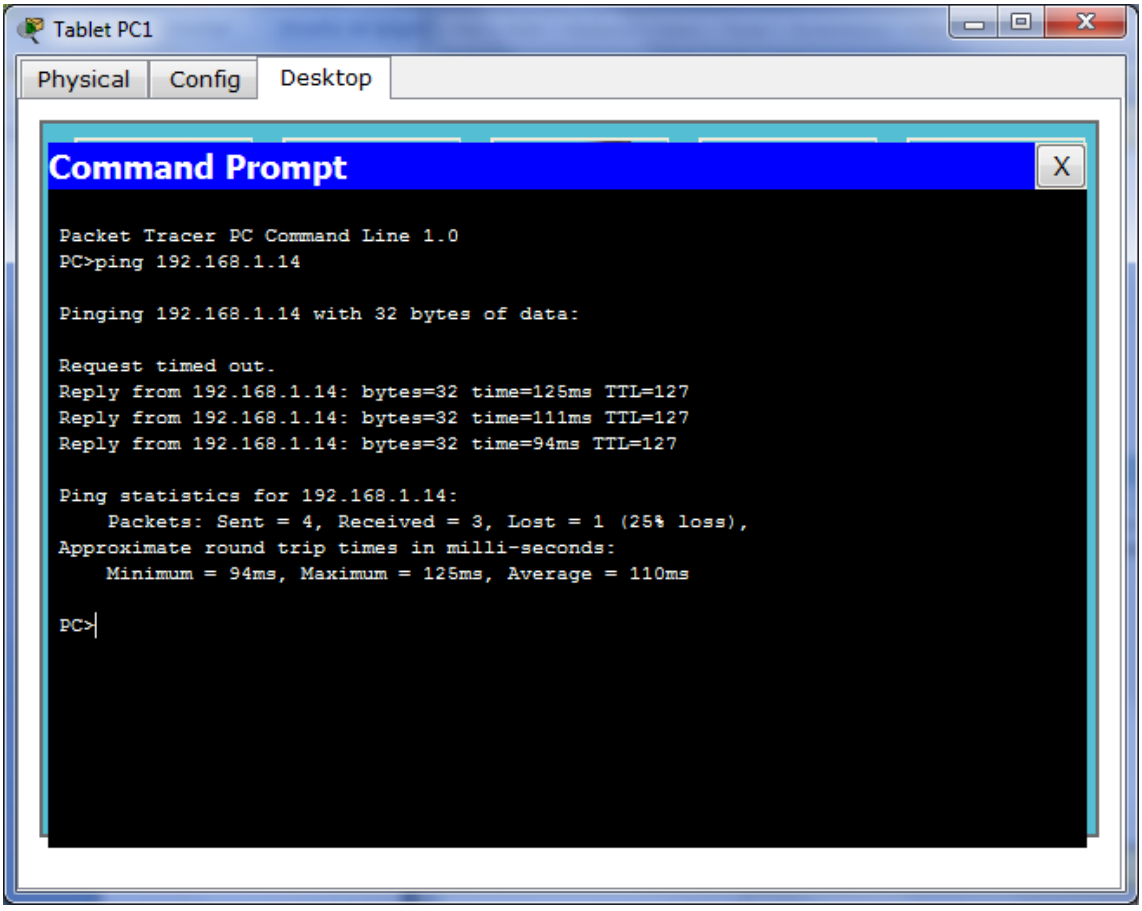
En el servidor Radius damos de alta en el protocolo AAA al cliente



En la tablet que hemos elegido ponemos el usuario y la contraseña



Y si hacemos un ping al servidor, vemos que nos da perfectamente



2.- Busca información sobre EDUROAM y elabora un breve informe sobre dicha infraestructura.

http://www.eduroam.es/

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 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 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).

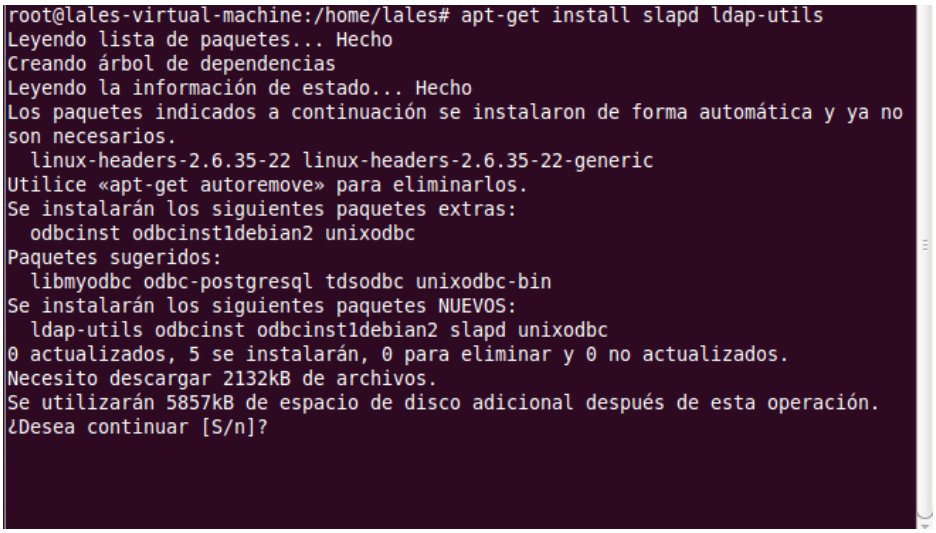
c) SERVIDOR LDAP:

