UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERIA
ESCUELA DE INGENIERIA EN SISTEMAS Y COMPUTACIÓN

TRABAJO DE GRADO

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
INGENIERA EN SITEMAS Y COMPUTACIÓN

MODALIDAD TESIS

TITULO:

"INVESTIGACION DEL SERVIDOR RADIUS PARA LA SEGURIDAD EN REDES LAN INALAMBRICAS"

AUTORA:

PONTÓN PORTILLA DIANA CAROLINA

DIRECTOR DE TESIS:
ING. YESENIA CEVALLOS

Riobamba-Ecuador
2011

CALIFICACIÓN

Los miembros del tribunal, luego de haber receptado la Defensa de trabajo escrito, hemos determinado la siguiente calificación.

Para constancia de lo expuesto firman:

MIEMBROS	**NOTA**	**FIRMA**
Ing. Yesenia Cevallos **Directora de Tesis**	**.....**	**.....**
Ing. Wilson Baldeón **Presidente del Tribunal**	**.....**	**.....**
Ing. Fernando Molina **Miembro del Tribunal**	**.....**	**.....**

DERECHO DE AUTOR

Declaro que soy responsable de las ideas, doctrinas, y desarrollo de la propuesta expuesta en el presente trabajo de investigación, y los derechos de autoría pertenecen a la Universidad Nacional de Chimborazo.

DEDICATORIA

Todo el esfuerzo realizado para lograr este éxito va dedicado a una persona muy especial, que siempre estuvo conmigo en las buenas y en las malas, que me enseño que la vida es una lucha constante, que me apoyo en todo momento, que siempre confió en mí y que lamentablemente ya no está a mi lado para ver realizado su sueño, pero que siempre vive en mi mete y en mi corazón…. a mi padre Mario Pontón

Se lo dedico también a Dios, a mi querida madre Carmen Portilla, a mi querido ahijado Moshe Villacrés, a mis abuelitos y tías que lamentablemente ya no están aquí pero me apoyaron en todo momento, para obtener esta grandiosa recompensa…

AGRADECIMIENTO

Agradezco especialmente a mis padres Mario Pontón y Carmen Portilla y a mi hermana Fanny, quienes me dieron ese apoyo incondicional durante el transcurso de mi vida.

A mi familia por haberme apoyado en los momentos más difíciles de mi vida y por haberme brindado tanta paciencia y cariño.

Mi agradecimiento a la UNACH, en cuyas aulas me formé; a mi director y mis asesores, a todos mis profesores y amigos por su apoyo incondicional.

Pero sobretodo a **DIOS**, como hacedor de todas las cosas...

RESUMEN

Se realizó la investigación del Servidor RADIUS para la seguridad en redes LAN inalámbricas, con el objetivo de identificar los estándares, protocolos, conectividad, funcionalidad y ventajas que ofrece este servidor.

Se utilizó el Sistema Operativo Windows XP Service Pack 2 como plataforma de instalación; Cisco Packet Tracer 5.3, como herramienta de implementación y pruebas de la configuración del Servidor RADIUS, donde se demuestra que el servidor autentica, autoriza y registra los usuarios que tienen permisos para utilizar los beneficios de la red.

Se evaluó de acuerdo a los indicadores viabilidad, confiabilidad, seguridad, inconvenientes de red, problema de conexión, integridad de los datos, obteniendo como resultados que la implementación del Servidor RADIUS como una política de seguridad es eficiente y eficaz la cual mejora notablemente la seguridad de las redes LAN inalámbricas.

Se concluyó que la implementación del Servidor RADIUS reúne los requisitos de ser una implementación de uso simple desde el punto de vista del usuario, pero a la vez reúne la complejidad suficiente dentro de sus procesos internos, para ser una solución lo suficientemente segura, por lo que se recomienda la implementación de este Servidor RADIUS.

SUMARY

Research was conducted RADIUS server for wireless LAN network security, with the aim of identifying the standards, protocols, connectivity, functionality and benefits offered by this server.

Operating System used Windows XP Service Pack 2 installation as a platform, Cisco Packet Tracer 5.3, a tool for implementation and testing of the RADIUS server configuration, which shows that the server authenticates, authorizes and records users have permissions to utilize the benefits of the network.

Assessed according to indicators feasibility, reliability, security, network problems, connection problems, data integrity, resulting in the implementation of the RADIUS server as a security policy is efficient and effective which greatly improves safety wireless LAN networks.

It was concluded that implementation of the RADIUS server meets the requirements of being simple to use an implementation from the user point of view, but also meets sufficient complexity in their internal processes, to be a solution secure enough, so recommended the implementation of the RADIUS server.

INTRODUCCIÓN

En los últimos años las redes de área local inalámbricas están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas. Las WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar.

Con las redes inalámbricas la red, por sí misma, es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red, y lo más importante incrementa la productividad y eficiencia en las empresas donde está instalada. Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas. La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes inalámbricas debido a ataques tanto pasivos como activos.

Por tal motivo se realiza la investigación de seguridad para la red inalámbrica con el fin de poder protegerla de ataques al entorno inalámbrico, es por esto que el Servidor RADIUS es uno de los principales componentes de la infraestructura de seguridad para la red inalámbrica ya que es un Conjunto de herramientas, procedimientos y protocolos que garantizan un tratamiento coherente de las tareas de autenticación, autorización y registro de actividad de las entidades que tienen acceso a un sistema de información.

CAPITULO I

1. FUNDAMENTACIÓN TEORICA

1.1 PROBLEMATIZACIÓN

1.1.1 Identificación y descripción del problema

Las redes inalámbricas tienen la particularidad de no necesitar un medio físico para funcionar. Esto fundamentalmente es una ventaja, pero se convierte en una desventaja cuando se piensa que cualquier persona con una computadora portátil solo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella.

El área de cobertura de una red inalámbrica no está definida por paredes o por ningún medio físico, a los posibles intrusos no les hace falta estar dentro de un edificio o estar conectado a un cable. Además, el sistema de seguridad que incorporan las redes Wi-Fi no es de lo más fiable.

Varios son los riesgos que se pueden presentar en las redes inalámbricas. Por ejemplo, se podría perpetrar un ataque por inserción, bien de un usuario no autorizado o por la ubicación de un punto de acceso AP (Access Point) ilegal más potente interceptando la red inalámbrica, es por esta razón que las instituciones deberían contar con un servidor de seguridad en redes LAN inalámbricas en este caso el Servidor RADIUS.

1.1.2. Formulación del Problema

Las redes inalámbricas por su naturaleza de cobertura son propensas a recibir ataques por personas no autorizadas quienes vulneran las seguridades configuradas en estas, para conseguir información vital de empresas u organizaciones públicas o privadas como bancos, regimientos militares, centros comerciales, empresas privadas etc., siendo el principal objetivo apropiarse de esta información para posibles fraudes o espionajes corporativos.

Este problema se da en redes donde el número de usuarios es generalmente grande y el administrador de la red se ve en la necesidad de gestionar el acceso de estos usuarios a

los recursos de la red, siendo los administradores de las redes, los encargados de investigar, configurar y evaluar las herramientas existentes en el mercado para robustecer la seguridad de la red bajo su administración

1.1.3. Objetivos:

1.1.3.1. Objetivo General

- Investigar el servidor RADIUS (Remote Authentication Dial-In User Server – Autenticación Remota Dial-In de un usuario en el servidor) para la Seguridad en Redes LAN (Local Area Network – Red de Área Local) Inalámbricas.

1.1.3.2. Objetivos Específicos

- Identificar los estándares y protocolos utilizados con el servidor RADIUS.

- Determinar la funcionalidad y conectividad del servidor RADIUS.

- Dar a conocer las ventajas que brinda el servidor RADIUS con respecto a otras opciones de seguridad inalámbrica.

- Desarrollar un modelo de configuración del servidor RADIUS utilizando Packet Tracer.

1.1.4. Justificación

Con la masificación del uso de Internet, tanto los computadores personales como las redes de computadores, pueden ser vulnerables a diversos tipos de ataques. Internet ha pasado a ser sin ningún tipo de dudas la mayor red pública de datos, a través de la cual se facilitan comunicaciones personales y empresariales en todo el mundo.

Conforme va aumentando el uso de esta red, aumentan las amenazas de intromisión no autorizadas sobre distintas redes de computadoras implementadas en empresas públicas y privadas, los ataques a estas redes por hackers pueden deshabilitar los servicios y recursos que brindan las empresas.

Existen muchas herramientas de seguridad disponibles como WEP (Wired Equivalent Privacy – Privacidad Equivalente a Cableado). WPA (Wi-Fi Protected Access – Acceso Protegido Wi-Fi) WPA2 (Wi-Fi Protected Access 2 – Acceso Protegido Wi-Fi 2), que presentan ciertas limitaciones en los niveles de seguridad en la red.

Es por esta razón que se desea investigar un sistema de seguridad inalámbrica más robusto, el mismo que sea capaz de gestionar el acceso a la red, de muchos usuarios autorizados en el uso de los recursos de la red; uno de estos sistemas de seguridad es un Servidor RADIUS.

1.1.5. Delimitación

La presente investigación estará dirigida al estudio del servidor RADIUS y las prestaciones que brinda en la seguridad de redes LAN Inalámbricas.

1.2. MARCO TEÓRICO

1.2.1. Antecedentes

Las redes de comunicaciones y los sistemas de información se han convertido en un factor esencial del desarrollo económico y social.

La informática y las redes se están convirtiendo en recursos omnipresentes, tal y como ha ocurrido con el suministro de agua y de electricidad. Por consiguiente, la seguridad de las redes de comunicación y de los sistemas de información, y en particular su disponibilidad, es un asunto que preocupa cada vez más a la sociedad, en particular, por la posibilidad de que surjan problemas en sistemas de información claves, debidos a la complejidad de los sistemas, errores o ataques de hackers.

El creciente número de fallos de seguridad ha causado ya importantes perjuicios económicos, ha minado la confianza de los usuarios y perjudicado el desarrollo del comercio electrónico.

Los particulares, las administraciones públicas y las empresas han reaccionado implementando tecnologías de seguridad y procedimientos de gestión de la seguridad.

1.2.2. Servidores de Seguridad en Redes LAN Inalámbricas

En los últimos años las redes de área local inalámbricas están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan, y; se descubren nuevas aplicaciones para ellas. Las WLAN (Wireless Local Area Network – Red de área local inalámbrica), permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar.

Con las redes inalámbricas, la red por sí misma es móvil y elimina la necesidad de usar cables, establece nuevas aplicaciones añadiendo flexibilidad, y; lo más importante incrementa la productividad y eficiencia en las empresas donde está instalada. Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas. La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes inalámbricas debido a ataques tanto pasivos como activos.[1]

Un servidor AAA (Authentication, Authorization and Accounting - Autenticación, Autorización y Contabilización), se refiere al proceso de autenticación, autorización y contabilidad utilizado por el acceso telefónico de autenticación remota de usuario de los servicios de protocolo de red. RADIUS permite a los usuarios remotos o equipos informáticos acceder a un servidor de red. Cuando el proceso del servidor AAA no es necesario, un servidor se llama "abierto" o "anónimo". El Protocolo RADIUS y el servidor AAA son utilizados generalmente por los proveedores de servicios Internet (ISP) para identificar y facturar a sus clientes. También se utiliza por las empresas para

[1] http://mygnet.net/articulos/redes/827/

identificar y permitir el acceso de red a sus empleados cuando están trabajando desde una ubicación remota.

Por tal motivo se realizará la investigación de seguridad para la red LAN inalámbrica, con el fin de poder protegerla de ataques al entorno inalámbrico, es por esto que el Servidor RADIUS es uno de los principales componentes de la infraestructura de seguridad para la red inalámbrica, ya que es un Conjunto de herramientas, procedimientos y protocolos que garantizan un tratamiento coherente de las tareas de autenticación, autorización y registro de actividad de las entidades que tienen acceso a un sistema de información.

1.2.3. ¿Qué son los Servidores de Seguridad en Redes Inalámbricas?

Es un software o hardware que ayuda a impedir el paso a los hackers, virus y gusanos que intenten entrar en su equipo a través de Internet. Si se tiene una red doméstica o una pequeña empresa, instalar un servidor de seguridad es el primer paso y el más efectivo para mejorar la protección de los equipos. Es importante tener un servidor de seguridad y un software antivirus activados antes de conectarse a Internet.

1.2.4. Características de los Servidores de Seguridad en Redes Inalámbricas

Un servidor de seguridad examina la información que viene y va a Internet, identifica y omite la información que procede de una ubicación peligrosa o parece sospechosa. Al configurar el servidor de seguridad correctamente, los hackers que buscan vulnerabilidades no las encontrarán fácilmente.

El primer paso al elegir un servidor de seguridad consiste en determinar el que resulta más adecuado. Las opciones disponibles son:

- Servidores de seguridad de software
- Ruteadores hardware
- Ruteadores inalámbricos

El servidor que se implementará dependerá del número de equipos que accederán a la red, y también la plataforma que se utiliza pudiendo ser Windows, Apple Macintosh o Linux, cada uno con sus ventajas e inconvenientes como se detalla en la tabla 1.1.

Los servidores de seguridad de software constituyen una buena elección para, equipos individuales y funcionan bien en plataformas como Windows 98, Windows ME y Windows 2000. (Windows XP tiene un servidor de seguridad incorporado, por lo que no es necesario uno adicional.)

Ventajas	Inconvenientes
No necesita hardware adicional.	Costo adicional: la mayoría de los servidores de seguridad de software cuestan dinero.
No necesita cables en el equipo.	Para comenzar puede ser necesarias la instalación y la configuración.
Una buena opción para equipos individuales.	Normalmente se necesita una copia para cada equipo.

TABLA 1.1 Ventajas e inconvenientes de los servidores de seguridad de software

Los Ruteadores hardware constituyen una buena opción para una red doméstica que esté conectada a Internet como se describe en la siguiente tabla 1.2.

Ventajas	Inconvenientes
Los Ruteadores hardware normalmente tienen al menos cuatro puertos de red para conectar otros equipos entre sí. Los enrutadores hardware proporcionan protección de servidor de seguridad para varios equipos.	Necesita cables, lo que puede provocar desorden en el área de trabajo.

TABLA 1.2 Ventajas e inconvenientes de los Ruteadores Hardware

Sólo pocos ruteadores inalámbricos vienen equipados con un servidor de seguridad incorporado, por lo que se necesitará adquirir uno por separado, en la tabla 1.3, se pueden identificar sus ventajas e inconvenientes.

Ventajas	Inconvenientes
Los ruteadores inalámbricos permiten conectar equipos, portátiles, agendas electrónicas e impresoras sin cables.	El empleo de un enrutador inalámbrico requiere, que se utilice un adaptador inalámbrico en cualquier equipo que se conecte a él. Por lo tanto, será necesario adquirir equipo adicional.
Los ruteadores inalámbricos son excelentes para conectar equipos portátiles a Internet y a las redes.	No todos los enrutadores inalámbricos vienen equipados con un servidor de seguridad incorporado, por lo que es necesario adquirir uno por separado.[2]

TABLA 1.3 Ventajas e inconvenientes de los Enrutadores Inalámbricos

1.2.5. Generalidades de los Servidores de Seguridad en Redes Inalámbricas

El nivel más básico de seguridad para redes inalámbricas es WEP, o Wired Equivalent Privacy, una característica estándar de todas las redes LAN inalámbricas certificadas con la norma Wi-Fi. WEP, creado por el Instituto de Ingenieros en Electricidad y Electrónica (IEEE), ha sido diseñado para proporcionar un nivel básico de seguridad, prevenir posibles copias no autorizadas de la información y proteger la red, mediante la encriptación de todos los datos que se envíen de forma inalámbrica.

Además de diseñar una solución de seguridad robusta, el evitar simples errores es algo bastante prudente. Evitar errores (como un fallo en la configuración, la instalación no correcta del punto de acceso, no cambiar la clave WEP que viene preestablecida, etc.), mejora de forma significativa el nivel de seguridad de una red LAN inalámbrica. En teoría, las claves WEP, son contraseñas secretas que permiten a los usuarios decodificar los datos encriptados de una comunicación.

[2] http://www.microsoft.com/latam/protect/viruses/fwbenefits.mspx

La construcción de una red inalámbrica requiere de dos tipos diferentes de componentes de hardware, puntos de acceso inalámbricos y tarjetas de acceso inalámbrico. El punto de acceso inalámbrico es un dispositivo, que se adjunta a una red informática existente a través de un cable Ethernet estándar. Tiene una antena en él, que le permite transmitir y recibir señales de PC y otros dispositivos. Cada dispositivo que desee comunicarse con el punto de acceso necesita una tarjeta de acceso inalámbrico, que también contiene una antena.

El estándar más utilizado el 802.11g, permite hasta 54 megabits de datos por segundo, que se transmite entre el punto de acceso deseado y la tarjeta de acceso. Si bien no es tan rápido como las redes de cable, que suelen funcionar a 100 megabits a 1000 megabits por segundo, las redes inalámbricas ofrecen una mayor flexibilidad, y puede ser menos costoso de instalar.[3]

1.2.5.1. Estándares y Protocolos

La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes inalámbricas. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red. Sin embargo, en una red inalámbrica desplegada en una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal. Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior.

Conscientes de este problema, el IEEE publicó un mecanismo opcional de seguridad, denominado WEP, en la norma de redes inalámbricas 802.11. Pero WEP, desplegado en numerosas redes WLAN, ha sido roto de distintas formas, lo que lo ha convertido en una protección inservible.

[3] http://www.coit.es/publicac/publbit/bit138/3com.pdf

No ajena a las necesidades de los usuarios, la asociación de empresas Wi-Fi decidió lanzar un mecanismo de seguridad denominada WPA, sus principales características son la mejora de la confidencialidad y nuevas técnicas de integridad y autentificación, para lo cual se utiliza el protocolo EAP y un servidor AAA (Authentication Authorization Accounting) como puede ser RADIUS (Remote Authentication Dial-In User Service). Wi-Fi a desarrollado nuevos cambios en el mecanismo de seguridad, WPA las mejoras se especifican en WPA2 el cual incluye el nuevo algoritmo de cifrado AES.[4]

1.2.5.2. Elección del Servidor de Seguridad en Redes Inalámbricas

¿Cómo minimizar o eliminar entonces el riesgo de que un hacker pueda entrar en una red inalámbrica?

Primero se debe controlar quién accede a ella a través, de procesos de autenticación y después proteger la información, que viaja a través de las ondas de radio mediante técnicas de encriptado.

Para ello se tienen que gestionar algunos procesos que se detallan a continuación, para hacer que el servidor de seguridad de redes inalámbricas que se adapten a nuestras necesidades y que cumplan con los requerimientos de seguridad de la red creada.

a) Integrar políticas inalámbricas y las de cable

La seguridad inalámbrica no es una infraestructura de red, aparte cuyos procedimientos o protocolos son completamente distintos. Se tiene que desarrollar una política de seguridad que combine tanto seguridad inalámbrica como seguridad para la red de cable, para impulsar las ventajas de gestión y de ahorro de costos.

[4] http://www.saulo.net/pub/inv/SegWiFi-art.htm

Por ejemplo, integrando la petición de nombre de usuario y contraseña para todos los usuarios, que accedan a la red ya sea mediante infraestructura de cable o inalámbrica.

b) Situar el punto de acceso en el lugar adecuado

En la configuración de una red empresarial, se debe asegurar que los puntos de acceso estecen fuera del firewall perimetral, en el caso de que no cuente con los sistemas de encriptación y autenticación requeridos, de esta manera el Firewall Perimetral controlará los accesos.

c) Utilizar una dirección MAC (Media Access Control - Control de Acceso al Medio)

Utilizar una dirección MAC basada en ACLs (Access Control Lists) hará que sólo los dispositivos registrados puedan acceder a la red. El filtro mediante direcciones MAC es como añadir otro cerrojo a la puerta principal, y; cuantos más obstáculos encuentre un hacker, más rápidamente desistirá en sus intenciones de intrusión a nuestra red.

d) Administrar el nombre de la red

Todas las redes inalámbricas tienen asignado por defecto un nombre de red o SSID (Service Set Identifier). Es recomendable cambiar el SSID de forma regular y deshabilitar, la función de propagación del nombre de la red, para evitar que sea identificado fácilmente.

e) Impulsar los servidores RADIUS existentes

Los usuarios remotos de las compañías más grandes, son a veces autenticados para utilizar la red a través; de un servidor RADIUS. Los directores de TI (Information Technology - Tecnologías de Información)

pueden integrar las redes LAN inalámbricas, en la infraestructura RADIUS ya establecida para hacer más sencilla su gestión.

Esto no sólo hace posible la autenticación inalámbrica, sino que además asegura que los usuarios de la red inalámbrica siguen el mismo proceso de aprobaciones que los usuarios remotos.

f) Instalar el Protocolo de seguridad WEP

WEP (Wired Equivalent Privacy) es el protocolo de seguridad inalámbrico del estándar 802.11b. Se ha diseñado para proporcionar protección mediante encriptación de datos al tiempo en que se transmite la información, exactamente igual que se hace en las redes de cable. Una vez instalado, habilitado se debe cambiar de forma inmediata la clave WEP, ya que aparecerá una por defecto.

Lo ideal es generar claves WEP de forma dinámica cuando un usuario se identifique, haciendo que la clave de acceso a la red inalámbrica sea diferente para cada usuario y en cada ocasión, de esta manera se consigue una mejor protección.

El protocolo WEP es sólo un nivel más de seguridad de entre muchos otros que se deben tener en cuenta.

g) Usar VPN como mecanismos de seguridad

Una VPN (Virtual Private Network) o red privada virtual es una cámara acorazada. Las VPN ofrecen un nivel más de seguridad basado en la creación de un túnel seguro entre el usuario y la red.[5]

La complejidad de las soluciones, topologías y el elevado número de usuarios que presentan las redes inalámbricas de las grandes empresas,

[5] http://www.coit.es/publicac/publbit/bit138/3com.pdf

hacen que las capacidades de seguridad básicas mencionadas anteriormente no sean las suficientes para brindar seguridad a la red.

En general, las grandes corporaciones requieren una tecnología de claves de encriptación más robusta, mecanismos de autenticación escalable y gestión de usuario, centralizada a lo largo de la infraestructura de red, algo que no puede ser almacenado en la memoria limitada de un punto de acceso inalámbrico (Access Point). Un sistema que gestione a miles de usuarios requerirá una solución de seguridad más sofisticada basada en una infraestructura RADIUS (Remote Authenticated Dial-In User Service), cuya gestión se realiza de forma centralizada. RADIUS proporciona la gestión y administración de un amplio número de usuarios autorizados a acceder a los recursos de la red.

Soportar RADIUS con 802.1x, protocolo definido tanto para una red Ethernet cableada como una inalámbrica, mejora aún más la capacidad de autenticación del "usuario inalámbrico". Dada la naturaleza mixta de las redes actuales y que la mayoría de sistemas operativos, desarrollados dentro de las empresas están basados en Windows, 802.1x proporciona capacidades de seguridades superiores y escalables.

Sea cual sea el nivel de seguridad que requiera la infraestructura de red, una solución por capas puede ser adaptada de forma que se ajuste a las necesidades específicas de seguridad de la red inalámbrica. Las soluciones de seguridad pueden ser ampliadas y extendidas más allá de la infraestructura de cable para cubrir también la infraestructura inalámbrica.

1.3 Conceptos y Definición Del Servidor RADIUS En Redes LAN Inalámbricas

1.3.1. Métodos para mantener la conexión y los datos Seguros en redes inalámbricas mediante el Servidor RADIUS.

Una buena red usa varios métodos para mantener la conexión y los datos seguros:

- Firewalls
- Encriptación
- IPSec (Internet Protocol Security – Seguridad del Protocolo Internet)
- Servidor AAA

1.3.1.1. Firewall o Cortafuegos

Provee de una fuerte barrera entre la red privada e Internet. Se puede configurar un firewall para restringir por número de puertos, tipo de paquete, protocolos utilizados, etc. Muchos router, llevan incorporado un firewall y se debería tener uno ya instalado antes de implementar una red ya que puede usarse para terminar sesiones.

1.3.1.2. Encriptación

Es el proceso de coger todos los datos que un ordenador está mandando a otro, y; codificándolo en un formato que solo el otro ordenador será capaz de decodificar.

La mayoría de los sistemas de encriptación entran en dos categorías:

- Encriptación de clave simétrica
- Encriptación de clave pública

En una clave simétrica, cada ordenador tiene una clave secreta (código) que puede usar, para encriptar un paquete de información antes de ser enviado sobre la red a otro ordenador. La encriptación por clave simétrica requiere que se conozcan los

ordenadores que van a hablar, para poder instalar la clave en cada uno de ellos. Esencialmente, tienen el mismo código para poder desencriptar los datos que se están pasando.

La encriptación por clave pública, utiliza una combinación de clave privada y clave pública. La clave privada solo la conoce tu ordenador, mientras que la clave pública se entrega a cualquier ordenador que quiere realizar una comunicación segura.

1.3.1.3. IPSec

Provee de funciones mejoradas de seguridad, como por ejemplo algoritmos de encriptación y una mejor autenticación. IPSec tiene dos modos de encriptación: túnel y transporte. Por túnel, se encripta la cabecera y los datos de cada paquete, mientras que en modo transporte solo se encriptan los datos. Solo los sistemas que soportan IPSec pueden beneficiarse de este protocolo. También hay que tener en cuenta, que todos los dispositivos y los firewalls de cada red, deben tener las mismas políticas de seguridad configuradas. IPSec puede encriptar datos entre varios dispositivos diferentes, como por ejemplo, entre routers, de firewall a router, de un ordenador a router o servidor, etc.

1.3.1.4. Servidores AAA

Sus siglas significan autorización, autenticación y accounting (registro de logs), se utilizan para una mayor seguridad en el acceso dentro de una red remota.

Cuando se hace una petición para poder establecer una sesión desde un cliente externo, dicha petición es enviada al servidor AAA y hace las siguientes tareas:

- Pregunta quién eres (autenticación)
- Qué es lo que puedes hacer (autorización)
- Qué es lo que haces mientras estás conectado (accounting)

Este último punto es especialmente útil, para hacer un seguimiento de clientes y poder realizar auditorías de seguridad, facturación y análisis de uso.[6]

La comunicación entre un NAS (Network Access Server - Servidor de Acceso a la Red) y un servidor RADIUS se basa en UDP (User Datagram Protocol - Protocolo de datagramas de usuario). En general, el protocolo RADIUS es considerado como un servicio sin conexión. Las cuestiones relacionadas con la disponibilidad del servidor, la retransmisión, y tiempos de espera son manejadas por el RADIUS dispositivos habilitados y no el protocolo de transmisión.

El cliente RADIUS es típicamente un NAS y el servidor RADIUS es generalmente un proceso demonio que se ejecuta en un sistema Macintosh, Linux o Windows NT. El cliente pasa la información al usuario designado servidores RADIUS y actúa sobre la respuesta que se devuelve. Los servidores RADIUS reciben las solicitudes de conexión de usuario, autenticar al usuario, y luego devuelven la información de configuración necesaria para el cliente para ofrecer un servicio al usuario. Un servidor RADIUS puede actuar como un cliente proxy para otros servidores RADIUS u otros tipos de servidores de autenticación.

Como se muestra en la figura 1.1 indicamos la interacción entre un usuario de acceso telefónico, el cliente y el servidor RADIUS.

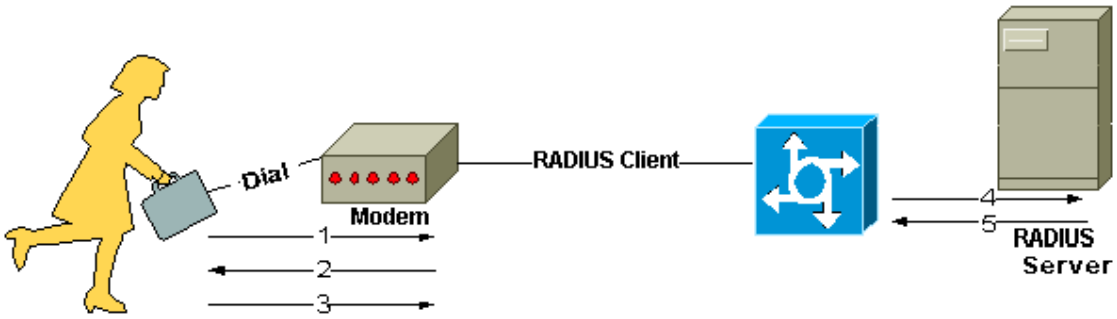

FIGURA 1.1 Interacción entre un usuario de acceso telefónico, el cliente y el servidor RADIUS.

[6] http://www.ordenadores-y-portatiles.com/red-privada-vpn-2.html

- ✓ El usuario inicia la autenticación PPP (Point to Point Protocol – Protocolo Punto a Punto) a la NAS.
- ✓ NAS pide nombre de usuario y contraseña PAP (Password Authentication Protocol – Protocolo de Autenticación de Contraseña), o un desafío CAP (Common Alerting Protocol – Protocolo de Alerta Común)
- ✓ Respuestas del usuario.
- ✓ El Cliente RADIUS envía nombre de usuario y contraseña cifrada con el servidor RADIUS.
- ✓ El Servidor RADIUS responde con aceptar, rechazar, o desafío. [7]

1.3.2. Definición

RADIUS es un protocolo que nos permite gestionar la "autenticación, autorización y registro" de usuarios remotos sobre un determinado recurso. La tupla "autenticación, autorización y registro" es más conocida como AAA, al ser éste su acrónimo de su denominación original inglesa "Authentication, Authorization, and Accounting".

A continuación veremos a qué se refiere cada uno de estos términos:

1.3.2.1. **Autenticación** (authentication)

Hace referencia al proceso por el cual se determina si un usuario tiene permiso para acceder a un determinado servicio, de red del que quiere hacer uso. El proceso de autenticación se realiza mediante la presentación de una identidad y unos credenciales por parte del usuario que demanda acceso.

Un tipo habitual de credencial es el uso de una contraseña (o password) que junto al nombre de usuario, nos permite acceder a determinados recursos. El nombre de usuario

[7]

http://translate.googleusercontent.com/translate_c?hl=es&langpair=en|es&u=http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800945cc.shtml&rurl=translate.google.com&usg=ALkJrhgbBpZeABMxjv2K4Jv02QGXzu1Chg#intro

es nuestra identidad, que puede ser públicamente conocida, mientras que la contraseña se mantiene en secreto, y sirve para que nadie suplante nuestra identidad.

Existen muchos métodos concretos que implementan el proceso de la autenticación. Algunos de ellos, soportados por RADIUS, son:

a) **Autenticación de sistema (system authentication),** típica en un sistema Unix, normalmente realizada mediante el uso del fichero /etc/password;

b) **Los protocolos PAP (Password Authentication Protocol),** y su versión segura CHAP (*Challenge Handshake Authentication Protocol*), que son métodos de autenticación usados por proveedores de servicios de Internet (ISPs) accesibles vía PPP;

c) **EAP (Extensible Authentication Protocol),** que no es un método concreto sino un entorno universal, de autenticación empleado frecuentemente en redes inalámbricas y conexiones punto a punto;

d) **Por último,** también se permite la autenticación basada en ficheros locales de configuración del propio servidor RADIUS.

1.3.2.2. Autorización (authorization)

Se refiere a conceder servicios específicos (entre los que se incluye la "negación de servicio") a un determinado usuario, basándose para ello en su propia autenticación, los servicios que está solicitando, y el estado actual del sistema. Es posible configurar restricciones a la autorización de determinados servicios en función de aspectos como, por ejemplo, la hora del día, la localización del usuario, o incluso la posibilidad o imposibilidad de realizar múltiples "logins" de un mismo usuario.

Los métodos de autorización soportados habitualmente por un servidor de RADIUS incluyen; bases de datos SQL (como Oracle, MySQL y PostgreSQL), o incluso el uso de ficheros de configuración locales al servidor.

No se debe confundir los términos autenticación con autorización. Mientras que la autenticación es el proceso de verificar un derecho reclamado, por un individuo (persona o incluso ordenador), la autorización es el proceso de verificar que una persona ya autenticada tiene la autoridad para efectuar una determinada operación.

1.3.2.3. Registro (accounting)

A menudo traducido también como contabilidad se refiere a realizar un registro del consumo, de recursos que realizan los usuarios. El registro suele incluir aspectos como la identidad del usuario, la naturaleza del servicio prestado, y cuándo empezó y terminó el uso de dicho servicio.[8]

1.3.3. Historia del Servidor de Seguridad RADIUS

El protocolo RADIUS fue desarrollado por las Empresas Livingston, como una autenticación del servidor de acceso y protocolo de contabilidad. Llevado a cabo por varias plataformas de servidores de acceso de red, RADIUS ha ganado soporte entre una gran cantidad de clientes, incluso el servicio de Internet, proveedores ISP (Internet Service Provider - Proveedor de Servicios de Internet).

RADIUS nace por la necesidad de una de las empresas más grandes de Internet como lo es Merit Networks que operaba en California.

Esta empresa trabajaba con grupos de usuarios Dial-Up y buscaba métodos de autenticación que sean flexibles y que permitan obtener reportes, es así que Merit se contactó con Livingston Enterprises y fue escrita la primera versión de RADIUS

Un servidor RADIUS puede proporcionar autenticación y la contabilidad para uno o más clientes. RADIUS es el protocolo de control de acceso. Fue creado por la necesidad de tener un método que Autentifique, Autorice y Contabilice los accesos de los usuarios a los diferentes recursos.

[8] http://www.scribd.com/doc/37641903/Radius-Fin

Los servidores RADIUS son responsables para recibir la conexión del usuario para autenticarlo, y entonces devuelve toda la información de la configuración, necesaria para el cliente y así entrega servicio a los usuarios. Un servidor de acceso RADIUS generalmente es una Workstation especializada conectada a la red.

El RADIUS es un sistema distribuido cliente\servidor, que afianza redes contra acceso desautorizados. En aplicaciones Cisco, los clientes RADIUS corren en routers y switch de Cisco y envían demandas de autenticación a un servidor RADIUS central que contiene toda la autenticación del usuario y acceso de servicio de red.
Cisco soporta RADIUS bajo su paradigma de seguridad AAA. El RADIUS puede usarse con otros protocolos de seguridad AAA, como; TACACS+. RADIUS soporta todas las plataformas de Cisco.

RADIUS se ha implementado en una variedad de ambientes de red, en los que requiere niveles altos de seguridad mientras se mantiene el acceso a la red por los usuarios remotos.

1.3.4. Características del Servidor RADIUS

- ✓ Es un protocolo no orientado a conexión basado en UDP que no usa conexiones directas.
- ✓ Soporta autenticación CHAP (Challenge Handshake Authentication Protocol – Protocolo de Autenticación por Desafío Mutuo), y; PAP vía PPP entre otros.
- ✓ Soporta el modelo AAA (authentication – authorization - accouting).
- ✓ Una característica interesante del servidor RADIUS es que en principio utiliza; segmentos UDP en lugar de TCP. Esto se debe a que RADIUS tiene algunas propiedades inherentes de los segmentos; UDP RADIUS requiere que las consultas fallidas hacia un servidor sean redirigidas a un segundo servidor, y para hacer esto, una copia del pedido original debe existir sobre la capa de transporte del modelo de red (modelo OSI). Esto, en efecto obliga a usar tiempo de retransmisión.

- ✓ UDP permite que RADIUS despache múltiples pedidos al mismo tiempo, además en cada sesión posee habilidades de comunicación sin restricciones entre el equipo de red y los clientes

1.3.5. Funcionamiento del Servidor RADIUS

Cuando un usuario intenta registrarse y autenticar en un servidor de acceso usando RADIUS se realiza los siguientes pasos:

a) Cuando el usuario está listo digita un nombre de usuario y contraseña.

b) Se envían el nombre de usuario y contraseña encriptada sobre la red al servidor RADIUS.

c) El usuario recibe una de las contestaciones siguientes del servidor RADIUS:

- **ACCEPT** El usuario es autenticado
- **REJECT** El usuario no se autentica y es incitado para volver a digitar el nombre de usuario y contraseña, o el acceso se niega.
- **CHALLENGE** El desafío es emitido por el servidor RADIUS. El desafío colecciona datos adicionales del usuario.
- **CHANGE PASSWORD** Es una demanda emitida por el servidor RADIUS y le pide al usuario que seleccione una nueva contraseña.
- **ACCEPT o REJECT** La respuesta se junta con datos adicionales que se usan para EXEC o autorización de red. Usted debe completar primero la autenticación RADIUS antes de usar la autorización RADIUS

1.3.6. Formato de Paquetes de RADIUS

Los datos entre el cliente y el servidor son intercambiados en paquetes RADIUS.
Cada paquete contiene la siguiente información como se muestra en la figura 1.2.

