PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN Y WLAN CON SISTEMA DE CONTROL DE ACCESO MEDIANTE SERVIDORES AAA

Tesis para optar el Título de Ingeniera de las Telecomunicaciones, que presenta la bachiller:

Nuttsy Aurora Lazo García

ASESOR: Ing. Antonio Ocampo Zuñiga

Lima, Julio de 2012

Resumen

La presente tesis consiste en el diseño e implementación de una red LAN (Local Area Network) y WLAN (Wireless Local Area Network) con sistema de control de acceso AAA (Authentication, Authorization and Accounting). El primer paso fue implementar una red LAN utilizando el mecanismo Etherchannel y el protocolo de balanceo de carga en la puerta de enlace GLBP (Gateway Load Balancing Protocol) para optimizar el uso de recursos de la red. Luego se implementó el servidor ACS (Access Control Server) que utiliza el protocolo TACACS+ para centralizar el acceso de los administradores de los equipos de la red. En lo que concierne a la WLAN, se instaló el servidor IAS de Windows, luego se verificó que el punto de acceso inalámbrico (Access Point - AP) cumpla con el estándar de autenticación IEEE 802.1x que se usó como intermediario entre la capa de acceso y el algoritmo de autenticación, finalmente se configuró con el mecanismo de autenticación WPA-Enterprise.

En el primer capítulo se definió todas las tecnologías que se emplearon en la implementación de la solución y cuál fue la evolución tecnológica para llegar a ellas. El estudio se hizo de manera separada para la LAN y para la WLAN porque al tratarse de redes con interfaces diferentes, cada una tiene definida de forma independiente métodos y estándares de seguridad para el acceso a la red.

En el segundo capítulo se planteó un estudio del problema y se le ubicó en un escenario real con el fin de especificar las exigencias de la empresa, la cual requiere una solución de una red LAN y WLAN que garantice la seguridad de la información y el uso adecuado de los recursos de la red.

En el tercer capítulo se diseñó la solución, realizando un análisis de los requerimientos propuestos en el segundo capítulo. Una vez terminado el análisis se decidió cuales de los métodos y estándares estudiados en el capítulo uno se usarían en la implementación.

En el cuarto capítulo se muestran los resultados y el análisis de la implementación de la solución diseñada en el laboratorio de redes de la especialidad

En el quinto capítulo se realizó el análisis económico para medir la rentabilidad del proyecto haciendo uso de la tasa interna de retorno (TIR) y el valor actual neto (VAN) como métodos financieros de inversión.

Dedicatoria

A mi madre Aurora García Jesús

Agradecimientos

Quiero agradecer a mis padres Carlos Lazo y Aurora García por su apoyo incondicional en todos los momentos de mi vida, a mi hermano Iván Lazo; a mis tíos: Aída, Zenaida, Bertha y Edwin García, a mi prima Hilda Vilcapoma.

A mi asesor Antonio Ocampo por su gran orientación y apoyo durante todo el desarrollo de la tesis

A todos mis amigos que compartieron conmigo la etapa universitaria.

Índice

Índice v
Lista de Figuras vi
Lista de Tablas viii
Introducción 9
Capítulo 1 Evolución y estudio de las tecnologías aplicadas en la seguridad y la optimización de las redes LAN y WLAN 10
1.1 Seguridad WLAN 10
1.1.1 Estándar de Autenticación y Encriptación IEEE 802.11i 10
1.1.1.1 Protocolos de Encriptación 11
1.1.1.2 Protocolos de confidencialidad e integridad de datos 13
1.1.1.3 IEEE 802.1x 14
1.1.1.4 EAP 16
1.1.2 RADIUS 16
1.1.2.1 Cliente RADIUS 16
1.1.2.2 Servidor RADIUS 17
1.2 Seguridad LAN 19
1.2.1 TACACS+ 19
1.2.2 ACS 22
1.3 Comparación entre servidores RADIUS y TACACS+ 23
Capítulo 2 Análisis y planteamiento de las exigencias que requiere la implementación 25
2.1 Definición del problema a resolver 25
2.2.1 Análisis del problema en un escenario inicial real 26
Capítulo 3 Diseño de la solución mediante el análisis de los requerimientos propuestos 28
3.1 Diseño de la LAN 28
3.2 Diseño de la WLAN 31
3.3 Requerimientos del diseño 33
Capítulo 4 Implementación del diseño planteado para la red y resultados de la autenticación y medición del ancho de banda 35
4.1 Implementación de la topología y configuración de la red LAN 35
4.2 Implementación del servidor ACS 38
4.3 Configuración de Clientes TACACS+ 43
4.4 Implementación del servidor RADIUS (IAS) 44
4.5 Configuración de punto de acceso inalámbrico como cliente RADIUS 48
4.6 Configuración de usuarios inalámbricos 49
4.7 Resultados en la LAN 50
4.8 Resultados en la WLAN 56
Capítulo 5 Análisis económico del proyecto 62
5.1 Análisis Económico 62
5.1.1 CAPEX 62
5.1.2 OPEX 65
5.1.3 Flujo de Caja 67
Conclusiones 71
Observaciones, Recomendaciones y Trabajos Futuros 72
Bibliografía 73

Lista de Figuras

FIGURA 1-1: PROCESO DE AUTENTICACIÓN WPA 12
FIGURA 1-2: INTERCONEXIÓN MEDIANTE IEEE 802.1X 14
FIGURA 1-3: PROCESO DE AUTENTICACIÓN IEEE 802.1X 15
FIGURA 1-4: INTERCAMBIO DE MENSAJES RADIUS 18
FIGURA 1-5: AUTENTICACIÓN TACACS+ 20
FIGURA 1-6: AUTORIZACIÓN PARA COMANDOS MEDIANTE TACACS+ 22
FIGURA 2-1: ORGANIGRAMA DE LA EMPRESA 26
FIGURA 3-1: TOPOLOGÍA FÍSICA DE LA RED LAN 31
FIGURA 3-2: TOPOLOGÍA FÍSICA DE LA RED INALÁMBRICA 32
FIGURA 3-3: TOPOLOGÍA FÍSICA DE LA RED 34
FIGURA 4-1: EMULACIÓN DE LA RED LAN EN GNS3 35
FIGURA 4-2: CONFIGURACIÓN DE SWITCHES Y ROUTERS EN GNS3 36
FIGURA 4-3: ACS EN VIRTUALBOX 38
FIGURA 4-4: EMULACIÓN DE LA RED LAN Y AUTENTICACIÓN EN GNS3 39
FIGURA 4-5: REGISTRO DE CLIENTES TACACS+ EN ACS 40
FIGURA 4-6: GRUPOS CREADOS EN EL ACS 41
FIGURA 4-7: CONFIGURACIÓN DE NIVEL MAXIMO DE PRIVILEGIO PARA EL GRUPO DE ADMINISTRADORES DE RED 41
FIGURA 4-8: CONFIGURACIÓN DE USUARIO EN EL GRUPO DE ADMINISTRADORES DE RED 42
FIGURA 4-9: CONFIGURACIÓN DE USUARIO EN EL GRUPO DE HELP DESK 43
FIGURA 4-10: ACTIVE DIRECTORY 45
FIGURA 4-11: PROPIEDADES DEL GRUPO USUARIOS INALÁMBRICOS DENTRO DEL DOMINIO 46
FIGURA 4-12: MIEMBROS DEL GRUPO USUARIOS INALÁMBRICOS 46
FIGURA 4-13: EMISOR DE CERTIFICADOS 47
FIGURA 4-14: SERVIDOR DE APLICACIONES 47
FIGURA 4-15: CONFIGURACIÓN DEL ACCESS POINT 48
FIGURA 4-16: PAGINA WEB DEL SERVIDOR DE CERTIFICADOS 49
FIGURA 4-17: DESCARGA DEL CERTIFICADO DE AUTENTICACIÓN 49
FIGURA 4-18: INSTALADOR DE CERTIFICADO 49
FIGURA 4-19: AUTENTICACIÓN Y AUTORIZACIÓN DE USUARIO DEL GRUPO ADMINISTRADORES DE RED 50
FIGURA 4-20: AUTENTICACIÓN Y AUTORIZACIÓN DE USUARIO DEL GRUPO HELP DESK 51
FIGURA 4-21: ANCHO DE BANDA EN PORT-CHANNEL CONFORMADO POR DOS ENLACES FISICOS 52
FIGURA 4-22: ANCHO DE BANDA EN PORT-CHANNEL CONFORMADO POR UN ENLACES FISICOS 52
FIGURA 4-23: DIAGRAMA GLBP 53
FIGURA 4-24: DIRECCIÓN IP DEL DEFAULT GATEWAY Y DEL SERVIDOR DHCP – PRUEBA 1 53
FIGURA 4-25: DIRECCIÓN IP DEL DEFAULT GATEWAY Y DEL SERVIDOR DHCP – PRUEBA 2 54
FIGURA 4-26: CONTINUIDAD DE PAQUETES LUEGO DE AVERIA DE UN ROUTER 55
FIGURA 4-27: PROTOCOLO GLBP – BALANCEO DE CARGA 55
FIGURA 4-28: PROTOCOLO GLBP - REDUNDANDIA 56
FIGURA 4-29: USUARIO INALAMBRICO CONECTADO A WLAN 56
FIGURA 4-30: CERTIFICADO DE AUTENTICACIÓN ISNTALADO EN USUARIO INALAMBRICO 57
FIGURA 4-31: TRAMA WIRESHARK DE INICIO DE AUTENTICACIÓN 58

FIGURA 4-32: TRAMA WIRESHARK EAP REQUEST 58
FIGURA 4-33: TRAMA WIRESHARK EAP RESPONSE 59
FIGURA 4-34: TRAMA WIRESHARK EAP-TLS ENVIADA POR ACCESS POINT 59
FIGURA 4-35: TRAMA WIRESHARK EAP-TLS ENVIADA POR USUARIO INALÁMBRICO 60
FIGURA 4-36: TRAMA WIRESHARK EAP – WPA KEY 60
FIGURA 4-37: TRAMA WIRESHARK EAP - SUCCESS 61
FIGURA 4-38: TRAMA WIRESHARK CON MENSAJES DHCP 61
FIGURA 4-39: TRAMA WIRESHARK ICMP 61
FIGURA 5-1: TASA DE RETORNO INTERNA 69
FIGURA 5-2: CURVA DE RETORNO DE LA INVERSIÓN 69

Lista de Tablas

TABLA 1-1: COMPARACIÓN ENTRE SERVIDORES DE AUTENTICACIÓN..... 19
TABLA 1-2: COMPARACIÓN ENTRE RADIUS Y TACACS+ 24
TABLA 2-1: TAMAÑO DE LA RED 26
TABLA 2-2: NIVELES DE AUTORIZACION 27
TABLA 3-1: EJEMPLO DE ASIGNACIÓN DE IPs PARA VLAN 29
TABLA 3-2: ASIGNACIÓN DE SUBREDES 30
TABLA 5-1: PAGO TOTAL A INGENIEROS POR DISEÑO 62
TABLA 5-2: PAGO TOTAL A INGENIEROS POR IMPLEMENTACIÓN..... 63
TABLA 5-3: PAGO A TÉCNICOS POR IMPLEMENTACIÓN..... 63
TABLA 5-4: INVERSIÓN EN HARDWARE PARA LA IMPLEMENTACIÓN..... 64
TABLA 5-5: INVERSION EN SOFTWARE PARA LA IMPLEMENTACION 65
TABLA 5-6: PRECIO FINAL DE IMPLEMENTACIÓN CONSIDERANDO MARGEN DE GANACIA 65
TABLA 5-7: PAGO MENSUAL INGENIERO POR MANTENIMIENTO PREVENTIVO 66
TABLA 5-8: PAGO MENSUAL INGENIERO POR MANTENIMIENTO CORRECTIVO66
TABLA 5-9: PAGO MENSUAL INGENIERO POR SOPORTE DE EMERGENCIA..... 66
TABLA 5-10: PRECIO FINAL DE OPERACIÓN Y MANTENIMIENTO CONSIDERANDO MARGEN DE GANACIA 67
TABLA 5-11: FLUJO DE CAJA..... 68

Introducción

Hoy en día estamos ante una novedosa forma de comunicación en un entorno globalizado debido al desarrollo de la Internet. Por ello, se ha hecho indispensable el aumento de la infraestructura tecnológica dentro de las empresas, tanto en la red convencional como en la red inalámbrica. Sin embargo, muchas empresas no toman en cuenta que dicha infraestructura esta en peligro por las vulnerabilidades que presenta, por lo que es necesario implementar un sistema de control de acceso a la red que permita proteger la información de posibles ataques de personas ajenas a ella mediante suplantación de identidad, lo cual podría provocar pérdidas financieras o espionaje corporativo. Para evitarlo se cuenta con estándares, protocolos y equipos que permiten construir soluciones de seguridad robustas.

La presente tesis busca diseñar e implementar una red LAN y WLAN que sea capaz de evitar la suplantación de identidad; así como reducir la brecha entre una red cableada convencional y una red inalámbrica, en términos de seguridad. Además de optimizar los recursos de la red usando Etherchannel y el protocolo GLBP como mecanismos de redundancia y control de ancho de banda mediante balanceo de carga.

El sistema de control de acceso AAA (Authentication, Authorization and Accounting) se implementó haciendo uso de los protocolos RADIUS y TACACS+, ambos protocolos son del tipo cliente/servidor. El servidor RADIUS tiene la función de autenticar a los usuarios que accedan a la red inalámbrica mientras que el servidor TACACS+ tendrá la función de administrar los perfiles de los administradores de los equipos y registrar los eventos. Para lograr un acceso seguro a la red inalámbrica se usó el estándar IEEE 802.11i (RSN, Robust Security Network) que esta basado en la encriptación AES y el mecanismo de autenticación WPA-Enterprise.

Capítulo 1

Evolución y estudio de las tecnologías aplicadas en la seguridad y la optimización de las redes LAN y WLAN

1.1 Seguridad WLAN

Las redes inalámbricas son vulnerables a diferentes tipos de ataques debido a que el aire es un medio de acceso para cualquier persona que se encuentre en la cobertura de un punto de acceso a la red, dejando la posibilidad de interceptar la transmisión de datos. Para garantizar la seguridad en este tipo de redes es necesario el cifrado de la información antes de ser enviada y la autenticación de los usuarios antes de acceder a la red.

A continuación se detallan los estándares y los protocolos utilizados en la implementación de la presente tesis.

1.1.1 Estándar de Autenticación y Encriptación IEEE 802.11i

El estándar IEEE 802.11i, también conocido como RSN (Robust Security Network), permite la implementación de una WLAN más segura a través del uso de la

encriptación y la autenticación mediante los protocolos WPA (Wi-Fi Protected Access), TKIP (Temporal Key Integrity Protocol), CCMP (Counter-mode/CBC-MAC), EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) y el estándar IEEE 802.1X. [PIN2009]

1.1.1.1 Protocolos de Encriptación

Los Protocolos de encriptación han pasado por un proceso evolutivo desde WEP hasta contar actualmente con WPA2 desarrollado dentro del estándar IEEE 802.11i.