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

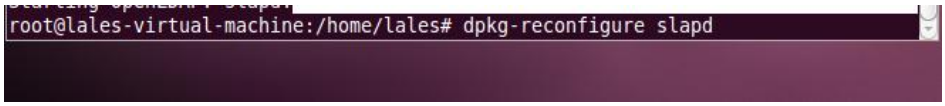
http://www.openldap.org/

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

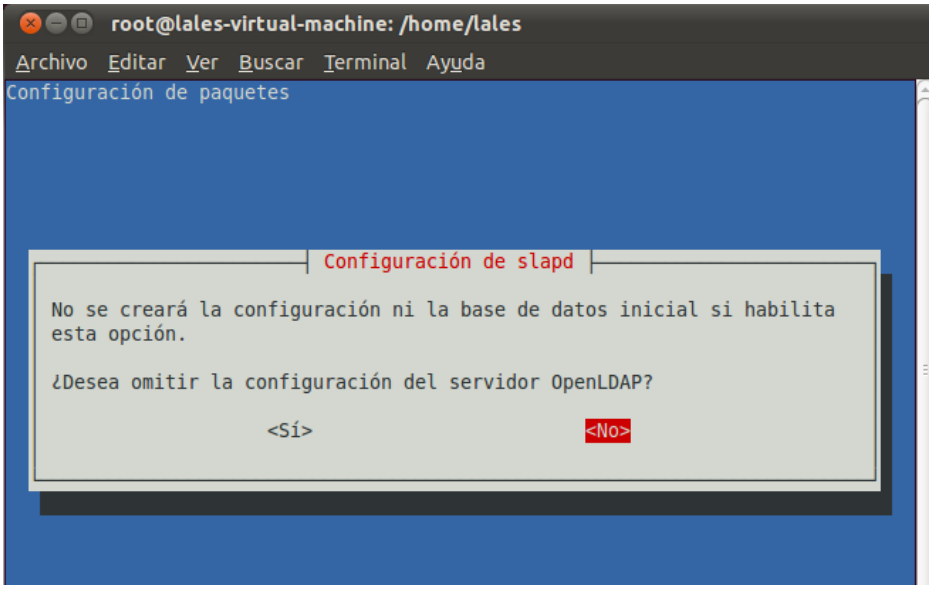
Instalamos ldap poniendo el siguiente comando



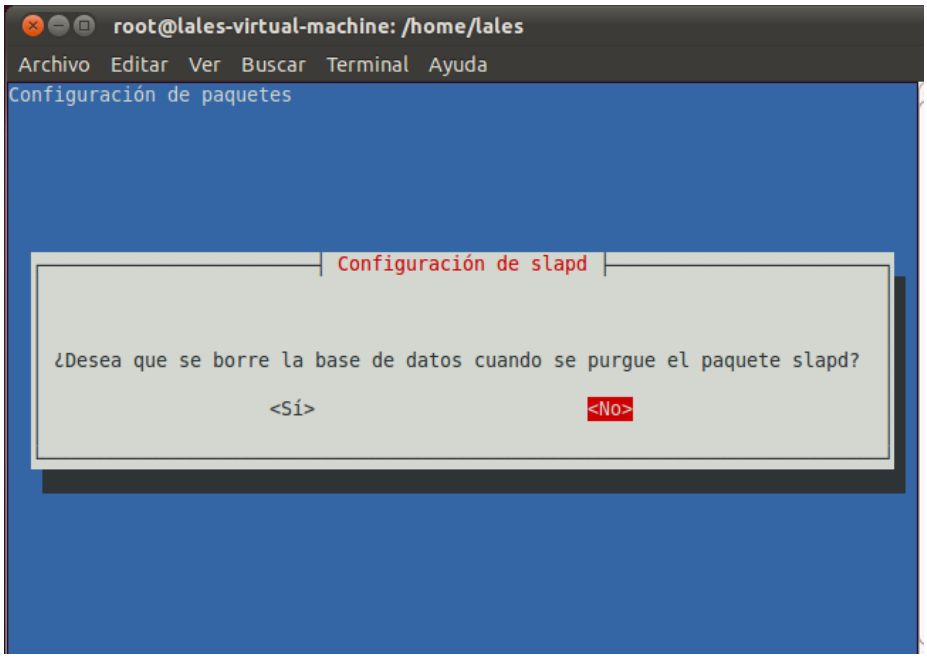
A continuación ponemos este comando para que nos salga el asistente