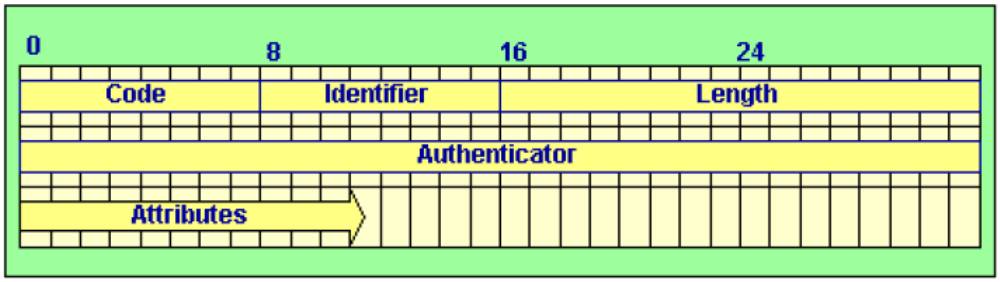

FIGURA. 1.2 Formato de Paquetes RADIUS .

Los campos en un paquete RADIUS son:

a) **Código:** Un octeto que contiene el tipo de paquete que se muestra en la TABLA 1.4.

Valor	Descripción
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

TABLA 1.4 Campo Código en un paquete RADIUS.

b) **Identificador:** Un octeto que permite al cliente RADIUS relacionar una respuesta RADIUS con la solicitud adecuada.

c) **Longitud**: Longitud del paquete (2 octetos).

d) **Verificador:** Valor usado para autenticar la respuesta del servidor RADIUS. Es usado en el algoritmo de encubrimiento de contraseña.

e) **Atributos:** Aquí son almacenados un número arbitrario de atributos. Los únicos atributos obligatorios son: el User-Name (usuario) y el User-Password (contraseña).

1.3.7. Tipos de mensajes RADIUS definidos por los RFC 2865 y 2866:

a) **Access-Request:** Enviado por un cliente RADIUS para solicitar autenticación y autorización, para conectarse a la red. Debe contener el usuario y contraseña; además del puerto NAS, si es necesario.

b) **Access-Accept:** Enviado por un servidor RADIUS en respuesta a un mensaje de Access- Request.

c) Informa que la conexión está autenticada y autorizada y le envía la información de configuración para comenzar a usar el servicio.

d) **Access-Reject**: Enviado por un servidor RADIUS en respuesta a un mensaje de Access- Request. Este mensaje informa al cliente RADIUS que el intento de conexión ha sido rechazado.

e) Un servidor RADIUS envía este mensaje ya sea porque las credenciales no son auténticas o por que el intento de conexión no está autorizado.

f) **Access-Challenge**: Envío de un servidor RADIUS en respuesta a un mensaje de Access- Request. Este mensaje es un desafío para el cliente RADIUS. Si este tipo de paquete es soportado, el servidor pide al cliente que vuelva a enviar un paquete Access-Request para hacer la autenticación. En caso de que no sea soportado, se toma como un Access- Reject.

g) **Accounting-Request:** Enviado por un cliente RADIUS para especificar información de cuenta para una conexión que fue aceptada.

h) **Accounting-Response:** Enviado por un servidor RADIUS, en respuesta a un mensaje de Accounting-Request. Este mensaje reconoce el procesamiento y recepción exitosa de un mensaje de Accouting-Response.

1.3.8. Diagrama de Secuencia

El siguiente diagrama muestra en la figura 1.3 la secuencia seguida cuando un cliente accede a la red y se desconecta de la misma.

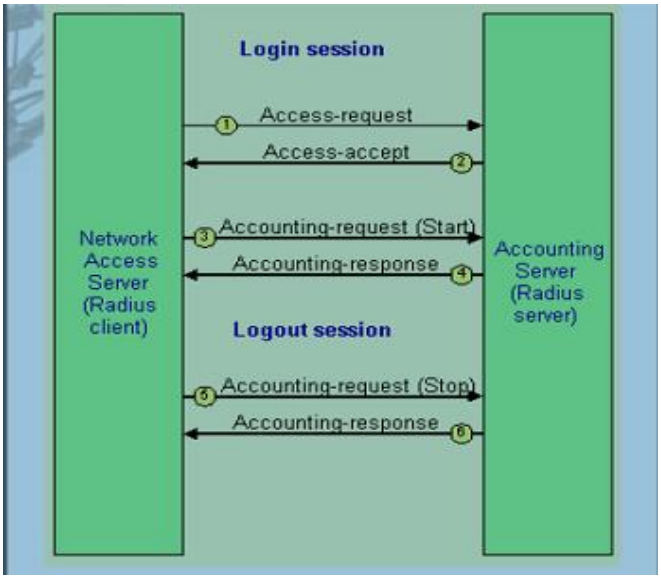

FIGURA 1.3. Diagramas de Secuencia

a) El cliente envía su usuario/contraseña, esta información es encriptada con una llave secreta y enviada en un Access-Request al servidor RADIUS (Fase de Autenticación).

b) Cuando la relación usuario/contraseña es correcta, entonces el servidor envía un mensaje de aceptación, Access-Accept, con información extra, (Por ejemplo: dirección IP, máscara de red, tiempo de sesión permitido, etc.) (Fase de Autorización).

c) El cliente ahora envía un mensaje de Accounting-Request (Start) con la información correspondiente, a su cuenta y para indicar que el usuario está reconocido dentro de la red (Fase de *Accounting*).

d) El servidor RADIUS responde con un mensaje Accounting-Response, cuando la información de la cuenta es almacenada.

e) Cuando el usuario ha sido identificado, éste puede acceder a los servicios proporcionados. Finalmente, cuando desee desconectarse, enviará un mensaje de Accounting-Request (Stop) con la siguiente información:
    - **Delay Time:** Tiempo que el cliente lleva tratando de enviar el mensaje.
    - **Input Octets:** Número de octetos recibido por el usuario.
    - **Output Octets:** Número de octetos enviados por el usuario.
    - **Session Time:** Número de segundos que el usuario ha estado conectado.
    - **Input Packets:** Cantidad de paquetes recibidos por el usuario.
    - **Output Packets:** Cantidad de paquetes enviados por el usuario.
    - **Reason:** Razón por la que el usuario se desconecta de la red.

f) El servidor RADIUS responde con un mensaje de Accounting-Response cuando la información de cuenta es almacenada.

La siguiente figura 1.4 presenta una vista simple de la topología de red, asumida al establecer una conexión RADIUS autenticada con un router.[9]

[9] http://www.scribd.com/doc/43768082/Radius

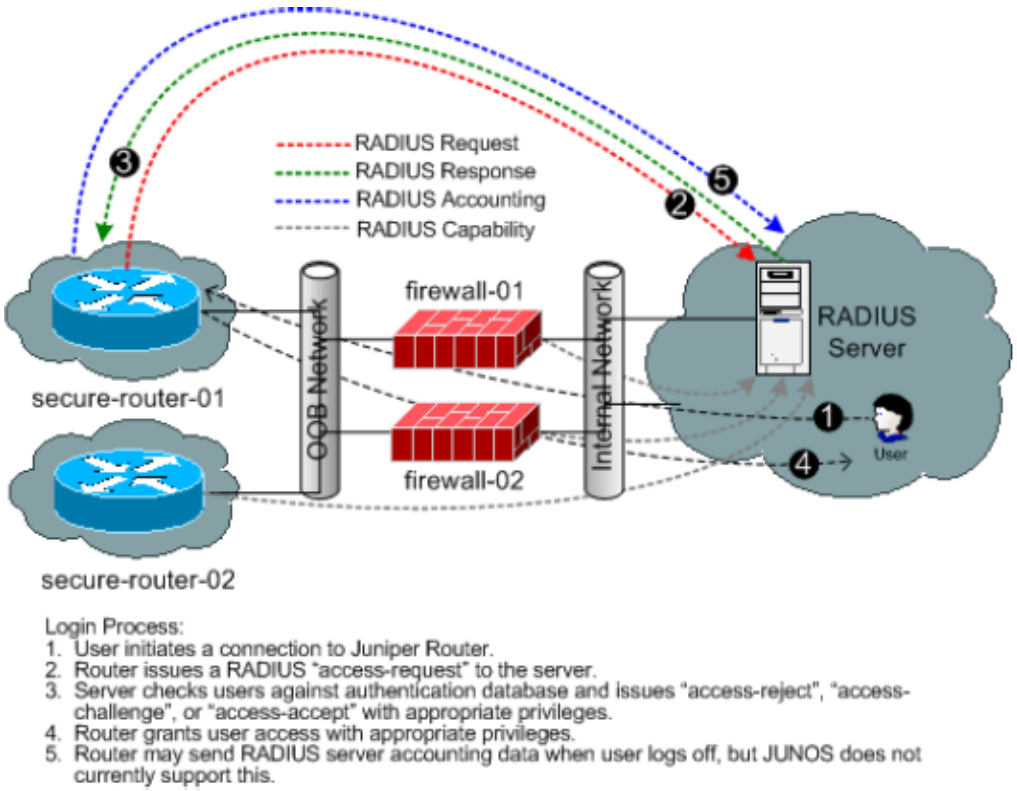

FIGURA 1.4 Topología de red en una conexión RADIUS .

1.3.9. Estándares y protocolos del Servidor RADIUS

Esta es una lista de IETF (Internet Engineering Task Force - Grupo Especial sobre Ingeniería de Internet[1]), normas y directrices relacionadas específicamente, con la autenticación remota y de autenticación remota telefónica de usuario Servicio de Protocolo o RADIUS.

El protocolo RADIUS está definido en los siguientes IETF normas:

RFC (Request for Comment – Solicitud de Comentarios) 2865 - Remote Authentication Dial In User Service (RADIUS). Esta norma describe la autenticación RADIUS y autorización, entre, un servidor de acceso a redes (NAS) y un servidor RADIUS de autenticación común. Este protocolo se utiliza también para llevar la información de configuración del servidor RADIUS para el NAS.

RFC 2866 - RADIUS Accounting. Esta norma describe cómo la información de contabilidad, se lleva de la NAS a un servidor RADIUS de contabilidad compartida.

RFC 2548 Microsoft específicos del proveedor de atributos RADIUS

RFC 2607 Proxy de encadenamiento y la aplicación de políticas en Roaming

RFC 2618 RADIUS Authentication Client MIB
MIB de autenticación RADIUS cliente

RFC 2619 RADIUS Authentication Server MIB
MIB de autenticación RADIUS del servidor

RFC 2620 RADIUS Accounting Client MIB
MIB de Contabilidad RADIUS cliente

RFC 2621 RADIUS Accounting Server MIB
MIB de servidor RADIUS de contabilidad

RFC 2809 Implementation of L2TP Compulsory Tunneling via RADIUS
La aplicación obligatoria del túnel L2TP a través de RADIUS

RFC 2867 RADIUS Accounting Modifications for Tunnel Protocol Support
Modificaciones de Contabilidad RADIUS para el protocolo de túnel de Apoyo

RFC 2868 RADIUS Attributes for Tunnel Protocol Support
Atributos de RADIUS para el protocolo de túnel de Apoyo

RFC 2869 RADIUS Extensions
Extensiones de RADIUS

RFC 2882 Network Access Servers Requirements: Extended RADIUS Practices
Servidores de acceso de redes Requisitos: extensión Prácticas RADIUS

RFC 3162 RADIUS and IPv6
RADIUS e IPv6

RFC 3575 IANA Considerations for RADIUS
Consideraciones IANA para RADIUS

RFC 3579 RADIUS Support for EAP (Updates: RFC 2869)
Soporte RADIUS para EAP (Actualizaciones: RFC 2869)

RFC 3580 IEEE 802.1X RADIUS Usage Guidelines
Instrucciones de uso de IEEE 802.1X RADIUS

RFC 4014 RADIUS Attributes Suboption for the DHCP Relay Agent Information Option
Atributos de RADIUS subopción para el Agente de retransmisión DHCP Opción de Información

RFC 4372 Chargeable User Identity
De identidad de usuario imputable

RFC 4675 RADIUS Attributes for Virtual LAN and Priority Support
Atributos de RADIUS para la LAN virtuales y Soporte Prioritario

RFC 4679 DSL Forum Vendor-Specific RADIUS Attributes
Foro de proveedores específicos RADIUS-DSL Atributos

RFC 4818 RADIUS Delegated-IPv6-Prefix Attribute
RADIUS IPv6 Prefijo atributo Delegada

RFC 4849 RADIUS Filter Rule Attribute
RADIUS atributo regla de filtrado

RFC 5080 Common RADIUS Implementation Issues and Suggested Fixes
RADIUS cuestiones de aplicación comunes y correcciones sugeridas[10]

1.3.10. Políticas de Manejo del Servidor RADIUS

Se ha considerado establecer las siguientes políticas de seguridad, que permitirán un uso apropiado del sistema; estas políticas serán aplicables a todos los usuarios y equipos que requieran utilizar el sistema.

1.3.10.1. Control de acceso mediante dirección MAC en el cliente RADIUS

El usuario para acceder a cualquier servicio de la red (Internet) debe tener asignada una dirección IP válida, la cual será otorgada por el servidor DHCP (Dynamic Host Configuration Protocol - Protocolo de Configuración Dinámica de Host) configurado en el cliente RADIUS, para ello el usuario debe configurar su computador como cliente DHCP.

Para evitar accesos no autorizado a la red, el servidor DHCP estará configurado para otorgar, una dirección IP (Internet Protocol – Protocolo de Internet) únicamente a los usuarios cuya dirección MAC haya sido previamente registrada, en un listado de direcciones MAC autorizadas. Se podrá registrar, modificar y eliminar la dirección MAC de los usuarios en el listado mediante el uso de la interfaz de administración.

[10] http://en.wikipedia.org/wiki/List_of_RADIUS_standards

Al momento de registrar las direcciones MAC será posible también, indicar una dirección IP fija para cada dirección MAC; si no se indica ninguna, el sistema asignará al usuario una dirección IP disponible, del rango que se haya definido en la configuración del servidor DHCP.

1.3.10.2. Filtros de direcciones MAC en puntos de acceso inalámbricos

Con el propósito de evitar que usuarios no autorizados hagan uso indebido del sistema, se va a configurar en los puntos de acceso inalámbricos (AP), un filtro de direcciones MAC de tal forma que únicamente lo usuarios autorizados, puedan hacer uso del segmento de red inalámbrico. Para conseguir esto se requiere que el equipo a emplearse sea compatible con esta funcionalidad.

1.3.10.3. Autorización de acceso a usuarios con dirección IP configurada de forma estática

Una vulnerabilidad identificada durante el proceso de implementación, fue que cuando se configuraba una dirección IP, perteneciente al segmento de red de los usuarios, de forma estática en un computador, era posible el acceso a la página de autenticación del cliente RADIUS.

Para evitar que esto suceda fue necesario, permitir el acceso a usuarios que hayan configurado su dirección IP de forma estática, únicamente si su dirección MAC fue previamente registrada en el sistema.

1.3.10.4. Empleo de nombre de usuario y clave de acceso segura para la autenticación de usuarios

Una vez que el usuario disponga de una dirección IP, podrá acceder al sistema de autenticación.

El sistema de autenticación solicitará; que se ingresen un "nombre de usuario" y una "clave", a estos dos parámetros estará asociado un perfil, que será asignado de acuerdo a los requerimientos y/o necesidades del usuario.

El nombre de usuario será asignado por el administrador del sistema; una vez que el usuario haya solicitado el servicio.

Para la creación del nombre de usuario se considerará, utilizar la primera letra del primer nombre del usuario seguido de su apellido, en caso de no encontrarse disponible este nombre, de usuario se deja a consideración del administrador alguna otra combinación (p.e. emplear la primera letra de los dos nombres seguidas del apellido).

Para garantizar que la clave de acceso de usuario sea segura, ésta deberá ser de al menos ocho caracteres alfanuméricos, de los cuales al menos tres y no más de cinco serán números.

Para la creación de la cuenta y asignación de un "nombre de usuario" y "clave", el usuario deberá indicar, la siguiente información, que será empleada para la creación de la cuenta de usuario en el servidor RADIUS:

Primeramente la información general del usuario que se lista a continuación:

- ✓ Nombre de usuarios (*Username*)
- ✓ Clave (*Password*)
- ✓ Grupo (*Group*)

Además se debe configurar la información que será intercambiada en el *Access Accept*, enviado por el servidor RADIUS, misma que se lista a continuación.

a) Protocolo (*Protocol*), que puede ser PPP, L2TP o IP; este campo no se empleará en la implementación.
b) Dirección IP (IP *Address*), corresponde al campo de la dirección IP del usuario.

c) Máscara de red de la dirección IP (IP *Netmask*), corresponde a la máscara de red empleada para el usuario.
d) Tramado MTU (Maximum Transmission Unit – Maxima Unidad de Transmisión) (*Framed*-MTU), corresponde al tamaño de la trama el valor por defecto empleado en el campo es de 1500
e) Compresión usada (*Compression Used*), el valor por defecto es *Van- Jacobson-TCP-IP* (*Transmission Control Protocol* - Protocolo de Control de Transmisión/ Internet Protocol – Protocolo de Internet), este campo no se lo emplea en la implementación.
f) Tipo de servicio (*Service Type*), campo que se empleará para enviar la información de perfil.
g) Duración de la sesión (*Session Timeout*), campo empleado, para indicar el tiempo máximo de duración de una sesión del usuario.
h) Tiempo máximo de inactividad (*Idle Timeout*), campo empleado para indicar el período de tiempo en el cual se considerará un usuario como inactivo.
i) Número máximo de sesiones (*Port Limit*), por política de utilización el número máximo de sesiones por usuario será de una sesión.
j) Mensaje presentado (*Lock Message*), campo opcional de tipo descriptivo.

Por defecto si el usuario no se ha autenticado y desea acceder a una dirección, web externa a la red a través de su navegador, en lugar de la dirección solicitada se le mostrará una página de autenticación, alojada en el cliente RADIUS, en esta página se le solicitará; ingresar el "nombre de usuario" y la "clave" que le fueron asignados. Una vez ingresada esta información se enviará una petición de *Access-Request* al servidor RADIUS, y dependiendo del resultado que el servidor RADIUS envié en respuesta a esta petición el usuario será aceptado o rechazado.

Si la respuesta es un *Access-Reject* se le mostrará, al usuario una página de error y se le solicitará ingresar nuevamente el "nombre de usuario" y la "clave".

Si la respuesta del servidor RADIUS, es un *Access-Accept* en el cliente RADIUS se crearán las reglas apropiadas que permitirán al usuario utilizar al cliente como *Gateway*, para el acceso a Internet y se ejecutarán un conjunto de comandos dependiendo del perfil asociado al usuario, los cuales permitirán el acceso hacia el Internet según su perfil; restringiendo y/o permitiéndole acceso a los servicios y controlando el uso del ancho de banda.

El sistema se ha diseñado para permitir una sola sesión simultanea por usuario, por lo cual si otro usuario intenta hacer uso del sistema con un "nombre de usuario" y "clave" que en ese momento estén siendo empleados, se le presentará un error indicando la dirección IP y la dirección MAC, del usuario que se encuentra empleando las credenciales ingresadas y solicitando que se envíe esta información al administrador de red.

1.3.10.5. Definir diferentes perfiles de acceso para los usuarios

En el sistema se establecerán distintas categorías de usuarios en función de las actividades que el usuario realizará.

A cada perfil estará asociado un conjunto de reglas que permitirán, al usuario realizar únicamente peticiones a ciertos puertos, dependiendo del perfil asignad a cada usuario del sistema se le asignarán los permisos correspondientes.

Todos los perfiles tendrán acceso al puerto http (80) y https (443) del cliente RADIUS, ya que el sistema empleará estos dos puertos para realizar la negociación de intercambio de credenciales, entre el usuario y el cliente RADIUS, credenciales que posteriormente serán enviadas al servidor RADIUS.

Por defecto se definirán tres perfiles, según el perfil asociado el usuario podrá acceder únicamente a cierto tipo de protocolos y/o aplicaciones como se describe a continuación:

Acceso Total: Podrá utilizar todos los servicios disponibles en la red.
Acceso Restringido: Se le permitirá acceso http, smtp, pop3 y ftp.

Invitado: Solo tendrá acceso http.

Para el caso de usuarios que no pertenezcan a ninguno de los perfiles no tendrán acceso a ninguno de los servicios de la red.

El administrador del sistema podrá hacer uso de la interfaz de administración del cliente RADIUS para la creación y/o modificación, de los perfiles de usuario existentes; esta interfaz permitirá asignar un nivel de acceso a la red diferente a cada grupo de usuarios pertenecientes a un determinado perfil, así como también limitar el uso del ancho de banda disponible.

El paso de trafico DNS (Domain Name System o DNS - Sistema de Nombres de Dominio) hacia el Internet estará permitido para todos los usuarios, de esta forma se permitirá al usuario emplear el servidor DNS de su elección, en caso que no desee emplear el servidor DNS que se configura vía DHCP.

1.3.10.6. Protección de la información que viaja por el segmento de red inalámbrico

La información de los usuarios que se conecten por medio inalámbrico viajará encriptada, para prevenir cualquier tipo de ataque que se pueda dar en este segmento de la red.

Para proteger la confidencialidad de la información, se podrá emplear mecanismos de encripción de información utilizados en comunicación inalámbrica como por ejemplo: WEP, TKIP, 802.1X/EAP, WPA y WPA2/802.11i.

1.3.10.7. Protección de la información de autenticación que el usuario envía al cliente RADIUS

Será un requisito obligatorio el emplear un mecanismo, de encriptación en el intercambio de información confidencial como son nombres de usuario y clave.

Por lo cual en la implementación se considerará emplear https, con el objetivo de proteger la confidencialidad de la información, importante intercambiada con el sistema de autenticación del cliente RADIUS. Es decir, la información que envíe el usuario viajará encriptada mediante el uso de Certificados Digitales.

El sistema de autenticación deberá presentar de forma automática, la página de autenticación empleando https, de tal manera que para el usuario sea transparente la utilización de encripción.

1.3.10.8. Protección de la información de autenticación que el cliente RADIUS, envía al servidor RADIUS

La información intercambiada entre el cliente RADIUS y el servidor RADIUS deberá ser encriptada, ya que esta información corresponde a datos confidenciales de los usuarios.

Con el objetivo de encriptar la información que se intercambia entre el cliente y el servidor RADIUS, se ha decidido levantar un túnel IPSec entre esos dos servidores, de tal manera que la información intercambiada sea únicamente comprendida entre estos dos participantes.

1.3.10.9. Registro del tiempo de conexión y el consumo medido en *bytes* que realice el usuario

El tiempo de conexión en segundos y la cantidad de información, que el usuario intercambie en *bytes* serán registrados en una base de datos, para poder tarifar la utilización del sistema.

Con el fin de registrar la utilización del sistema se definió un mecanismo automático, que permita ir actualizando el tiempo de conexión y los *bytes* consumidos en la base de datos.

El sistema debe determinar de forma automática, si un usuario se encuentra o no en actividad, esto se lo realiza mediante la comparación del consumo acumulado medido

cinco segundos antes, con el consumo acumulado hasta ese instante; en caso que no se registre consumo del usuario por un tiempo mayor al tiempo máximo de inactividad configurado (*Idle Timeout*), el sistema finalizara la sesión actual del usuario y procederá a aplicar las restricciones de acceso correspondientes.[11]

1.3.11. Parámetros de Selección del Servidor RADIUS

1.3.11.1. Seguridad

En grandes redes, la seguridad de la información puede estar dispersa en toda la red en diferentes dispositivos. RADIUS, permite que la información del usuario se almacene en un host, reduciendo al mínimo el riesgo de fallos de seguridad. Toda la autenticación y el acceso a los servicios de red es gestionada por la acogida que funciona como el servidor RADIUS.

1.3.11.2. Flexibilidad

El software del servidor RADIUS se distribuye en formato de código fuente a los clientes de Livingston. Usando modificables "talones", RADIUS puede ser adaptado para trabajar con los sistemas y protocolos de seguridad. El servidor RADIUS puede ser adaptado a la red, en lugar de ajustar su red para trabajar con RADIUS. RADIUS se puede usar con cualquier servidor de comunicaciones que soporta el protocolo RADIUS. Cuando la nueva tecnología de seguridad se convierte en aumento de las necesidades, o de seguridad, RADIUS puede ser ampliado para ofrecer nuevos servicios.

1.3.11.3. Administración

La Información de seguridad se almacena en archivos de texto en una ubicación central en el servidor RADIUS. La adición de nuevos usuarios a la base de datos o modificar la información, de usuarios existentes se puede lograr fácilmente mediante la edición de estos archivos de texto.

[11] http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/995/4/T10761CAP2.pdf

1.3.11.4. Amplia capacidad de registro

RADIUS ofrece amplias capacidades de auditoría, que se refiere a la contabilidad, como la información recopilada en un archivo de registro se pueden analizar por razones de seguridad, o utilizados para la facturación.

1.3.11.5. Multiplataformas

El servidor RADIUS está disponible para los siguientes sistemas operativos:

- Windows
- SunOS 4.1.4 SunOS 4.1.4
- Solaris 2.5 Solaris 2.5
- HP/UX 10.01 HP / UX 10.01
- Linux 1.2.13 (ELF) Linux 1.2.13 (ELF)
- AIX 3.2.5 AIX 3.2.5
- SGI Irix 5.2 SGI Irix 5.2
- DEC Alpha OSF/1 3.0 DEC OSF Alpha / 1 3,0
- BSD/OS 2.0 BSD / OS 2.0 [12]

[12] http://www.stat.ufl.edu/system/man/portmaster/RADIUS/guide/1overview.html

CAPITULO II

2. METODOLOGÍA

2.1. TIPO DE ESTUDIO

Para este proyecto se utilizarán los siguientes métodos de investigación.

2.1.1. Método Científico

Al observar que las redes inalámbricas tienen múltiples inseguridades al ser implementadas, y; el robo de los datos de la cuenta como el nombre de usuario y contraseña, la rotura de varios estándares de seguridad WIFi como WEP, WPA, WPA2 a cargo de los Hackers, etc, sucede; es porque no se implementan políticas de seguridad lo suficientemente robustas para evitar estas inseguridades, de esta forma la investigación se basará en el análisis de las políticas de seguridad que brinda la implementación de un servidor RADIUS para que autentiquen, autoricen y registren a los usuarios que se conectan a la red inalámbrica implementada, dando a conocer las ventajas que brinda a parte de la mayor protección a la red e implícitamente a la información que por ahí fluya.

2.1.2. Método Deductivo.

Para demostrar que la implementación de un Servidor Radius es una solución viable para obtener mayor seguridad en las redes inalámbricas, se configura un ejemplo básico utilizando el software Cisco Packet Tracer 5.3, que indica las utilidades que brinda el servidor RADIUS, como un servidor de seguridad en redes LAN inalámbricas.

2.2. POBLACIÓN MUESTRA

2.2.1. POBLACIÓN.

Para el proyecto se tomará en consideración los usuarios que acceden a una red inalámbrica en un Campus Universitario de la ciudad de Riobamba, ya que la conexión a internet en una universidad en estos tiempos es una necesidad fundamental, de allí que

se puede analizar la posibilidad de ofrecerle al estudiante cualquier tipo de material investigativo a través de la red inalámbrica, de esta forma se ha tomado en consideración que en una universidad podemos trabajar con una población de 200 estudiantes que solicitan el servicio inalámbrico.

2.2.2.- MUESTRA

Fórmula

$$\text{Tamaño Muestra } = \frac{N\, z^2 pq}{r^2(N-1)+z^2 pq}$$

Donde:

N: Tamaño de la población, numero de total de historias,

z: Valor de z, 1.96 para α=0.05 y 2.58 para α=0.01.

p: Prevalecía esperada del parámetro a evaluar. En Caso de desconocerse aplicar la opción más desfavorable (p = 0.5), que hace mayor el tamaño muestral.

q: 1 – p

i: Error que se prevé cometer

$$n = \frac{200 * (1.96)^2(0.5)(0.5)}{(0.1)^2(200-1) + (1.96)^2(0.5)(0.5)}$$

$$n = \frac{200 * (3.84)(0.25)}{(0.01)(199) + (3.84)(0.25)}$$

$$n = \frac{192}{2.95}$$

$$n = 65$$

Muestra Indirecta= 65 estudiantes.

2.3. OPERACIONALIZACIÓN DE VARIABLES

En la tabla 2.1 se explicará la operacionalización de variables.

VARIABLE	TIPO	DEFINICION	INDICADORES
Instalación y configuración de un Servidor RADIUS	INDEPENDIENTE	Implementación de un ejemplo básico, utilizando el software Cisco Packet Tracer 5.3, el cual describe el proceso mediante el cual los usuarios de una red inalámbrica tienen que ser autenticados, autorizados y registrados por el Servidor RADIUS para acceder a los beneficios que brinde dicha red.	• Viabilidad • Confiabilidad • Seguridad • Inconvenientes de Red • Problema de conexión • Integridad de los datos
Seguridad en la red inalámbrica	DEPENDIENTE	Con la seguridad en la red inalámbrica se puede controlar y gestionar el acceso a los usuarios.	• Autenticación • Autorización • Registro

TABLA 2.1. Operacionalización de variables

En la tabla 2.2, se explican los indicadores que caracterizan a la variable independiente.

Indicador	Definición	Propósito
Viabilidad	Que tiene probabilidades de llevarse a cabo.	Conocer las posibilidades reales de las instituciones públicas o privadas de llevar a cabo, la instalación de una WLAN en sus instalaciones.
Confiabilidad	Probabilidad del buen funcionamiento de una cosa o proyecto.	Conocer el grado de confiabilidad que las instituciones depositarían en la tecnología inalámbrica WLAN.
Seguridad	Relativo a la persona o cosa en que se puede confiar en	Conocer el grado de seguridad que las

	absoluto. Exento de todo riesgo o peligro.	instituciones confiarían a una red WLAN con la implementación de un servidor RADIUS.
Inconvenientes de red.	Todo tipo de problemas que se surgen al momento de utilizar la red.	Conocer los problemas que las instituciones enfrentan cuando interactúan con redes WLAN.
Integridad de los datos	Aspectos en los cuales se puede confiar la seguridad de la información.	Exenta de todo riesgo o peligro Informar a las instituciones sobre la integridad de la información mediante la utilización de una WLAN con servidor RADIUS.

TABLA 2.2 Indicadores de la variable independiente

En la tabla 2.3, se explican los indicadores que caracterizan a la variable dependiente.

Indicador	Definición	Propósito
Autenticación	Acto de establecimiento o confirmación de algo (o alguien) como auténtico	Verificar la identidad del usuario (cliente) que intenta beneficiarse de los recursos de la red Wlan
Autorización	Acto o documento a través del cual se permite a una persona realizar aquello que solicita	Exigir a los usuarios (clientes) que cumplan con los requisitos exigidos para poder hacer uso de los requisitos de la red Wlan
Registro	Anotar o incluir una cosa en una lista o relación	Realizar un registro del consumo, de recursos que realizan los usuarios.

TABLA 2.3 Indicadores de la variable dependiente.

2.4. PROCEDIMIENTOS

2.4.1. Configuración básica del servidor RADIUS en una red LAN inalámbrica

En esta configuración se mostrará cómo actúa el servidor RADIUS, validando y dando acceso a los usuarios dentro de una red local inalámbrica, utilizando el simulador de redes Cisco Packet Tracer 5.3

2.4.1.1 Configuración de los Equipos

Una vez ingresado al programa, ubicamos el servidor RADIUS en el área de trabajo, seleccionando de los dispositivos terminales el elemento marcado como *Generic (Server-PT)* como se muestra en la figura 2.1.

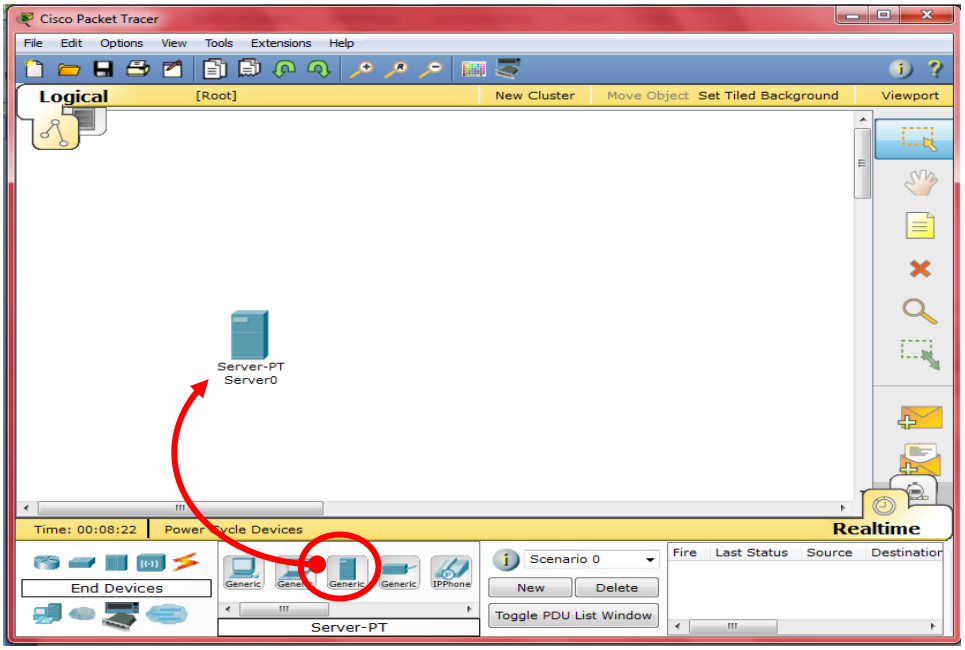

FIGURA 2.1 Server PT en el área de trabajo

Ubicamos el router inalámbrico linksys-WRT300N en el área de trabajo, seleccionando de los dispositivos wireless el elemento marcado como *Linksys (Linksys-WRT300N)*, como se muestra en la figura 2.2.

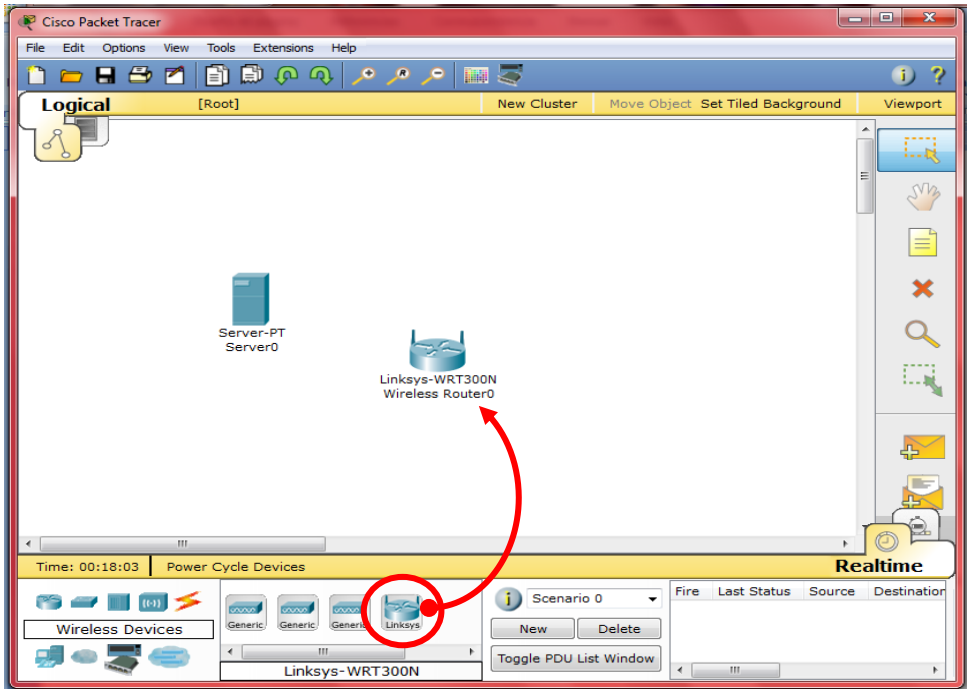

FIGURA 2.2 Linksys-WRT300N en el área de trabajo

Ubicamos las portátiles en el área de trabajo, seleccionando de los dispositivos terminales el elemento marcado como *Generic(Laptop-PT)*, como se muestra en la figura 2.3.