- WEP (Wired Equivalent Privacy) es el protocolo de encriptación incluido originalmente en el estándar IEEE 802.11, emplea CRC (Cyclic Redundancy Check) como algoritmo de verificación de integridad, y como algoritmo de encriptación utiliza RC4, el cual viene acompañado de una clave secreta de 40 ó 104 bits que es combinada con el vector de inicialización (IV) de 24 bits. El envío de la clave es en texto plano, lo que lo hace vulnerable a ataques basados en el uso de analizadores de tramas (sniffers) y decodificadores de código WEP (WEP crackers). [LEH2006]

- WPA (Wi-Fi Protected Access) fortalece el algoritmo de encriptación utilizado por el WEP con el incremento de la clave secreta de 104 a 128 bits, el incremento del vector de inicialización de 24 a 48 bits y la implementación del protocolo de claves dinámicas TKIP (Temporal Key Integrity Protocol). De esta forma se soluciona el problema del tamaño y reutilización del vector, con esto se evita los ataques estadísticos que permiten recuperar la clave WEP. WPA también implementa el código MIC (Message Integrity Code) para el control de integridad, debido a que el control CRC (Cyclic Redundancy Check usado por el WEP) es inseguro al permitir alterar la información sin conocer la clave WEP para luego actualizar el CRC haciendo que el cambio no sea perceptible. [LOP2008] [WIF2009]

  Además incluye un contador de tramas para la protección contra ataques de repetición (reply attacks). Su principal mejora fue incorporar un proceso de autenticación que implementa el EAP (Extensible Authentication Protocol) y el estándar 802.1X para distribuir claves diferentes a cada usuario mediante un servidor de autenticación; sin embargo, también se puede utilizar claves

precompartidas (PSK - Pre Shared Key) para usuarios domésticos. [LOP2008] [WIF2009]

En la siguiente figura se describe el proceso de autenticación WPA:

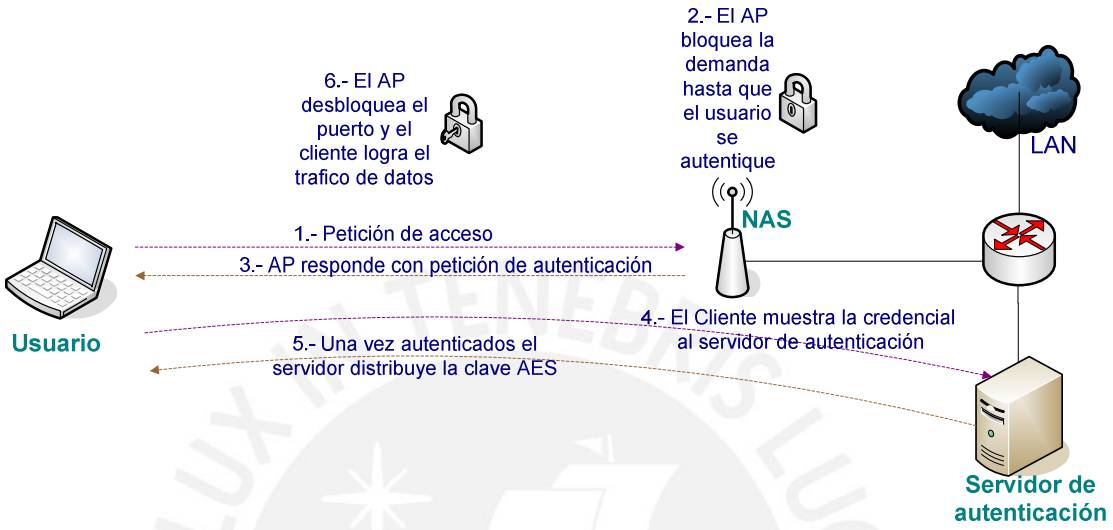

FIGURA 1-1*: PROCESO DE AUTENTICACIÓN WPA*

Fuente: "Seguridad Avanzada En Redes Inalámbricas" [PIN2009]

- WPA2 (Wi-Fi Protected Access 2) es compatible con WPA y WEP. Las principales diferencias respecto a WPA son: el empleo de otro algoritmo de cifrado, mientras WPA usa TKIP basado en RC4, WPA2 emplea CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) basado en AES; además usa la siguiente versión del código MIC para el algoritmo de control de integridad. Existen dos tipos del protocolo WPA2: Personal y Enterprise. [LOP2008] [WIF2009]

  WPA2-Personal, diseñado para uso doméstico o empresas pequeñas, encripta los datos con AES y utiliza una contraseña para establecer el acceso a la red Wi-Fi. Por otro lado, WPA2-Enterprise cifra los datos con AES, verifica la identidad de los usuarios de la red utilizando el protocolo EAP y ofrece cinco tipos de EAP para atender a una variedad de escenarios y tipos de dispositivos. [LOP2008] [WIF2009]

1.1.1.2 Protocolos de confidencialidad e integridad de datos

Los Protocolos de confidencialidad e integridad de datos han pasado por un proceso evolutivo desde TKIP incorporado en el protocolo de encriptación WAP hasta el protocolo CCMP incorporado en el protocolo de encriptación WAP2.

- **TKIP (Temporal Key Integrity Protocol):** Protocolo de integridad de clave temporal, surgió como una actualización (Wi-Fi CERTIFIED nombra esta actualización como WAP) para reforzar los sistemas WEP, sin tener que cambiar el antiguo hardware de red. Por ello, al igual que WEP, se basa en el algoritmo de encriptación RC4, lo que acarrea limitaciones de seguridad que son remediadas con la desconexión de 60 segundos y establecimiento de nuevas claves cuando se produzcan más de 2 fallas de MIC por minuto.
  Corrige las siguientes vulnerabilidades de WEP:
  - Integridad de mensaje: Lo logra usando un nuevo control de integridad del mensaje MIC basado en el algoritmo Michael de Niels Ferguson con 20 bits de seguridad, que impide la modificación de los datos dentro de un paquete mientras es trasmitido.
  - Reutilización de claves de inicialización: Incluye nuevas reglas de selección y va incrementando su valor, evitando su reutilización, genera una nueva clave cada 10000 paquetes o 10 Kbytes de información trasmitida.
  - Gestión de claves: Aplica el algoritmo “hash” al vector de inicialización para la distribución y modificación de claves. Ahora el vertor de inicialización es encriptado y repartido por distintas ubicaciones del paquete.

  [LEH2006] [WIF2009] [MED2009]

- **WRAP (Wireless Robust Authenticated Protocol):** Basado en el algoritmo de encriptación AES, fue el primer protocolo elegido por el estándar IEEE 802.11i, pero se abandonó por motivos de propiedad intelectual y posibles licencias. [LEH2006] [MED2009]

- **CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol):** A diferencia de TKIP, este protocolo no nació para acomodarse al hardware WEP, por ello tiene un nuevo diseño basado en el algoritmo de encriptación de bloques AES (cuenta con un contador extra inicializado en 1 y se incrementa en cada bloque). Además utiliza el método de autenticación de

mensajes CBC – MAC (Cipher Block Chaining) para producir un MIC. Usa una clave única pero con diferentes vectores de inicialización, el vector es incrementado en cada fragmento del paquete. La cabecera CCMP no viaja encriptada pero los datos si, incluido el vector. [LEH2006] [MED2009]

1.1.1.3 IEEE 802.1x

Estándar de autenticación conocido como Port-Based Network Access Control, originalmente fue desarrollado para redes cableadas, ahora también ha sido adoptado por las redes inalámbricas. Establece una capa entre la capa de acceso y los diferentes algoritmos de autenticación, donde traduce las tramas enviadas a un formato entendible por el sistema de autenticación que utilice la red. Para autenticar al cliente móvil usa el protocolo EAP y para controlar el proceso de autenticación en la red usa PAE (Port Authentication Entity). [LEH2006][LOP2008]

En la siguiente figura se muestra la interconexión de los protocolos de autenticación y las diversas redes mediante 802.1x

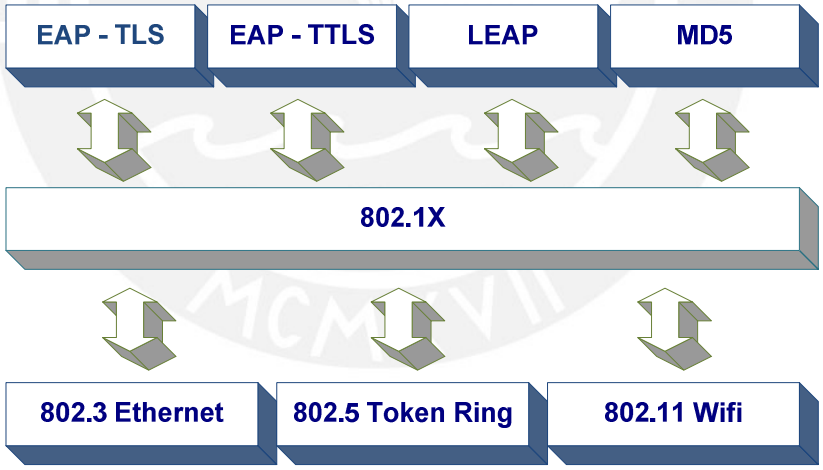

FIGURA 1-2*: INTERCONEXIÓN MEDIANTE IEEE 802.1X*

Fuente: "Seguridad Avanzada En Redes Inalámbricas" [PIN2009]

Esta compuesta por tres entidades funcionales: el usuario (suplicante), el NAS (Network Access Server) o autenticador y el servidor de autenticación. La autenticación de mensajes se incorpora para asegurar que el usuario y el NAS calculen sus claves secretas y activen la encriptación antes de acceder a la red, se

comunican mediante el protocolo EAP. El NAS cumple un rol pasivo, pues se limita a enviar los mensajes al servidor de autenticación, EAP es un entorno para el transporte de varios métodos de autenticación, una vez terminado el proceso ambas entidades tendrá una clave maestra secreta (MK). EAP es transportado por el protocolo EAPOL (EAP Over LAN). [LEH2006][LOP2008]

La comunicación entre NAS y servidor de autenticación requiere un protocolo de capa más alta, como RADIUS si usamos un servidor RADIUS. Este proceso finaliza cuando el servidor envíe un mensaje "Radius Accept" que contiene la MK y un mensaje final "EAP Success" para el usuario. [LEH2006][LOP2008]

En la siguiente figura se muestra el proceso de autenticación IEEE 802.1X

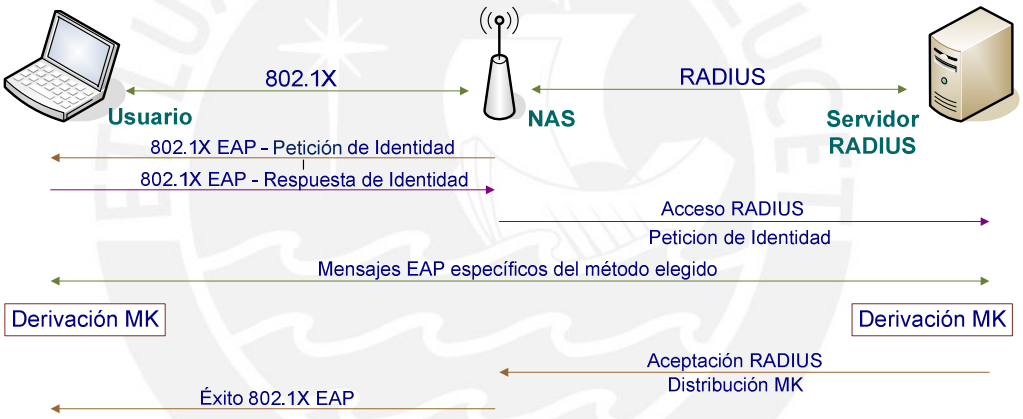

FIGURA 1-3*: PROCESO DE AUTENTICACIÓN IEEE 802.1X*

Fuente: "Seguridad Wi-Fi – WEP, WPA y WPA2" [LEH2006]

Este estándar trae las siguientes ventajas:

- Alto nivel de seguridad porque puede usar nombres de usuarios y contraseñas o certificados de usuario
- Cifrado mas seguro
- Autenticación y cohesión a la WLAN transparentes
- Autenticación por separado de usuarios y de equipos
- Bajo costo de hardware de red
- Alto rendimiento porque el cifrado se lleva a cabo en el hardware de la WLAN y no en el procesador del equipo cliente

[PIN2009]

1.1.1.4 EAP

EAP (Extensible Authentication Protocol) es una extensión del protocolo PPP (Point-to-point Protocol), proporciona un mecanismo estándar para aceptar métodos de autenticación, al usar EAP se puede agregar varios esquemas de autenticación como: RADIUS, Kerberos, tarjetas de identificación, certificados entre otros.

Al usar EAP, cuando se de una nueva petición de conexión a un punto de acceso (NAS), este consulta la veracidad del dispositivo móvil al servidor de autenticación, una vez comprobada el servidor envía una respuesta de conclusión de autenticación al punto de acceso, solo si la respuesta fue satisfactoria. Por esta razón los puntos de acceso que implementen EAP no necesitan implementar un método concreto de autenticación, actuando como simples pasarelas entre el dispositivo móvil y el servidor de autenticación.

Entre los principales métodos de autenticación tenemos: EAP-TLS. EAP-TTLS, PEAP, EAP–SIM. Algunos fabricantes de puntos de acceso inalámbricos han implementado sus propias versiones de EAP, como Cisco, que incorpora en algunos de sus puntos de acceso el Protocolo de Autenticación Extensible Ligero (LEAP).
[LOP2008][PIN2009]

1.1.2 RADIUS

RADIUS (Remote Authentication Dial-In User Server) es un protocolo cliente/servidor, donde el cliente es un NAS (Network Access Server) y el servidor es un software ejecutado en un equipo UNIX, LINUX o Windows. Como protocolo de transporte emplea UDP, para establecer comunicación utiliza dos puertos: el 1813 para contabilidad y el 1812 para autenticación y autorización. [LOP2008] [TEC2008]

1.1.2.1 Cliente RADIUS

También denominado NAS, es un equipo de comunicación, puede ser un access point, un switch, un RAS entre otros, los cuales serán la puerta de ingreso a la red, al cual los usuarios se conectan físicamente por medio de cable, wireless, ADSL o RTB.
Este punto de paso entre el cliente y el servidor será el encargado de derivar las peticiones de acceso a los servidores, y acuerdo a la respuesta recibida del servidor dará permiso o negara acceso al usuario.

Para su correcto funcionamiento el cliente requiere los siguientes datos:

- Dirección IP o nombre del servidor RADIUS
- Puerto de autenticación y autorización
- Puerto de contabilidad, por donde recibe los eventos de conexión
- Clave de autorización, que codifica la información enviada en la negociación con el servidor.

[LOP2008] [TEC2008]

1.1.2.2 Servidor RADIUS

Software instalado como servicio en el sistema operativo de una computadora, es el encargado de administrar las cuentas de acceso. Recibe la autenticación y luego de realizar la comparación con sus registros envía un mensaje permitiendo o negando el acceso, además ira almacenando los eventos de dichos procesos. Para aceptar las consultas del cliente debe tener un perfil del NAS con la dirección IP del cliente y la clave de autorización.