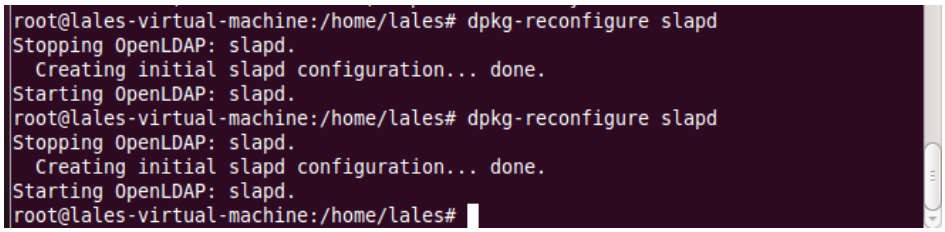
Aquí le decimos que no, para que continúe con la instalación



Aquí le decimos que no borre la base de datos



Y a continuación se nos sale al terminal, he probado a decirle a la base de datos que si y también se sale



Esta práctica está sin terminar, pero estoy buscando información sobre ello para poder terminarla.

3.- Busca información sobre LDAP y su implementación en productos comerciales.
http://www.rediris.es/ldap/

LDAP son las siglas de **L**ightweight **D**irectory **A**ccess **P**rotocol (en español Protocolo Ligero de Acceso a Directorios) que hacen referencia a un protocolo a nivel de aplicación el cual permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

Un directorio es un conjunto de objetos con atributos organizados en una manera lógica y jerárquica. El ejemplo más común es el directorio telefónico, que consiste en una serie de nombres (personas u organizaciones) que están ordenados alfabéticamente, con cada nombre teniendo una dirección y un número de teléfono adjuntos.

Un árbol de directorio LDAP a veces refleja varios límites políticos, geográficos u organizacionales, dependiendo del modelo elegido. Los despliegues actuales de LDAP tienden a usar nombres de Sistema de Nombres de Dominio (DNS por sus siglas en inglés) para estructurar los niveles más altos de la jerarquía. Conforme se desciende en el directorio pueden aparecer entradas que representan personas, unidades organizacionales, impresoras, documentos, grupos de personas o cualquier cosa que representa una entrada dada en el árbol (o múltiples entradas).

Habitualmente, almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc). A manera de síntesis, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.

Muchas de sus aplicaciones

Active Directory Active Directory es el nombre utilizado por Microsoft (desde Windows 2000) como almacén centralizado de información de uno de sus dominios de administración. Un Servicio de Directorio es un depósito estructurado de la información de los diversos objetos que contiene el Active Directory, en este caso podrían ser impresoras, usuarios, equipos... Bajo este nombre se encuentra realmente un esquema (definición de los campos que pueden ser consultados) LDAP versión 3, lo cual permite integrar otros sistemas que soporten el protocolo. En este LDAP se almacena información de usuarios, recursos de la red, políticas de seguridad, configuración, asignación de permisos, etc.

Novell Directory Services También conocido como eDirectory es la implementación de Novell utilizada para manejar el acceso a recursos en diferentes servidores y computadoras de una red. Básicamente está compuesto por una base de datos jerárquica y orientada a objetos, que representa cada servidor, computadora, impresora, servicio, personas, etc. entre los cuales se crean permisos para el control de acceso, por medio de herencia. La ventaja de esta implementación es que corre en diversas plataformas, por lo que puede adaptarse fácilmente a entornos que utilicen más de un sistema operativo.

OpenLDAP Se trata de una implementación libre del protocolo que soporta múltiples esquemas por lo que puede utilizarse para conectarse a cualquier otro LDAP. Tiene su propia licencia, la OpenLDAP Public License. Al ser un protocolo independiente de la

plataforma, varias distribuciones GNU/Linuxy BSD lo incluyen, al igual que AIX, HP-UX, Mac OS X, Solaris, Windows (2000/XP) y z/OS. OpenLDAP tiene cuatro componentes principales:
Slapd - demonio LDAP autónomo.
Slurpd - demonio de replicación de actualizaciones LDAP autónomo.
Rutinas de biblioteca de soporte del protocolo LDAP.
Utilidades, herramientas y clientes.

Apache Directory Server Apache Directory Server (ApacheDS), es un servidor de directorio escrito completamente en Java por Alex Karasulu y disponible bajo la licencia de Apache Software, es compatible con LDAPv3 certificado por el Open Group, soporta otros protocolos de red tal como Kerberos y NTP, además provee Procedimientos Almacenados, triggers y vistas; características que están presente en las Base de Datos Relacionales pero que no estaban presentes en el mundo LDAP.
Open DS Basado en los estándares LDAPv3 y DSMLv2, OpenDS surgió como un proyecto interno de SUN, aunque posteriormente se puso a disposición de la comunidad. Está desarrollado en JAVA y precisa de un entorno de ejecución (Java Runtime Environment) para funcionar. Es multiplataforma. La primera versión estable fue liberada en julio de 2008.