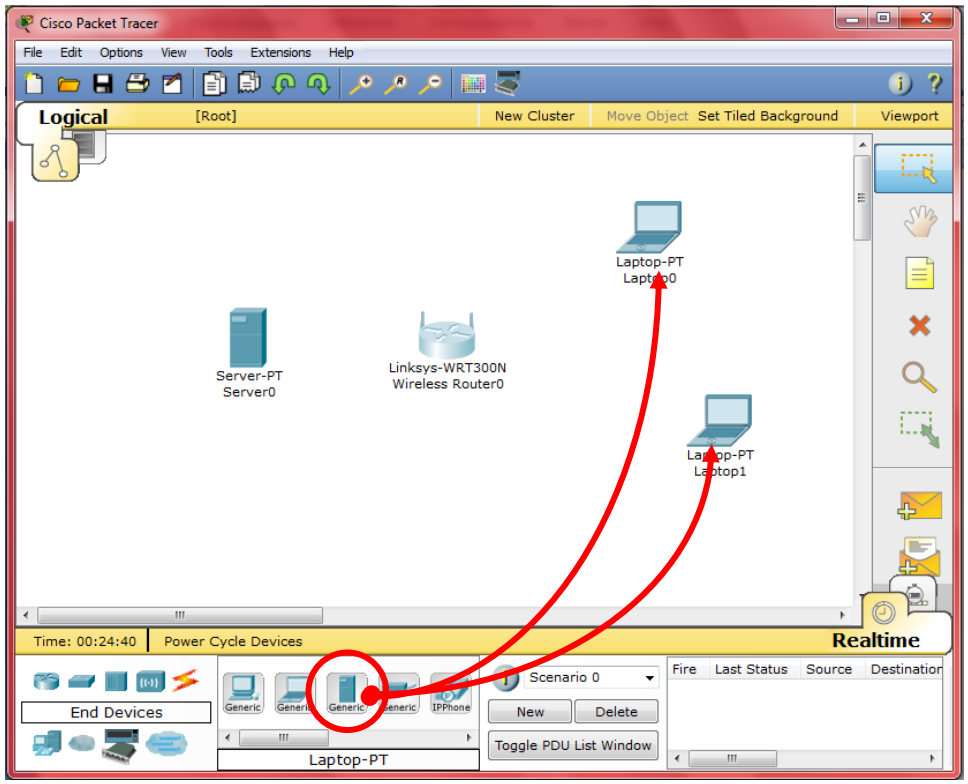

FIGURA 2.3 Laptop-PT en el área de trabajo

Procedemos a cambiar los nombres de los elementos que forman este esquema, con la finalidad de ubicarlos e identificarlos dentro del área de trabajo; damos clic sobre la segunda línea de cada dispositivo el cual contiene el nombre del elemento, quedando de la forma que se muestra en la figura 2.4.

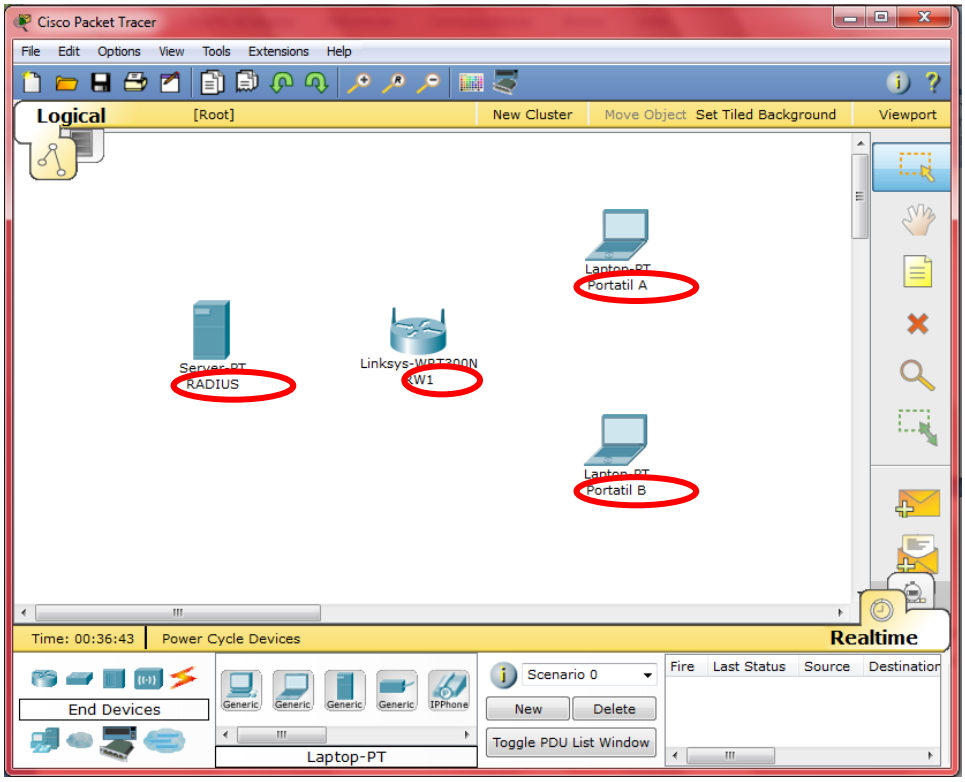

FIGURA 2.4 Cambio de nombres de los equipos

2.4.1.2 Configuración de las Portátiles.

Las laptops por defecto tienen instaladas tarjetas de red alambicas Fast-Ethernet, por lo que es necesario cambiar este módulo por uno que trabaje inalámbricamente, para conseguir este objetivo se realiza el siguiente procedimiento en las dos Portátiles del esquema.

Dar clic sobre el icono de la Portátil A, donde podemos identificar las siguientes características en la ficha *Physical*, como se muestra en la figura 2.5.

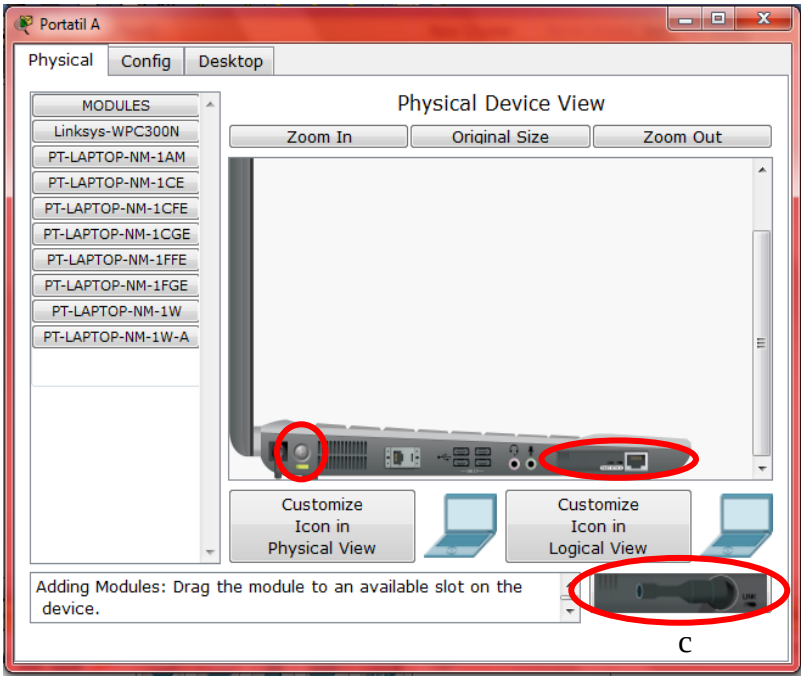

FIGURA 2.5 Características Portatil

a) Estado del equipo (Encendido)

b) Tarjeta Fast-Ethernet instalada

c) Modulo Wireless

Apagar el equipo pulsando sobre el botón de encendido (1), para poder cambiar los módulos, una vez apagado el equipo, retirar la tarjeta de red fast ethernet y colocar la inalámbrica (2), finalmente encender nuevamente la portátil (3) como se muestra en las figuras 2.6 y 2.7.

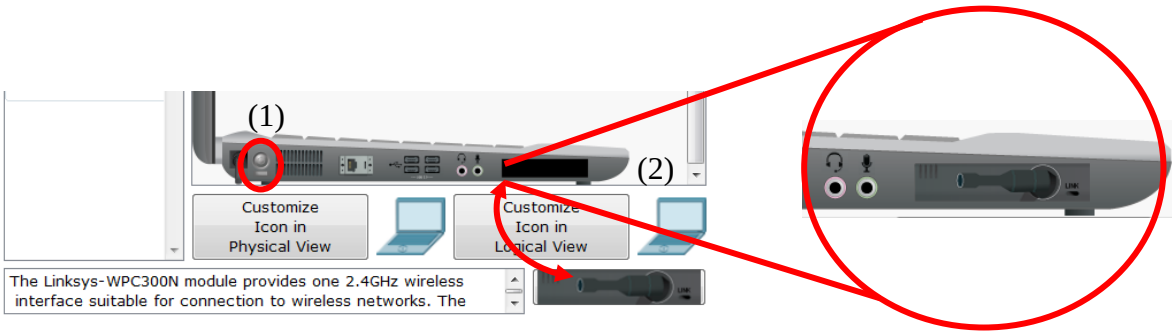

FIGURA 2.6 Cambio de tarjeta de red

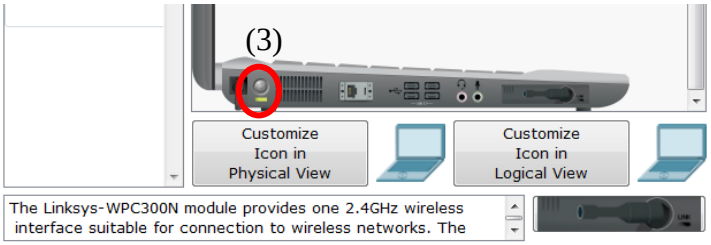

FIGURA 2.7 Laptop con tarjeta de red inalámbrica

Luego de realizado el procedimiento anterior en ambas portátiles, estas se conectan automáticamente con el Router inalámbrico (WR1), como muestra la figura 2.8.

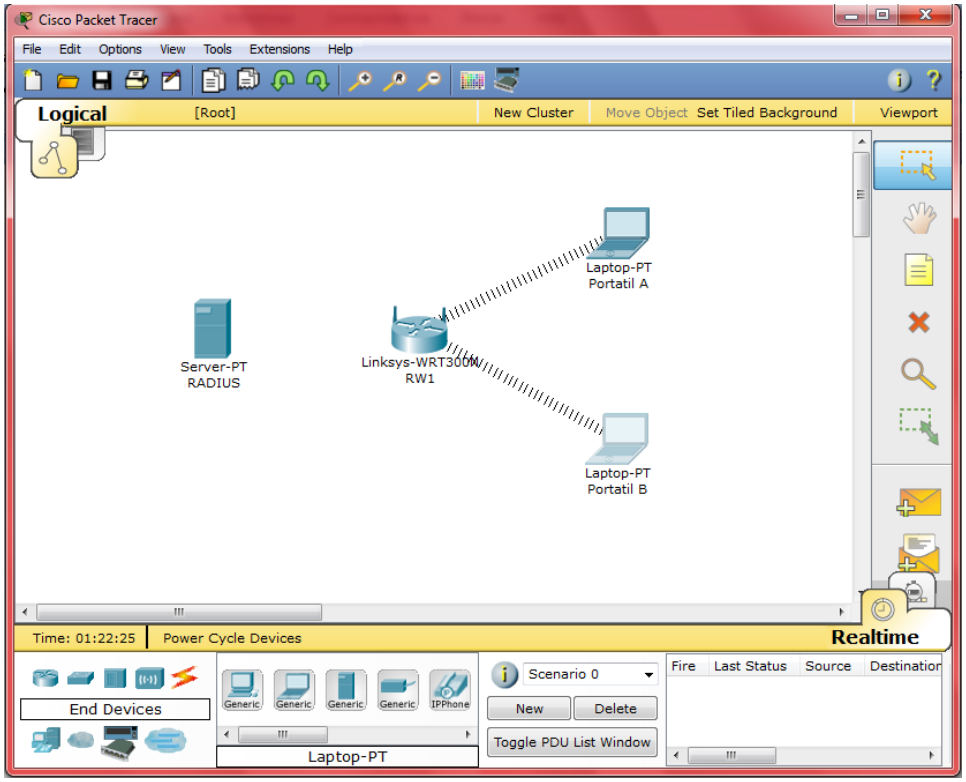

FIGURA 2.8 Conexión de red inalámbrica

Configurar la obtención de las direcciones IP para las portátiles, de forma que se les sean asignadas desde WR1 automáticamente (DHCP), a la vez que configuramos el tipo de seguridad que usaran las mismas para compartir información, en este caso será a través del uso de usuario y contraseña (WPA Enterpraise), y; el tipo de encriptación (AES) que serán posteriormente registrados en el servidor RADIUS de la siguiente forma:

Dar clic sobre el icono de la Portátil A, seleccionar la ficha *Config*, por defecto el router WR1 asigna automáticamente direcciones IP de la red 192.168.0.0, y; como puerta de enlace (Gateway) la dirección 192.168.0.1 como muestra la figura 2.9.

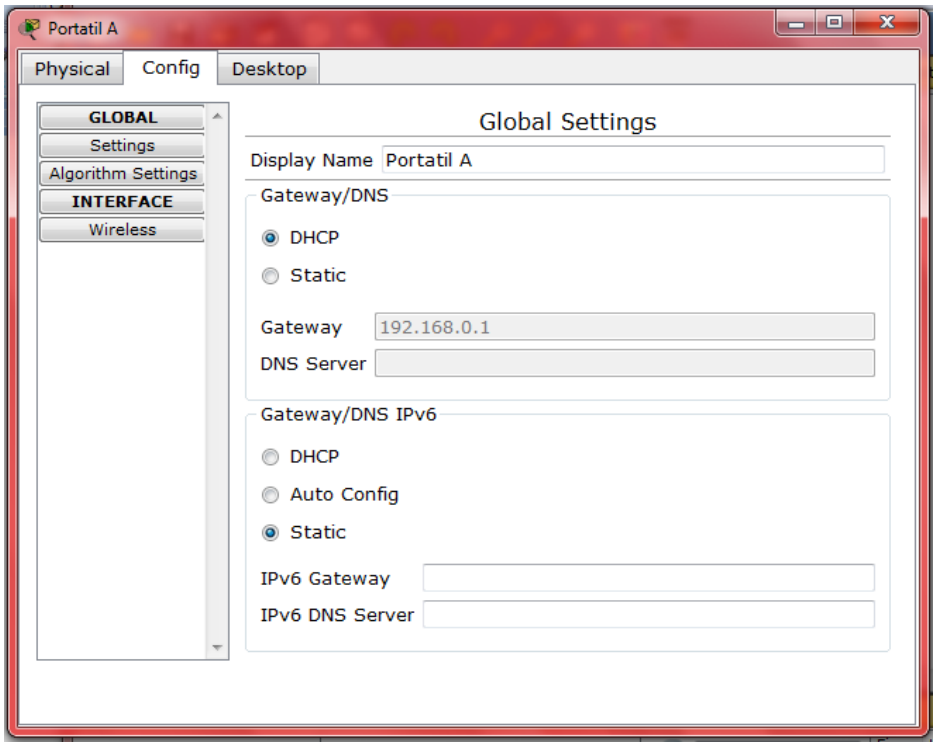

FIGURA 2.9 Conexión de red inalámbrica

Dar clic en el botón Wireless de la sección izquierda del cuadro de diálogo y seleccionar las siguientes opciones:

Verificar que se encuentre activa la tarjeta inalámbrica (a), ubicar el nombre de la SSID de la red inalámbrica a WLAN (b), en sección *Authentication* marcar WPA (c), llenar los casilleros USER ID y PASSWORD con usuarioa y passusuarioa respectivamente (d), en *Encryption Type* AES (e), y; finalmente en la sección *IP Configuration* activar la opción DHCP (f) quedando como se muestra en la figura 2.10.

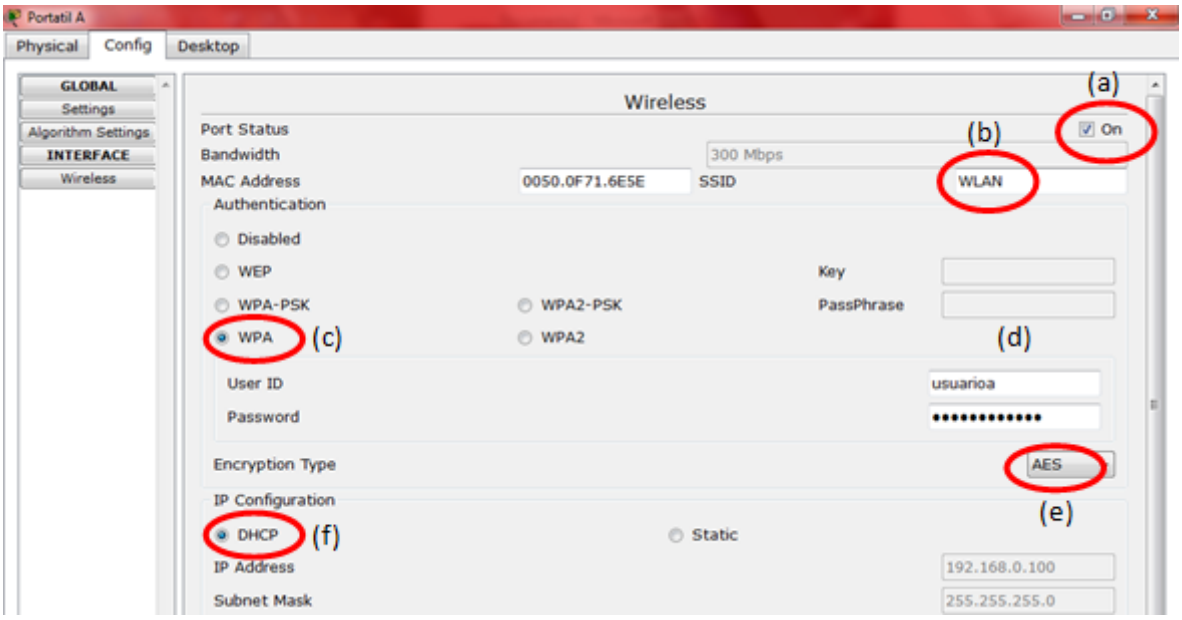

FIGURA 2.10 Configuracion Wireless Portatil A.

El mismo procedimiento se debe desarrollar en la portátil B, únicamente con los cambios en el usuario y contraseña, dejándolos usuariob y passusuariob en USER ID y PASSWORD respectivamente como muestra la figura 2.11.

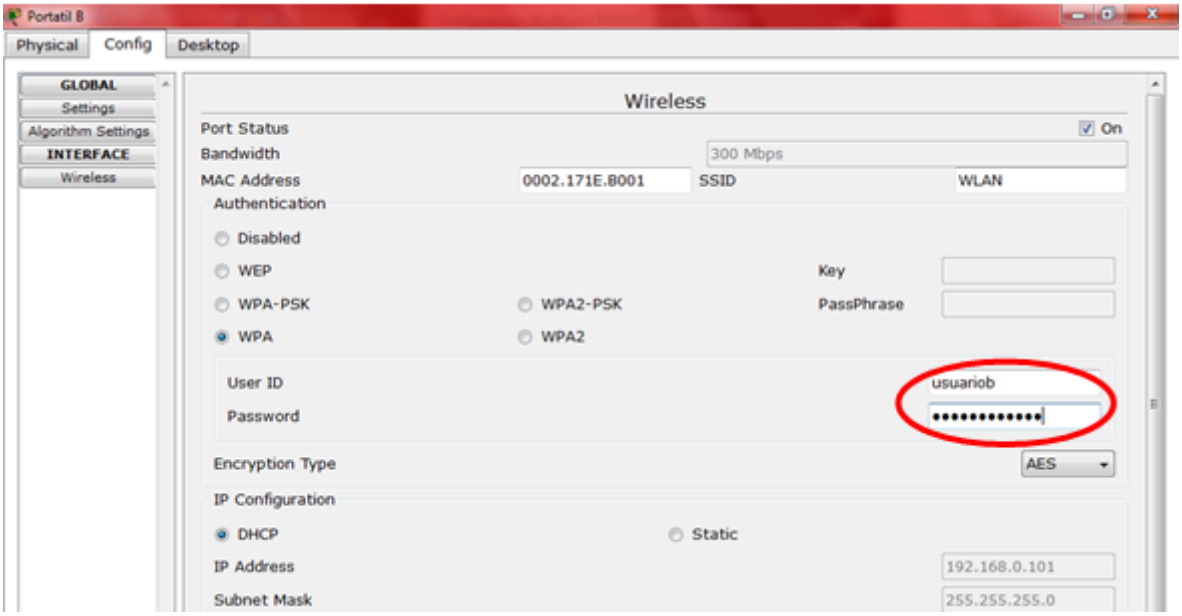

FIGURA 2.11 Configuracion Wireless Portatil B.

Realizados los cambios, se verá en el esquema que ya no se muestran las conexiones inalámbricas entre WR1 y las portátiles como muestra la figura 2.12.

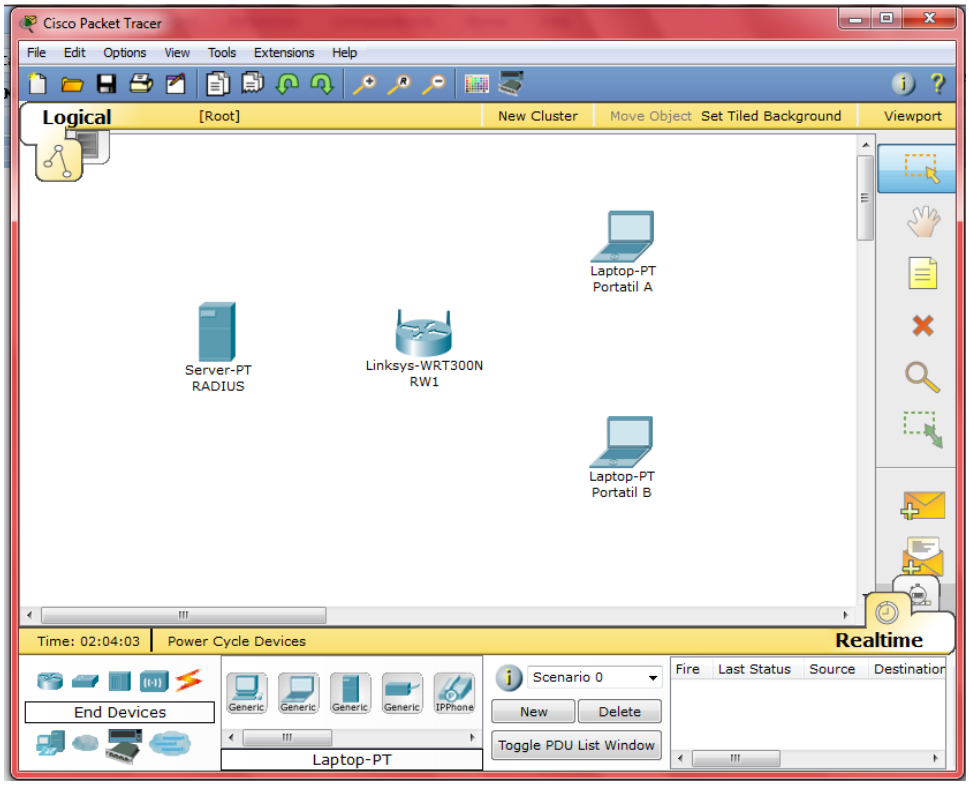

FIGURA 2.12 Esquema de configuración luego de cambiar configuración en las portátiles.

2.4.1.3 Ruteador Linksys-WRT300N

Es necesario añadir ciertos cambios en este dispositivo de manera que sea este dispositivo quien brinde conectividad entre los usuarios que pretenden conectarse a la red, distinguiendo entre quienes poseen permiso para hacerlo y quienes no, una vez que sean validados en el servidor RADIUS.

Este dispositivo es el punto de entrada a la red, y; es quien facilita las direcciones IP solamente a los usuarios que han pasado por el proceso de validación en el servidor RADIUS, para lo cual se debe configurar el equipo con el siguiente procedimiento:

Dar clic en el icono que identifica al dispositivo y seleccionar la ficha *Config*, como se muestra en la figura 2.13..

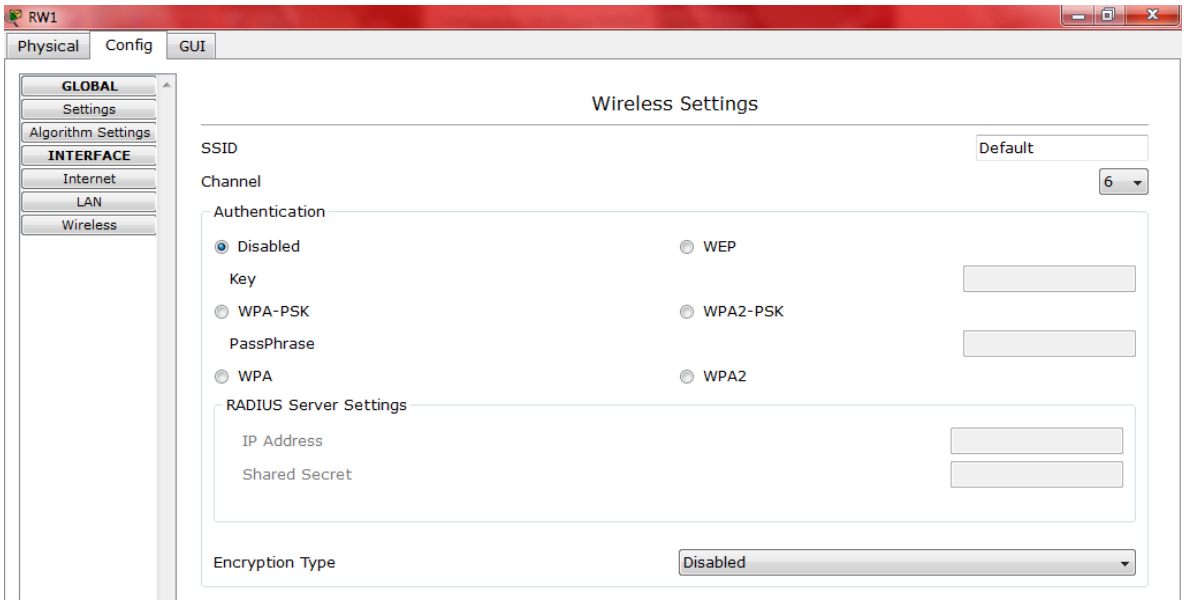

FIGURA 2.13 Configuración Ruteador

Escribir el SSID de la red inalámbrica WLAN (a), el canal de comunicación utilizado será el 6 (b), en la sección *Authentication* seleccionar WPA (c), colocar la dirección IP que tendrá el servidor RADIUS en nuestra red (192.168.0.10) y la clave secreta con la que se validará a WR1 en el servidor RADIUS (accesowlan) (d), y por último el tipo de encriptación en AES (e), como se muestra en la figura 2.14.

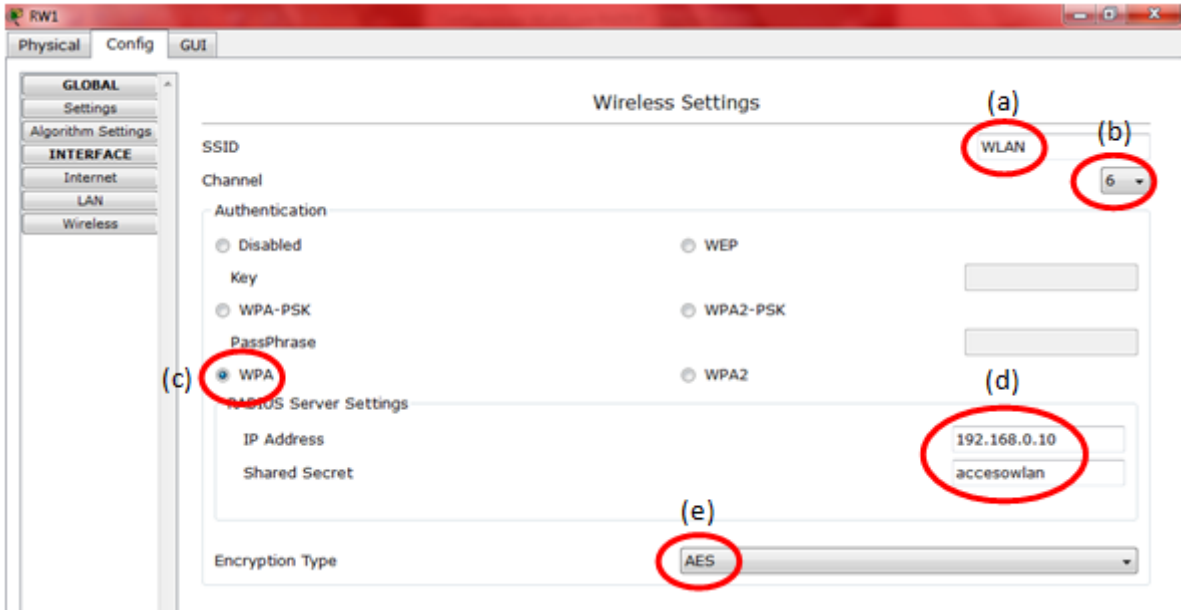

FIGURA 2.14 Configuración Ruteador con cambios

2.4.1.4 Servidor RADIUS

Conectar con un cable directo, seleccionando en la sección *connections (Copper Straight-Through)(a)* a nuestro servidor RADIUS al puerto FastEthernet, y; el otro extremo a WR1 al puerto Ethernet 1(b) como muestra la figura 2.15.

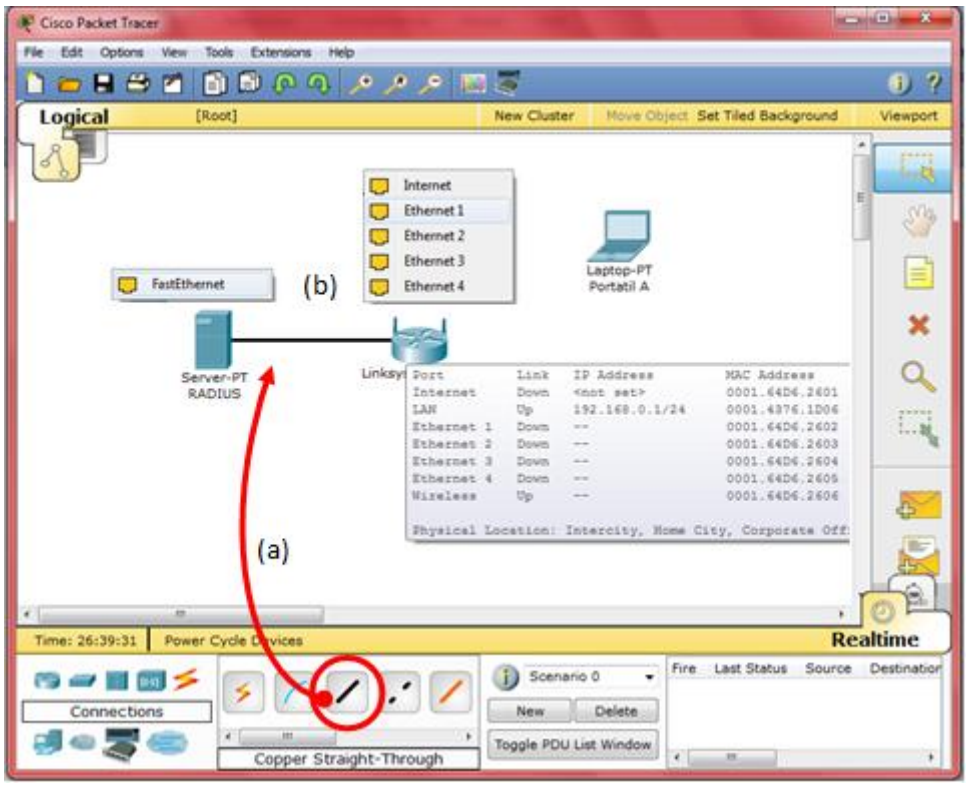

FIGURA 2.15 Conexión Server Radius – Ruteador Linksys

Quedando la conexión como muestra la siguiente figura (a), y pasados unos segundos figura (b), como se muestra en la figura 2.16.

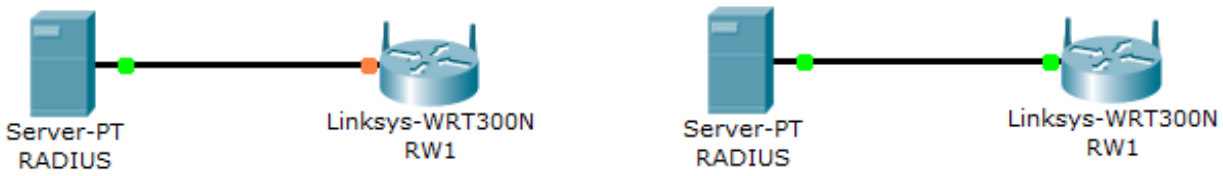

figura (a) figura (b)

FIGURA 2.16 Conexión Server Radius – Ruteador Linksys

Dar clic en el icono que identifica al servidor RADIUS y se muestra la ficha *Config*, como se indica en la figura 2.17.

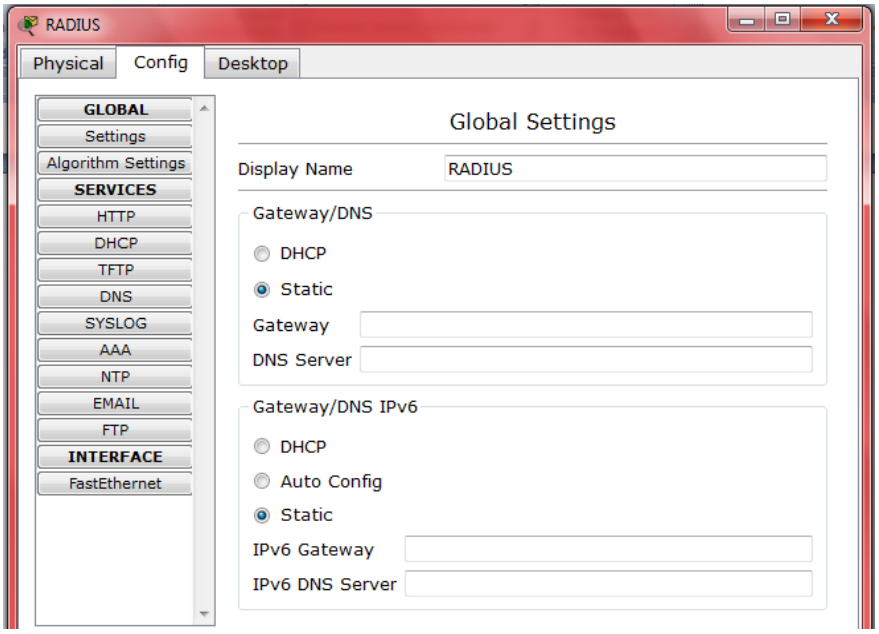

FIGURA 2.17 Config Servidor Radius

Ingresar la dirección IP de nuestra puerta de enlace G*ateway y servidor DNS* (192.168.0.1), como se indica en la figura 2.18.