[LOP2008] [TEC2008]

En la comunicación con el cliente, se intercambian los siguientes mensajes:

- Access - Request: Solicitud de atención para autenticación
- Access - Accept: Acepta la autenticación
- Access - Reject: No acepta la autenticación
- Accounting - Request: Registra eventos
- Accounting – Response: Confirmación de evento registrado

En la siguiente figura se muestra la secuencia de intercambio de mensajes

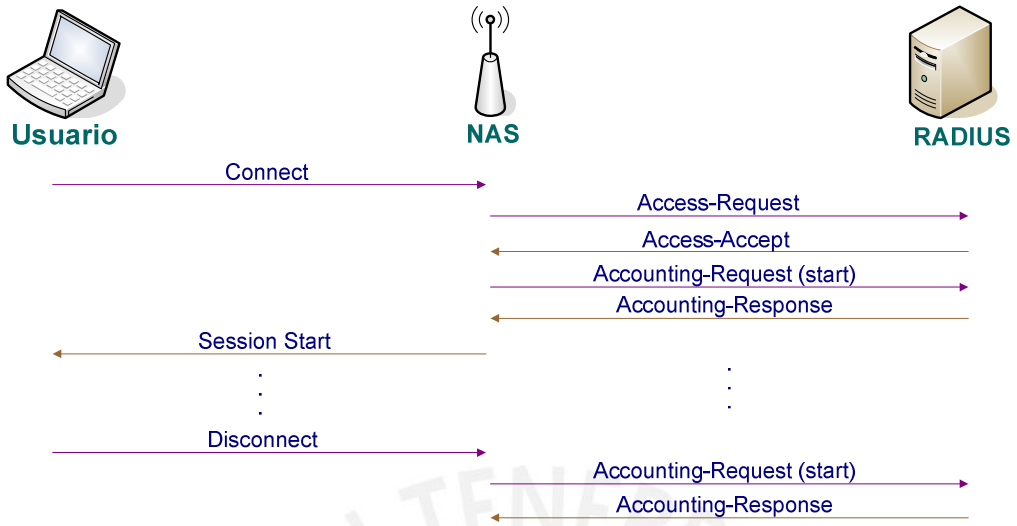

FIGURA 1-4*: INTERCAMBIO DE MENSAJES RADIUS*

Fuente: "Sistema de Autenticación y Cifrado" [TEC2008]

Dentro de los mensajes se envían atributos que contienen información necesaria para una adecuada comunicación. A continuación se detalla los atributos que son transportados en cada mensaje:

Access – Request

- User - Name: Cuenta del usuario
- User - Password: Pasword del usuario

Access – Accept

- Frame - IP - Address: Dirección IP a entregar
- Frame - IP - Netmask: Mascara de la dirección IP a entregar

Accounting – Request

- Acct - Status - Type: Estado de conexión
- Acct - session Time: Tiempo de sesión
- Acct - Terminate - Cause: Causa de desconexión

[LOP2008] [TEC2008]

En la tabla 1.1 se hace una breve comparación de los principales servidores de autenticación.

TABLA 1-1: COMPARACIÓN ENTRE SERVIDORES DE AUTENTICACIÓN

Nombre	S.O.	802.1x	Libre
IAS Windows	Windows	TLS, PEAP Y LEAP	No
Tekradius	Windows	MD5, PEAP y TLS	Sí
EmeraldV5	Windows Linux	PEAP, TTLS y LEAP	No
RAD-series	Windows	MD5, TLS, PEAP, TTLS y LEAP	No
Odyssey	Windows	MD5, TLS, PEAP, TTLS y LEAP	No
Steef Belted Radius 4.0	Windows Sun Solaris	MD5, TLS, PEAP, TTLS y LEAP	No
FreeRadius	Linux	MD5, TLS, PEAP, TTLS y LEAP	Sí

Fuente: “Seguridad en WLAN IEEE 802.11” [MED2009]

1.2 Seguridad LAN

Para controlar las conexiones dentro de misma la LAN, se va contar con un sistema centralizado de administración de cuentas de los usuarios para el acceso a los recursos de la red y administración de todos los dispositivos de la red. Lo cual va proveer un mayor grado de escalabilidad a nivel de línea y una administración rápida y precisa para el control de acceso de usuarios y administración de los dispositivos.

El encargado de esta administración será un servidor de autenticación TACACS+, basado en el protocolo de su mismo nombre, fue desarrollado por Cisco Systems. Al igual que RADIUS es un protocolo de control de acceso, y trabaja bajo el modelo cliente/servidor. Los clientes serán todos los equipos de red (switches y routers) que tengan integrados un cliente AAA, obligando al usuario a establecer comunicacion con el servidor, para enviar una credencial que permitirá la habilitación del puerto. [CRA2004] [TEC2008]

1.2.1 TACACS+

TACACS+ es un protocolo de la capa de aplicación, usa TCP como protocolo de transporte (garantizando la transmisión) que tiene como puerto asociado al 49, cifra todo el cuerpo del paquete, pero dejará la cabecera TACACS+ intacta. Separa autenticación, autorización, y contabilidad. [CRA2004]

Cada transacción entre el cliente y servidor AAA usa una conexión dedicada TCP. Pero para tener menos carga en el servidor y una mejor detección de caídas en la comunicación también una sola sesión puede ser establecida. Esta sesión permanece mientras el servidor o el dispositivo de red se encuentren operacionales. [CIS2009]

- **Autenticación TACACS+:**

  El proceso de autenticación es manejado por el servidor TACACS+, mediante el protocolo TACACS+, se da por medio de una comunicación arbitraria que recopila suficiente información para autenticar al usuario. Normalmente esta información es el usuario y password, pero además puede incluir otros ítems como: nombre de tu mejor amigo, pasatiempo preferido, entre otros similares. [CIS2009]

En la siguiente figura se muestra la secuencia de mensajes TACACS+ que son intercambiados entre el usuario, el NAS y el servidor cuando se produce la autenticación de un usuario

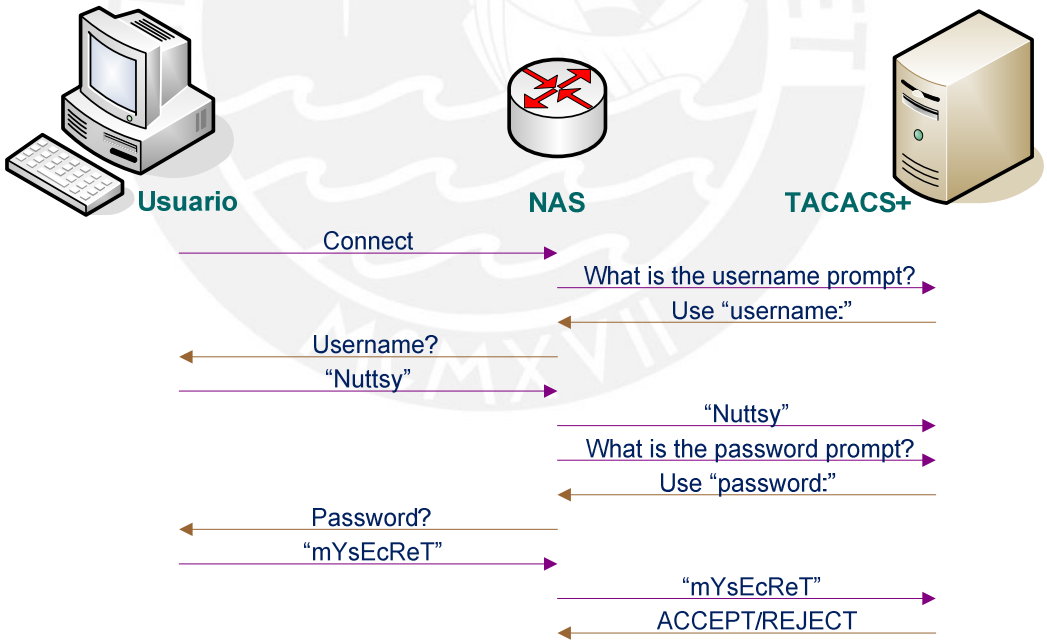

FIGURA 1-5*: AUTENTICACIÓN TACACS+*

Fuente: "Servidor TACACS+" [CIS2009]

Al igual que el protocolo RADIUS, TACACS+ realiza la comunicación entre el servidor y el usuario por medio de un cliente TACACS+ el cual brindara acceso o lo negara dependiendo de la respuesta dada por el servidor, estas pueden ser:

- ACCEPT: Acepta la autenticación y si el cliente esta configurado para solicitar autorización, comenzara en este momento
- REJECT: No acepta la autenticación
- ERROR: Informa que ocurrió en error durante la autenticación, puede ocurrir en la conexión con el servidor o en el mismo servidor. Luego de este mensaje el cliente intenta utilizar un método alternativo para la autenticación
- CONTINUE: Manda que el usuario realice autenticaciones adicionales

[CIS2009]

- **Autorización TACACS+:**

  Si la autenticación se realizo de manera correcta y el cliente tiene habilitada la fase de autorización, el usuario debe continuar con esta.

  Para ello el cliente se contacta nuevamente con el servidor, para recibir una respuesta que puede ser:

  - ACCEPT: Acepta la autorización, y contiene información en forma de atributos que determinaran a que servicios puede acceder el usuario.
  - REJECT: Autorización denegada

  Entre los atributos contenidos en el mensaje ACCEPT están: parámetros de conexión, host o dirección IP, ACL, Timeouts para el usuario.

  Este control de acceso a los servicios de la red representa una gran medida de seguridad. Además el contar con un control de acceso a comandos de configuración restringe de manera significativa los ataques internos. El proceso de autorización de comandos se realizara cada vez que el usuario ingrese un comando, para que el servidor pueda determinar si es aceptado o rechazado de acuerdo al perfil del usuario.

  [CRA2004] [CIS2009]

  En la siguiente figura se muestra el proceso de autorización para comandos.

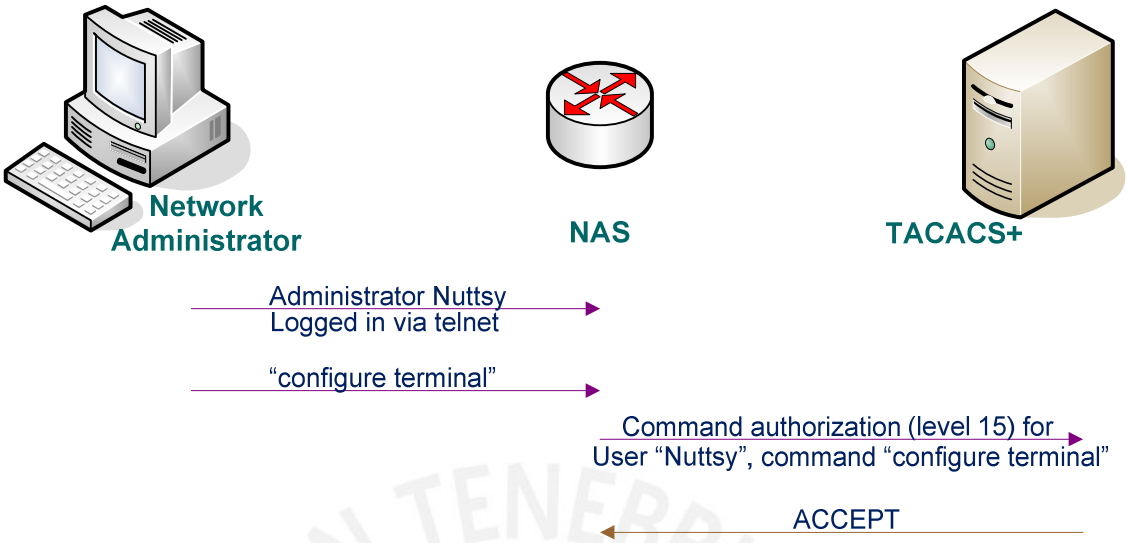

FIGURA 1-6*: AUTORIZACIÓN PARA COMANDOS MEDIANTE TACACS+*

Fuente: "Servidor TACACS+" [CIS2009]

- **Contabilidad TACACS+:**

  El servidor se encarga de registrar los diversos eventos, para ellos realiza un seguimiento previo a cada sesión que se establece a través de este, para luego almacenarla en un archivo de log o en una base de datos dependiendo de la configuración. Los archivos de logs son fácilmente exportables a diferentes tipos de base de datos o archivos de hoja de cálculo. Esta información es muy útil para la administración de la red, auditorias de las cuentas, sistemas billing y generación de reportes. [CRA2004] [CIS2009]

1.2.2 ACS

ACS (Access Control Server) es una solución de Cisco para proveer un servidor AAA altamente escalable, optimo para el control de acceso opera como servidor centralizado TACACS+ o RADIUS, para su instalación requiere que el sistema operativo sea Windows Server, además de las características brindadas por el protocolo AAA con que decida trabajar, cuenta con las siguientes características:

- Define diferentes niveles de servicio por usuario o por grupo, una vez que la autenticación se ha dado de manera correcta, ACS envía un profile del usuario al cliente, conteniendo políticas que indicaran a que servicios de la red puede acceder dicho usuario

- Los accesos pueden ser diferenciados por: servicios, tiempo de acceso, y niveles de seguridad. Además puede aplicar políticas de control acceso ACL, restringiendo el acceso a determinadas áreas.
- Puede deshabilitar cuentas cuando se producen reintentos fallidos de ingreso o por vencimiento en la fecha.

Componentes internos de ACS:

ACS esta formado por 7 capas las cuales son instaladas como servicios en Windows al momento de instalar el programa:

- CSAdmin: Provee la interfaz web para la administración, soporta múltiples procesos que permiten múltiples sesiones, por defecto usa el protocolo HTTP en el puerto 2002.
- CSAuth: Provee el servicio de autenticación, permitiendo o negando el acceso, maneja la base de datos ACS o reenvía la autenticación a una base de datos externa.
- CSDBSync: Maneja la sincronización y replicación de la base de datos hacia otros servidores AAA ACS
- CSLog: Provee el servicio de logging, para la contabilidad y actividad del sistema. Para ello monitorea y registra: actividades de los usuarios y administradores, backups y restauraciones, replicación de bases de datos, sincronización, servicios centrales de ACS, contabilidad TACACS+, contabilidad VoIP.
- CSTacacs: Provee comunicación entre clientes TACACS+ y el servicio CSAuth.
- CSRadius: Provee comunicación entre clientes RADIUS y el servicio CSAuth.
- CSMon: Monitorea el estado de los servicios ACS y los recursos, registra y reporta todos los errores críticos, envía alertas vía e-mail al administrador, realiza test de login.

[TEC2008]

1.3 Comparación entre servidores RADIUS y TACACS+

Una diferencia entre TACACS+ y RADIUS, es que TACACS+ utiliza TCP como protocolo de transporte mientras que RADIUS utiliza UDP. Debido a esto el protocolo TACACS+ es más confiable que el protocolo RADIUS porque tendrá retransmisión de mensajes en caso se produzca una pérdida.

Otras diferencias notables entre RADIUS y TACACS+ esta en que RADIUS sólo encripta la contraseña en la petición de acceso hasta un máximo de 16 bytes TACACS +, por otra parte, cifra todo el cuerpo del paquete, pero dejará la cabecera TACACS+ intacta. Por ello podemos decir que la encriptación que maneja el protocolo TACACS+ es más robusta que la encriptación usada por el protocolo RADIUS

Además RADIUS combina la autenticación y la autorización como un solo servicio, mientras TACACS+ los ofrece como servicios independientes. Esto hace que TACACS+ pueda ser utilizado en implementaciones donde no solo se requiera autenticarse sino que se requiera definir diversos niveles de autorización.