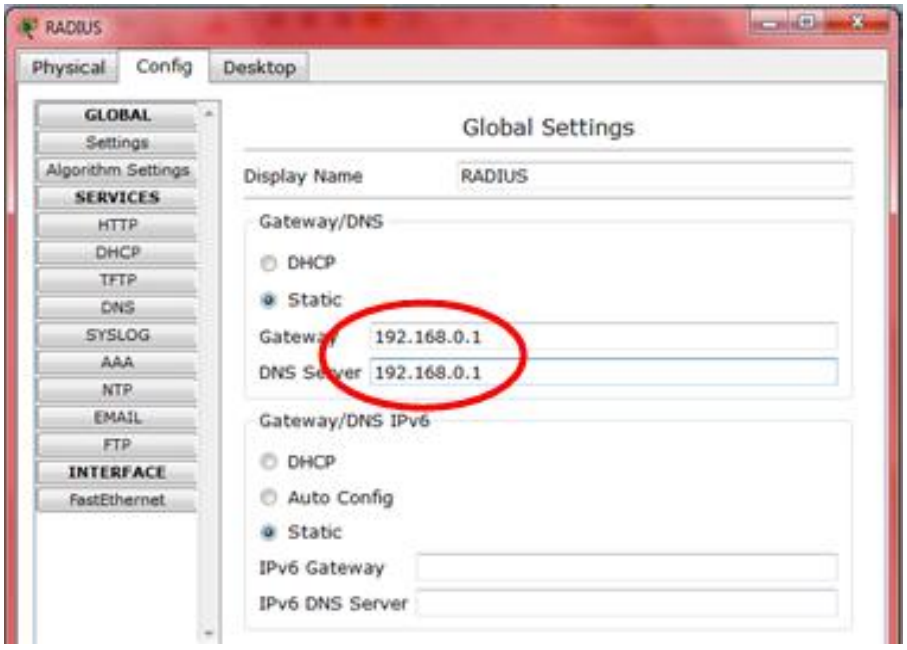

FIGURA 2.18 Configuración Servidor Radius

Pulsar en el botón FastEthernet para configurar la IP estática y su máscara de subred que usará el servidor RADIUS en nuestra red (192.168.0.10 255.255.255.0), como se indica en la figura 2.19.

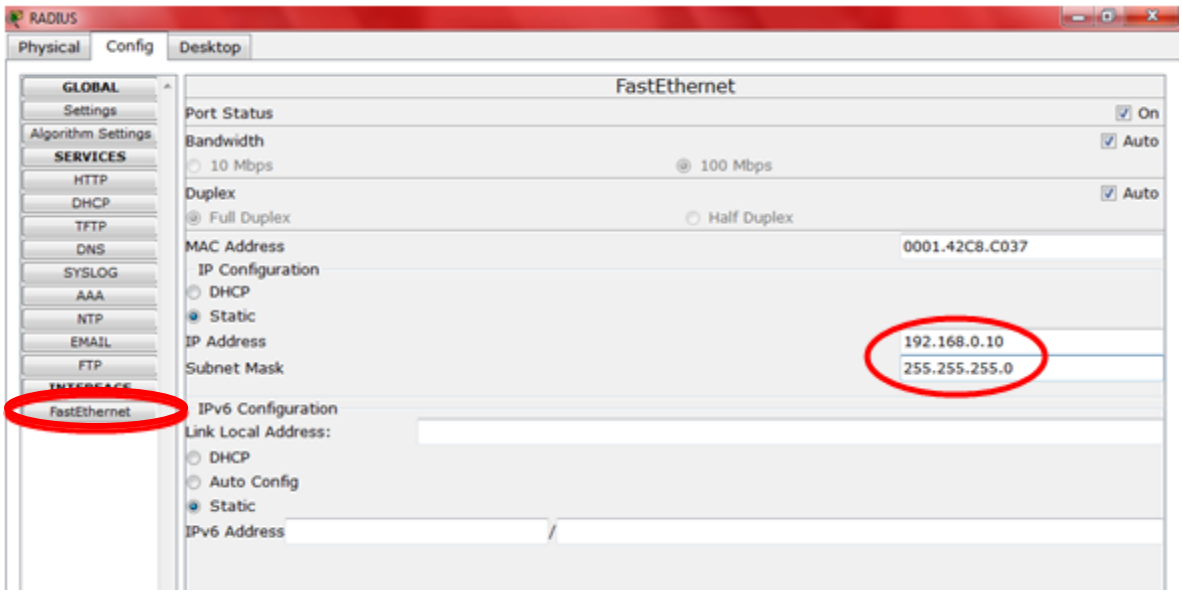

FIGURA 2.19 Configuración Servidor Radius FastEthernet

Pulsar en el botón AAA para configurar el servicio de autenticación de usuarios, ingresar en la sección *Network Configuration* como *Client Name* WR1, *Secret* accesowlan, *Client IP* 192.168.0.1, *Service Type* RADIUS y presionar el botón con el signo + para añadir la configuración, como se indica en la figura 2.20.

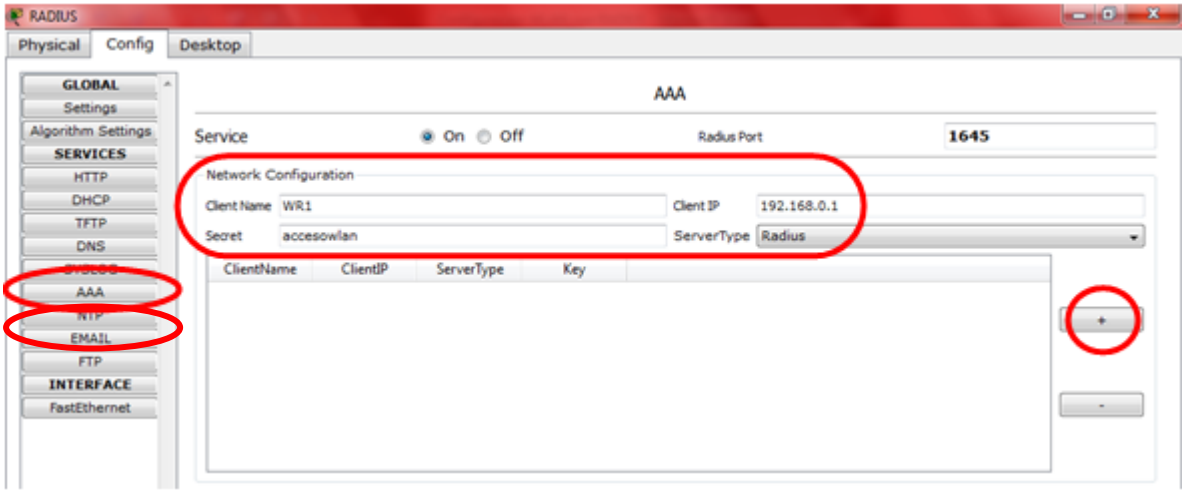

FIGURA 2.20 Configuración Servidor Radius AAA

En la sección User Setup, se debe añadir a los usuarios a quienes se permitirá conectarse al WR1, colocando los datos usuarioa y passusuarioa de la portátil A y usuariob y passusuariob de la portátil B, uno a uno en sus casilleros correspondientes quedando como muestra las figuras 2.21.1, 2.21.2, 2.21.3.

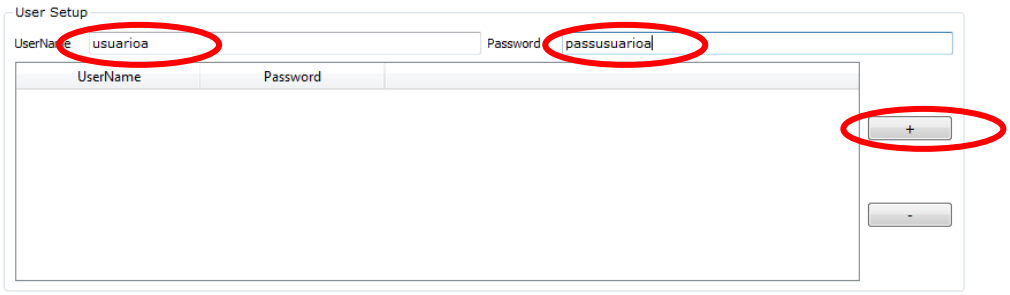

FIGURA 2.21.1 Añadir usuarios y contraseña

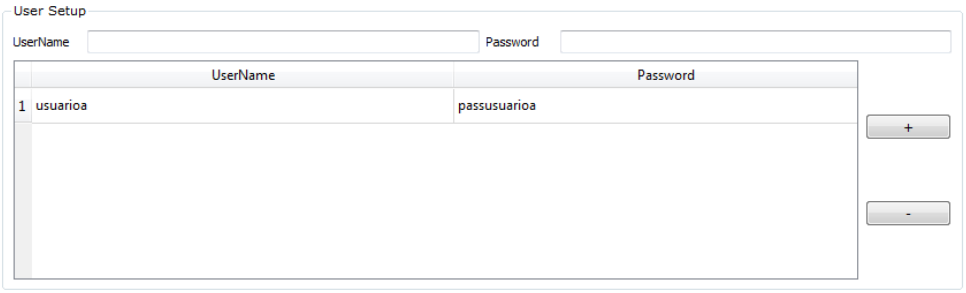

FIGURA 2.21.2 Añadir usuarios y contraseña

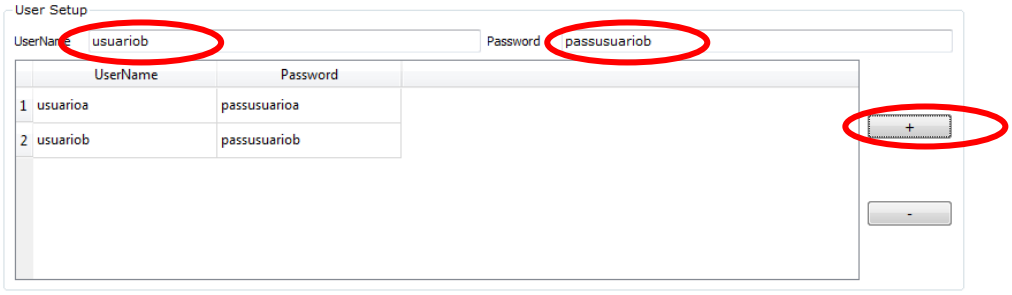

FIGURA 2.21.3 Añadir usuarios y contraseña

Quedando el cuadro de diálogo como se muestra en la figura 2.22.

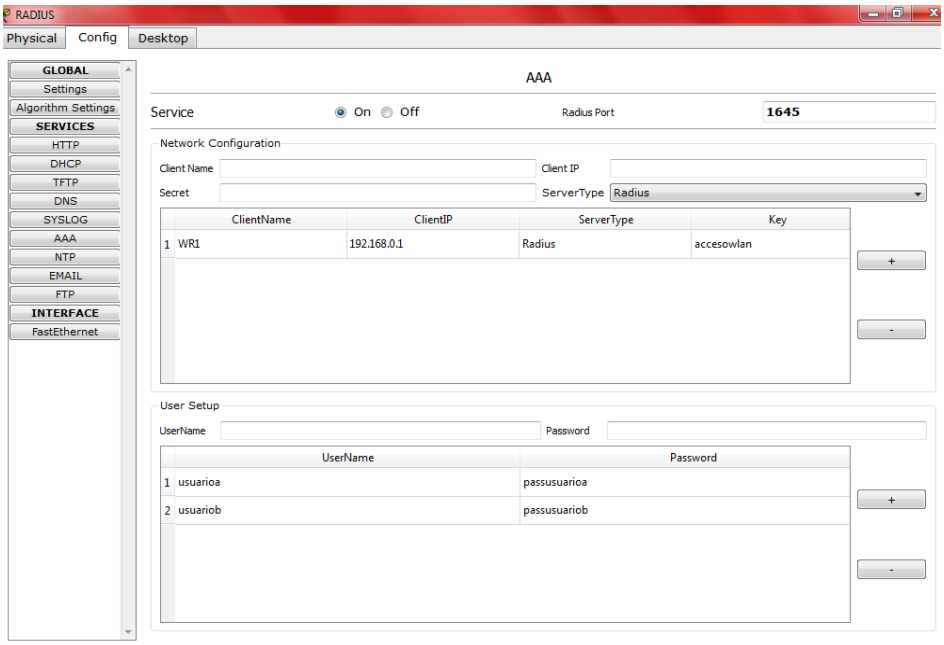

FIGURA 2.22 Configuración final AAA

2.4.1.5 Pruebas

Una vez realizada la configuración de todos los dispositivos como se indica anteriormente, el esquema muestra total conectividad, se envia mensajes entre los dispositivos para comprobar que exista conexión entre equipos como muestran las figuras 2.23.1, 2.23.2, 2.23.3.

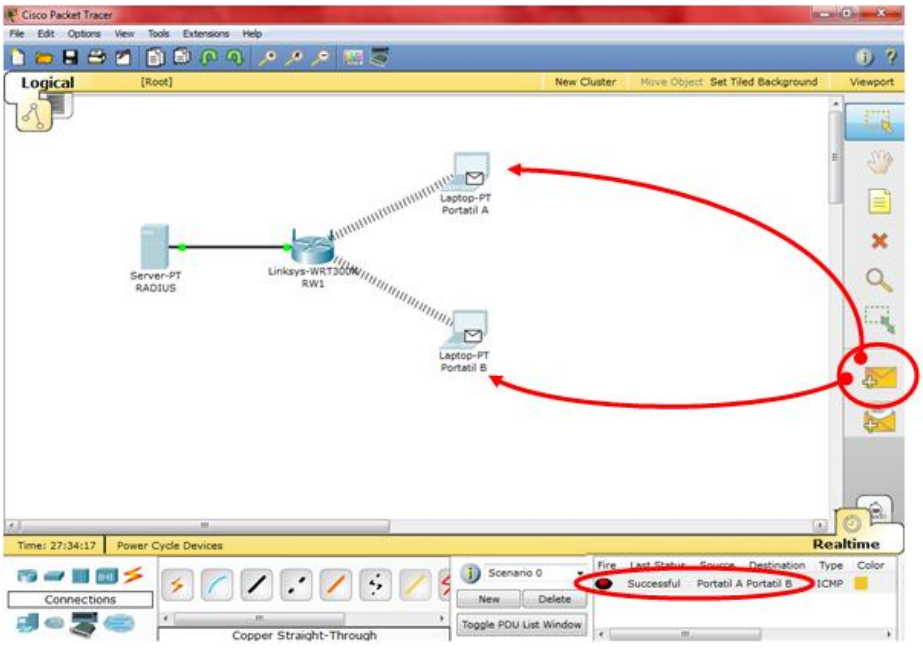

FIGURA 2.23.1 Comunicación entre equipos

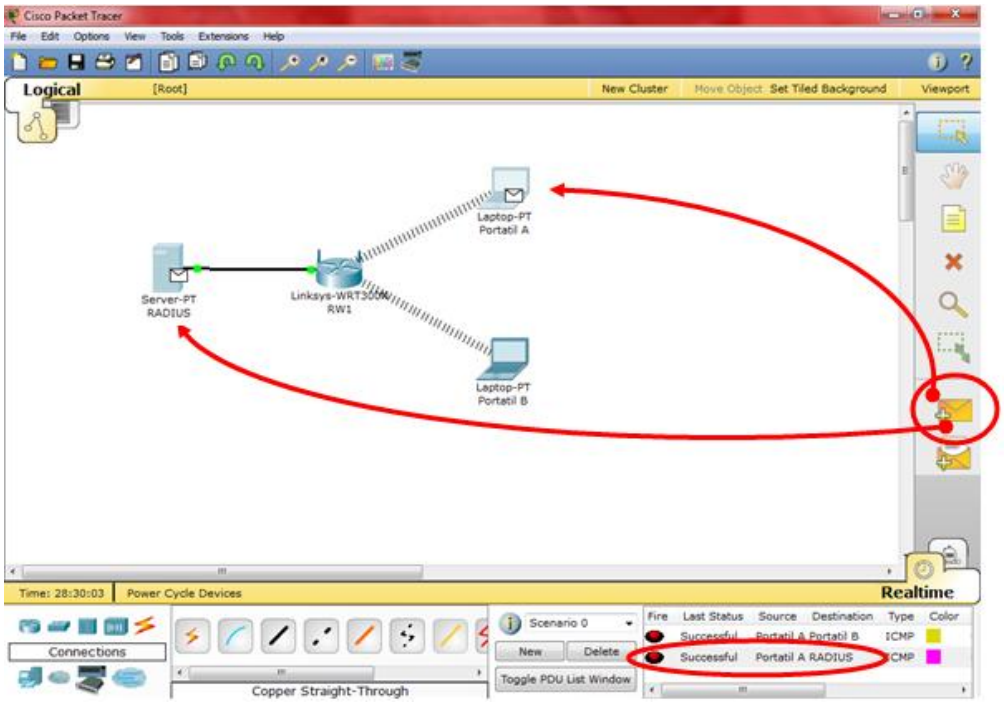

FIGURA 2.23.2 Comunicación entre equipos

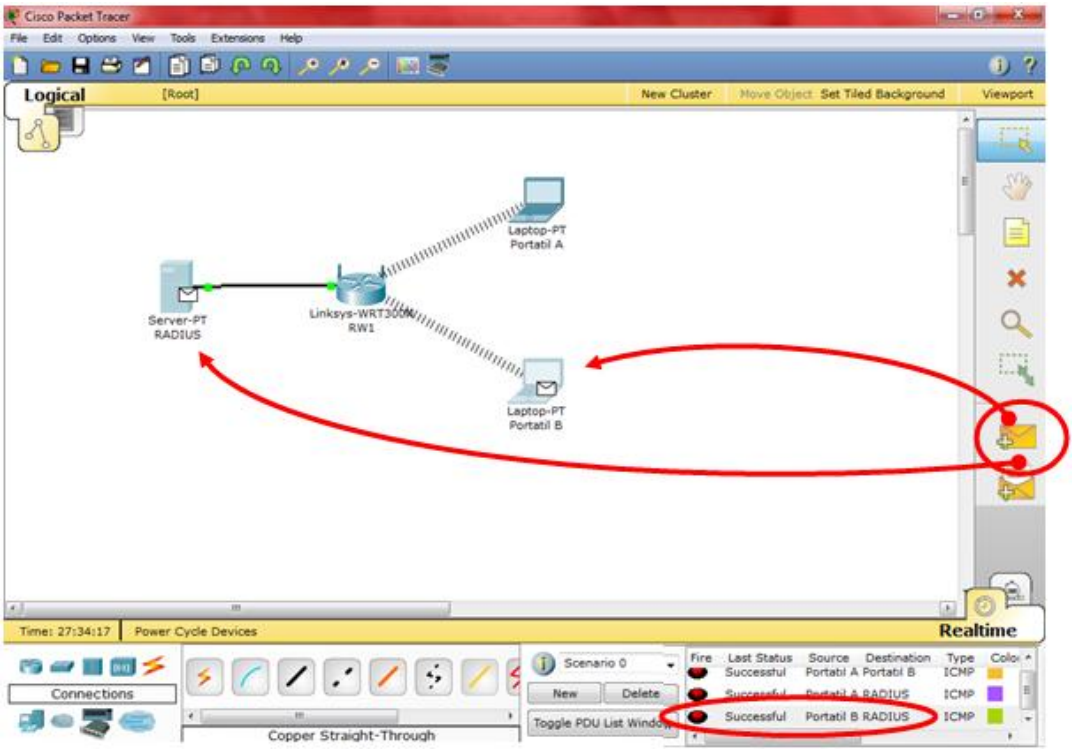

FIGURA 2.23.3 Comunicación entre equipos

2.5 PROCESAMIENTO Y ANÁLISIS

MODELO DE CONFIGURACION DEL SERVIDOR RADIUS PARA LA SEGURIDAD EN REDES LAN INALAMBRICAS MEDIANTE Packet Tracer 5.3

En esta configuración, se pretende demostrar la conectividad de una red de área local LAN, con usuarios en redes locales inalámbricas, estos usuarios de las redes LAN (WLAN1 – WLAN2), son autenticados y autorizados a conectarse a sus respectivas redes inalámbricas por el servidor RADIUS ubicado distantemente en otra red.

2.5.1.- Análisis

En la tabla 6.1, se muestra un resumen del direccionamiento IP, del esquema que presento para indicar el funcionamiento del Servidor Radius en Packet Tracer 5.3.

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway por defecto
Portátil Wr1-1	Wireless	DHCP (192.168.1.10 - 192.168.1.30)	DHCP (255.255.255.0)	DHCP (192.168.1.1)
Portátil Wr1-2	Wireless	DHCP (192.168.1.10 - 192.168.1.30)	DHCP (255.255.255.0)	DHCP (192.168.1.1)
Portátil Wr1-3	Wireless	DHCP (192.168.1.10 - 192.168.1.30)	DHCP (255.255.255.0)	DHCP (192.168.1.1)
Portátil Wr2-1	Wireless	DHCP (192.168.2.10 - 192.168.2.30)	DHCP (255.255.255.0)	DHCP (192.168.2.1)
Portátil Wr2-2	Wireless	DHCP (192.168.2.10 - 192.168.2.30)	DHCP (255.255.255.0)	DHCP (192.168.2.1)
Portátil Wr2-3	Wireless	DHCP (192.168.2.10 - 192.168.2.30)	DHCP (255.255.255.0)	DHCP (192.168.2.1)
WR1	Fa0/1	192.168.1.2	255.255.255.0	192.168.1.1
WR2	Fa0/1	192.168.2.2	255.255.255.0	192.168.2.1
R1	Fa0/0	192.168.1.1	255.255.255.0	
	S0/0/0 (DCE)	10.10.10.1	255.255.255.252	
	S0/0/1 (DTE)	10.10.10.10	255.255.255.252	
R2	Fa0/0	192.168.2.1	255.255.255.0	
	S0/0/0	10.10.10.5	255.255.255.252	

	(DCE)			
	S0/0/1 (DTE)	10.10.10.2	255.255.255.252	
R3	Fa0/0	192.168.3.1	255.255.255.252	
	S0/0/0 (DCE)	10.10.10.9	255.255.255.252	
	S0/0/1 (DTE)	10.10.10.6	255.255.255.252	
PC-A	NIC	192.168.3.3	255.255.255.0	192.168.3.1
Servidor RADIUS	NIC	192.168.3.2	255.255.255.0	192.168.3.1

TABLA 2.4 Tabla de direccionamiento IP del esquema

2.5.2 Diseño

Ubicar los dispositivos que intervendrán en la configuración, en el área de trabajo del Packet Tracer como muestra la siguiente figura 2.24.

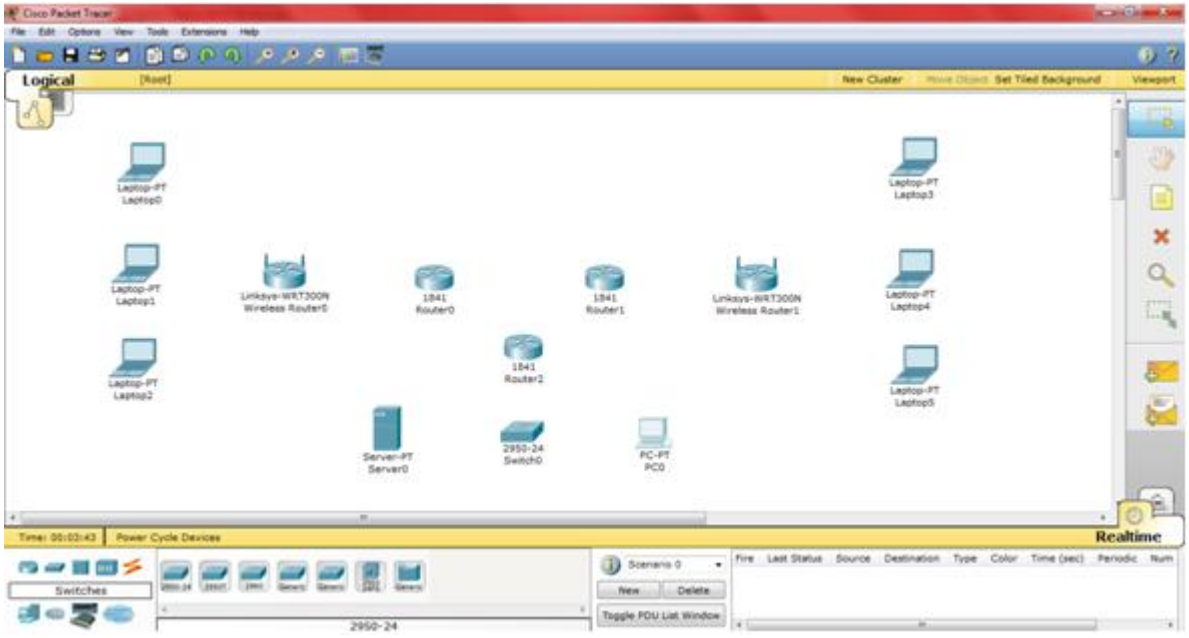

FIGURA 2.24 Ubicación de equipos

Cambiar los nombres que aparecen por defecto en la figura 2.24, por los descritos en la tabla 6.1, dar clic sobre la segunda línea de cada elemento quedando de la siguiente manera, como se indica en la figura 2.25.

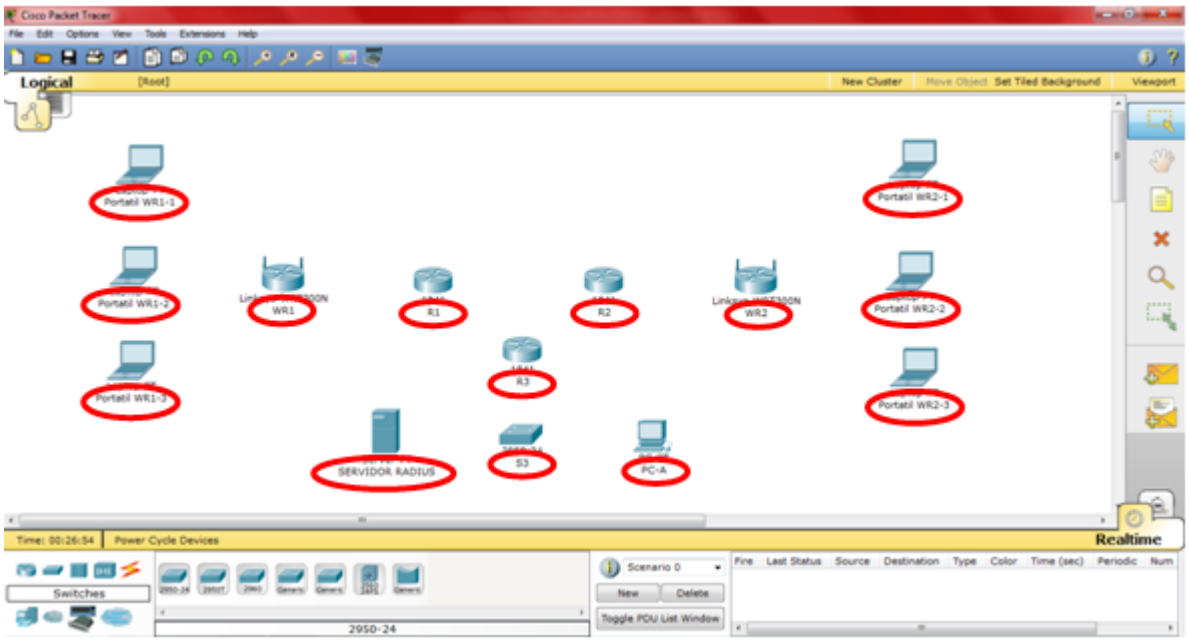

FIGURA 2.25 Nombres de equipos

2.5.3 Implementación

2.5.3.1 Configuración De Interfaces - Computadores Portátiles

Las laptops por defecto tienen instaladas tarjetas de red alambicas Fast-Ethernet, por lo que es necesario cambiar este módulo por uno que trabaje inalámbricamente.

Para activar el Wireless, se debe apagar el equipo (Laptop) e intercambiar la tarjeta Ethernet por una tarjeta Wireless, como se indicó en las figuras 2.5, 2.6 y 2.7 de la configuración WLAN anterior de la pag. 45.

Realizado el procedimiento en todas las portátiles, estas se conectan automáticamente con el Router inalámbrico (WR1 o WR2) más cercano, como muestra la figura 2.26.

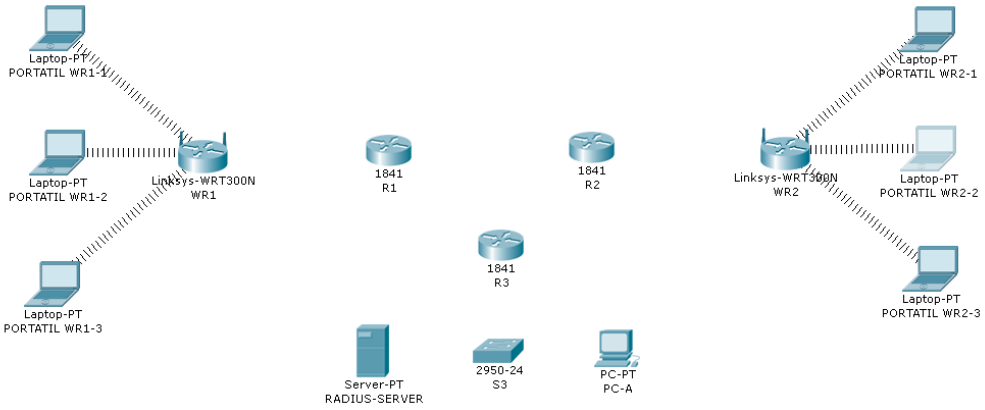

FIGURA 2.26 Conexión Router - Portátiles

Es necesario configurar en cada portátil un usuario y contraseña, de manera que sea este autenticado en el servidor RADIUS, y le sea proporcionado el permiso al equipo para conectarse a la red inalámbrica respectiva, esta configuración se describe a continuación.

Dar clic en el icono que identifica a la portátil que se desea configurar, seleccionar la ficha *Config* como se muestra en la figura 2.27.

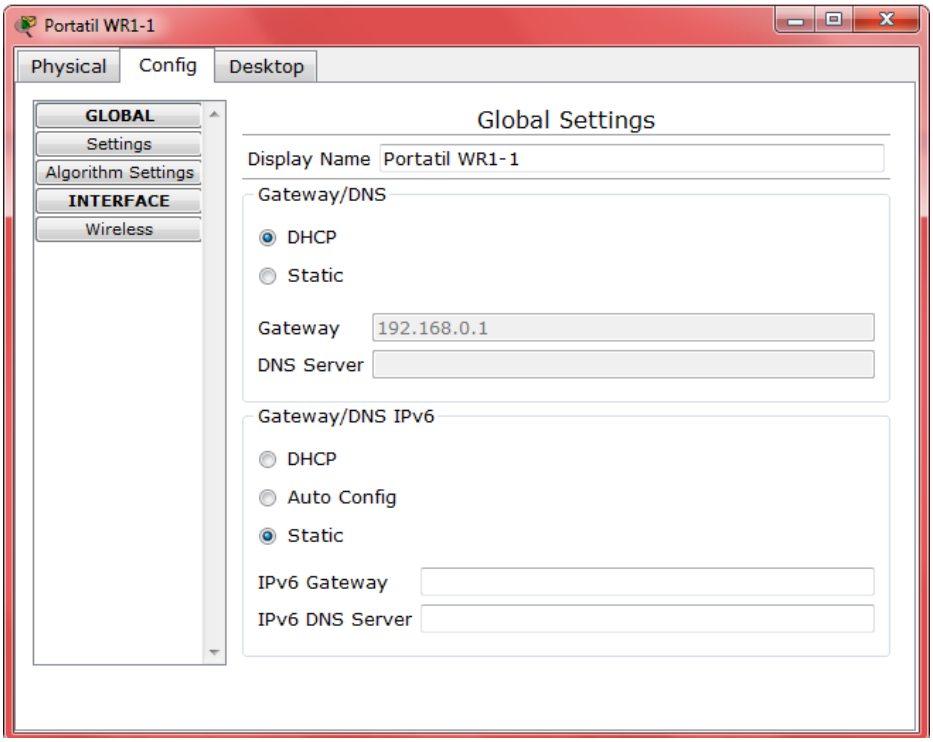

FIGURA 2.27 Configuración Global Portátil

Pulsar en el botón *Wireless* de la sección *INTERFACE* (a), en el casillero *SSID* ingresar en nombre de la red inalámbrica WLAN1 (b), en la sección *Autentication* seleccionar el WPA(c), en *User ID* y *Password* ubicar el nombre del usuario y la contraseña del usuario que será autenticado en el servidor RADIUS portatilwr11 y portatilwr11 respectivamente (d) y finalmente activar *DHCP* en la sección *IP Configuration* (e), como se muestra en la figura 2.28.