Por otro lado el protocolo RADIUS es libre mientras que TACACS+ al ser un protocolo propietario de Cisco requiere de una licencia para su implementación.
[CRA2004]

TABLA 1-2: COMPARACIÓN ENTRE RADIUS Y TACACS+

Nombre	Protocolo de Transporte	Parte de Encriptación	Autenticación y Autorización	Licencia
RADIUS	UDP	La contraseña	Combina como un solo servicio	Libre
TACACS+	TCP	Cuerpo del paquete TACACS+	Servicios independientes	Propietaria CISCO

Fuente: “Security Protocols Used for AAA Services” [CRA2004]

Capítulo 2

Análisis y planteamiento de las exigencias que requiere la implementación

2.1 Definición del problema a resolver

La seguridad informática es vulnerada fácilmente en muchas empresas y actualmente han surgido nuevas técnicas de robo informático: técnicas de suplantación de identidad, donde individuos u organizaciones ajenas acceden a la red para manipular información confidencial que puede tener la empresa, trayendo pérdidas financieras y espionaje corporativo.

La vulnerabilidad de las redes inalámbricas es el medio de transporte, ya que el aire es un medio de acceso para cualquier persona. Por lo tanto cualquiera que capte señal del punto de acceso, podrá acceder a la red. Con la posibilidad de navegar gratis en Internet, emplear la red como punto de ataque hacia otras redes, robar software o información, introducir virus o software maligno, entre otras cosas.

Además los dispositivos de acceso son manejados con niveles de autorización de forma individual, donde es necesario registrar a los usuarios en cada dispositivo. Lo cual demanda al administrador mayor tiempo para gestionar el acceso de autorización, ocasionando que con el tiempo se pierda este control y eso causa que se dejen puertos abiertos para el ingreso de usuarios no autorizados o de usuarios con cuentas caducadas.

2.2.1 Análisis del problema en un escenario inicial real

La empresa MindTek ha sido creada recientemente y requiere el diseño y la implementación de su red, para ellos se sabe que tiene un local central de dos pisos, donde trabajarán 120 usuarios, ubicados en diversas áreas de trabajo. De acuerdo al organigrama de la empresa:

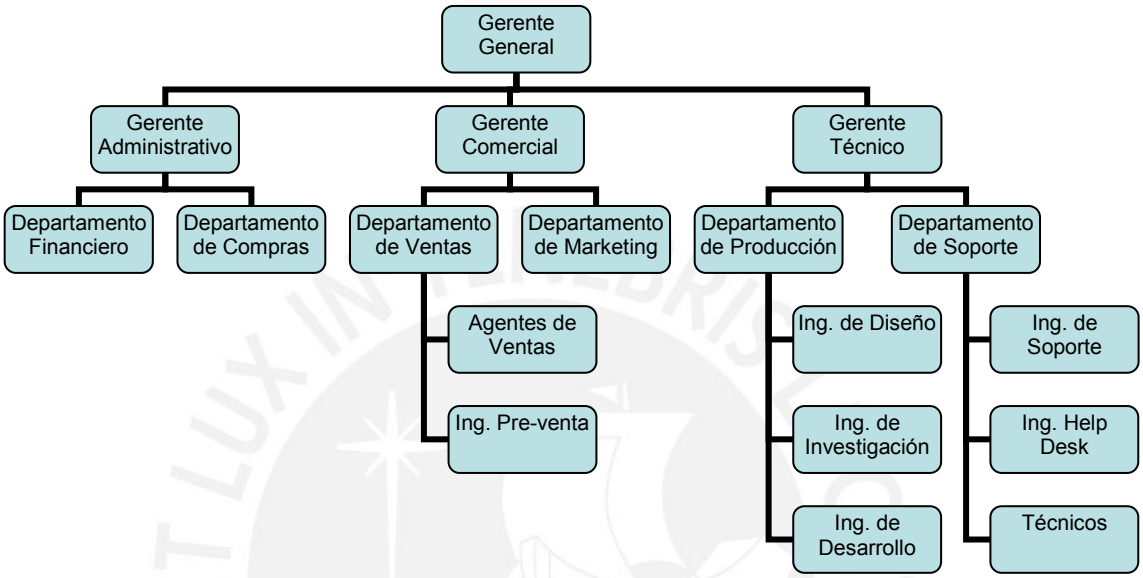

FIGURA 2- 1*: ORGANIGRAMA DE LA EMPRESA*

Fuente: Elaboración propia

Cada usuario tendrá asignado una computadora para realizar su trabajo, dependiendo de sus necesidades algunos tendrán PCs y otros tendrán Laptops:

TABLA 2- 1: TAMAÑO DE LA RED

Área	Número de Computadoras Personales	Número de Laptops
Ventas	10	10
Marketing	10	10
Soporte	20	10
Administración	20	5
Producción	20	5

Fuente: Elaboración propia

Estos usuarios podrán acceder a los equipos de la red de acuerdo a su nivel de autorización, definidos en los siguientes grupos:

TABLA 2- 2: NIVELES DE AUTORIZACIÓN

Usuario	Acceso a Equipos	Ejecución de Comandos
Administrador de Red	Equipos de toda la Red	Todos los comandos
Help Desk	Equipos de toda la Red	Comandos para ver configuración
General	Ninguno	Ninguno

Fuente: Elaboración propia

La infraestructura del local, no permite realizar un cableado horizontal en todas las áreas de trabajo, y por ello se ha decidido implementar un red inalámbrica para que pueda cubrirlas, además será utilizada por usuarios que tengan dispositivos portátiles como Pockets PCs, laptops, palms, y en lugares donde los puntos de red no sean suficientes, como en la sala de reuniones. Esta red debe contar con un sistema de gestión de control de acceso a los usuarios por seguridad.

El administrador de la red será el encargado de otorgar privilegios a los grupos, o de manera individual a los usuarios que lo requieran, además debe estar informado de todos los eventos de la red. Por seguridad se requiere que la topología de la red no sea descubierta. También se requiere optimizar el uso de recursos a través de la implementación de un adecuado balanceo de carga y dimensionamiento de enlaces.

Capítulo 3

Diseño de la solución mediante el análisis de los requerimientos propuestos

Para implementar una red segura debemos tener una visión separa de la red LAN y la WLAN porque ambas usan interfaces de comunicación diferentes, por lo tanto las tecnologías, protocolos y estándares son diferentes. El sistema de seguridad debe ser diseñado de acuerdo a la infraestructura de cada una.

3.1 Diseño de la LAN

Definiremos la topología de la red LAN, el servidor de autenticación a utilizar en la implementación, distribución de direcciones IP dentro de la red y la configuración adecuada para su funcionamiento.

La empresa Mindtek cuenta con 120 empleados, para que la red sea escalable en 5 años se debe tomar 50% de crecimiento, con lo cual tendremos que realizar el dimensionamiento para 180 usuarios. Además se tendrá en cuenta el organigrama de la empresa para la adecuada segmentación y ordenamiento de la red, se ha considerado que en cada área habrá aproximadamente 25 usuarios y 50 usuarios inalámbricos.

Respecto al direccionamiento IP, se decidió utilizar dos redes clase C tomando en cuenta el número de usuarios de la empresa, una para la red LAN y otra para la red WLAN. La red LAN estará dividida en subredes mediante un mecanismo de subneteo,

asimismo se implementará un sistema de VLANs para segmentar la red de manera mas óptima y segura. A cada VLAN le corresponderá una subred.

Se tiene que como máximo van a haber 25 usuarios por cada área, lo que quiere decir que se deberá usar 5 bits para el host. Esto nos da un total de 32 direcciones IP para cada departamento, de las cuales se reservarán 3 direcciones para el gateway, la red y el broadcast.

192.168.10.0 0 0 0 0 0 0 0 / 27
Red Host

Por ejemplo para la primera subred 192.168.10.0/27, que corresponde a la VLAN 3 - Administrativa, se tiene el siguiente direccionamiento:

TABLA 3- 1: EJEMPLO DE ASIGNACIÓN DE IPs PARA VLAN

Dirección IP	Máscara	Uso
192.168.10.0	255.255.255.224	Red
192.168.10.1	255.255.255.224	Gateway
192.168.10.2	255.255.255.224	Host
192.168.10.3	255.255.255.224	Host
192.168.10.4	255.255.255.224	Host
192.168.10.5	255.255.255.224	Host
192.168.10.6	255.255.255.224	Host
192.168.10.7	255.255.255.224	Host
192.168.10.8	255.255.255.224	Host
192.168.10.9	255.255.255.224	Host
192.168.10.10	255.255.255.224	Host
…	255.255.255.224	Host
192.168.10.28	255.255.255.224	Host
192.168.10.29	255.255.255.224	Host
192.168.10.30	255.255.255.224	Host
192.168.10.31	255.255.255.224	Broadcast

Fuente: Elaboración propia

Teniendo en cuenta el ejemplo anterior la segmentación de la red y la asignación de direcciones IPs para las diversas áreas de la red LAN y para la WLAN se realizará de la siguiente manera:

TABLA 3- 2: ASIGNACIÓN DE SUBREDES

VLAN ID	VLAN	Dirección de Red	Máscara
3	Administrativa	192.168.10.0	255.255.255.224
20	Ventas	192.168.10.32	255.255.255.224
30	Marketing	192.168.10.64	255.255.255.224
40	Soporte	192.168.10.96	255.255.255.224
50	Administración	192.168.10.128	255.255.255.224
60	Producción	192.168.10.160	255.255.255.224
70	Visitantes	192.168.10.192	255.255.255.224
10	WLAN	192.168.20.0	255.255.255.0

Fuente: Elaboración propia

Para evitar los bucles lógicos en la red LAN se implementará el protocolo RSTP (Rapid Spanning Tree Protocol) para conseguir una convergencia rápida para optimizar la red. Además implementaremos Etherchannel para optimizar los enlaces de los switches, agrupando dos enlaces FastEthernet en una solo interfaz lógica (Port-channel), con ello podremos ampliar el ancho de banda a 400 Mbps, obtener balanceo de carga entre las interfaces físicas del Port-channel y redundancia de enlace, ya que si una interfaz física deja de funcionar las tramas serán recibidas por el enlace restante. Como protocolos de negociación tenemos: PAgP (Port Aggregation Protocol) propietario de Cisco y LACP (Link Aggregation Control Protocol) descrito en la norma IEEE 802.3ad, ambos protocolos se configuran de forma similar; sin embargo, usaremos PAgP porque tiene como ventaja la modificación automática del Port-channel en un extremo si el otro extremo es modificado.

Para implementar redundancia al gateway de la red tenemos dos protocolos: Protocolo de intercambio para Router HSRP (Hot Standby Router Protocol) y GLBP (Gateway Load Balacing Protocol), usaremos GLBP porque además de brindar redundancia como HSRP, ofrece balanceo de carga. Asociaremos dos routers en un grupo GLBP y funcionarán como un solo router virtual, haciendo ambos el trabajo de reenvío de paquetes de manera balanceada. Utilizaremos Round Robin como tipo de balanceo de carga, esto será transparente para los usuarios porque ellos direccionan a una misma

puerta de enlace (IP virtual de router), pero el balanceo se dará por las MACs virtuales que el protocolo GLBP enviará como respuesta a los mensajes ARP de los clientes.

Para autenticar a los usuarios y centralizar el control de acceso a los equipos de la red instalaremos un servidor ACS, pues soporta el protocolo TACACS+. Su principal función es la gestión de acceso de acuerdo al nivel de autorización de cada usuario o grupo de usuarios, esto gracias que tiene separada la autenticación de la autorización permitiendo el filtrado de comandos, además debe registrar todos estos eventos para que el administrador pueda acceder a ellos. [TEC2008]

La topología de la red será la siguiente:

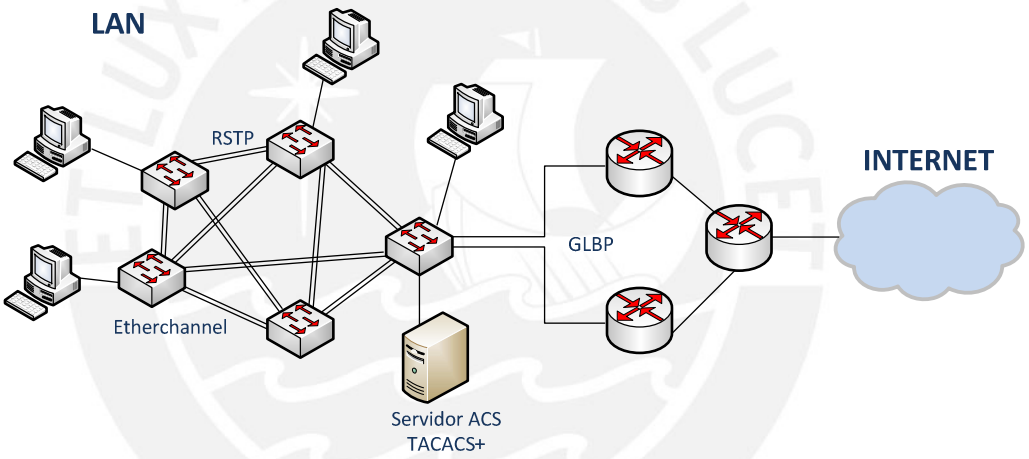

FIGURA 3- 1*: TOPOLOGÍA FÍSICA DE LA RED LAN*

Fuente: Elaboración propia

3.2 Diseño de la WLAN

Ahora definiremos la topología de la WLAN, los servidores a utilizar en la implementación, el access point y la configuración adecuada para su funcionamiento.
Cuando la red LAN ya esta implementada y la WLAN cuenta con una VLAN debemos implementar el servidor de autenticación. Tomando en cuenta el análisis comparativo de los diversos servidores RADIUS realizado en el capítulo 1, se ha optado por implementar el ISA Windows (Internet Authentication Service) porque este servicio viene con la licencia del sistema operativo Windows 2000 en adelante. No se ha

tomado en cuenta a los servidores con sistema operativo Linux pues la empresa no cuenta con soporte para este sistema operativo, por lo cual no se le puede garantizar eficiencia en el servicio.

Antes de habilitar el IAS se debe contar con otros servicios que se levantarán en el mismo Server 2003. Primero debemos definir un grupo en el Active Directory del servidor, el cual tiene como función almacenar los usuarios que van a poder acceder a la red. Luego se va habilitar el servicio de emisión de certificados de autenticación, al cual solo podrán acceder los usuarios pertenecientes al dominio creado en el Active Directory. Finalmente se habilitara el IAS donde se debe configurar el cliente RADIUS y las directivas de acceso.

El AP (Access Point) será el cliente RADIUS, es decir será el encargado de establecer la comunicación entre el usuario inalámbrico y el servidor de autenticación. Para ello debe ser configurado con los mismos protocolos de autenticación y cifrado que se configuro en el servidor RADIUS. Para que la autenticación se realice de manera exitosa el usuario debe contar previamente con un certificado de autenticación otorgado por el servidor de certificados.

La siguiente será la topología de la WLAN:

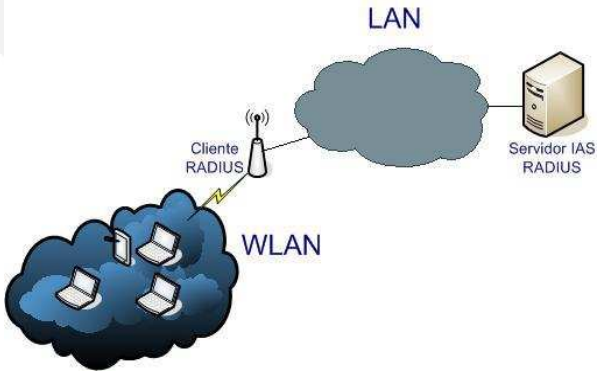

FIGURA 3- 2*: TOPOLOGÍA FÍSICA DE LA RED INALÁMBRICA*

Fuente: Elaboración propia

3.3 Requerimientos del diseño

- **Punto de Acceso Inalámbrico (Access Point – AP)**

  Para el acceso inalámbrico se va contar con un AP que será el encargado de comunicar a los usuarios con el servidor de autenticación (RADIUS), cumplirá el rol de cliente RADIUS, este deberá soportar como mecanismo de autenticación a WPA-Enterprise (basado en el estándar IEEE 802.11i y cifrado AES) y su mecanismo de autenticación debe estar basado en el estándar IEEE 802.1x (con EAP y PAE). La empresa cuenta con 50 usuarios inalámbricos.

- **Servidor RADIUS**

  El encargado de autenticar a los usuarios antes de permitir su acceso a la red va ser el servidor RADIUS, para ello se va instalar el servicio IAS en una PC con sistema operativo Windows Server 2003. La empresa MindTek únicamente cuenta con licencia para este sistema operativo.

- **Servidor ACS**

  Este servidor será el encargado de centralizar los perfiles de los administradores de red y realizar el registro de eventos, para su implementarlo se requiere una PC con sistema operativo Windows Server 2003. Se usó una versión del software ACS descargado de la página WEB de Cisco y no el hardware de Cisco, para este tipo de implementación, la configuración y el rendimiento de ambos (software y hardware ACS) es similar.

- **Switches**

  La empresa cuenta con 120 usuarios cada uno cuenta con una PC o Laptop, tomando en consideración el crecimiento de la red a 5 años se contara con 180 usuarios. Para cubrir dicho número de usuarios vamos a necesitar 4 switches de 48 puertos, por donde se comunicarán el servidor ACS (usando el protocolo TACACS+) y los equipos de la LAN. También se comunicarán por ahí el servidor RADIUS y el Cliente RADIUS y los usuarios inalámbricos.

- **Routers**

  Tendrá la función de puerta de enlace de la red y de servidor DHCP, se usarán dos routers en redundancia de acceso con balanceo de carga para ofrecer mayor calidad de servicio mediante GLBP.

La siguiente topología de la red en conjunto será la siguiente:

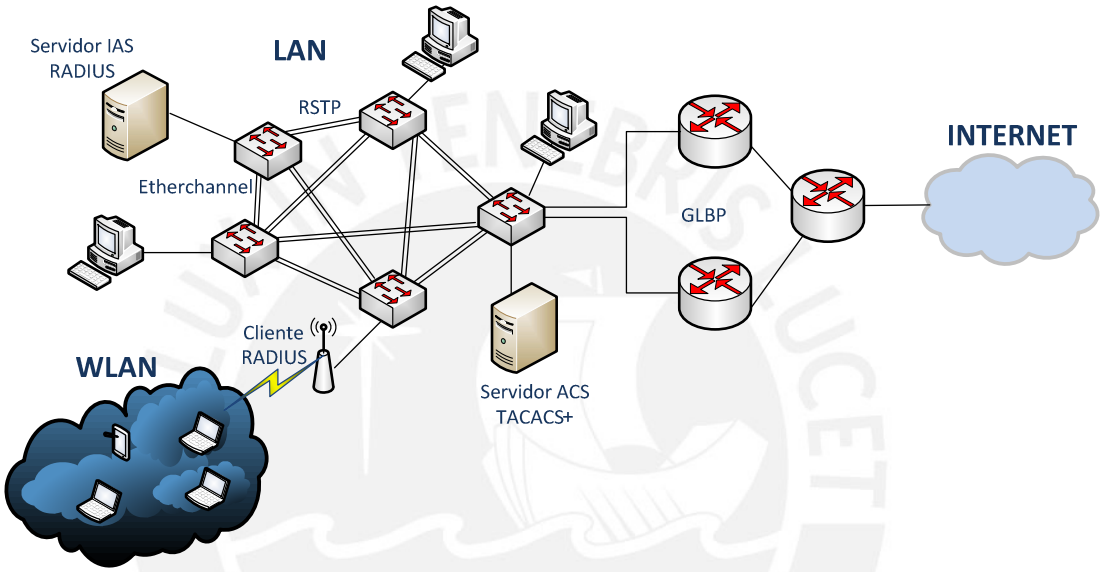

FIGURA 3- 3*: TOPOLOGÍA FÍSICA DE LA RED*

Fuente: Elaboración propia

Capítulo 4

Implementación del diseño planteado para la red y resultados de la autenticación y medición del ancho de banda

4.1 Implementación de la topología y configuración de la red LAN

Antes de realizar la implementación se realizó una emulación de red LAN usando el emulador GNS3:

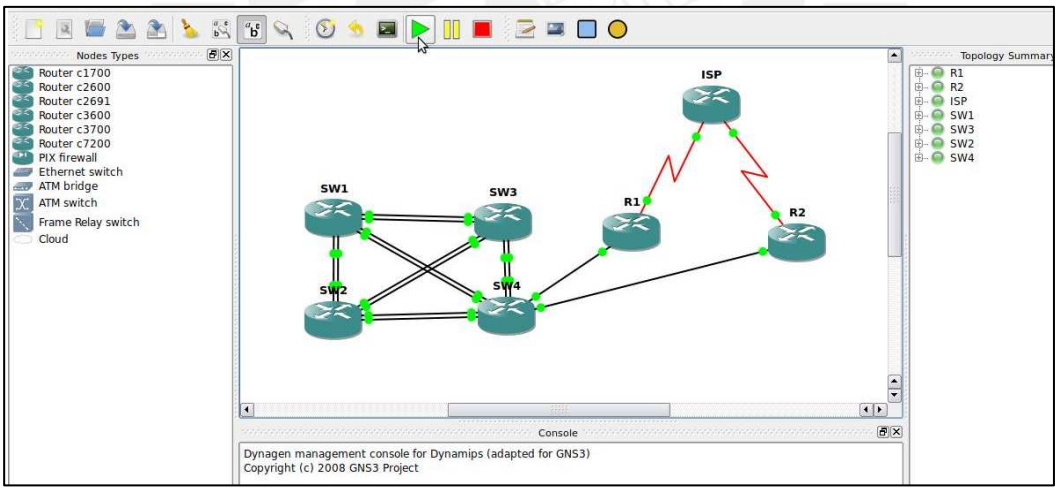

FIGURA 4- 1*: EMULACIÓN DE LA RED LAN EN GNS3*

Fuente: Elaboración propia

En esta emulación se cargaron las configuraciones en los switches y routers como se muestra a continuación en la figura 4-2:

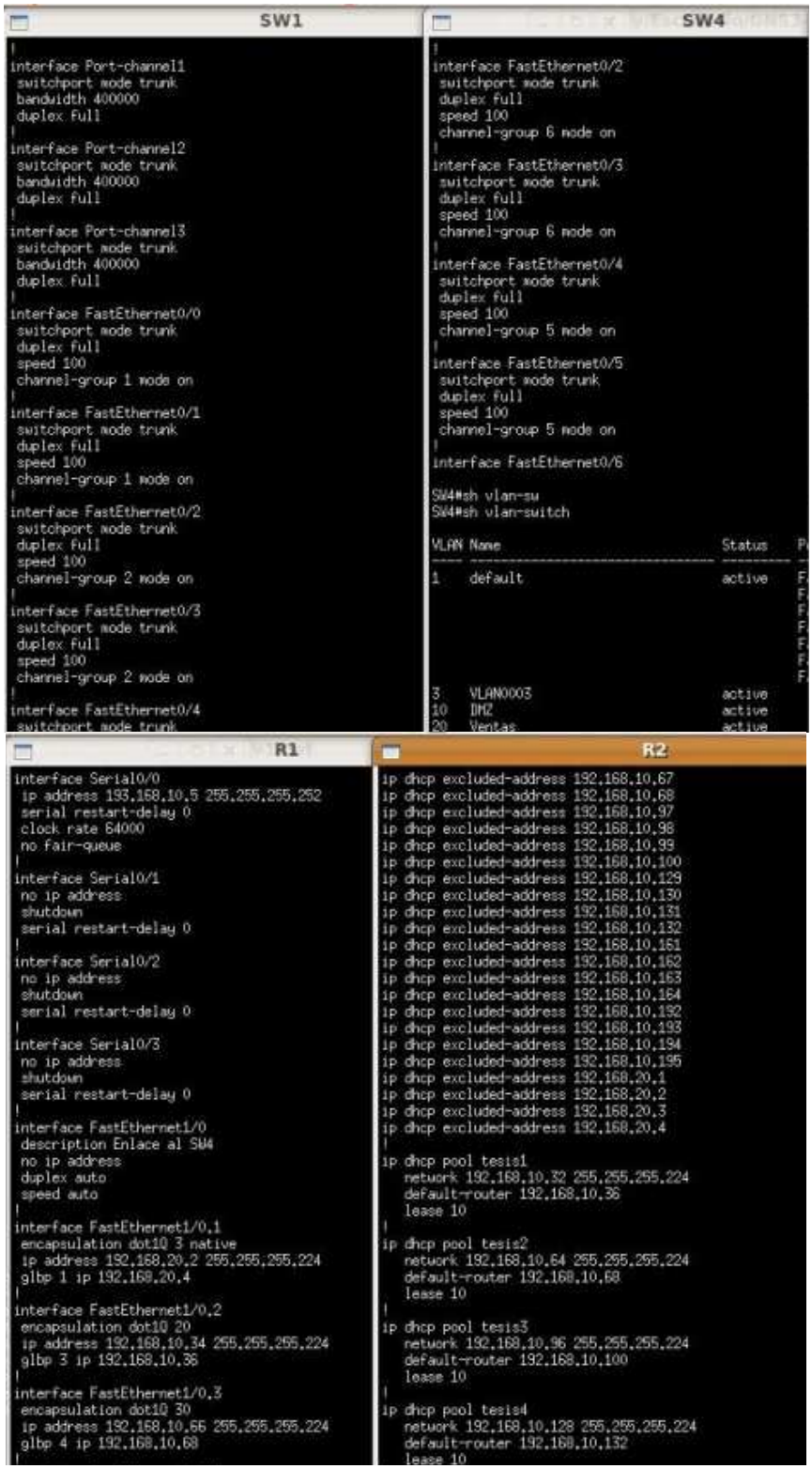

FIGURA 4- 2*: CONFIGURACIÓN DE SWITCHES Y ROUTERS EN GNS3*

Fuente: Elaboración propia

En la emulación no se pudo usar el protocolo RSTP por las limitaciones que presentan los módulos de switching, en lugar de este solo se usó el protocolo STP. Para la configuración del mecanismo Etherchannel en el modulo de switching no se pudo configurar el protocolo de negociación PAgP propuesto en el diseño, ni el protocolo LACP porque el módulo de switching no lo soporta, en lugar de estos se realizó la configuración manual. El protocolo GLBP no tuvo ninguna limitación de configuración. Los demás protocolos propuestos en el diseño sí se pudieron configurar, además se crearon las VLANs y se difundieron de manera rápida mediante VTP y se probó la comunicación entre ellas haciendo uso de máquinas virtuales con sistema operativo Windows XP.

La implementación se realizó en el laboratorio de redes de la especialidad de Ingeniería de las Telecomunicaciones; donde se usaron 5 switches, 3 routers y 5 PCs para realizar las pruebas de interconexión y comunicación intra e inter VLAN. Se implementó la topología propuesta en el capítulo 3 en la FIGURA 3-1, con todos los protocolos propuestos sin ningún limitante: RSTP, Etherchannel, GLBP.

Cada switch se conectó por 2 enlaces FastEthernet configurados en full duplex a una velocidad de 100 Mbps, con lo que se consiguió un ancho de banda entre switches sea de 400 Mbps. Cada switch se conectó a todos los restantes de manera directa para tener redundancia y la caída de uno no afecte la comunicación entre los demás. Los puertos han sido configurados como troncales para que todas las VLANs creadas en la red puedan comunicarse entre ellas y alcanzar cualquier destino permitido.

Debido al número de usuarios y la cantidad de subredes, se decidió implementar servidores DHCP en los routers de salida, con esto se evitará un conflicto de direcciones. Gracias a la redundancia y balanceo de carga, si uno de ellos presenta problemas de funcionamiento se contará con un servidor de backup. Se reservan las 4 primeras direcciones IPs de cada subred para configuraciones de las puertas de enlace, IP virtual de ambos routers y una para uso del administrador de red.

La VLAN administrativa usada para equipos de la red contará con direccionamiento estático. Las configuraciones correspondientes a cada equipo se encuentran en el anexo 2.

4.2 Implementación del servidor ACS

Una vez implementada la red LAN debemos implementar el servidor ACS encargado de autenticar a los usuarios que accedan a equipos de la red. Antes de implementarla se simuló la autenticación usando el emulador de red GNS3 y una máquina virtual en Virtualbox con sistema operativo Windows Server 2003 donde se implemento el ACS de CISCO.

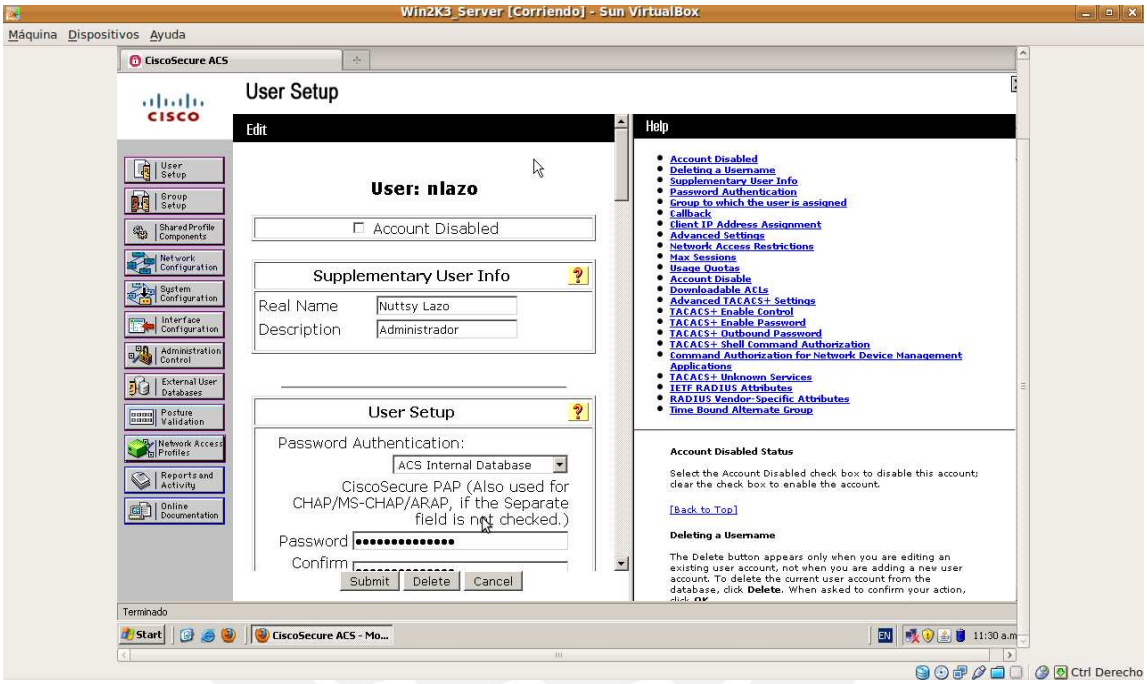

FIGURA 4- 3*: ACS EN VIRTUALBOX*

Fuente: Elaboración propia

Una vez implementado el servidor ACS en la maquina virtual se agregó este nuevo elemento a la red y se ingresó a los equipos de la red mediante la autenticación y autorización que permite el ACS configurado.