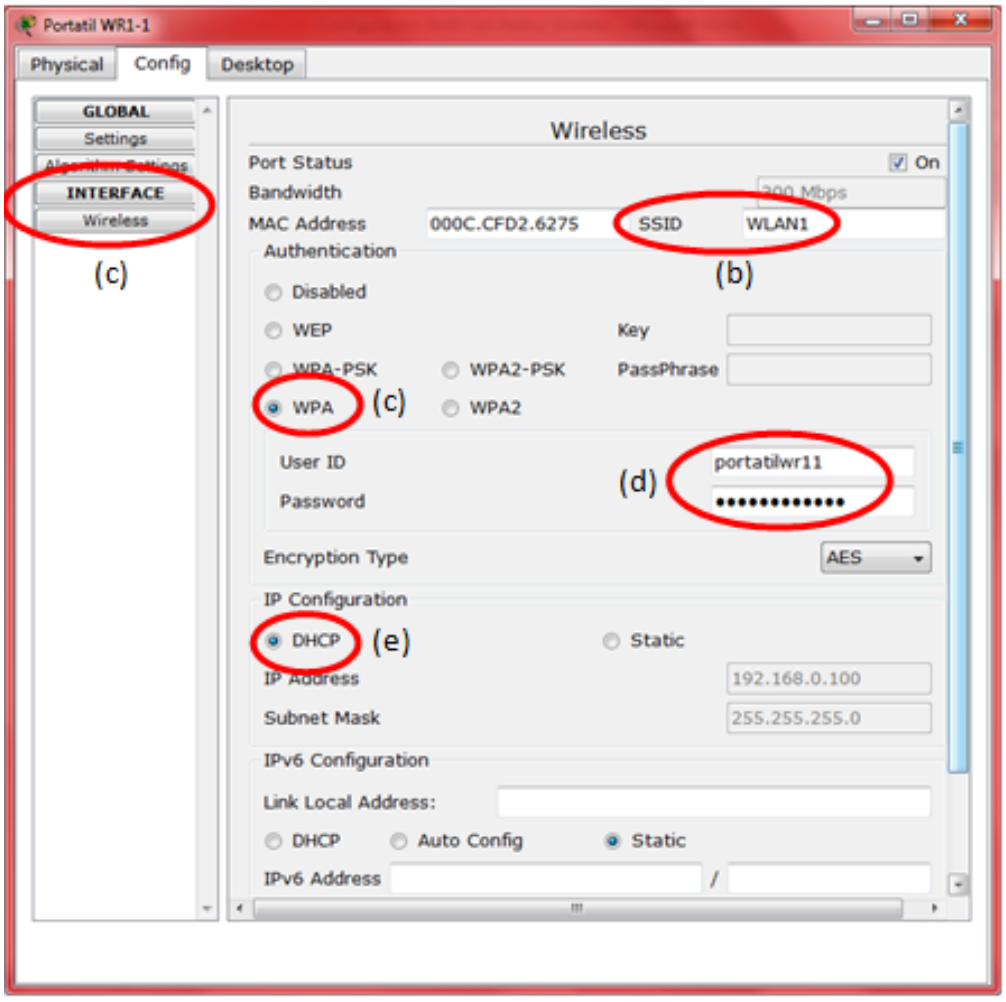

FIGURA 2.28 Configuración Interface Wireless WR1-1 de la red WLAN 1

Procedimiento que se repite en cada portátil cambiando el usuario y contraseña por su correspondiente nombre del esquena como se indica en las figuras 2.29, 2.30, 2.31, 2.32, 2.33

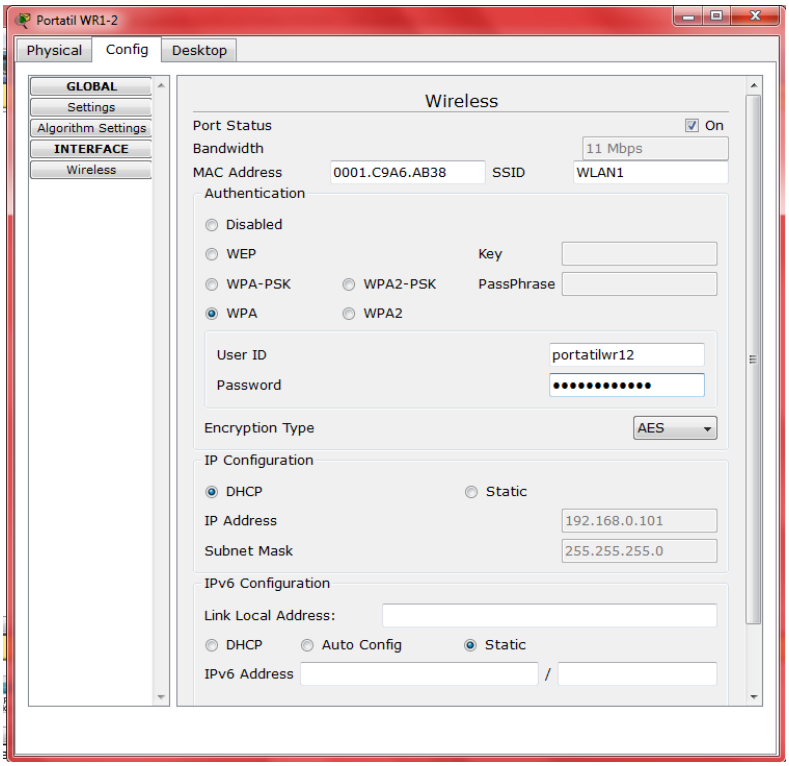

FIGURA 2.29 Configuración Interface Wireless WR1-2 de la red WLAN1

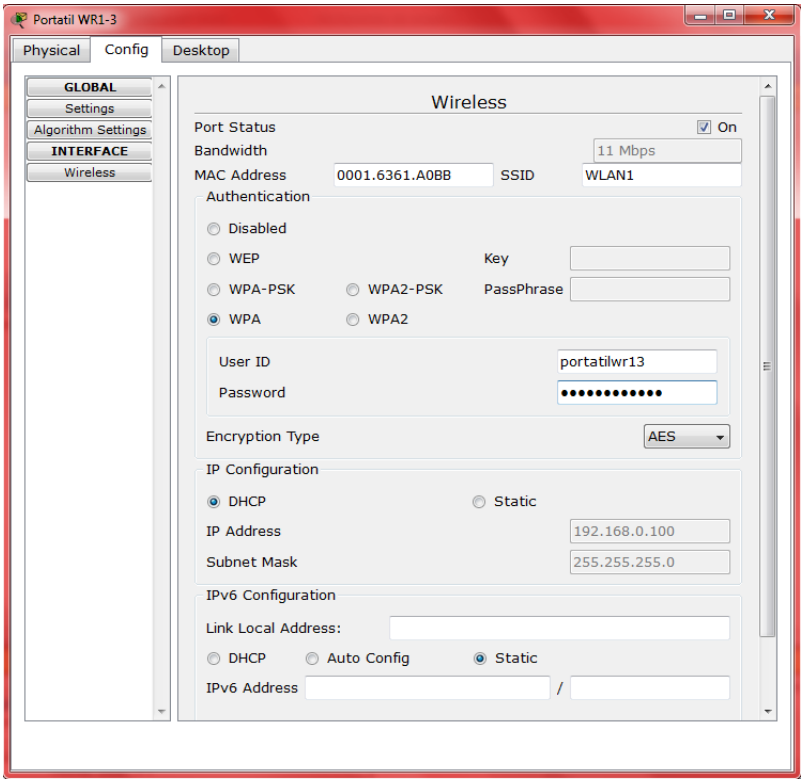

FIGURA 2.30 Configuración Interface Wireless WR1-3 de la red WLAN1

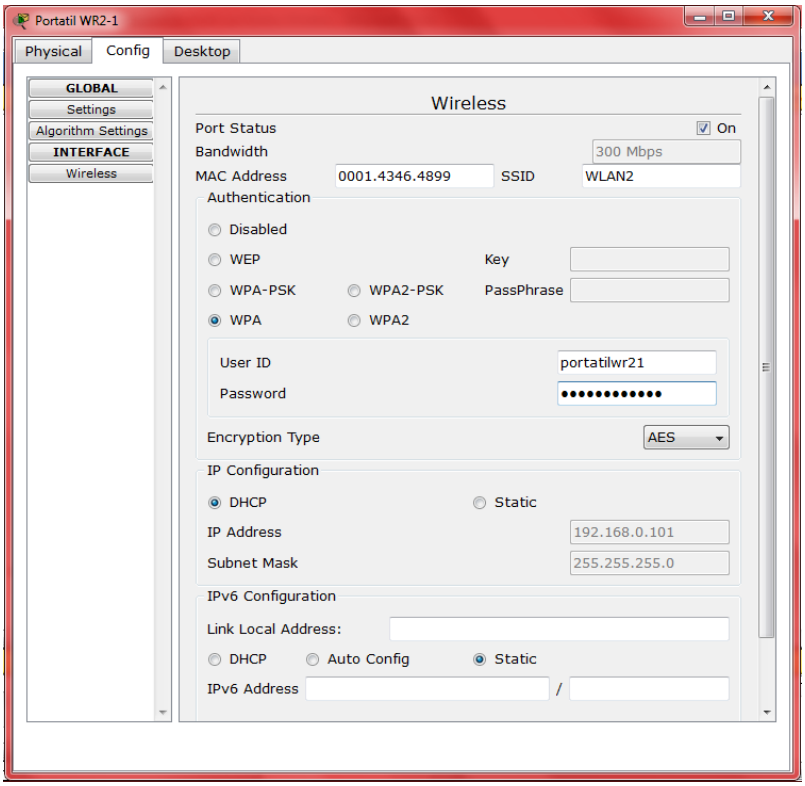

FIGURA 2.31 Configuración Interface Wireless WR2-1 de la red WLAN2

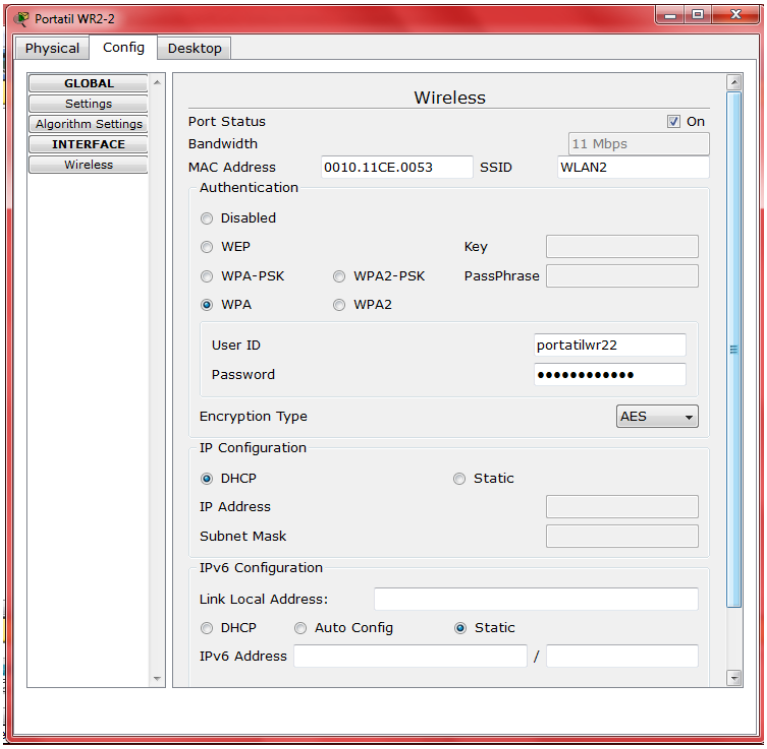

FIGURA 2.32 Configuración Interface Wireless WR2-2 de la red WLAN2

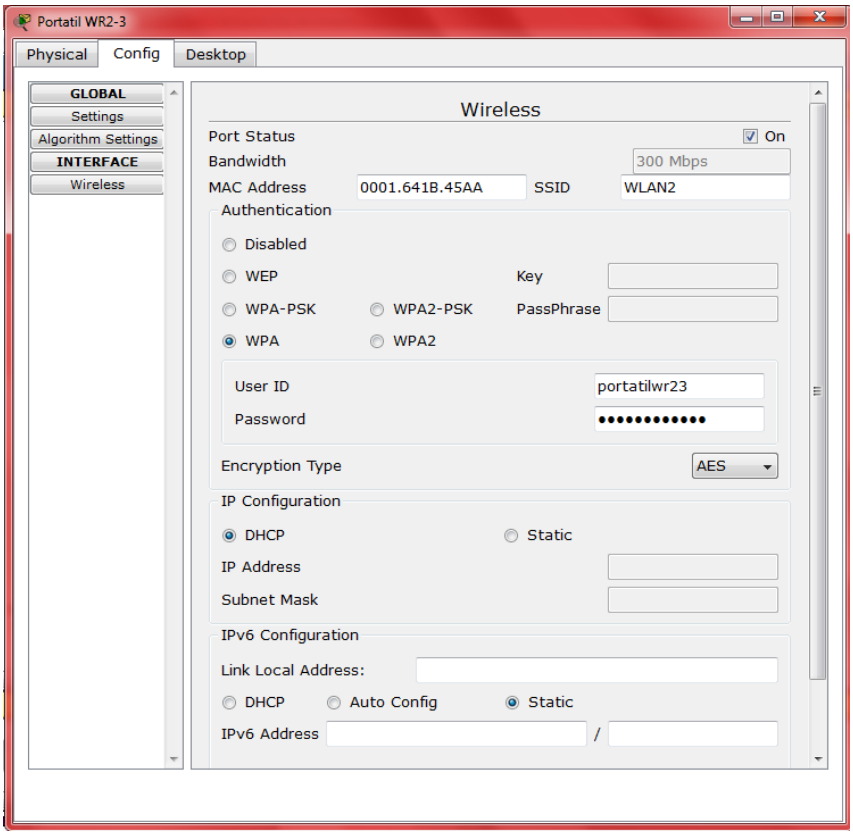

FIGURA 2.33 Configuración Interface Wireless WR2-3 de la red WLAN2

2.5.3.2 Routers

Incrementar un módulo de interfaces seriales en los Routers (R1; R2; R3), ya que por defecto estos dispositivos no las tienen instaladas y son las que nos ayudan a conectar redes distantes, para conseguir este objetivo seguimos el siguiente procedimiento en cada Router, como se muestra en la figura 2.34.

Dar clic sobre el icono del Router a configurar, donde podemos identificar las siguientes características en la ficha *Physical:*

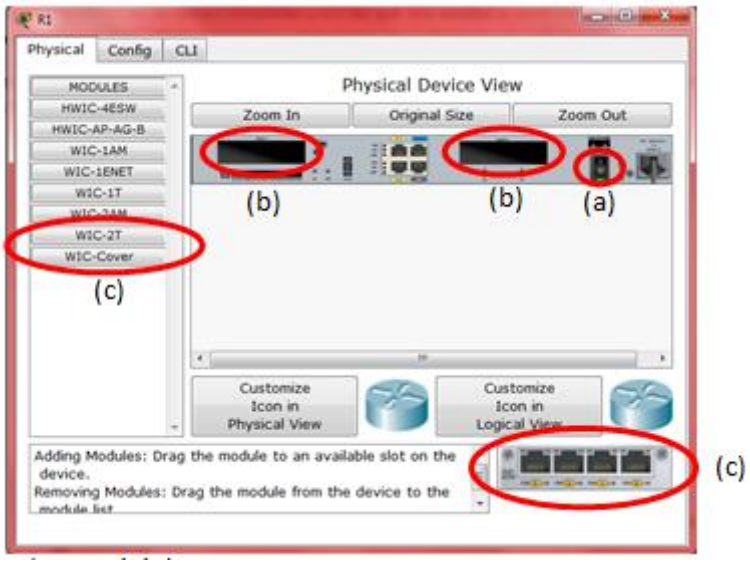

FIGURA 2.34 Modulo de interfaces seriales

a) Estado del equipo (Encendido)
b) Slot del equipo que se encuentran vacios y donde se pueden instalar diversos módulos de interfaces
c) Módulos que serán instalados en los slot vacios

Apagar el equipo cambiando el estado del botón de encendido (a), arrastrar los módulos que necesitamos desde la parte inferior del cuadro diálogo hasta ubicarlos sobre los slots vacios del dispositivo que se encuentra apagado como se muestra en la figura 2.35.

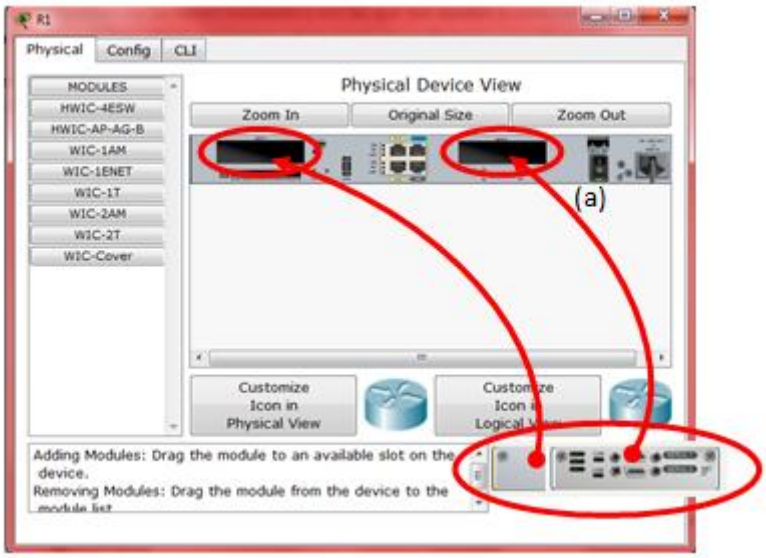

FIGURA 2.35 Cambio modulo de interfaces seriales

Finalmente lo vuelve a encender quedando como se muestra en la figura 2.36.

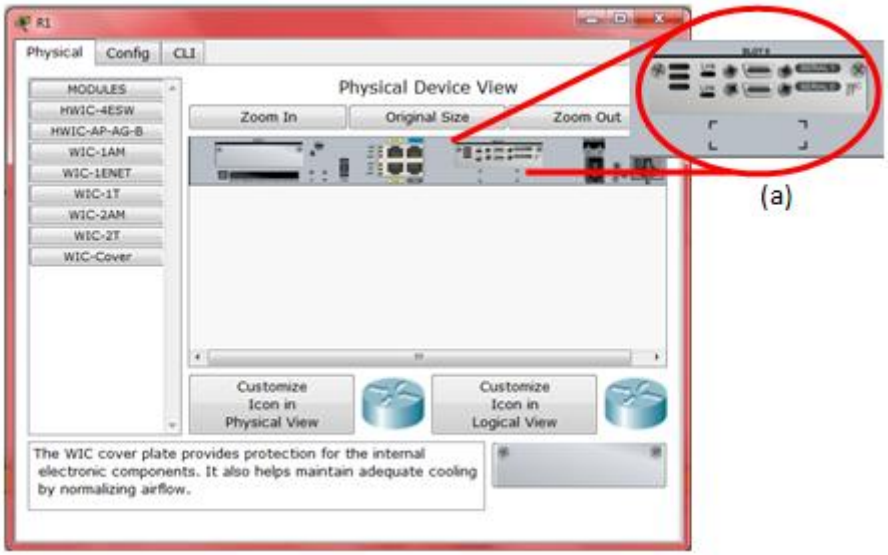

FIGURA 2.36 Nuevo modulo de interfaces seriales

El módulo con las interfaces seriales se encuentra instalada y funcionando (a), este procedimiento se debe repetir en los Routers restantes (R2, R3)

2.5.4 Interconexion

En la interconexión de los equipos es necesario colocar los cables en las interfaces indicadas en la tabla 2.4, y; señaladas en la figura 2.37, los cuales establecerán la conexión entre los dispositivos, siendo imperioso escoger el tipo de cable adecuado para cada tramo de conexión.

En el esquema se utilizarán cables directos (Copper Straight-Through) para conectar equipos en cada LAN y cables seriales (serial DCE) para conectar los Routers distantes, quedando como muestra la figura 2.38.

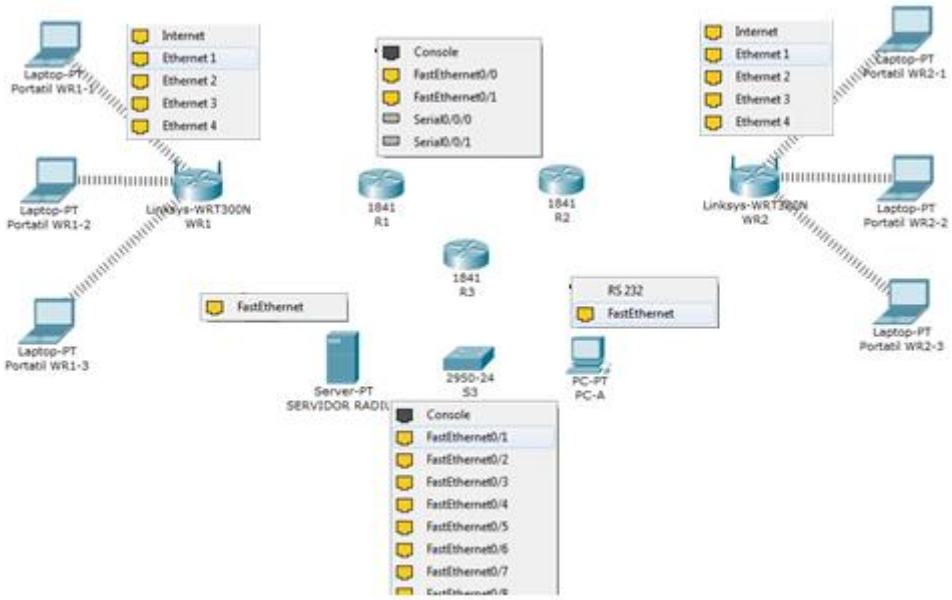

FIGURA 2.37 Interfaces de conexión

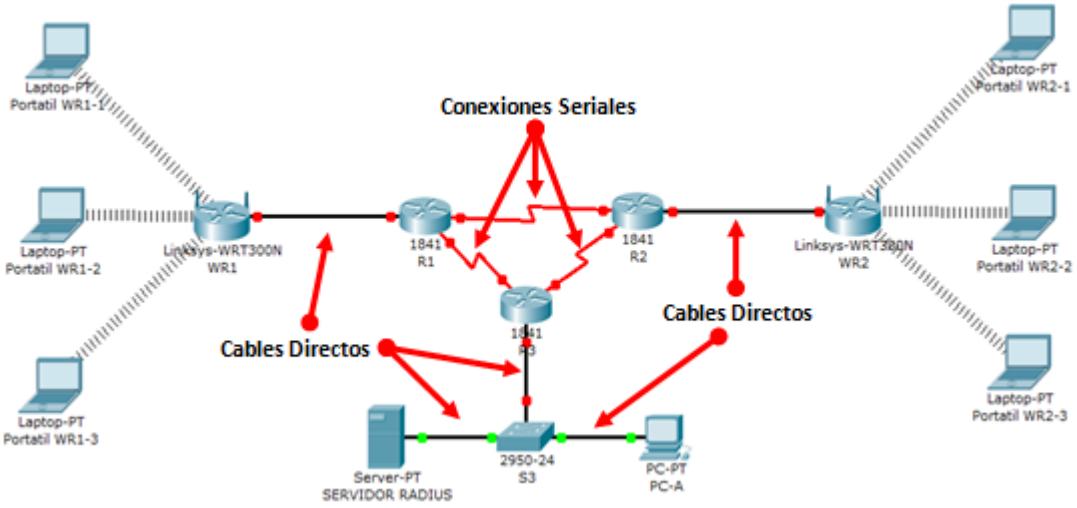

FIGURA 2.38 Tipos de cables de conexión

2.5.5 Configuración de los Equipos

- **LINKSYS WRT300N (WR1-WR2)**

Al configurar estos elementos, se pretende que actúen como dispositivos de enlace entre las portátiles que quieren conectarse a la red inalámbrica, y; los recursos de la red alámbrica, para ello estos elementos actúan como clientes del servidor RADIUS, son estos dispositivos quienes se comunican con el servidor y le solicitan la validación, autenticación de los usuarios de las portátiles y la autorización para establecer la conexión entre equipos (portátil-WR), configuración que se detalla a continuación:

Dar clic sobre el icono que identifica a WR1, seleccionar la ficha GUI como se muestra en la figura 2.39.

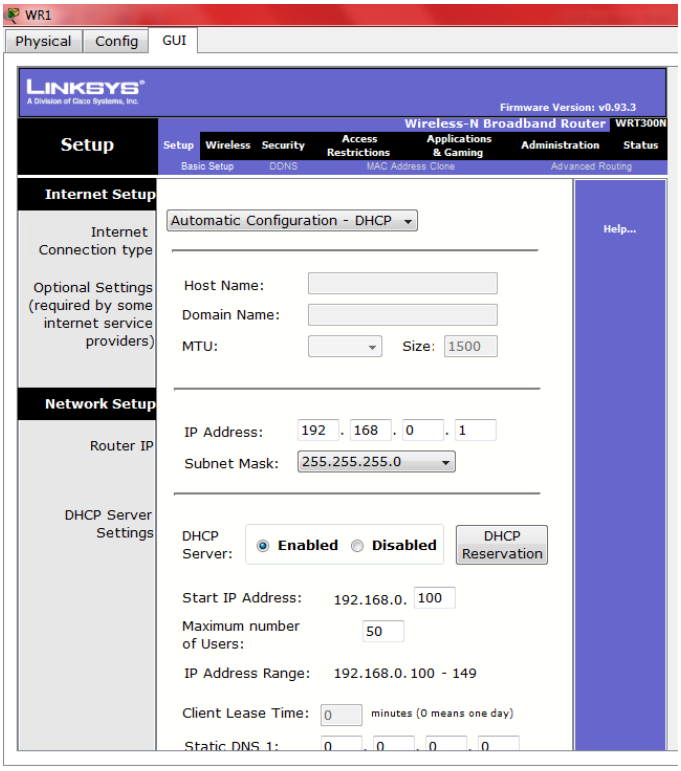

FIGURA 2.39 GUI Linksys WR1

Esta pantalla es la misma que encontraremos en el equipo WRT300N, las configuraciones necesarias para este equipo son las descritas a continuación:

En la configuración básica se debe establecer la dirección IP del equipo y mascara de subred, con las indicadas en la figura 2.24, en las casillas identificadas como *IP Address* y *Subnet Mask*(a), guardar la configuración al pulsar en el botón *Save Settings* (b), configurar la asignación IP dinámica(DHCP) que asignará hasta 21 IPs máximo desde la 192.168.1.10(c), guardar la configuración al pulsar en el botón *Save Settings* (b), verificar la configuración(d), como se muestra en las figuras 2.40.1, 2.40.2, 2.40.3, 2.40.4.

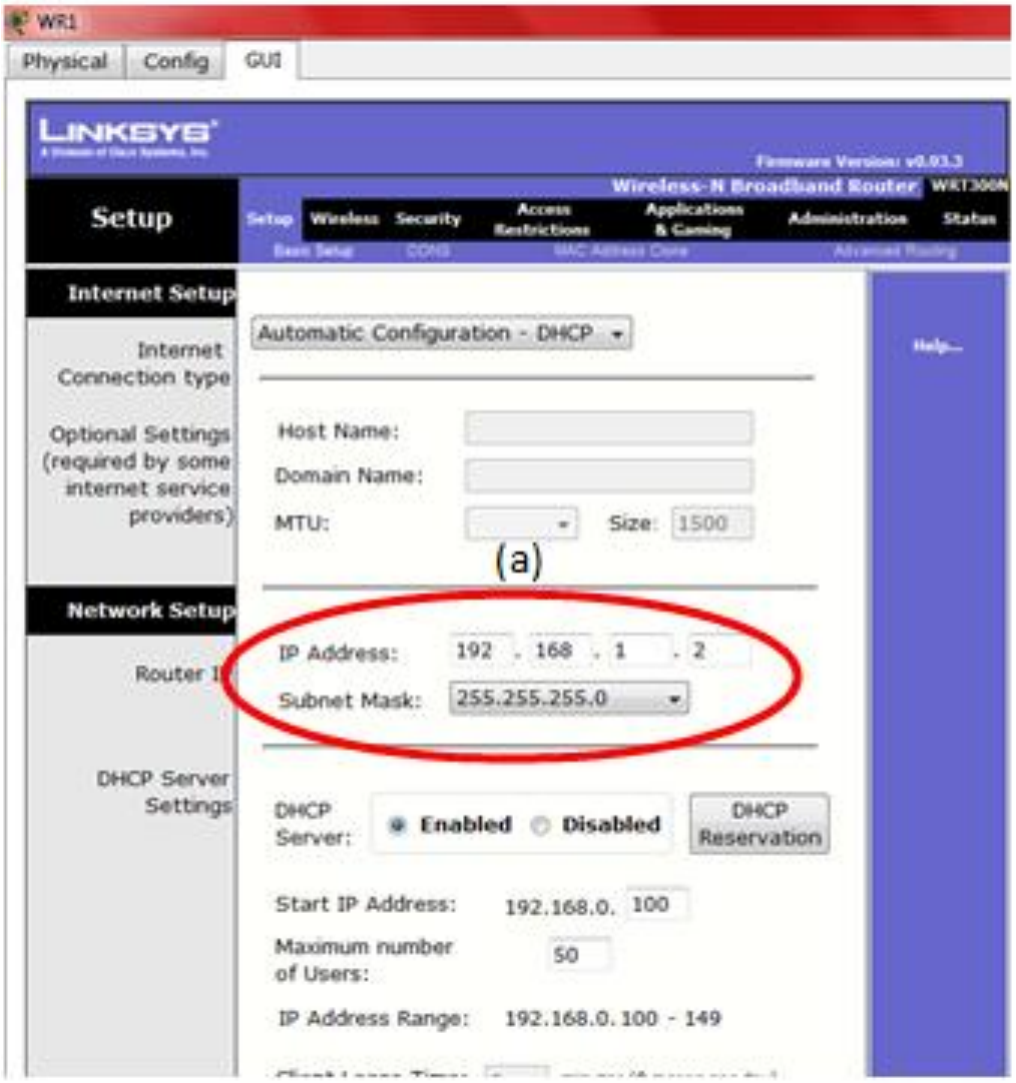

FIGURA 2.40.1 IP Linksys WR1

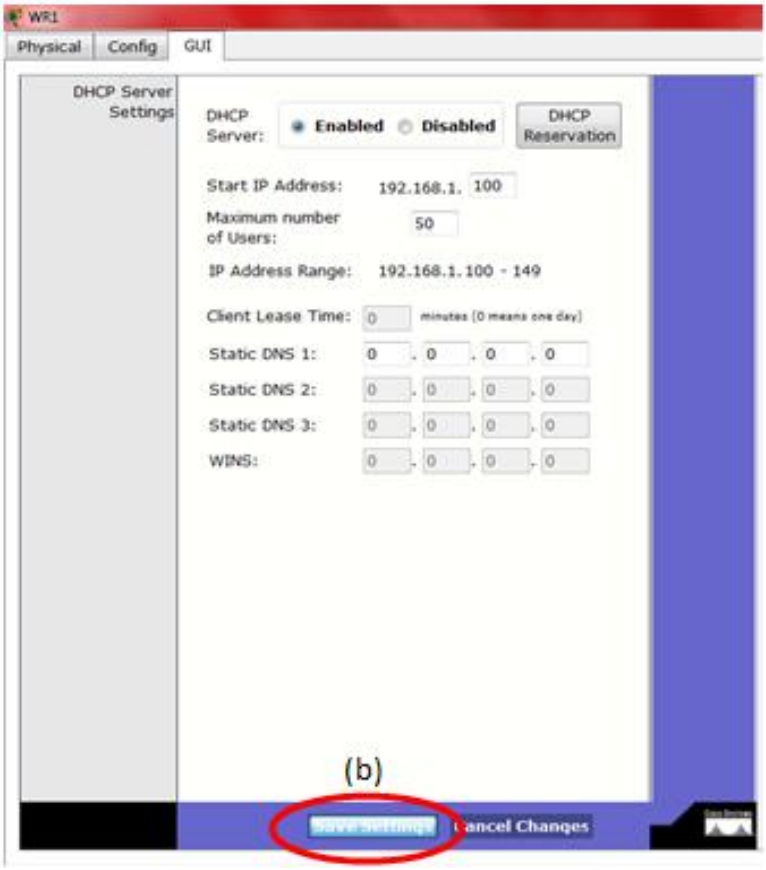

FIGURA 2.40.2 Guardar cambios Linksys WR1

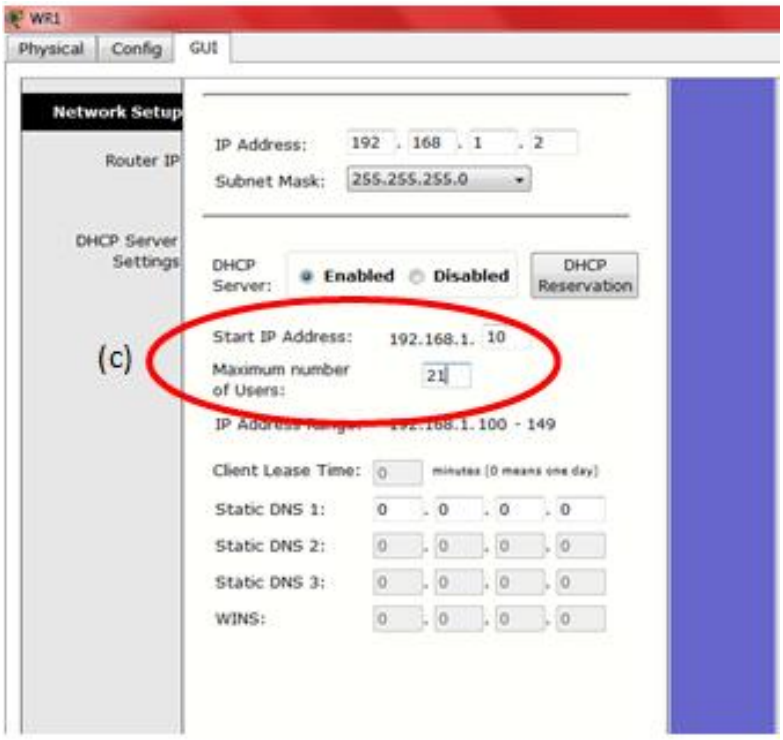

FIGURA 2.40.3 Configuración DHCP Linksys WR1

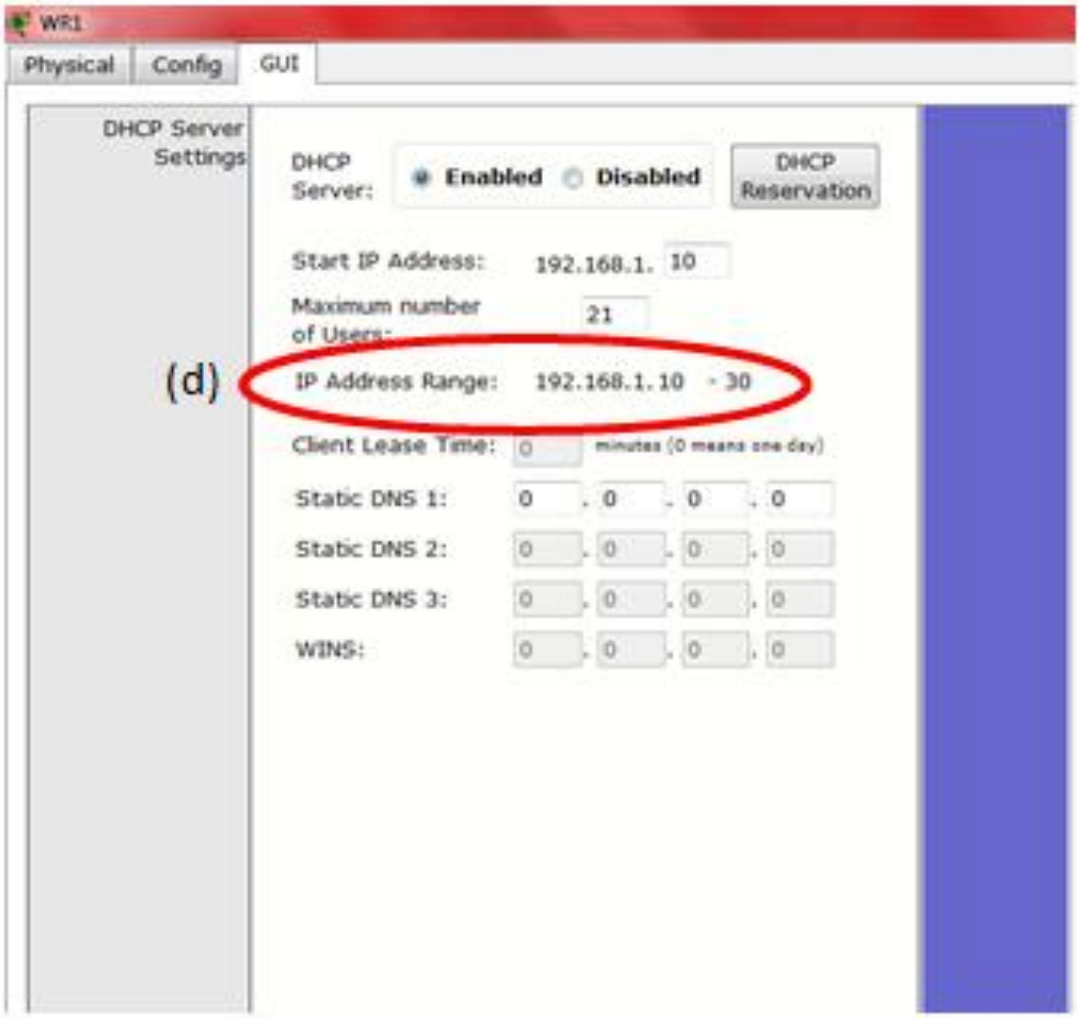

FIGURA 2.40.4 Rango de asignaciones IP Linksys WR1

En la configuración Básica Wireless(a), figura 2.41.1; se debe seleccionar el estándar de conexión entre 802.11b, 802.11g, 802.11n o en conjunto (b), figura 2.41.2; para nuestra red escogemos *Mixed,* el nombre que identificará a la red Wireless del WR1 (SSID) será WLAN1, frase que se coloca en el casillero identificado como *Network Name (SSID)* (c) y el canal de comunicación que usarán los equipos Wireless será el numero 6 – 2.437Ghz (d), guardar la configuración al pulsar en el botón *Save Setting*, verificar la configuración figura 2.41.3.