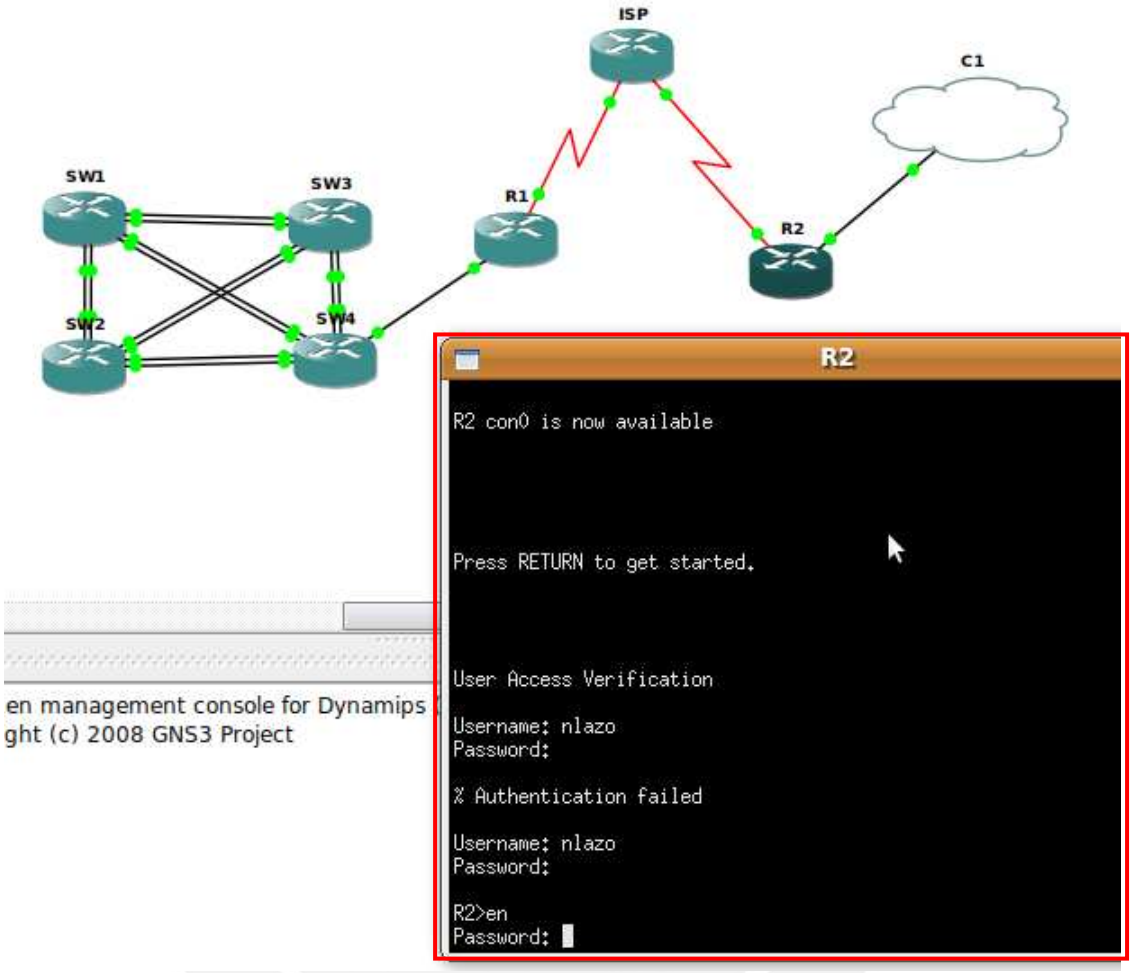

FIGURA 4- 4: *EMULACIÓN DE LA RED LAN Y AUTENTICACIÓN EN GNS3*

Fuente: Elaboración propia

Para implementar el servidor TACACS+ escogimos una PC del laboratorio que cuenta con las siguientes características: Procesador: Intel Core 2 Duo a 2.13 GHz, Memoria RAM: 1.99 GB

Primero se puso el servidor en la VLAN Administrativa y se instaló una versión de prueba del software ACS descargado de la página web de CISCO, luego se creo un administrador del servidor ACS.

Ahora ingresamos los clientes TACACS+ que tiene la red: SW1, SW2, SW3, SW4, R1 y R2 con sus respectivas direcciones IPs (pertenecientes a la VLAN Administrativa).

Además se ingresa la llave de seguridad que debe ser la misma en la configuración del cliente.

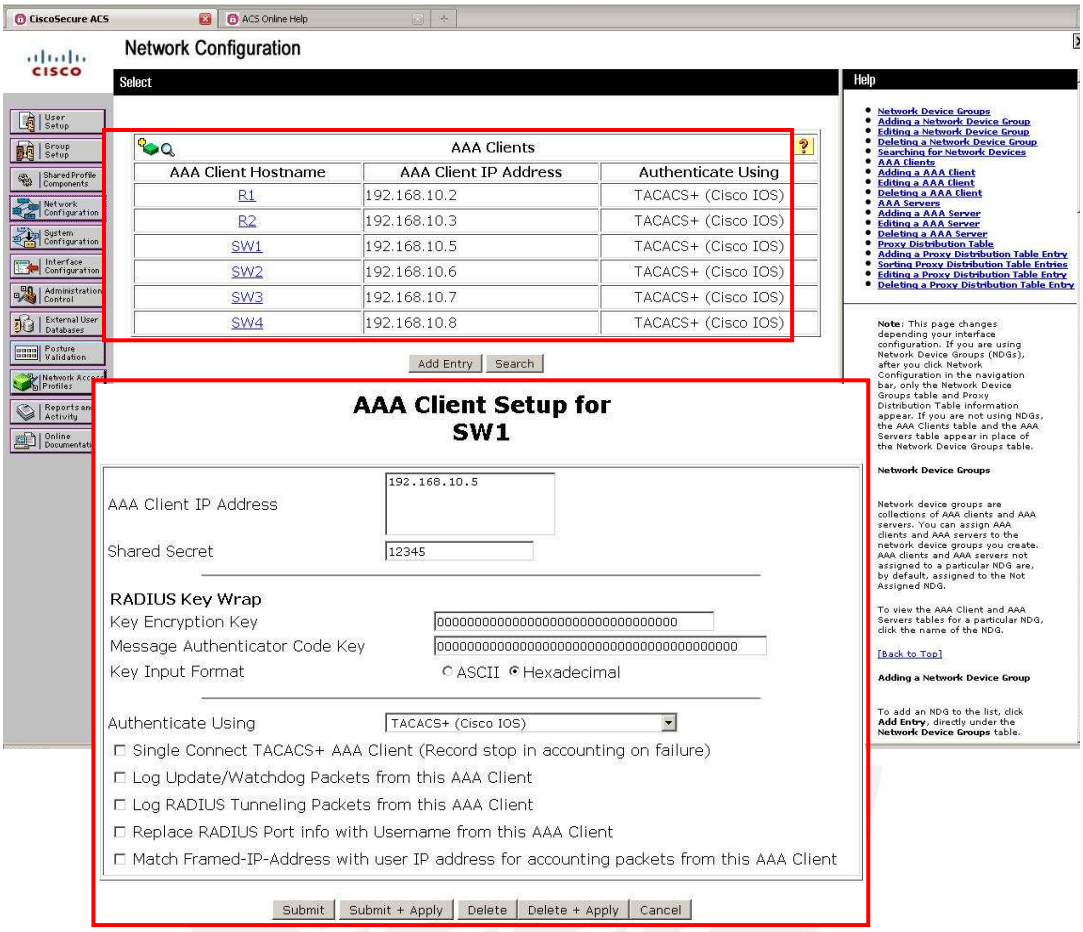

FIGURA 4- 5*: REGISTRO DE CLIENTES TACACS+ EN ACS*

Fuente: Elaboración propia

Cuando los Clientes TACACS+ ya se encuentran registrados, creamos los grupos de usuarios que van a poder ingresar a los equipos de la red. Cada grupo tendrá un nivel de autorización diferente ya que como se indicó en el capitulo 2 los administradores de red y los trabajadores de Help Desk tendrán diferentes niveles de privilegios dentro de los equipos.

Los administradores van a tener nivel de privilegio 15 que es el nivel máximo, ellos podrán ver y realizar cambios en la configuración, a diferencia de los trabajadores del área de Help Desk que solo podrán ver detalles de la red mas no la configuración del equipo ni realizar algún cambio en ella.

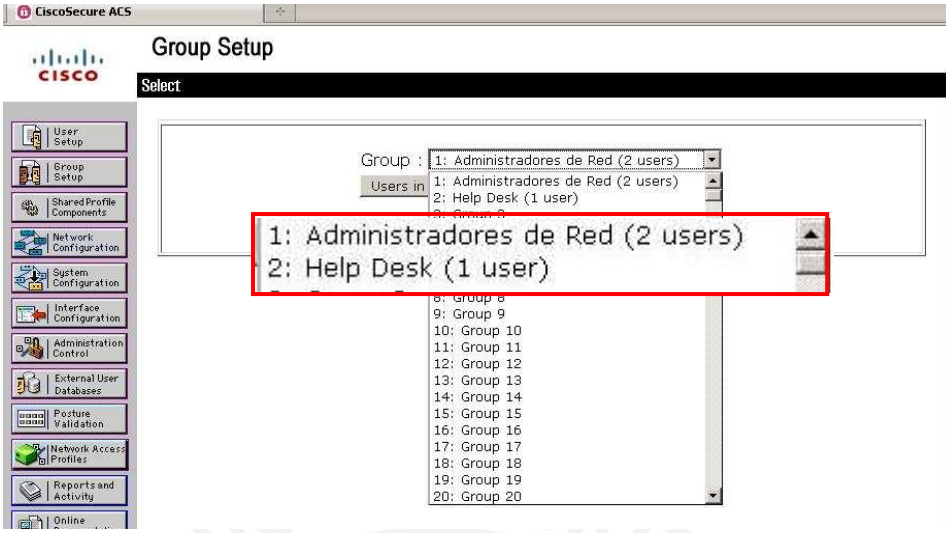

FIGURA 4- 6*: GRUPOS CREADOS EN EL ACS*

Fuente: Elaboración propia

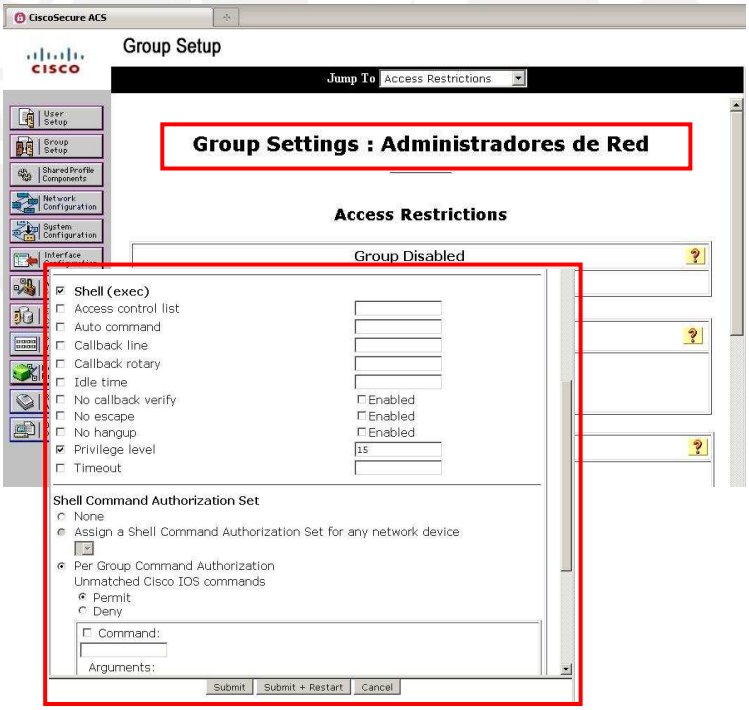

FIGURA 4- 7*: CONFIGURACIÓN DE NIVEL MAXIMO DE PRIVILEGIO PARA EL GRUPO DE ADMINISTRADORES DE RED*

Fuente: Elaboración propia

Una vez creados los grupos, se crearon los usuarios y se asociaron a un grupo, cada usuario debe tener un nombre y una contraseña para realizar la autenticación de manera exitosa. Se debe especificar la base de datos que usamos, en esta

implementación se utilizó la base de datos interna del ACS. Además se debe escoger el grupo al que pertenece y el nivel de privilegio con el que cuenta y seleccionar que los grupos de autorización se hereden de lo contrario se puede definir diversos niveles de autorización para cada usuario. A continuación se muestran la configuración de un usuario del grupo administrador y otro usuario del grupo Help Desk