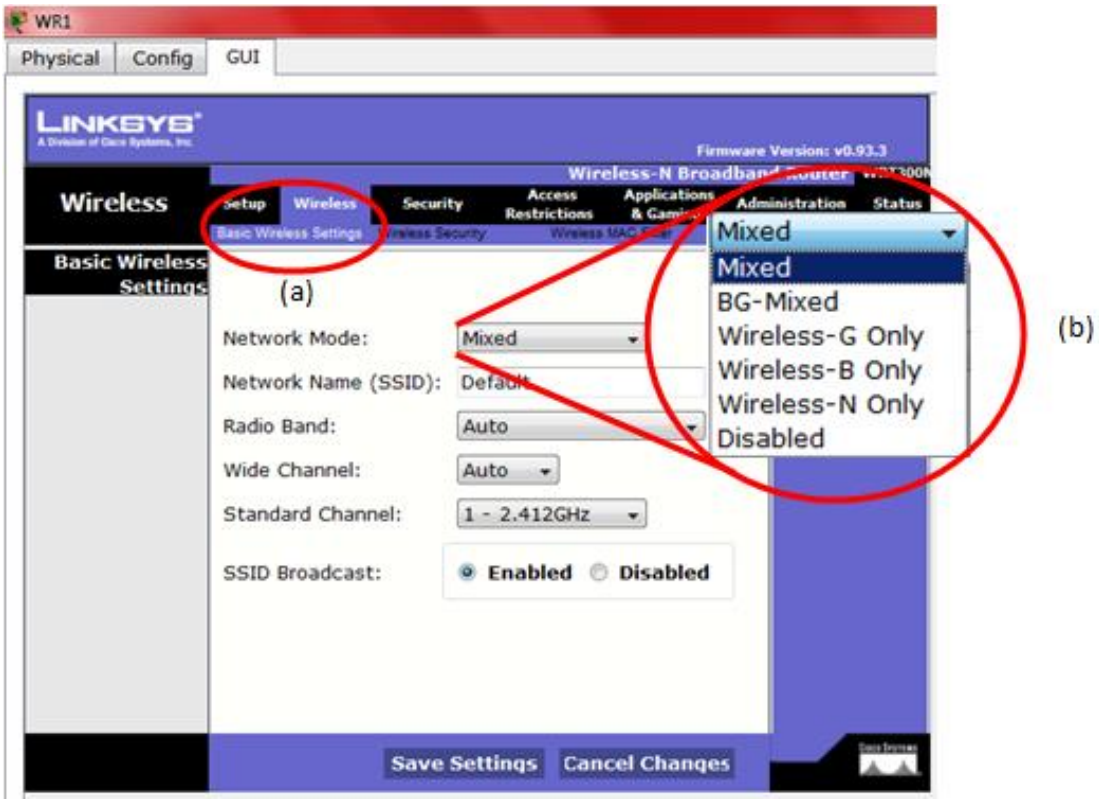

FIGURA 2.41.1 Estándares de conexión wireless Linksys WR1

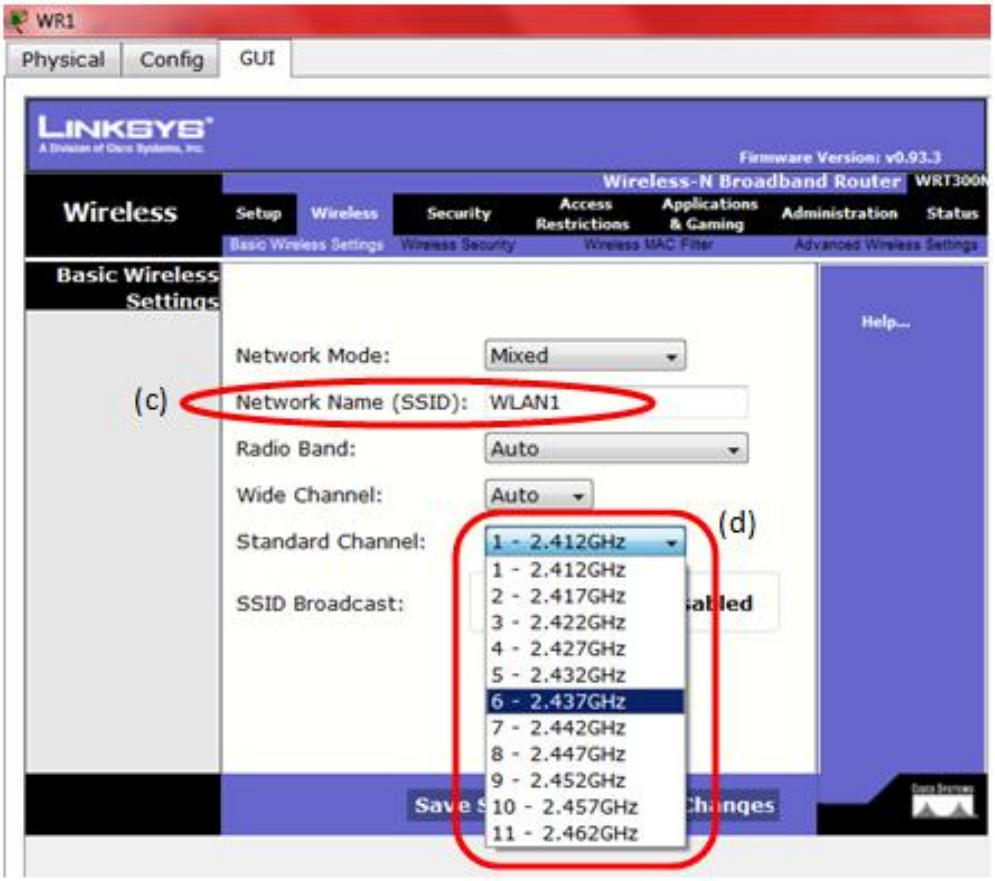

FIGURA 2.41.2 Canal de comunicación Linksys WR1

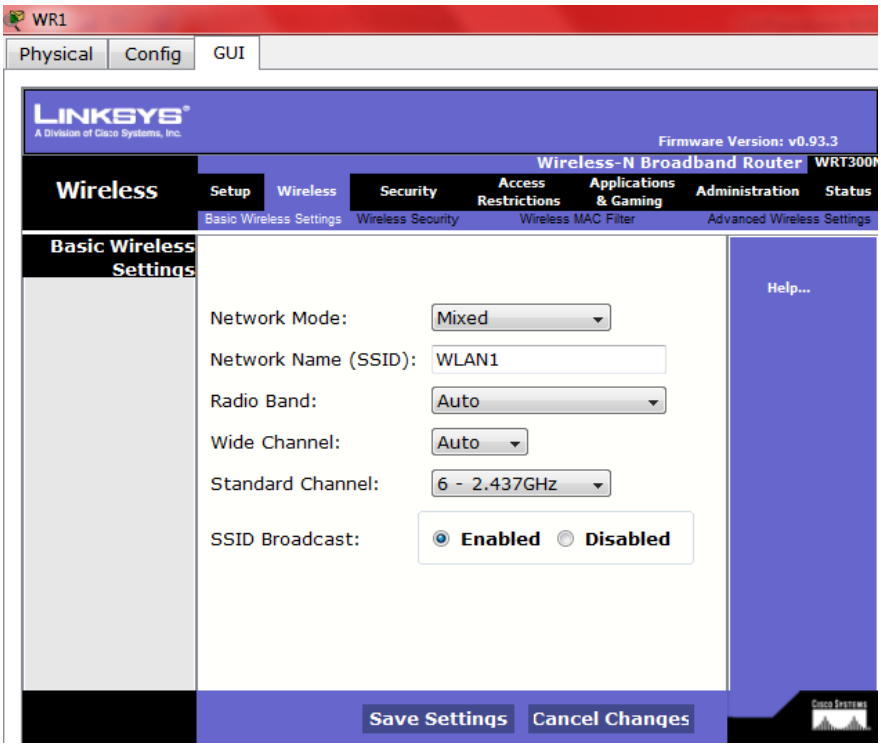

FIGURA 2.41.3 Datos wireless Linksys WR1

En la ficha *Wireless Security* (a), se configura el tipo de seguridad que utilizarán los equipos wireless de la red, en nuestro caso se debe establecer los parámetros para que esta seguridad sea mediante un servidor RADIUS con el siguiente procedimiento; como se muestra en la figura 2.42.

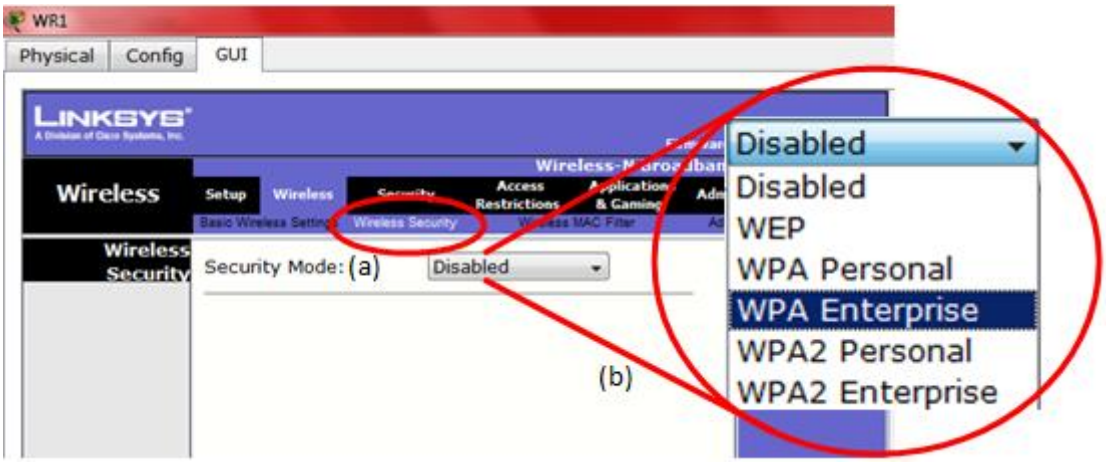

FIGURA 2.42 Wireless Security Linksys WR1

Seleccionar la opción *WPA Enterprise*, permite configurar la seguridad con el servidor RADIUS (b), en el tipo de encriptación seleccionar *AES* (c), en los casilleros marcados

con *RADIUS SERVER* ingresar la dirección IP del equipo, indicada en la tabla 2.4. (d), en la casilla *Shared Secret* ingresar la clave secreta que será validada en el servidor RADIUS (e), guardar la configuración pulsando en el botón *Save Setting*, como se muestra en la figura 2.43.

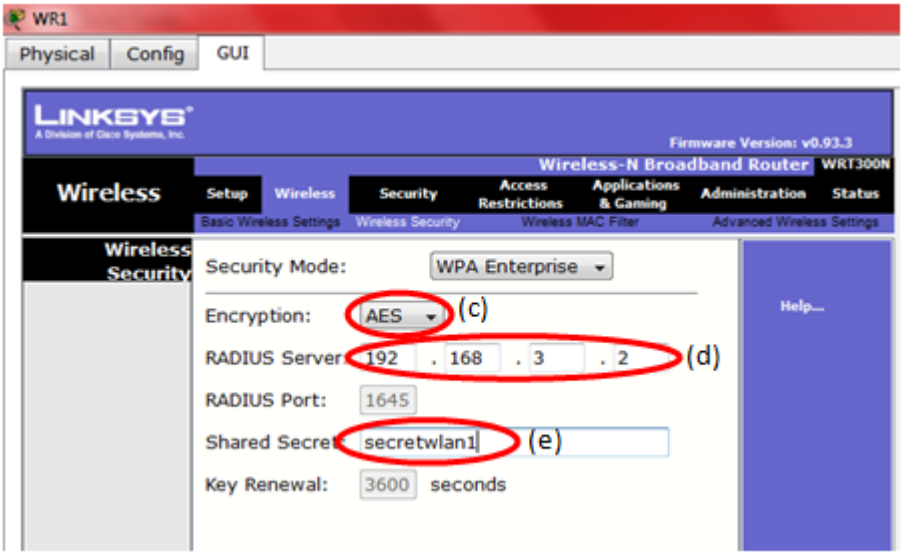

FIGURA 2.43 Wireless Security Linksys WR1

Finalmente en la ficha *Config*, pulsar en el botón *Internet* de la sección *INTERFACE* (a), activar la opción *Static* (b), ingresar la dirección IP de la puerta de enlace en la casilla *Default Gateway* (c), como se muestra en la figura 2.44.

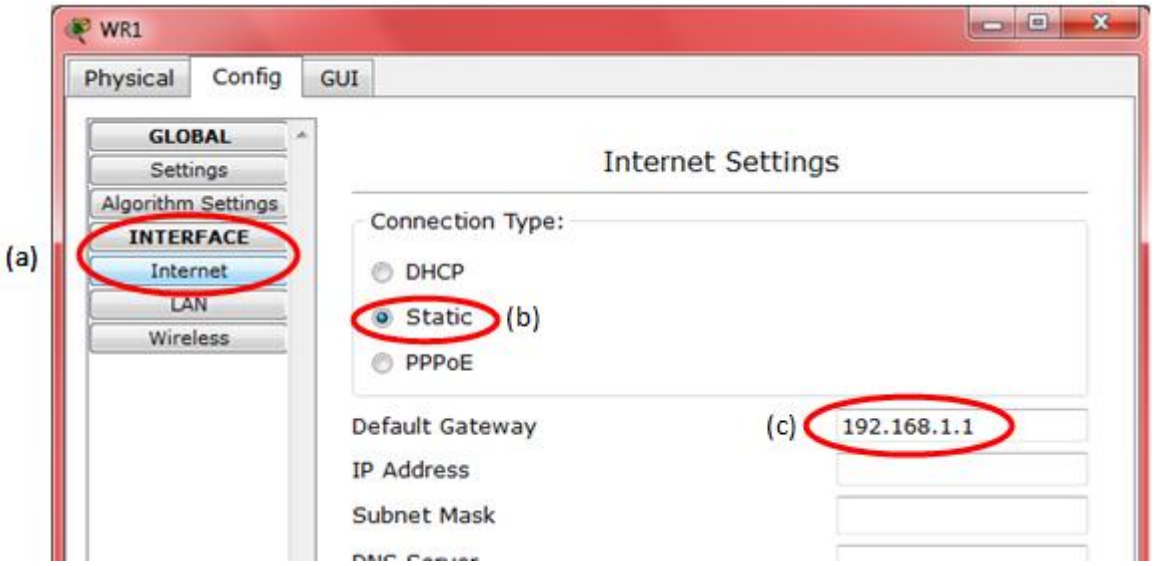

FIGURA 2.44 Configuración puerta de enlace Linksys WR1

Este procedimiento se repite para el WR2 cambiando los datos necesarios para la red que conecta este elemento el SSID es *WLAN2* y la clave secreta con el servidor RADIUS es *secretwlan2* y las direcciones IP se establecen según la tabla 2.4, quedando como se muestra en las figuras 2.45, 2.46, 2.47, 2.48.

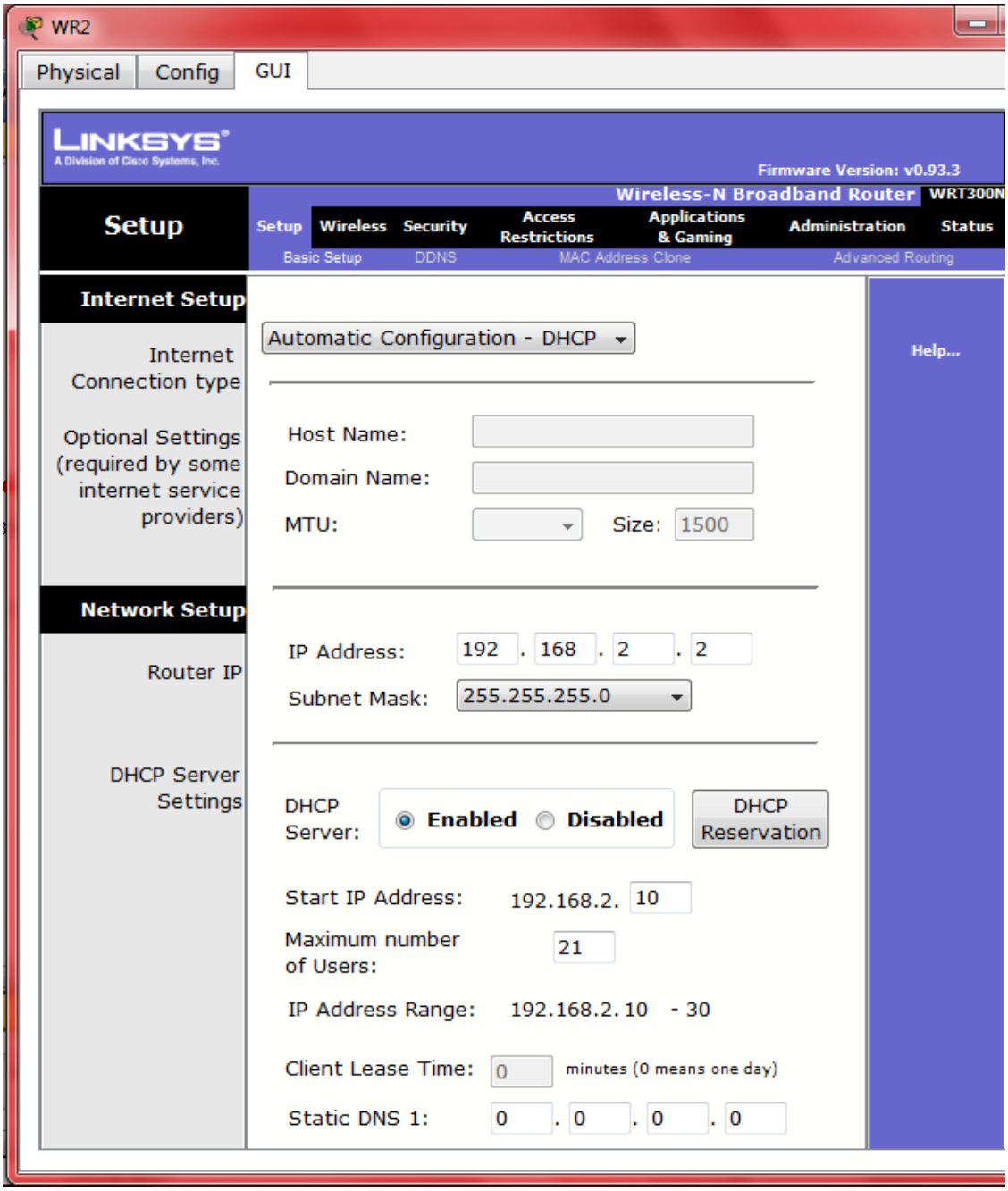

FIGURA 2.45 IP Linksys WR2

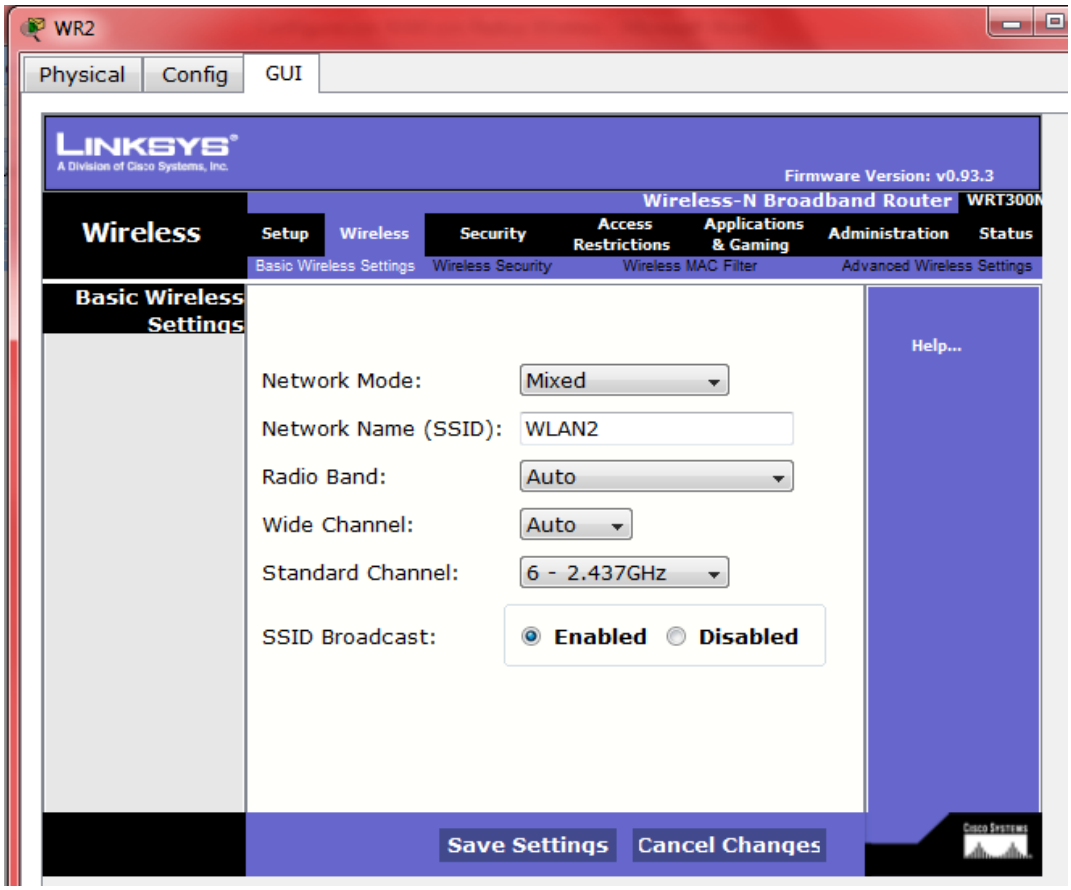

FIGURA 2.46 Datos wireless Linksys WR2

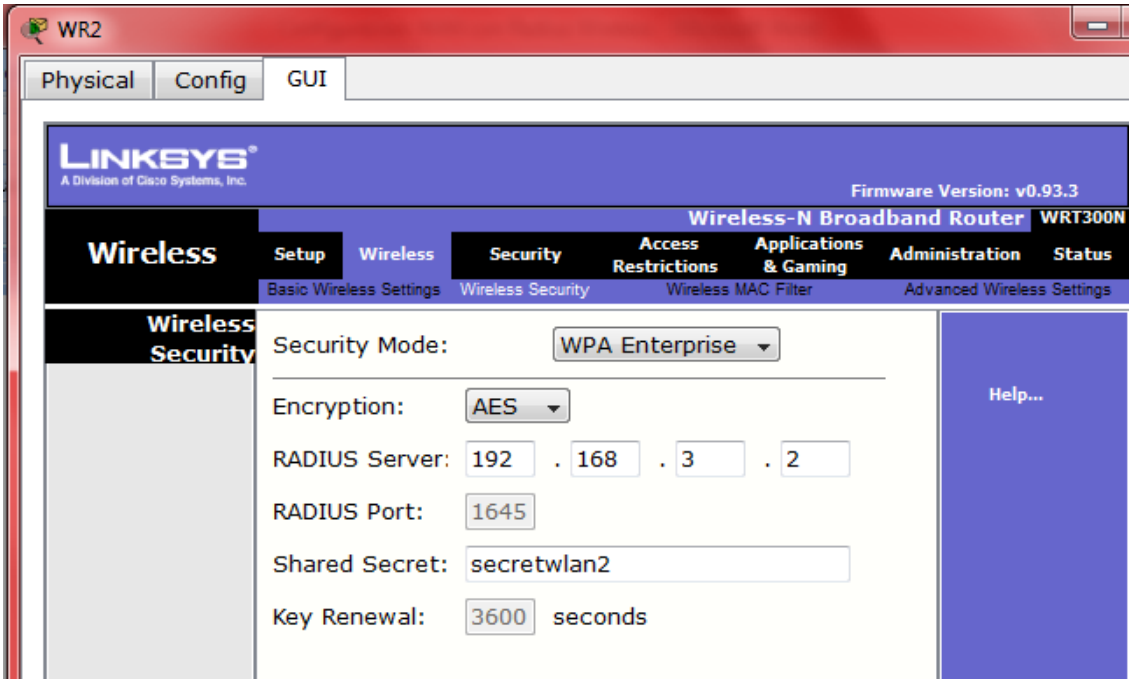

FIGURA 2.47 Wireless Security Linksys WR2

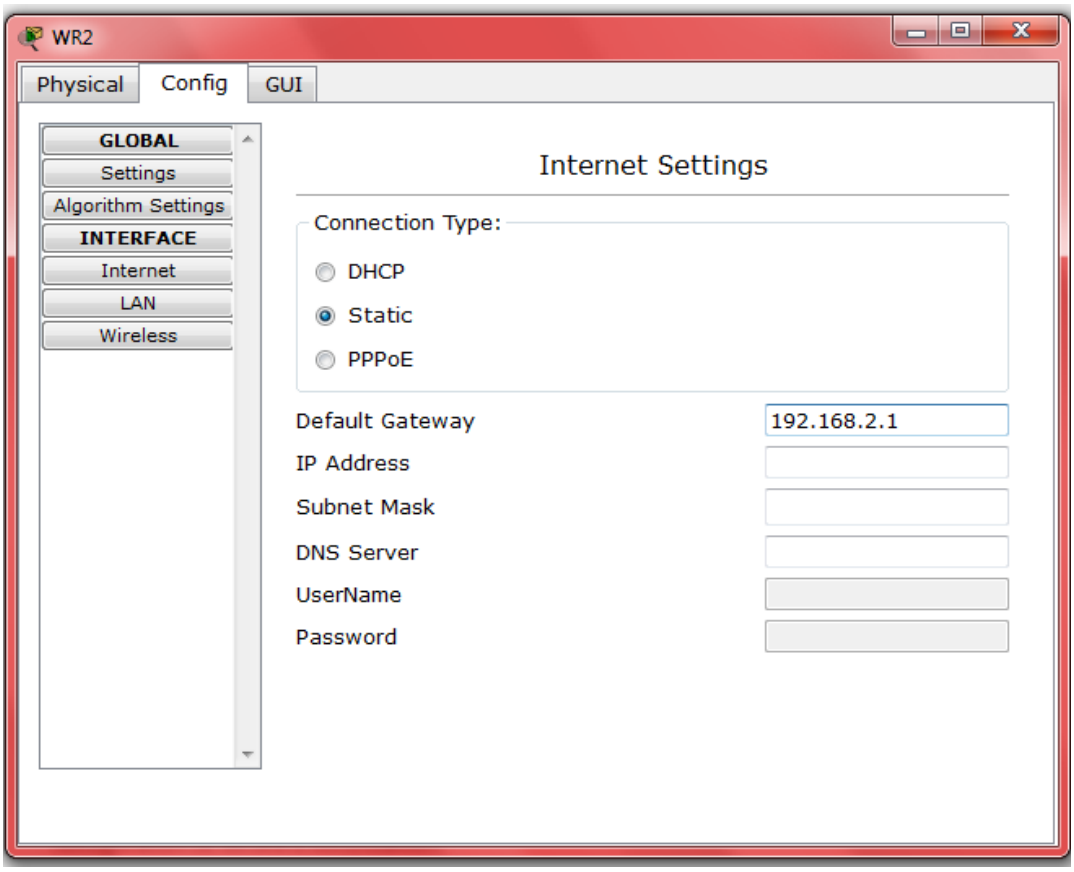

FIGURA 2.48 Configuración puerta de enlace Linksys WR1

- **ROUTERS 1841 (R1-R2-R3)**

Al configurar estos equipos damos conectividad a nuestras redes LAN administradas por WR1 y WR2 con la red del servidor RADIUS, que se encuentra ubicado distantemente. Es necesario administrar estos equipos dándoles las direcciones IP para cada interfaz como se indica en la tabla 2.4, y finalmente gestionar las tablas de rutas en cada Router usando un ruteamiento Estático de forma que cada Router conozca cómo alcanzar a equipos en otras redes, esta configuración se detalla a continuación:

Dar clic sobre el icono que identifica a R1, seleccionar la ficha CLI, como se muestra en la figura 2.49.

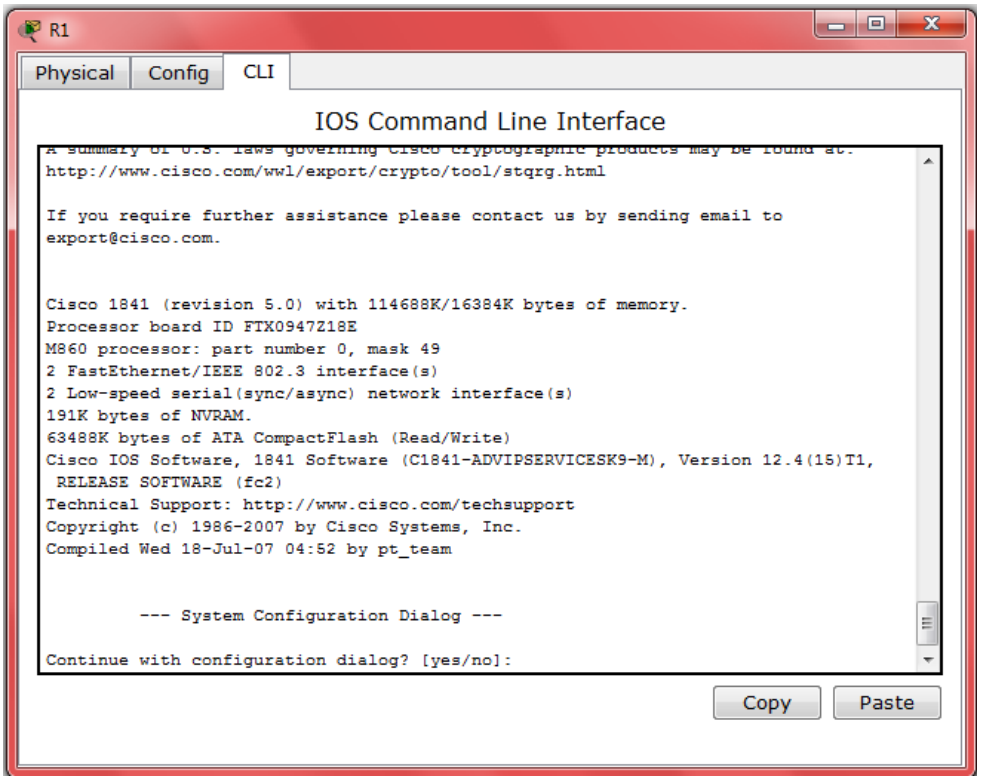

FIGURA 2.49 Terminal de comandos R1

Para cambiar el nombre del equipo a R1 ingresar los siguientes comandos que se indican en la figura 2.50.

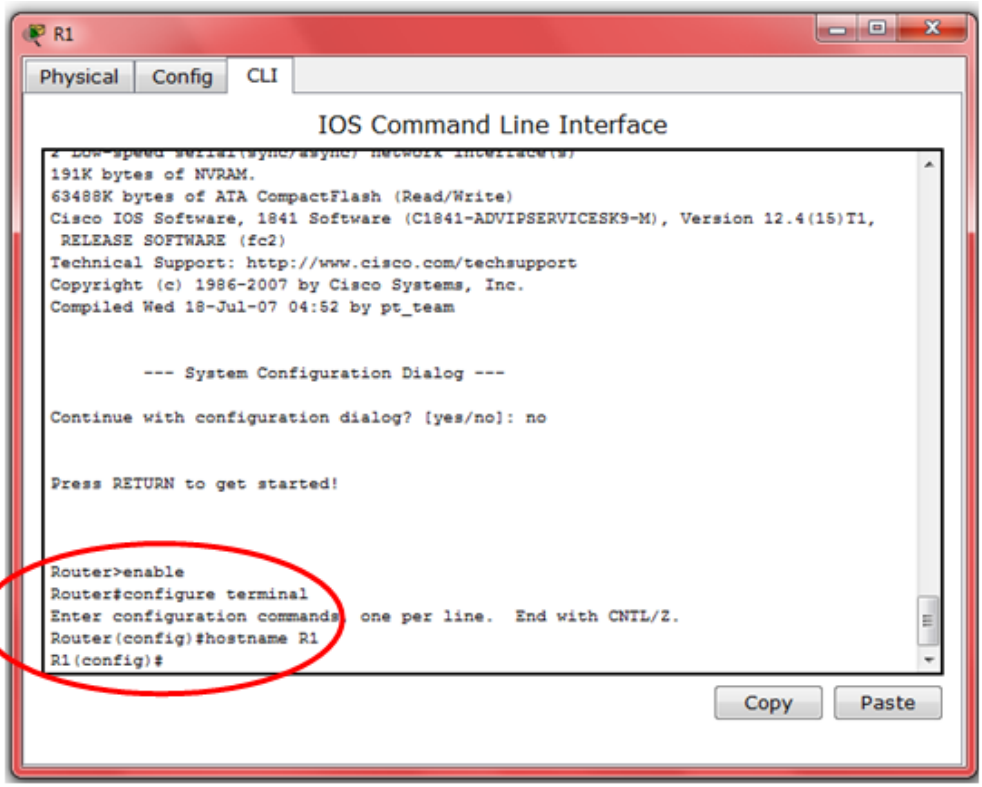

FIGURA 2.50 Comandos terminal R1

Establecer las direcciones IP en las interfaces del Router Fast-Ethernet0/0, Serial0/0/0 y Serial0/0/1 con las indicadas en la tabla 6.1, con los siguientes comandos, que se indicanm en las figuras 2.51.1, 2.51.2, 2.51.3.

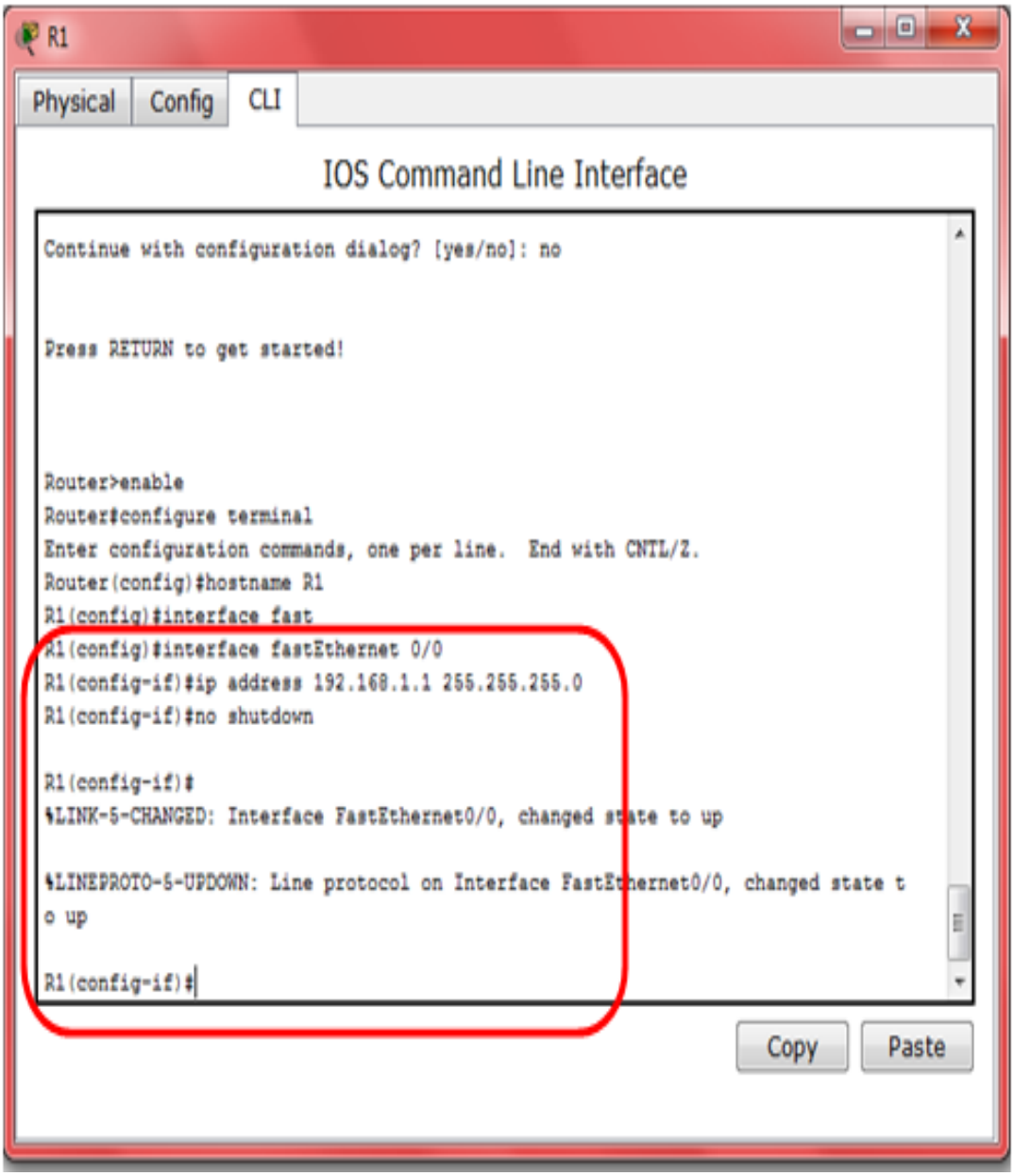

FIGURA 2.51.1 Interface Fast Ethernet 0/0 R1

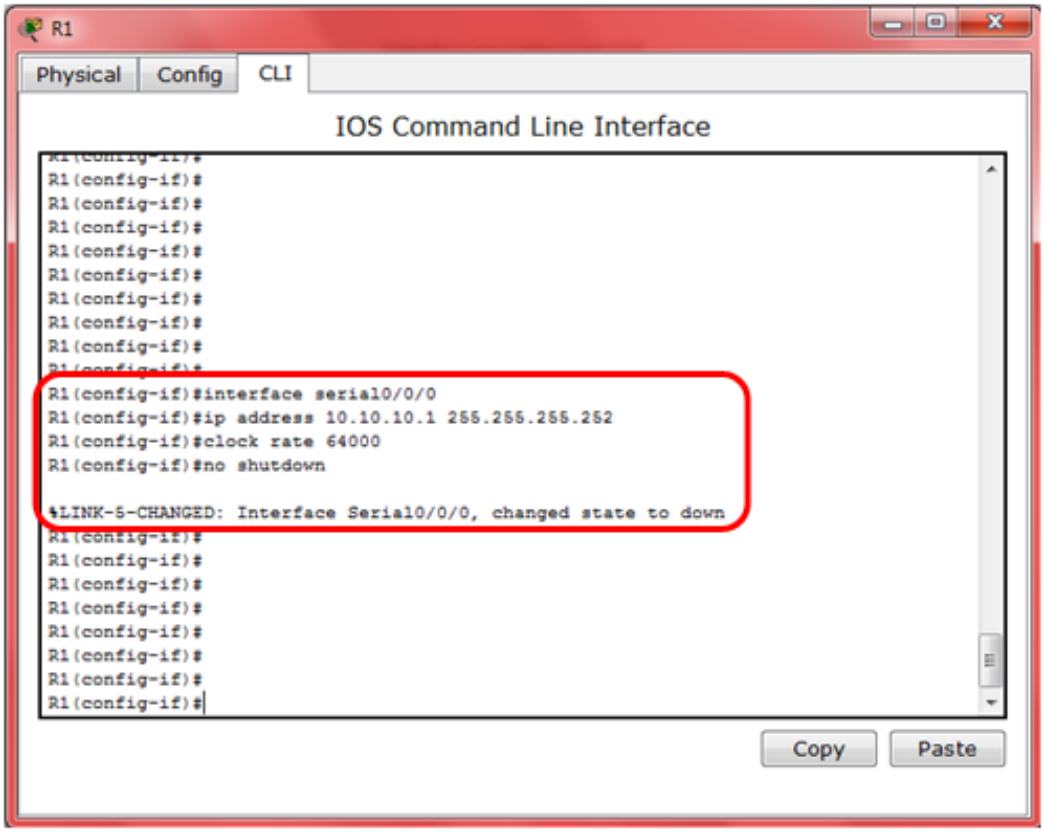

FIGURA 2.51.2 Interface Serial0/0/0 R1

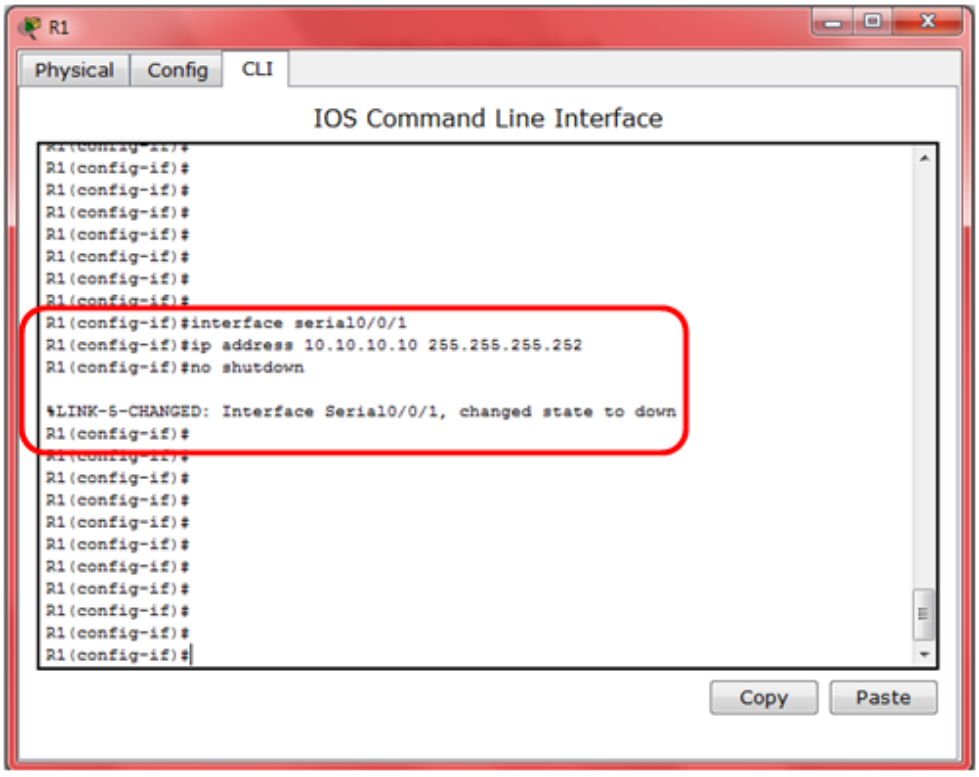

FIGURA 2.51.3 Interface Serial0/0/1 R1

Se debe seguir el mismo procedimiento para los otros Routers R2 y R3 cambiando las direcciones de sus interfaces quedando como muestran en las figuras 2.52.1, 2.52.2.

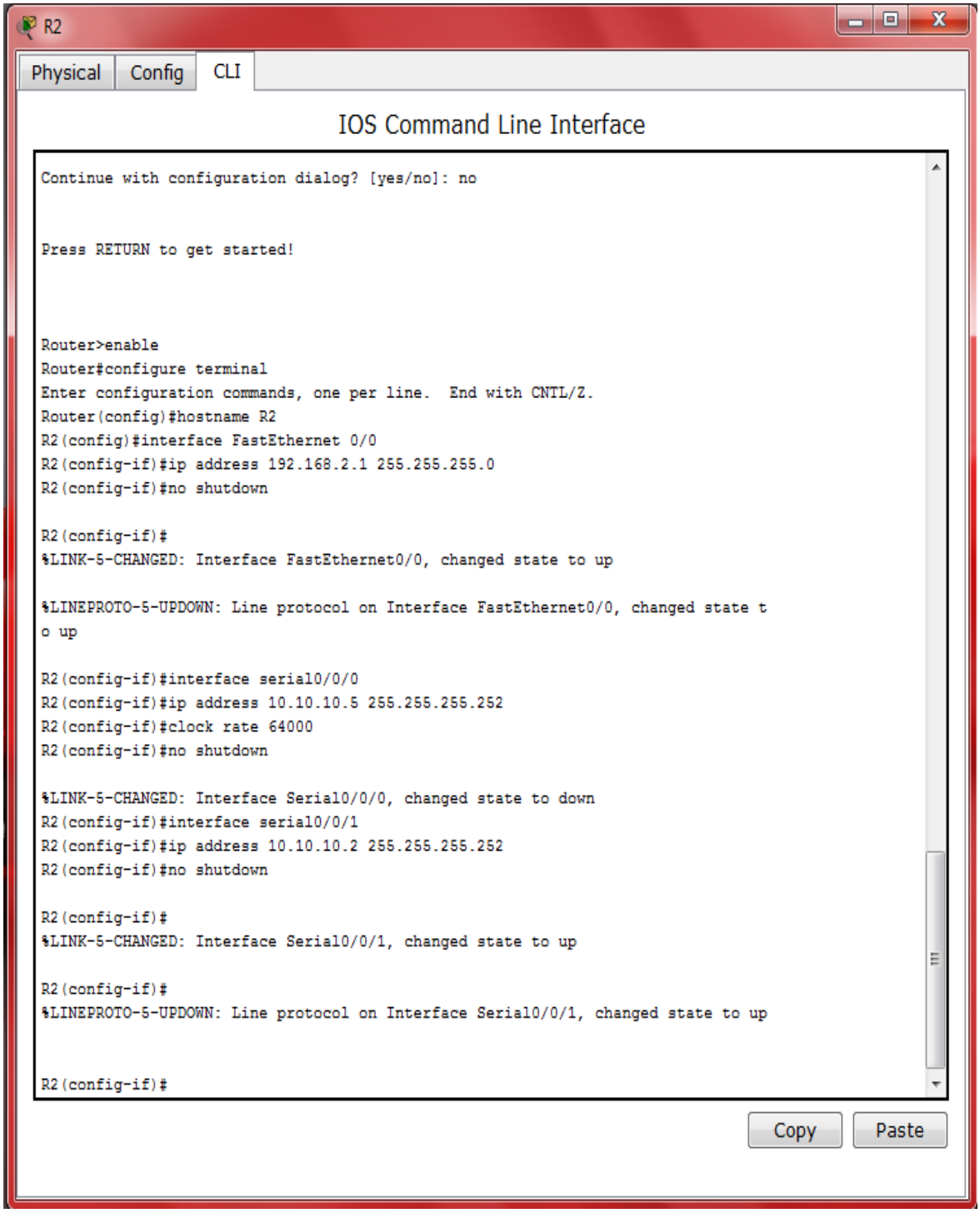

FIGURA 2.52.1 Configuración de direcciones IP en el Router R2

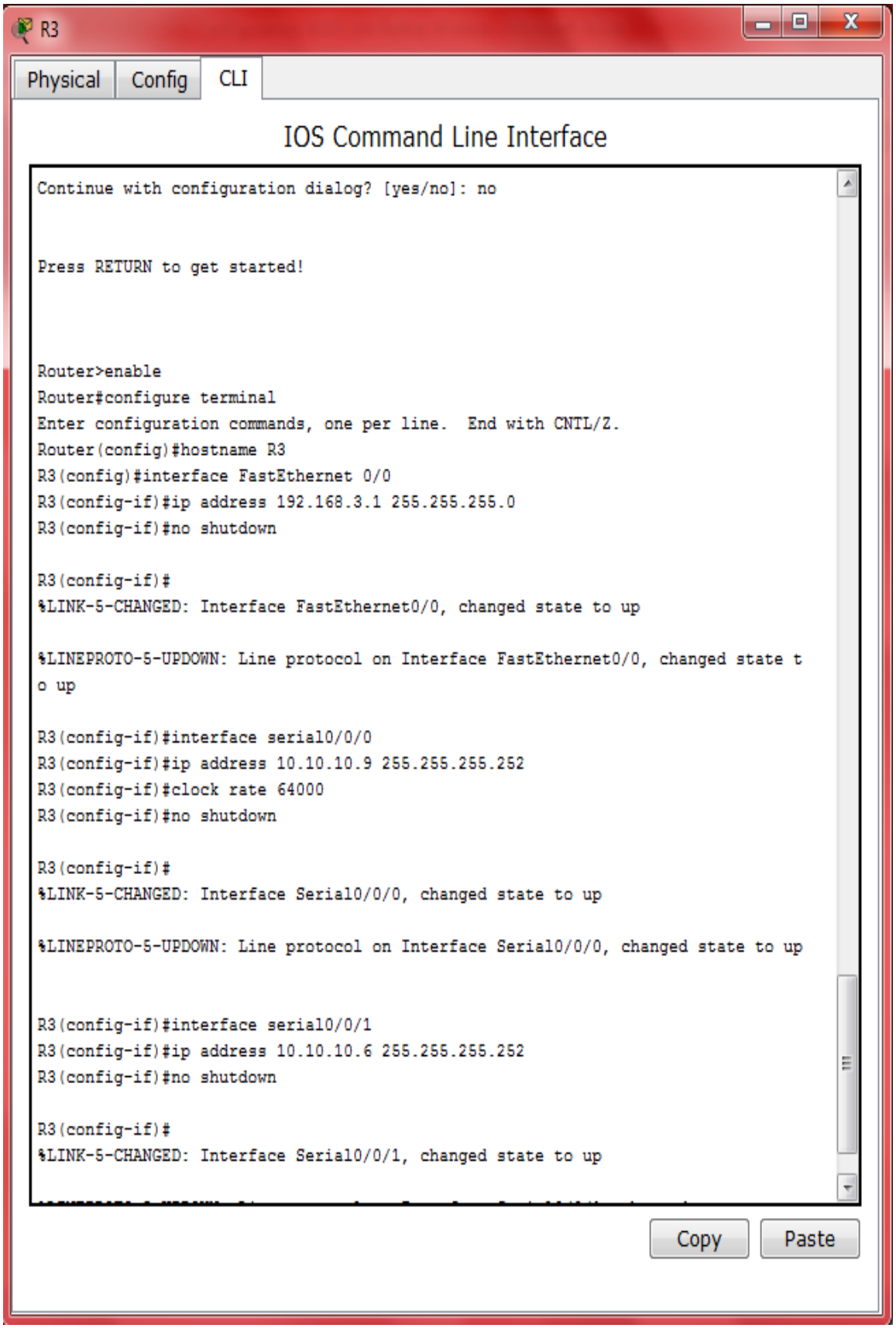

FIGURA 2.52.2 Configuración de direcciones IP en el Router R3

Una vez configuradas las direcciones IP en las interfaces de los Routers, cambiarán los estados de las conexiones como muestra en la figura 2.53.

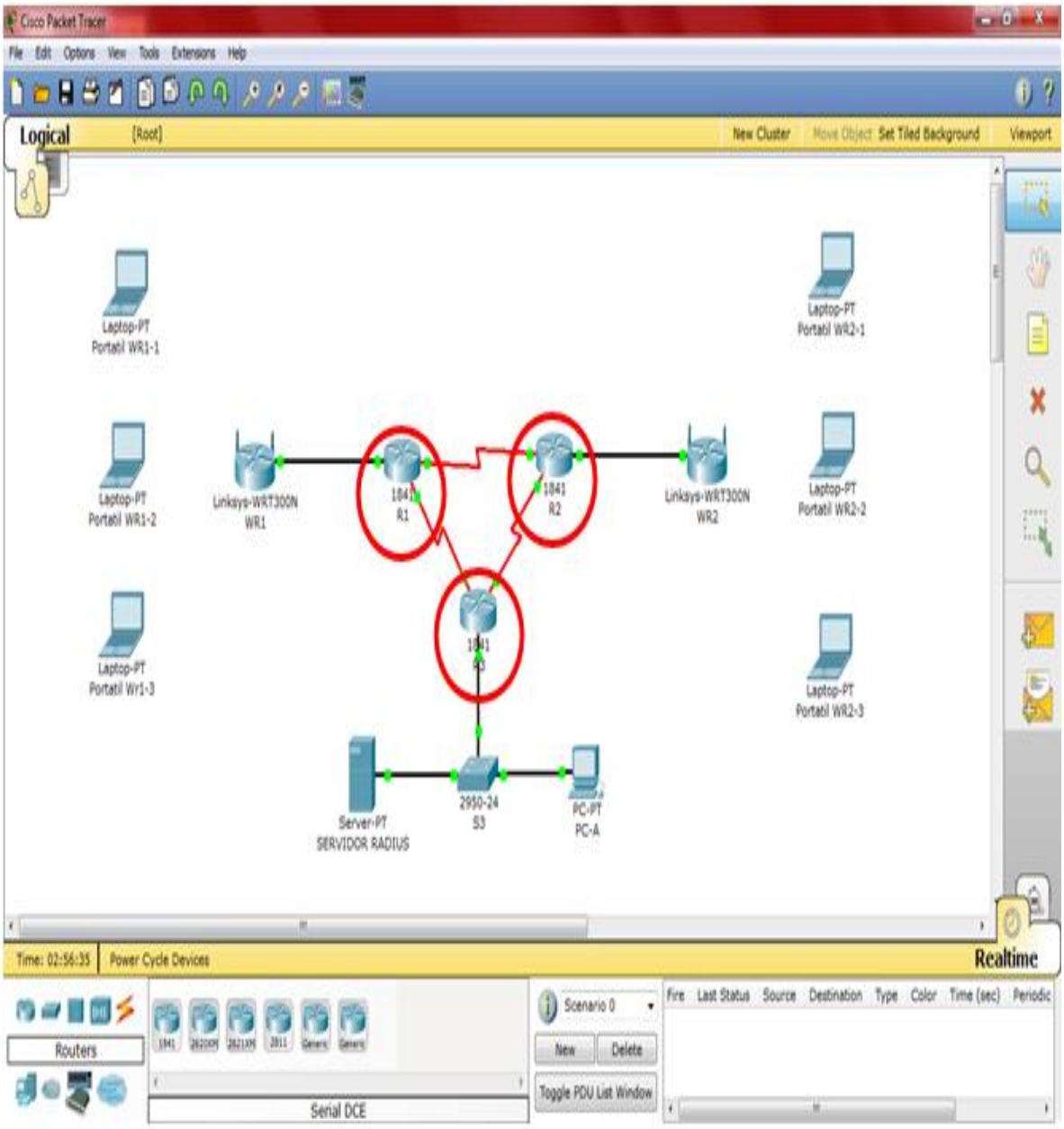

FIGURA 2.53 Cambio del estado de las interfaces en los Routers

Configuramos las tablas de rutas en cada Router (R1-R2-R3) con los comandos que muestran las figuras 2.54, 2.55, 2.56.

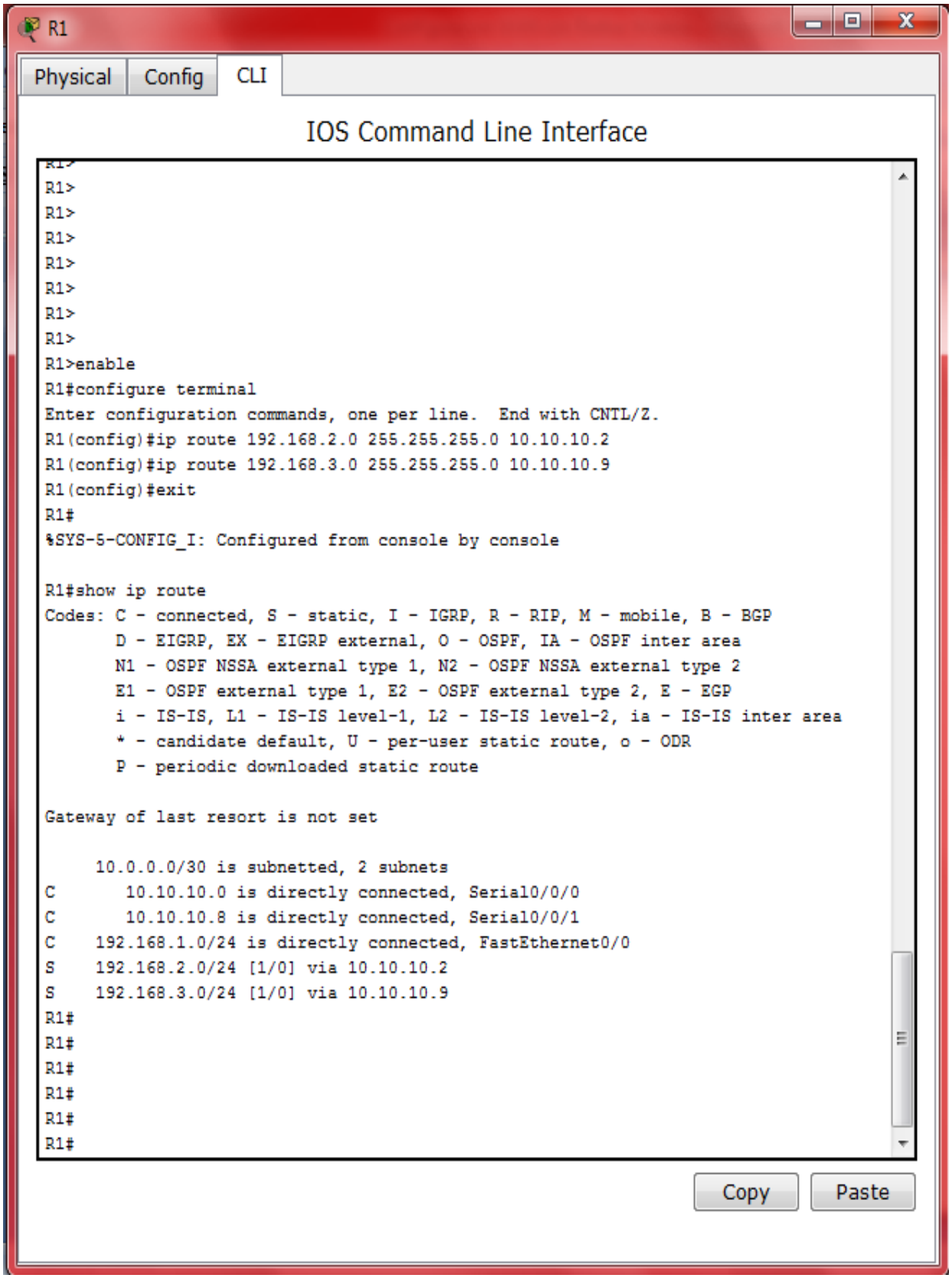

FIGURA 2.54 Ingreso de rutas estáticas a R1

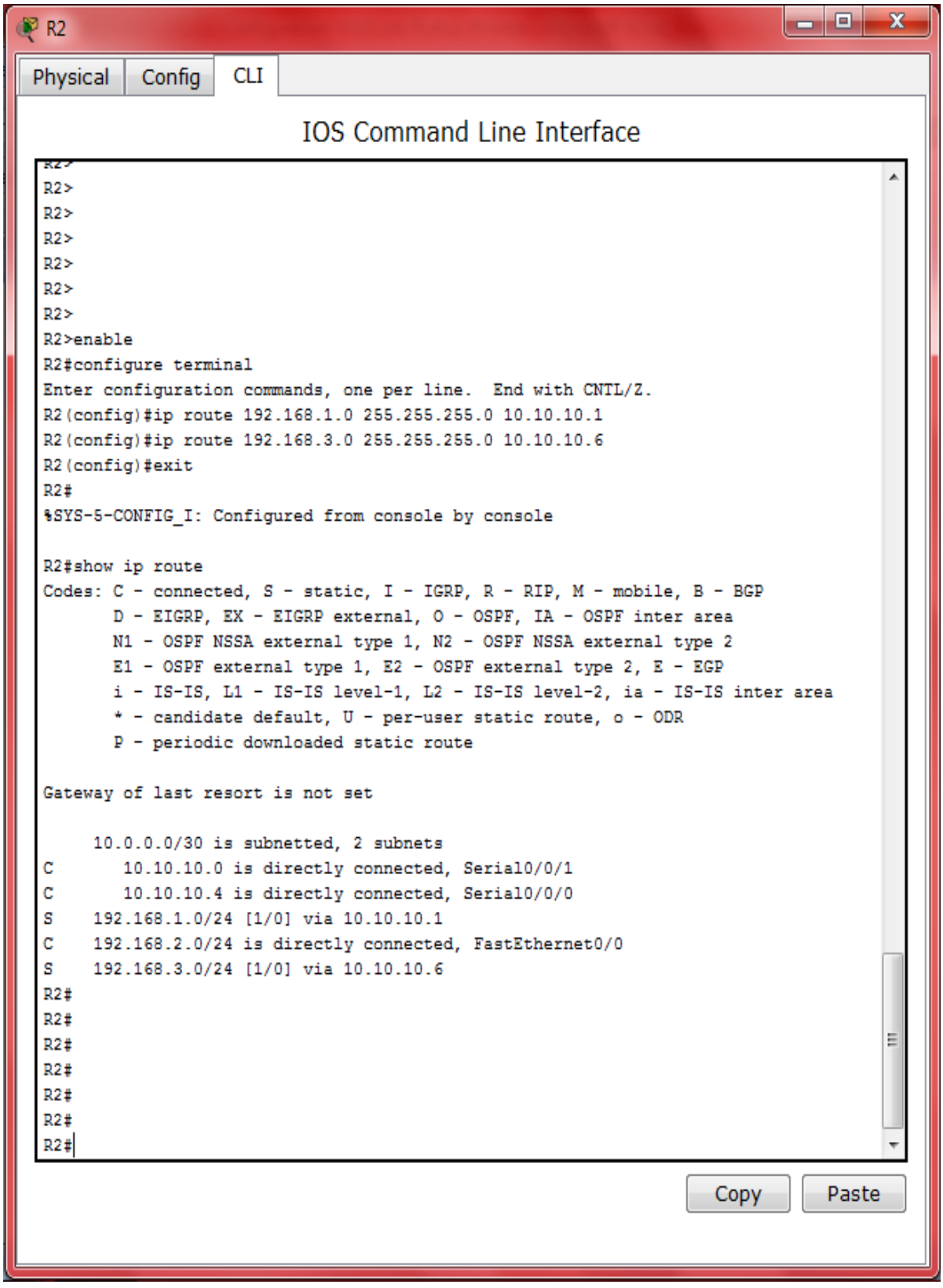

FIGURA 2.55 Ingreso de rutas estáticas a R2

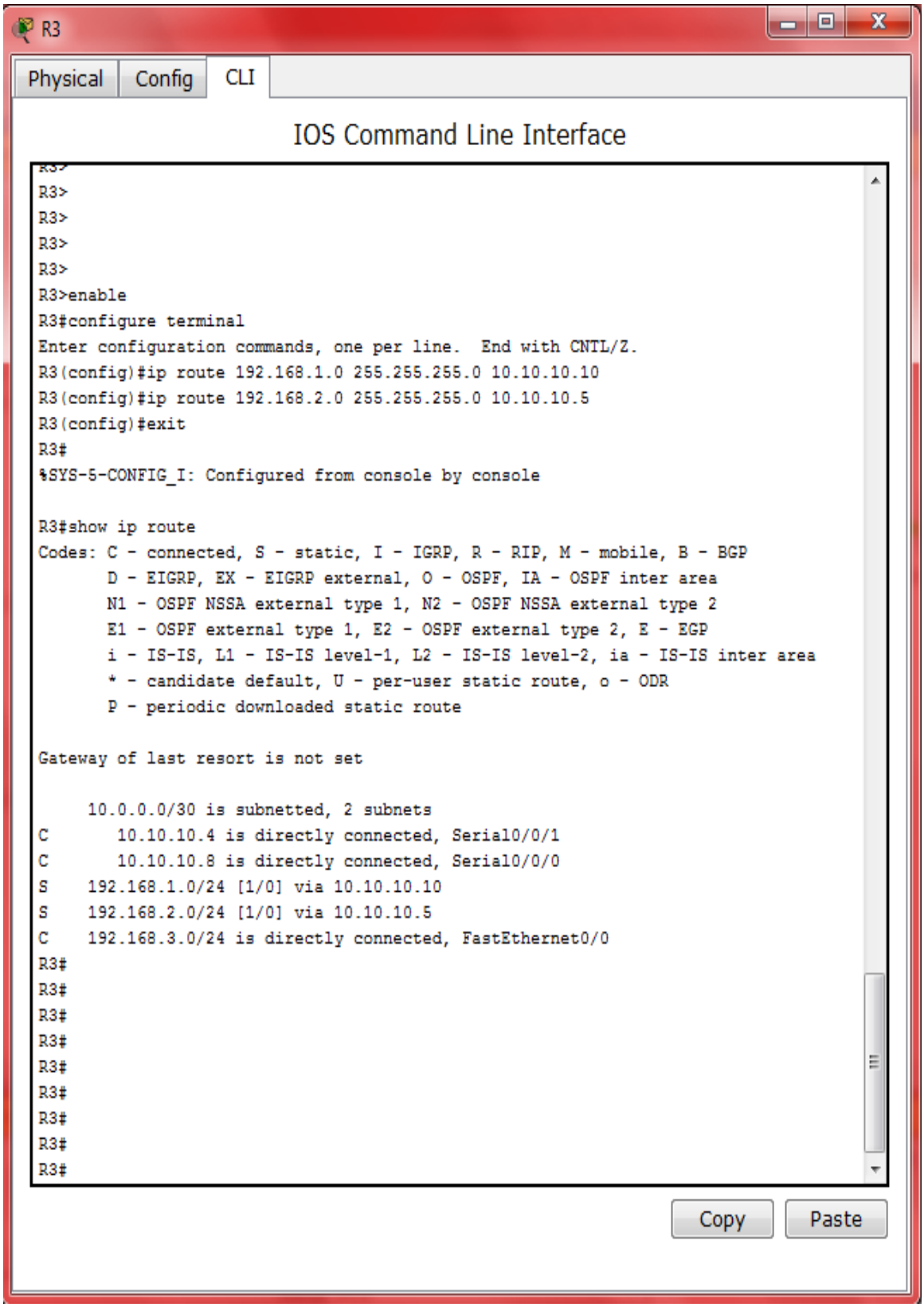

FIGURA 2.56 Ingreso de rutas estáticas a R3

Establecidas las rutas estáticas en los Routers la conectividad se extiende a través de las conexiones entre los equipos WR1 a WR2 y viceversa como se muestra en las figuras 2.57, 2.58.

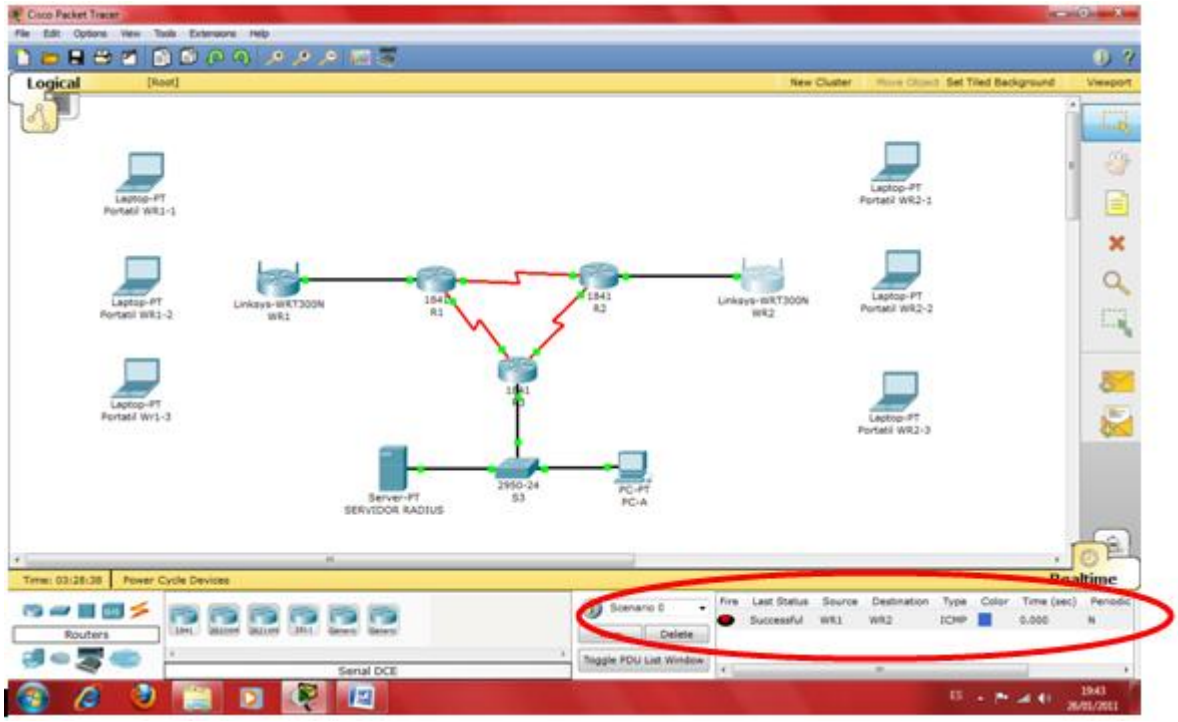

FIGURA 2.57 Conexión exitosa de WR1 a WR2

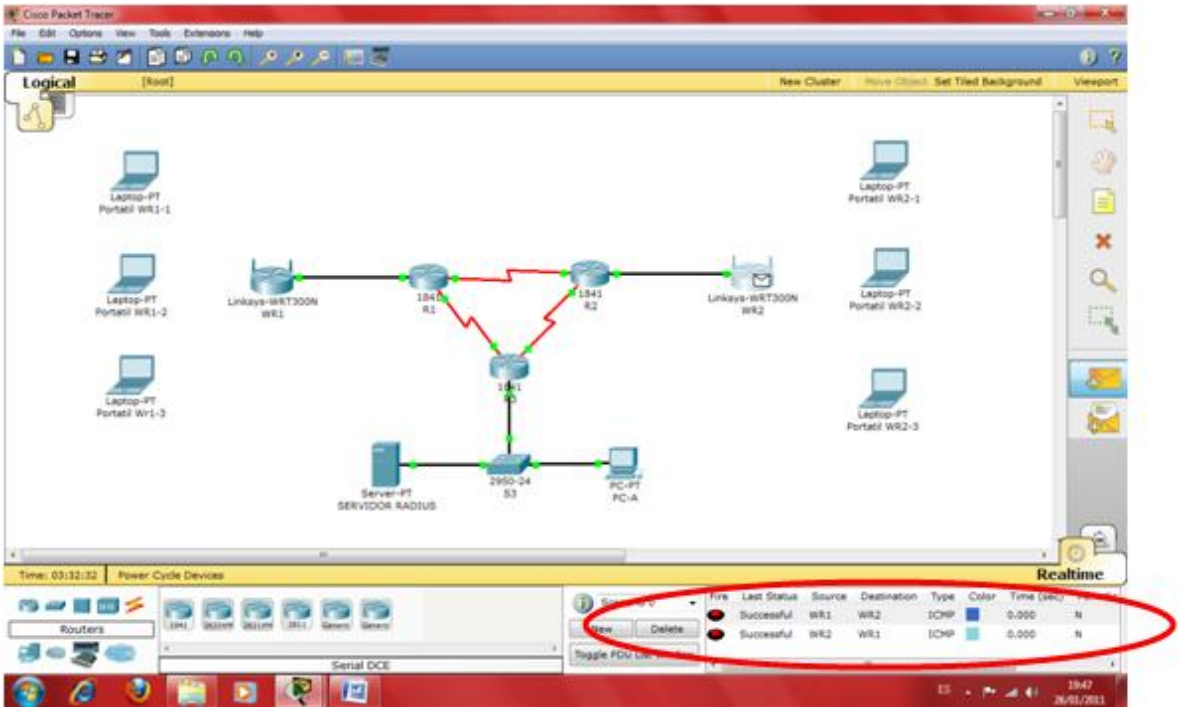

FIGURA 2.58 Conexión exitosa de WR2 a WR1

- **SERVIDOR RADIUS**

En la administración del servidor RADIUS, es necesario configurar la dirección IP del dispositivo de forma estática de manera que siempre tenga esta dirección y sus clientes (WR1-WR2), lo encuentren a través de la red WAN, además este dispositivo valida, autentica a los usuarios y claves creados en cada portátil, así como también la clave secreta con WR1 - WR2, y autoriza a sus clientes proveer a los usuarios autenticados la conectividad a la red, configuración que se detalla a continuación.

Dar clic sobre el icono que identifica al servidor RADIUS y seleccionar la ficha *Config*, en la casilla *Gateway* llenar con la dirección IP 192.168.3.1 como muestra la figura 2.59.