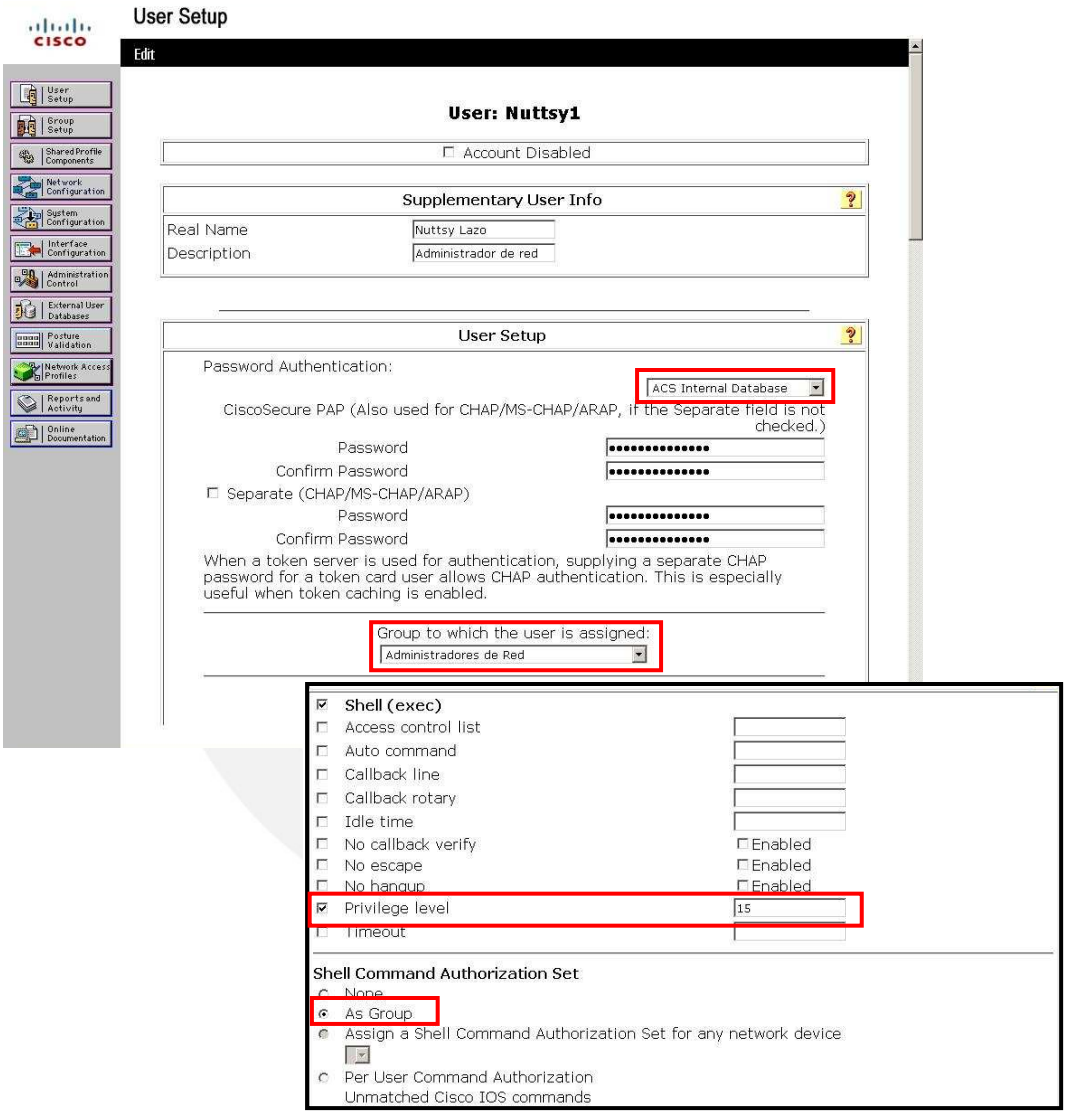

FIGURA 4- 8*: CONFIGURACIÓN DE USUARIO EN EL GRUPO DE ADMINISTRADORES DE RED*

Fuente: Elaboración propia

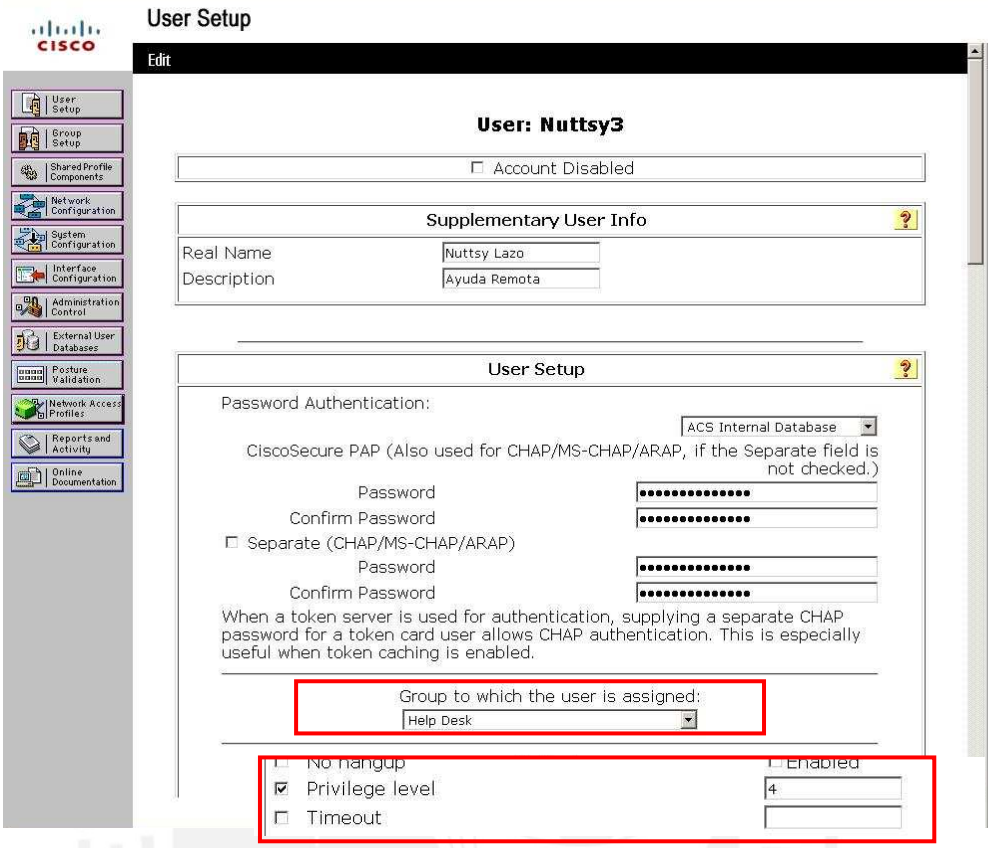

FIGURA 4- 9*: CONFIGURACIÓN DE USUARIO EN EL GRUPO DE HELP DESK*

Fuente: Elaboración propia

4.3 Configuración de Clientes TACACS+

Una vez implementado el servidor TACACS+ se procede a configurar clientes AAA en todos los equipos de la red, esta configuración se realiza de manera similar. A continuación se muestra y se explica cual es la configuración que debe tener cada equipo para que se convierta en un cliente TACACS+:

Primero se creo un usuario para el acceso desde consola, para que este pueda ser habilitado cuando el equipo no se encuentre conectado al servidor. Luego se definieron dos usuarios uno con nivel de privilegio 15 y otro con nivel de privilegio 4, esto se configura porque si bien ambos niveles están por defecto en los equipos de red, para que el servidor TACACS+ pueda ingresar con cualquier nivel este debe estar definido, por esta misma razón se debe definir ambos niveles para la conexión remota VTY

Después se comienza a configurar al equipo como cliente TACACS+ creando un modelo AAA y se indica cual es el servidor y cual es la llave que debe coincidir con la configurada en el servidor. También se define que el servidor soportará 5 intentos fallidos antes de expulsarlo.

Para configurar la autenticación se usa el comando: authentication login, además se define que todas las interfaces y líneas van a ser autenticadas por el protocolo TACACS+ con los usuarios registrados en el servidor (usuarios locales del autenticador). Con el tercer comando se define que cuando la autenticación con el servidor este deshabilitada se pueda acceder por medio de la contraseña enable del equipo. También debemos definir que el servidor no acepte mas de 5 intentos de autenticación.

Para configurar autorización primero definimos que va ser por comandos (modo commands). Luego definiremos que en cuanto la autorización se permitirá el uso de los comandos de acuerdo al nivel con que se ingrese, para esta implementación solo hemos definido los niveles: 0, 1, 4 y 15.

El proceso de accounting se iniciará cuando se intente o se inicie una sesión en el modo exec y se detendrá cuando se salga de este modo. De la misma manera cuando se ejecuten comandos de nivel 1, 4 y 15 se iniciara el proceso y se tendrá cuando se salga del nivel. Todas las peticiones de servicio de red también serán contabilizadas (como las peticiones de ARP, SLIP o PPP), además cada vez que se inicie una sesión remota como Telnet también se realizara el proceso de accounting.

4.4 Implementación del servidor RADIUS (IAS)

Como se definió en el diseño, el servidor encargado de realizar la autenticación a los usuarios inalámbricos será el servidor IAS (servicio que viene con el sistema operativo Windows Server 2003)

Para implementar el servidor TACACS+ escogimos una PC del laboratorio que cuenta con las siguientes características: Procesador: Intel Core 2 Duo a 2.13 GHz, Memoria RAM: 1.99 GB

Primero se puso el servidor en la VLAN inalámbrica (WLAN) con una dirección IP excluida del pool de direcciones del DHCP. Luego se tuvo que habilitar 3 servicios antes de habilitar el IAS: el servidor de aplicaciones (IIS y ASP.net), Active Directory y servidor de Certificados (entidad emisora CA)

- **Active Directory**

  Creamos un dominio con el nombre de la empresa, adicionalmente se creó un grupo denominado “Usuarios Inalámbricos” y se registraron usuarios dentro de él.

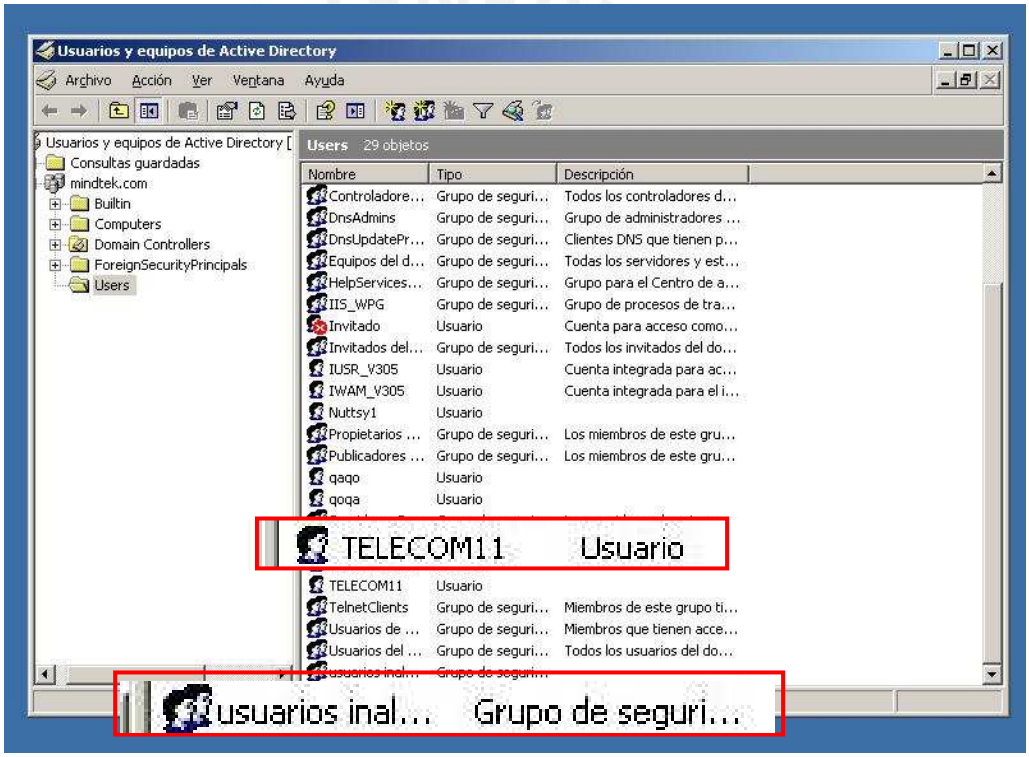

FIGURA 4- 10*: ACTIVE DIRECTORY*

Fuente: Elaboración propia

El grupo de usuarios inalámbricos fue definido como un grupo local del tipo seguro.

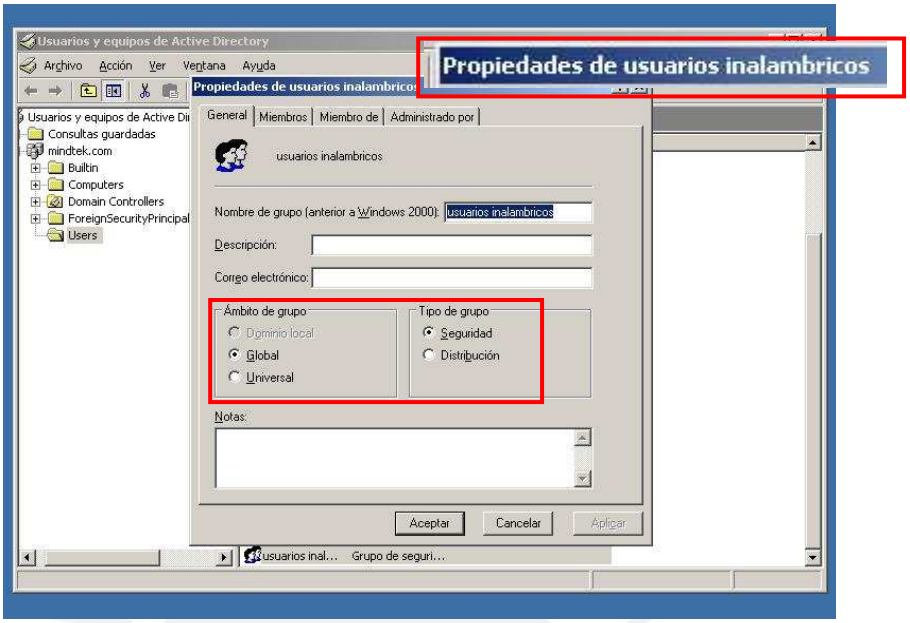

FIGURA 4- 11*: PROPIEDADES DEL GRUPO USUARIOS INALÁMBRICOS DENTRO DEL DOMINIO*

Fuente: Elaboración propia

Dentro del grupo, se ingresaron miembros que posteriormente podrán acceder a la red inalámbrica

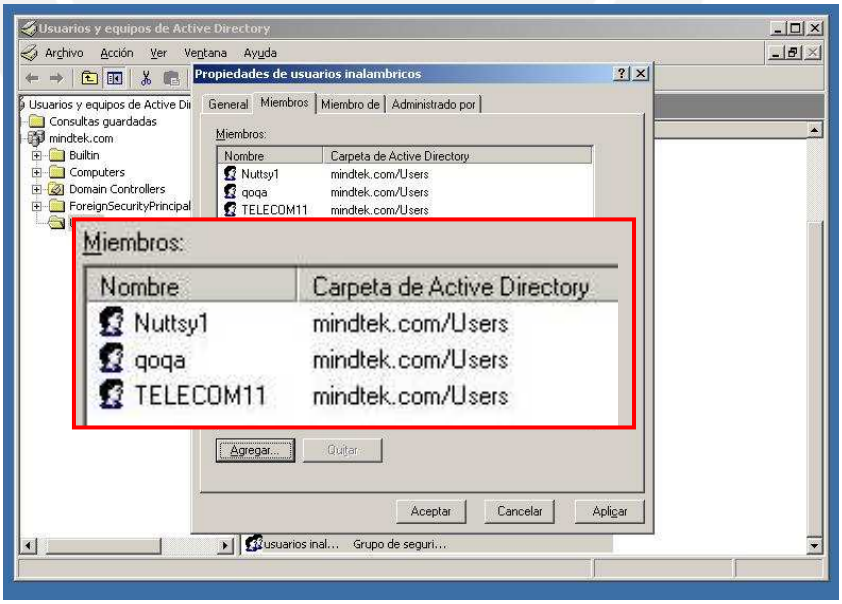

FIGURA 4- 12 *MIEMBROS DEL GRUPO USUARIOS INALÁMBRICOS*

Fuente: Elaboración propia

- **Servidor de Certificados**

  Ahora que contamos con usuarios registrados en el dominio del active directory podemos instalarles certificados de autenticación a través de un servidor de certificados instalado en el mismo equipo.

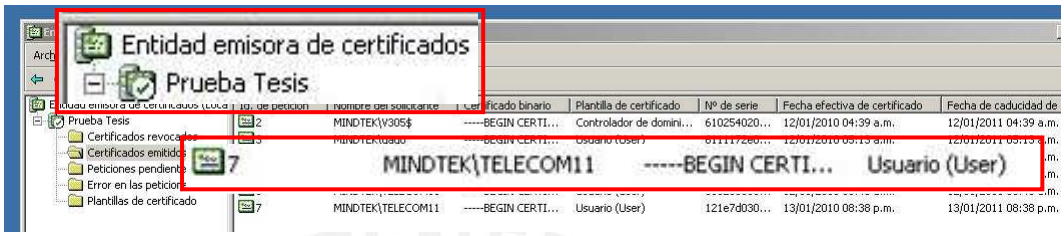

FIGURA 4- 13*: EMISOR DE CERTIFICADOS*

Fuente: Elaboración propia

Los usuarios deben tener conectividad con el servidor para poder acceder a este servicio.