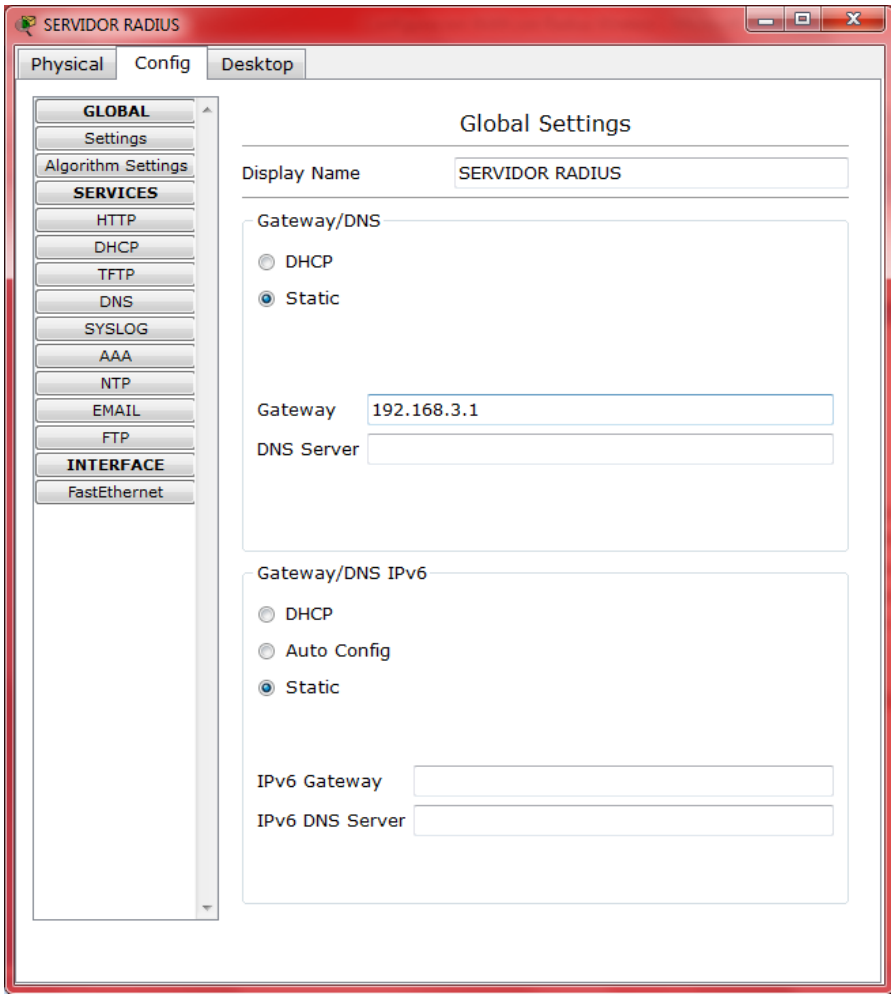

FIGURA 2.59 Configuración General Servidor Radius

Pulsar sobre el botón *FastEthernet* de la sección *INTERFACE* (a), activar la opción *Static* (b), llenar las casillas *IP Address y Subnet Mask* con las indicadas en la tabla 2.4, y; señaladas en (c), como se muestra en la figura 2.60.

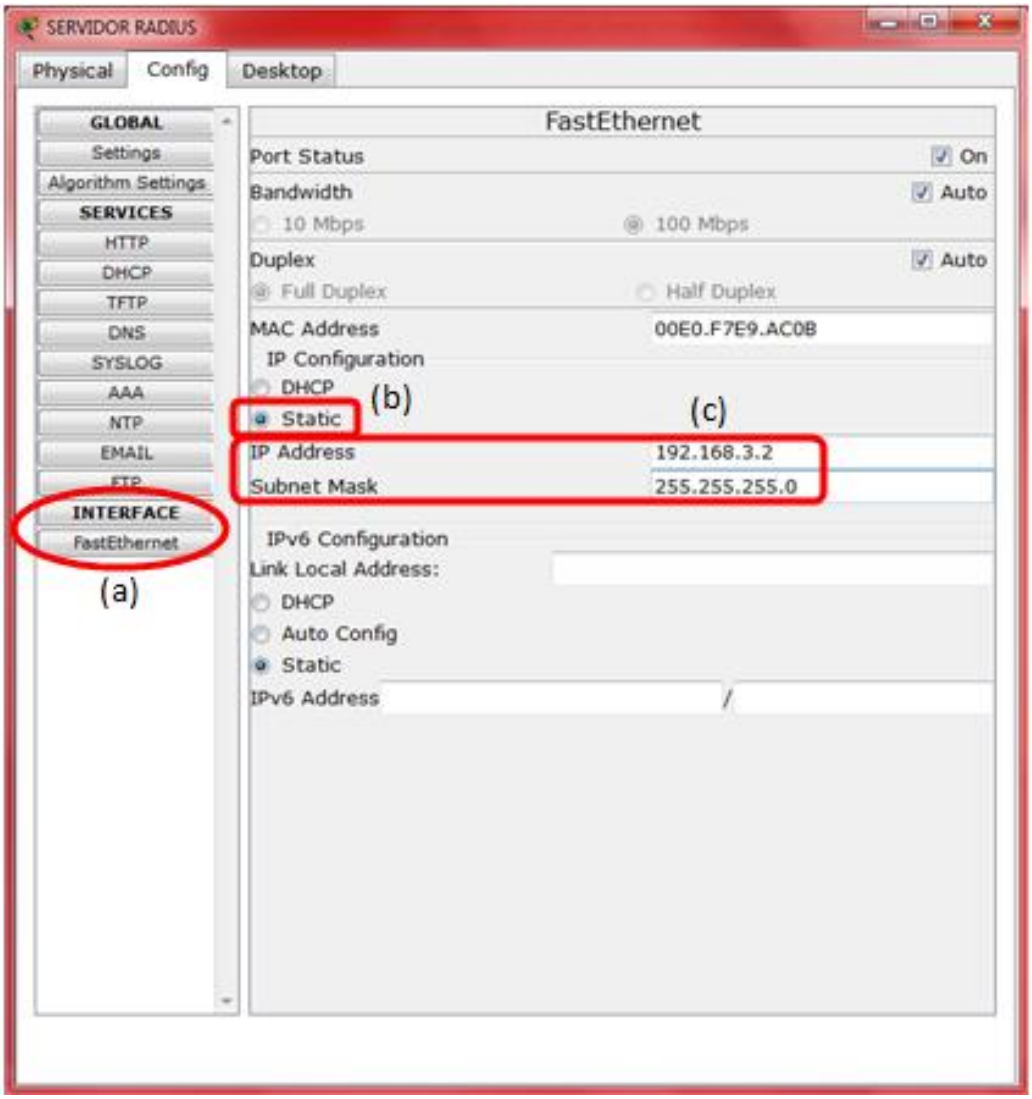

FIGURA 2.60 Configuración FastEthernet Servidor Radius

Pulsar sobre el botón *AAA* de la selección *SERVICES* (a), y en la configuración de red llenar los casilleros *Client Name, Secret, Client IP y ServerType* con los gestionados anteriormente en WR1 y WR2 para validar la clave secreta configurada (b), pulsar el botón con el signo + (c), finalmente ingresar los datos correspondientes a WR2 (d) y agregar a la lista (e), como se muestran en las figuras 2.61.1, 2.61.2, 2.61.3.

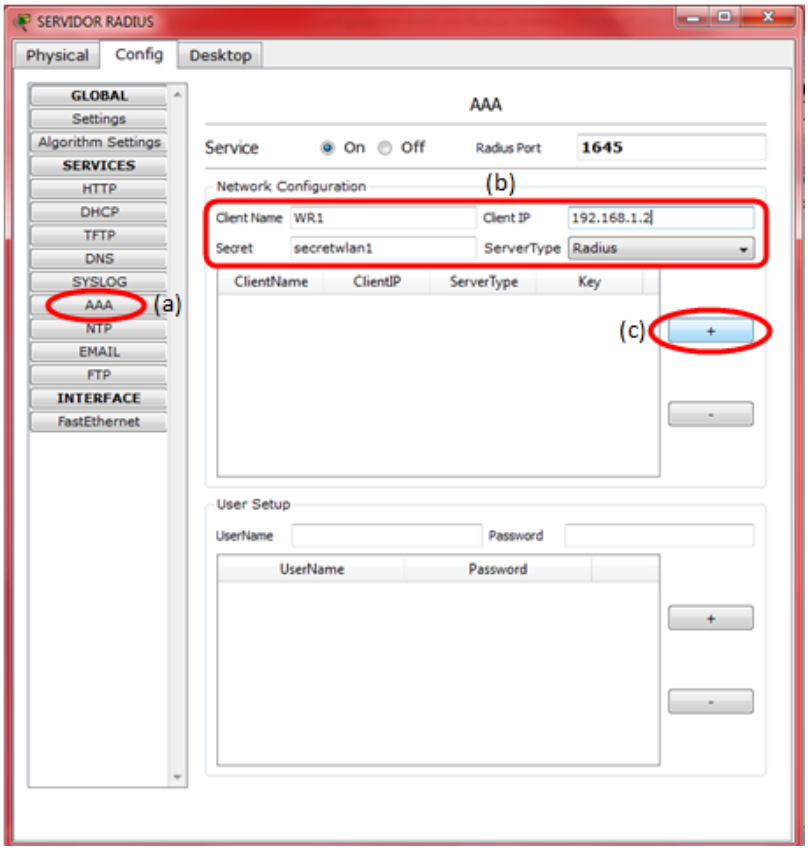

FIGURA 2.61.1 Configuración AAA Servidor Radius

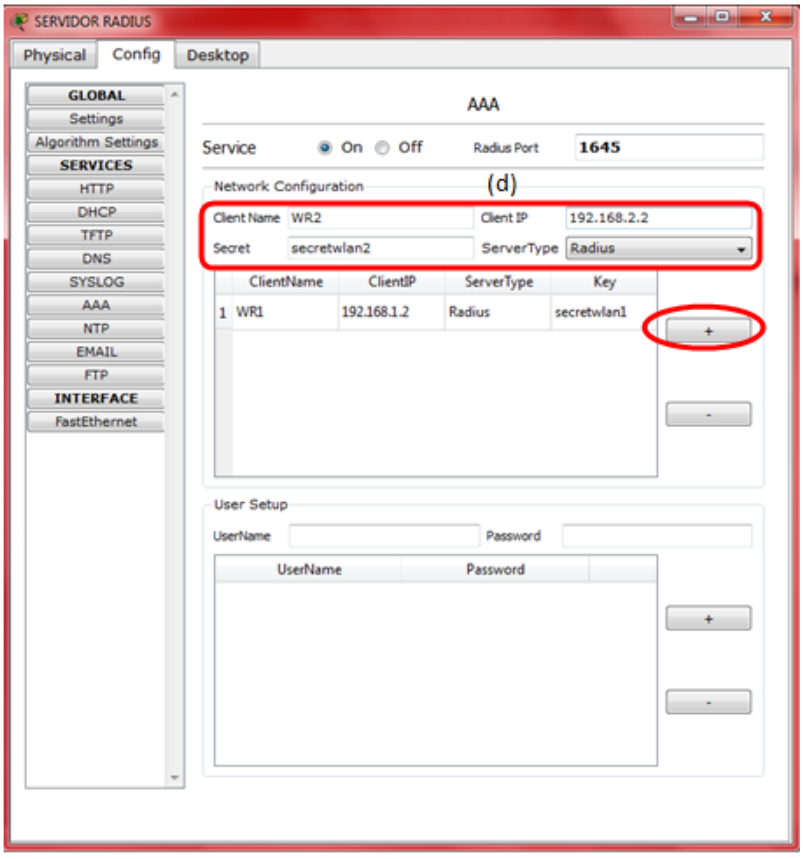

FIGURA 2.61.2 Configuración AAA Servidor Radius

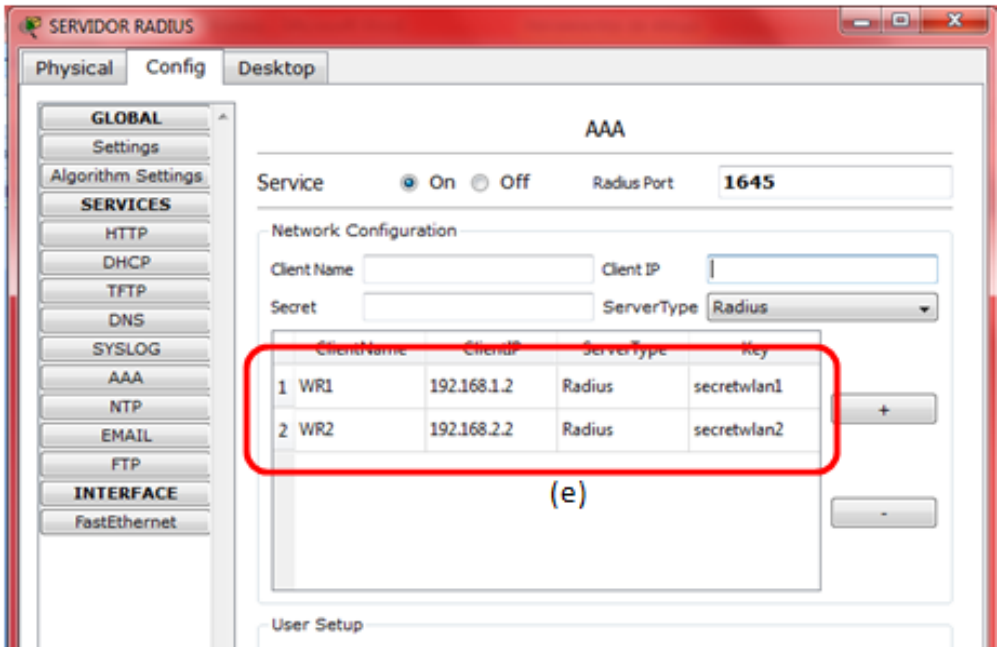

FIGURA 2.61.3 Configuración AAA Servidor Radius

El paso final es ingresar a los usuarios y contraseñas de las portátiles en *UserName y Password* respectivamente (a), pulsar el botón con el signo + para añadir a la lista (b), como se muestra en la figura 2.62.1 y 2.62.2.

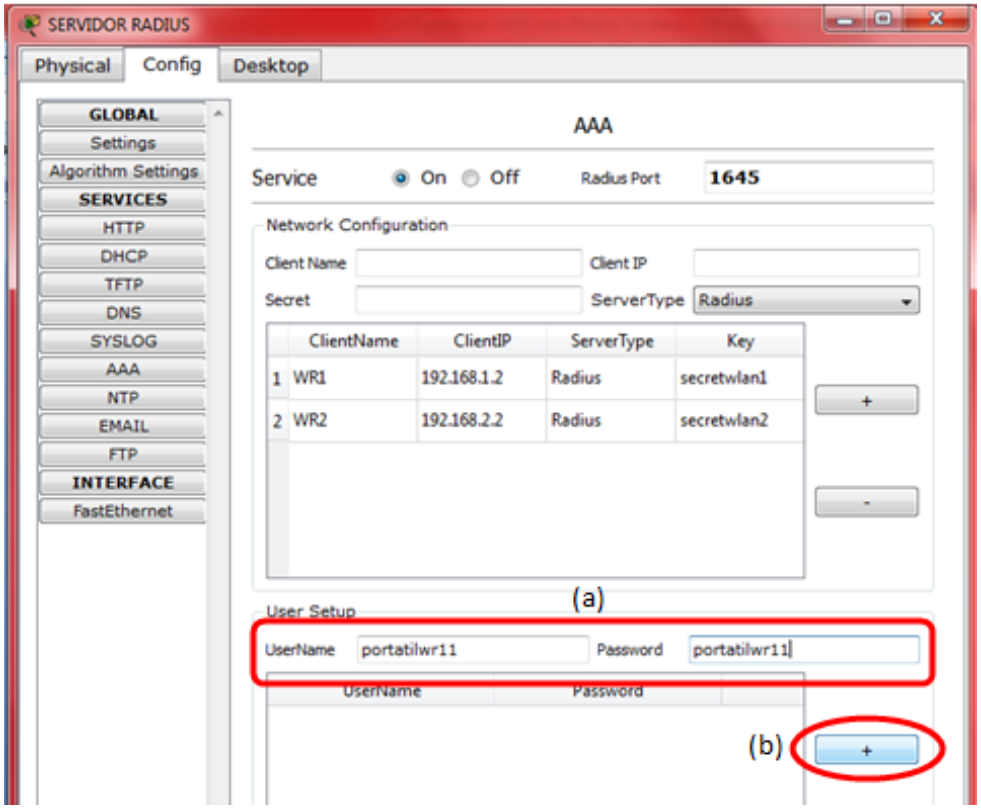

FIGURA 2.62.1 Usuarios y contraseña AAA Servidor Radius

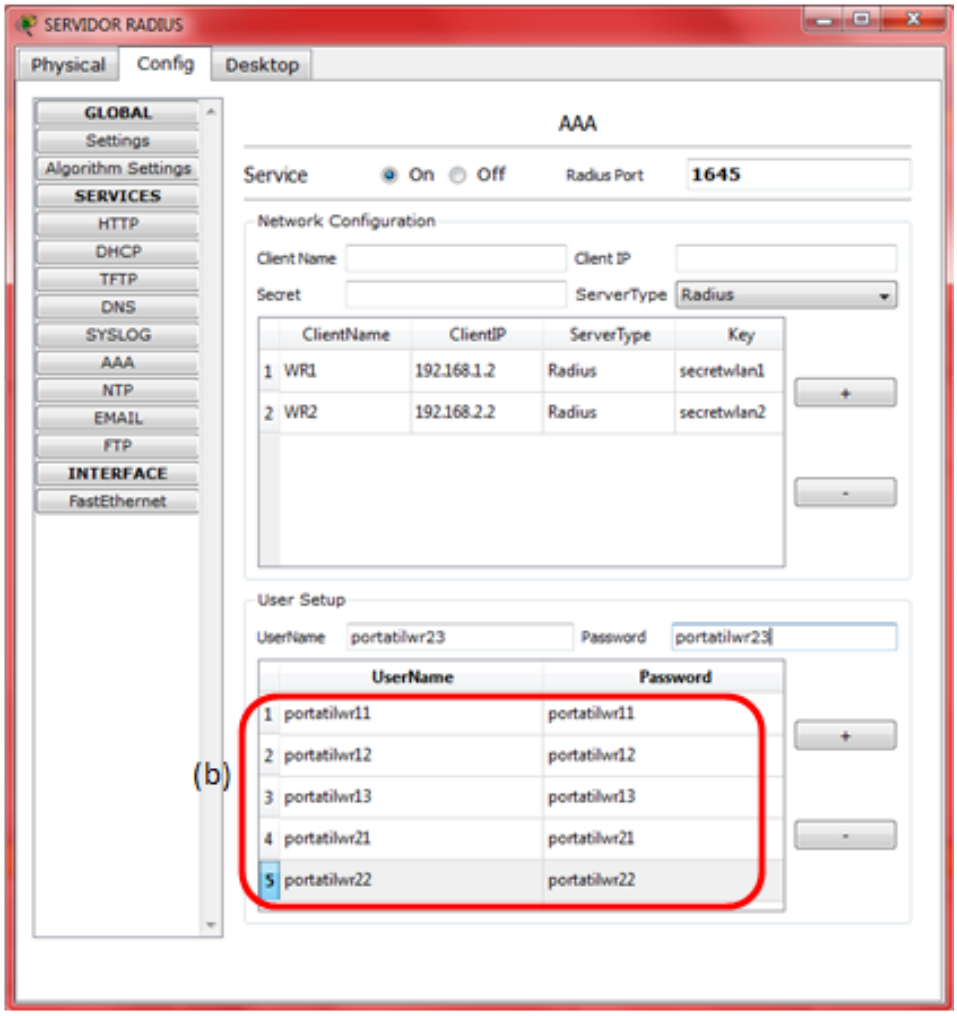

FIGURA 2.62.2 Usuarios y contraseña AAA Servidor Radius

Establecida esta configuración nuestro esquema se muestra en la siguiente figura 2.63.

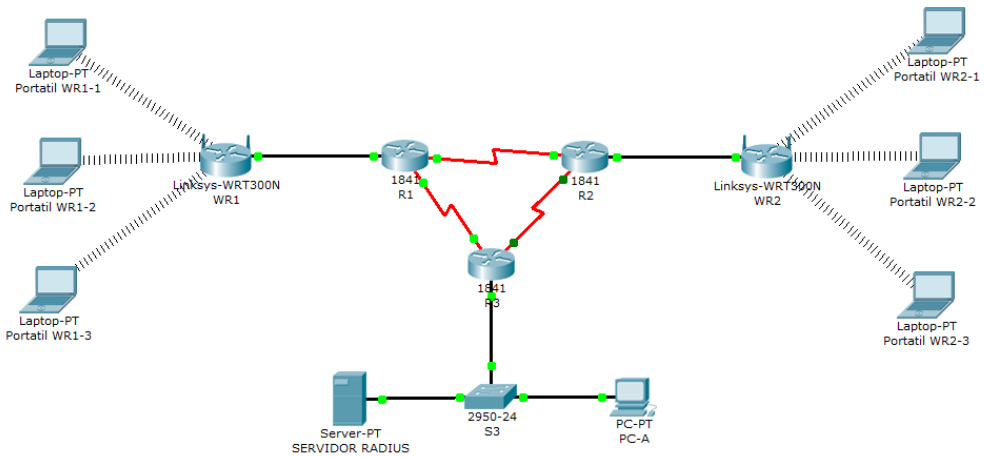

FIGURA 2.63 Validación, Autenticación y Autorización Servidor Radius

2.5.6 RESULTADOS

Verificar la conectividad entre las portátiles que forman la red WLAN1 y WLAN2 con se indica en las siguientes figuras 2.64.1, 2.64.2, 2.64.3.

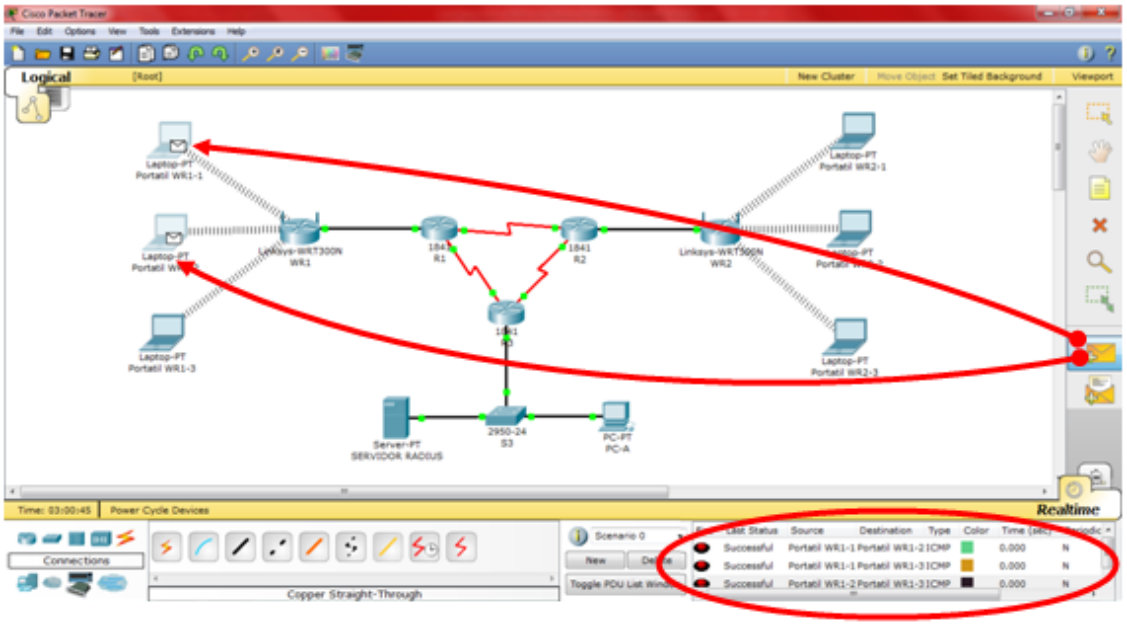

FIGURA 2.64.1 Conexión Portatil WR1-1 / Portatil WR1-2

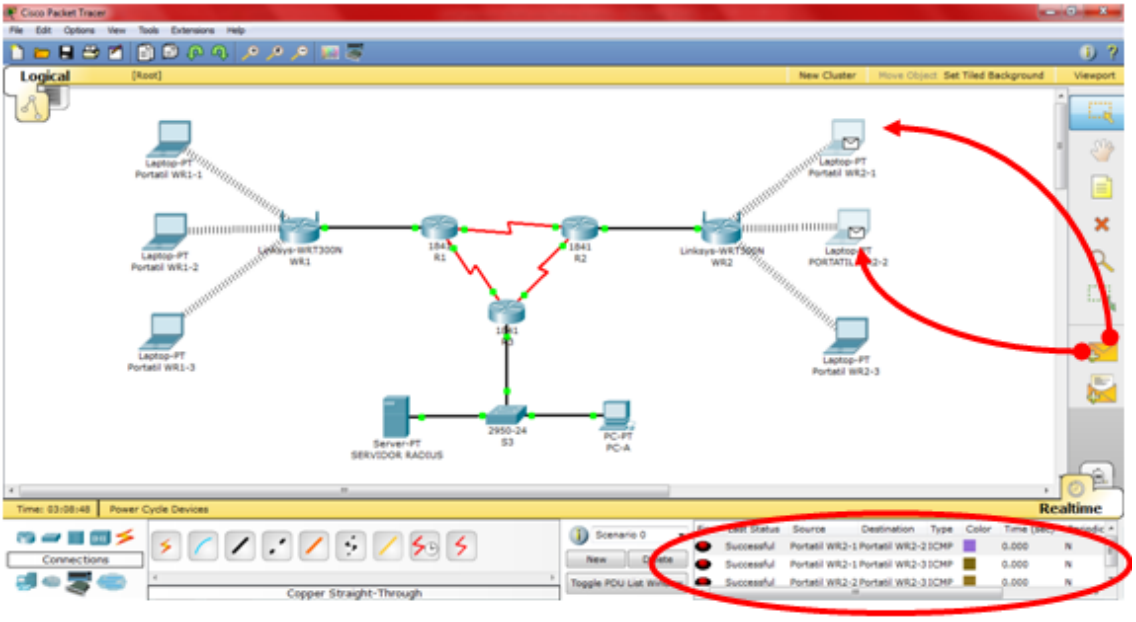

FIGURA 2.64.2 Conexión Portatil WR2-1 / Portatil WR2-2

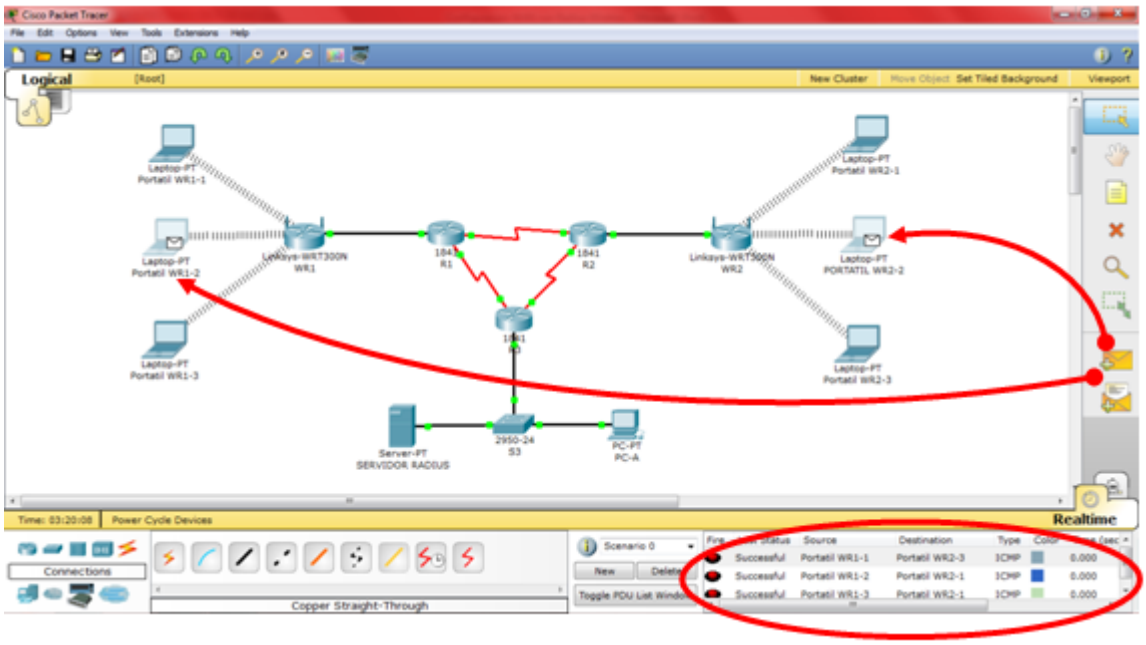

FIGURA 2.64.3 Conexión Portatil WR1-2 / Portatil WR2-2

Al momento que se tiene interconexión entre los computadores de una red y otra, como se muestra en la figura 2.64.3, se verifica que la configuración del servidor RADIUS es funcional, ya que en él se especifican los parámetros de conexión de los usuarios que pueden o no acceder a la red.

CAPITULO III

3. DISCUSIÓN Y PROPUESTA

3.1 DISCUSIÓN

El término **red inalámbrica** *(Wireless network)* en inglés es un término que se utiliza en informática para designar la conexión de nodos sin necesidad de una conexión física (cables). La transmisión y la recepción se realizan a través de puertos.

Una de sus principales ventajas es notable en los costos, ya que se elimina todo el cable ethernet y conexiones físicas entre nodos, pero también tiene una desventaja considerable ya que para este tipo de red se debe de tener una seguridad mucho más exigente y robusta para evitar a los intrusos.

¿Por qué las redes inalámbricas tienen inseguridades?

En la actualidad, la mayoría de los operadores pre-configuran los routers con encriptación WEP, u, opcionalmente, WPA-PSK, anotando las claves, al igual que el SSID por defecto, que por pereza no personalizamos sino las dejamos así.

La seguridad es una de las principales preocupaciones de las instituciones públicas o privadas que están interesadas en implementar redes inalámbricas. Afortunadamente, tanto el conocimiento de los usuarios sobre la seguridad como las soluciones ofrecidas por los proveedores de tecnología están mejorando.

Las redes inalámbricas actuales incorporan funciones completas de seguridad, y cuando estas redes cuentan con una protección adecuada, las instituciones públicas o privadas pueden aprovechar con confianza las ventajas que ofrecen. Sin embargo, las amenazas aún se consideran importantes, y los proveedores de algún servicio siempre necesitan tener en cuenta la percepción inamovible de que las redes WLAN son inseguras.

De hecho, la seguridad es el principal obstáculo para la adopción de redes LAN inalámbricas. Y esta preocupación no es exclusiva de las instituciones públicas o privadas grandes o pequeñas. En lo que respecta a la conexión de redes inalámbricas, "la seguridad sigue siendo la preocupación nº1 de dichas instituciones de todos los tamaños".

Tener un mejor conocimiento de los elementos de la seguridad de LAN inalámbricas y el empleo de algunas de las mejores prácticas o políticas de seguridad pueden ser de gran ayuda para beneficiarse de las ventajas de las redes inalámbricas.

3.2 PROPUESTA

Implementación de un ejemplo práctico utilizando el software Cisco Packet Tracer 5.3 para mejorar la seguridad en redes inalámbricas mediante la instalación y configuración de un servidor RADIUS para autenticar, autorizar y registrar a todos los usuarios que intentan ingresar a la red a solicitar los servicios que esta nos brinda.

CAPITULO IV

4. CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

Se comprobó que el servidor RADIUS realiza un control de utilización de los recursos de la red, ya que no únicamente permite tener un control de acceso al usuario, sino que también permite realizar un control del tipo de autorizaciones que tiene y almacena los datos de la petición realizada.

Mientras más mecanismos de seguridad se empleen en sistemas de control de acceso, el sistema será más seguro, aun cuando un sistema con seguridad absoluta no exista, el hecho de implementar un mayor número de mecanismos de control ayudará a que el sistema sea menos vulnerable.

El mecanismo empleado para la autenticación de los usuarios inalámbricos en la red es bastante seguro y eficiente, pero conlleva de un procedimiento de instalación adicional en cada usuario, que debe ser considerado en los tiempos de implementación.

La identificación de cada uno de los procesos y las tareas asociadas a cada organización, permitirán que se pueda realizar una implementación, reduciendo los riesgos de interrupciones de la organización y ayudando en una más rápida adopción de nuevas soluciones de seguridad.

El Servidor RADIUS podrá ser implementado en cualquier ambiente que se lo pueda aplicar, realizando pequeñas modificaciones, siendo la principal idea que el presente sistema provea de una fácil implementación.

4.2 RECOMENDACIONES

Si se emplea mecanismos de autenticación con nombres de usuario y clave, es necesario concientizar a los usuarios de la importancia de mantener sus claves seguras con normas básicas como que no deben anotarlas en ningún lugar como recordatorio o que no deben facilitárselas a otras personas.

Los sistemas de seguridad inalámbrica deben estar basados en una infraestructura que emplea como elementos principales servidores, es recomendable establecer políticas de respaldo de la información, de los equipos más críticos, en este caso del cliente RADIUS y del servidor RADIUS, así como también de una política de respaldo continua de la información de base de datos y configuraciones de los equipos.

La seguridad física de los servidores es un aspecto muy importante, para prevenir posibles accesos por parte de personas no autorizadas a los mismos, los servidores deberán colocarse en un área donde el acceso lo tengan únicamente las personas que administren estos equipos.

Se recomienda en el proceso de adopción de una nueva solución de tecnología de comunicaciones, realizar un seguimiento del proyecto a través de un esquema, que permite en primer lugar levantar los requerimientos del usuario tanto técnicos como de negocios, para que una vez identificados estos requerimientos poder definir como cumplir con los requerimientos de usuario, que elementos emplear, como implementar dichos elementos, como van ha ser adoptados dichos elementos, el proceso de implementación y el proceso de administración de estos nuevos elementos en la red.

Es importante para la óptima operación del sistema, que el administrador mantenga un estricto cumplimiento de las políticas de seguridad descritas e implementadas como parte de la solución presentada, ya que el incumplimiento de alguna de las mismas puede dar lugar a un incremento de la vulnerabilidad del sistema y este puede ser un blanco fácil para que usuarios mal intencionados hagan un mal uso de este.

CAPITULO V

V. BIBLIOGRAFÍA

5.1 Bibliografía de Internet

http://mygnet.net/articulos/redes/827/

http://www.microsoft.com/latam/protect/viruses/fwbenefits.mspx

http://www.coit.es/publicac/publbit/bit138/3com.pdf

http://www.saulo.net/pub/inv/SegWiFi-art.htm

http://translate.googleusercontent.com/translate_c?hl=es&langpair=en|es&u=http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800945cc.shtml&rurl=translate.google.com&usg=ALkJrhgbBpZeABMxjv2K4Jv02QGXzu1Chg#intro

http://en.wikipedia.org/wiki/List_of_RADIUS_standards

http://www.ordenadores-y-portatiles.com/red-privada-vpn-2.html

http://www.scribd.com/doc/37641903/Radius-Fin

http://www.scribd.com/doc/43768082/Radius

http://www.stat.ufl.edu/system/man/portmaster/RADIUS/guide/1overview.html

http://www.taringa.net/posts/downloads/1047902/Mejores-Simuladores-de-Redes.html

http://es.wikipedia.org/wiki/Packet_Tracer

http://www.udb.edu.sv/Academia/Laboratorios/electronica/Comunicacion%20de%20Datos%20I/guia4CDAI.pdf

5.2 Bibliografía de Libros

- ✓ LAN inalámbrica y conmutada: guía de estudio de CCNA Exploration: Lewis, Wayne, (aut.); Pearson Prentice Hall (editorial); 1ª ed.
- ✓ Redes inalámbricas: Luis Miguel Cabezas Granado y Francisco José González Lozano, (aut.); Anaya multimedia - Anaya interactiva (editorial).
- ✓ Fundamentos de redes inalámbricas: Cisco Systems, (aut.); Pearson Prentice Hall (editorial); 1ª ed.
- ✓ Cómo funcionan las redes inalámbricas: Gralla, Preston, (aut.); Anaya Multimedia-Anaya Interactiva (editorial); 1ª ed
- ✓ Manual práctico de seguridad de redes: Harrington, Jan L., (aut.); Anaya Multimedia-Anaya Interactiva (editorial); 1ª ed