- **Servidor de Aplicaciones**

  Adicionalmente el equipo debe contar con un servidor de aplicaciones que permita a los usuarios ubicar al emisor de certificados vía WEB.

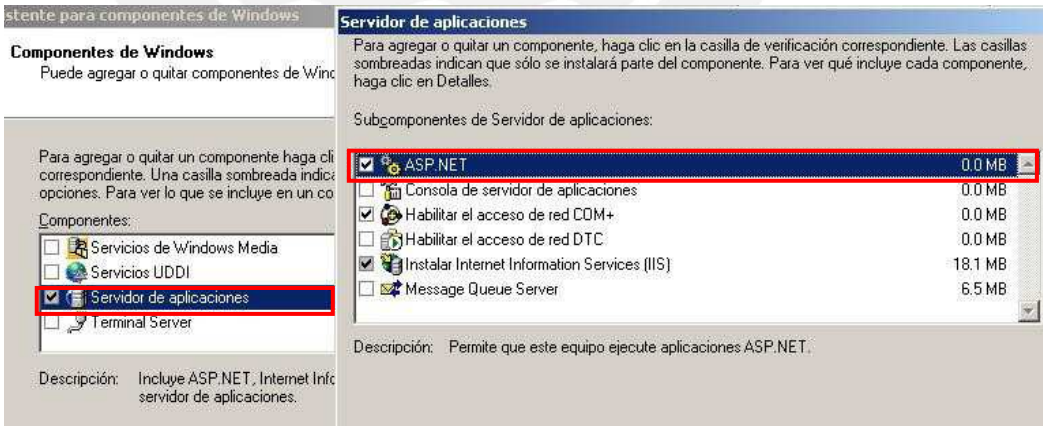

FIGURA 4- 14*: SERVIDOR DE APLICACIONES*

Fuente: Elaboración propia

Una vez instalados los tres servicios anteriores se procede a instalar el IAS, este servidor será el encargado de autenticar a los usuarios inalámbricos luego de

comprobar que los certificados de autenticación que posee cada usuario haya sido emitido por el mismo y pertenezca al grupo de usuarios inalámbricos.

4.5 Configuración de punto de acceso inalámbrico como cliente RADIUS

El Access Point que se usó en la implementación es un D-Link modelo DWL-3200AP 802.11g Managed cuya hoja técnica se encuentra en el anexo 4

Se configuró el AP en la VLAN inalámbrica (WLAN), para ello se le asigna una dirección IP excluida del pool de direcciones del servidor DHCP y se colocó un SSID para identificar la red. Luego se configura el tipo de autenticación como WPA, se indica cual es la dirección del servidor RADIUS el puerto por el que pasa la autenticación y autorización además del puerto que usará el proceso de accounting.

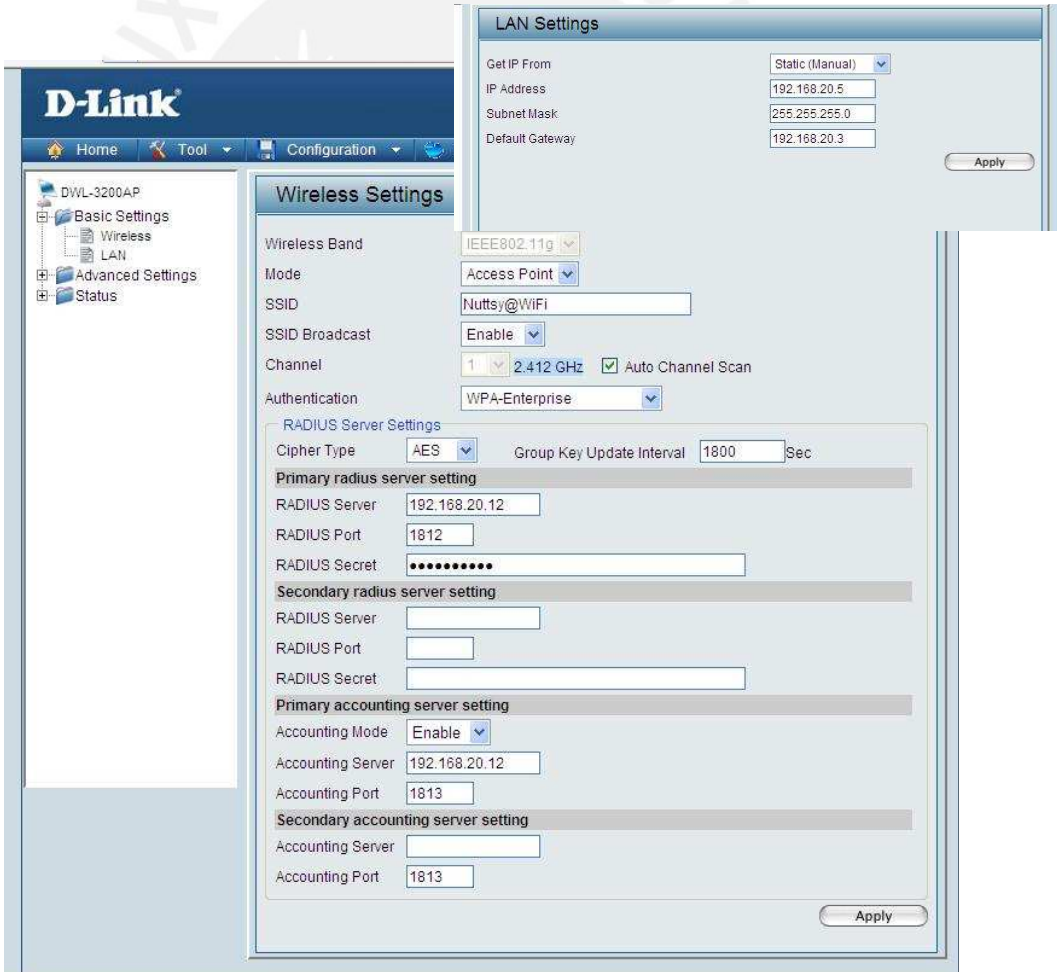

FIGURA 4 -15*: CONFIGURACIÓN DEL ACCESS POINT*

Fuente: Elaboración propia

4.6 Configuración de usuarios inalámbricos

Para que los usuarios puedan acceder a la red inalámbrica deben tener instalado un certificado de autenticación emitido por el servidor. Para ello primero deben encontrase dentro de la red y acceder al servidor vía WEB, para poder acceder antes se debe ingresar el usuario y la contraseña creados en el Active Directory. Una vez instalado el certificado tendrá vigencia por un mes.

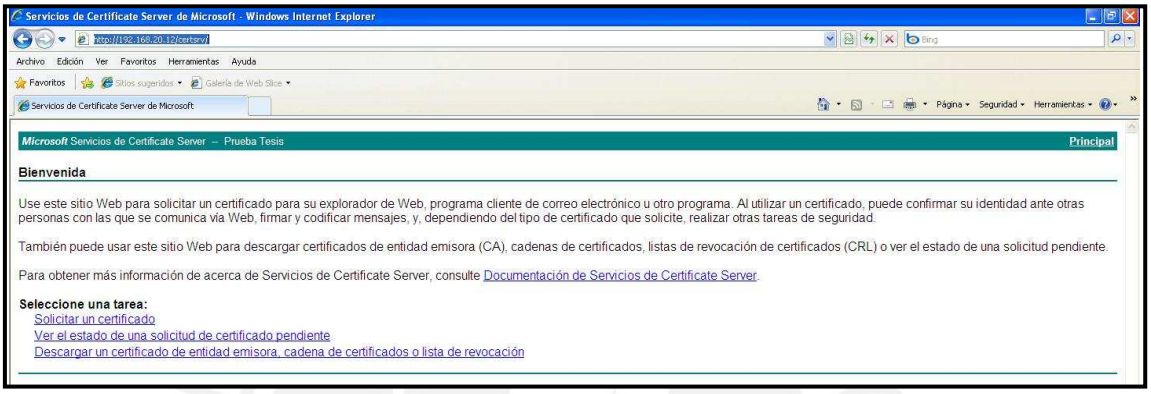

FIGURA 4- 16*: PAGINA WEB DEL SERVIDOR DE CERTIFICADOS*

Fuente: Elaboración propia

FIGURA 4- 17*: DESCARGA DEL CERTIFICADO DE AUTENTICACIÓN*

Fuente: Elaboración propia

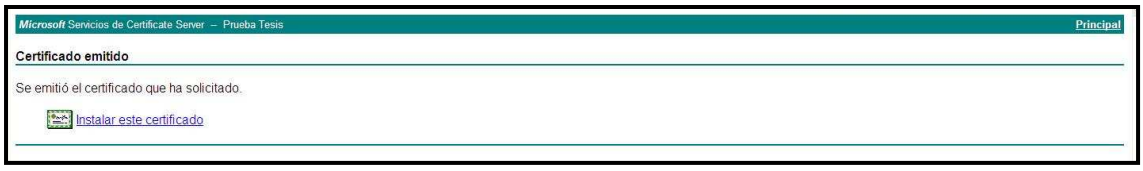

FIGURA 4- 18*: INSTALADOR DE CERTIFICADO*

Fuente: Elaboración propia

Para terminar se debe configurar el tipo de autenticación para la red inalámbrica como WPA-Enterprice, con cifrado AES y como método de autenticación, tarjeta inteligente u otro certificado.

4.7 Resultados en la LAN

Terminada la implementación se probó el acceso a los equipos de la red desde diversas VLANs. Desde la WLAN ingresamos con un usuario perteneciente al grupo de administradores de red y este ingreso con el máximo nivel de privilegios, como se puede observar en la siguiente figura. Con ello se verifica que el servidor esta autenticando y autorizando correctamente.

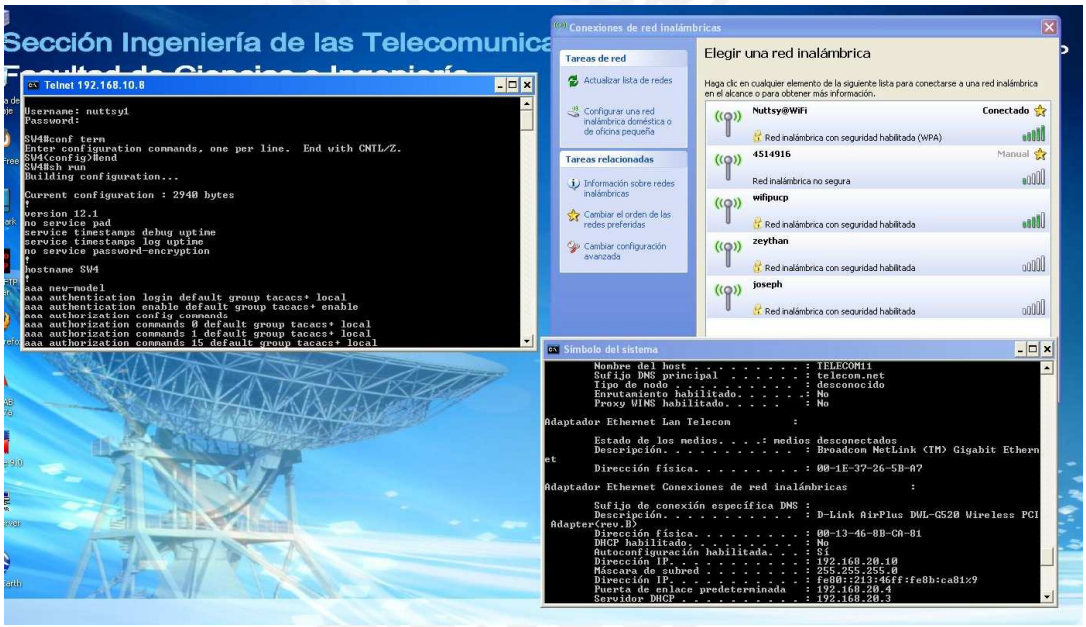

FIGURA 4- 19*: AUTENTICACIÓN Y AUTORIZACIÓN DE USUARIO DEL GRUPO ADMINISTRADORES DE RED*

Fuente: Elaboración propia

Desde la VLAN Soporte ingresamos con un usuario del grupo Help Desk y el servidor solo permitió ejecutar comandos pertenecientes al nivel de privilegio de grupo (level 4).

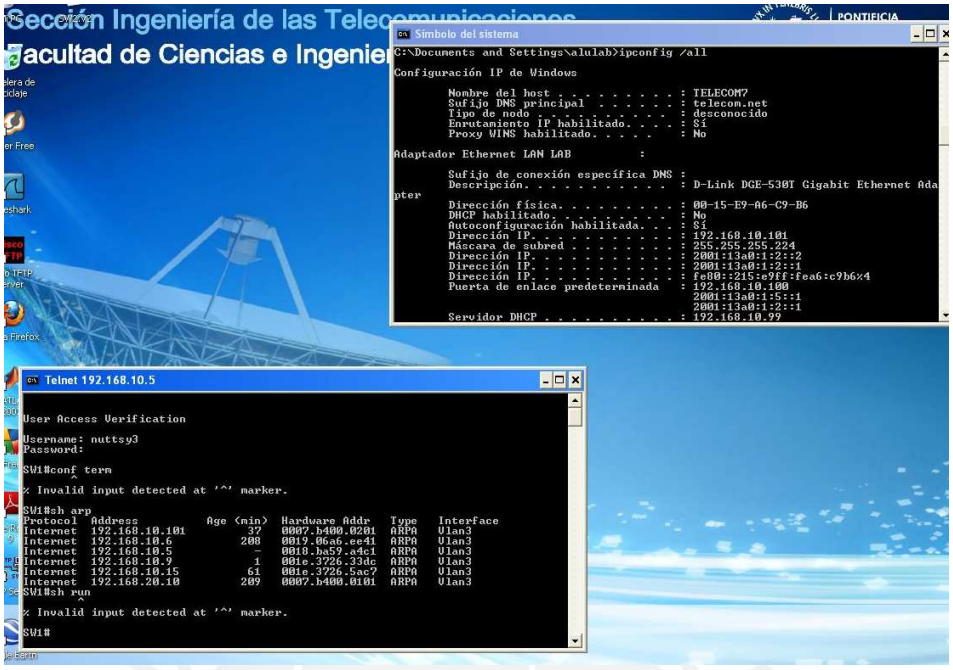

FIGURA 4- 20 *AUTENTICACIÓN Y AUTORIZACIÓN DE USUARIO DEL GRUPO HELP DESK*

Fuente: Elaboración propia

Para probar que con la Tecnología Etherchannel se puede optimizar el ancho de banda dentro de la red LAN se realizaron los siguientes pasos:

- Paso 1: Para saturar los enlaces de la red con tráfico de datos, se implementaron siete servidores FTP con sus respectivos clientes.

- Paso 2: Se configuraron dos enlaces de la red LAN como un enlace lógico con la Tecnología Etherchannel y se obtuvo como resultado que por un enlace lógico podía pasar más de 200 Mbps de la suma de input y output, que es lo máximo que puede pasar un enlace físico Fast Ethernet. Debido a las limitaciones para generar flujo de datos en el laboratorio se llegó a 283.164 Mbps (como se muestra en la figura 4-20), en un escenario real con más tráfico la velocidad podría acercarse a los 400 Mbps (En un escenario ideal debería llegar a 400 Mbps pero debido a las limitaciones de la categoría del cable, desgaste de conectores, puertos entre host y puertos del switch esta velocidad no es posible de alcanzar) Generalmente se trabaja sobre el 80% de la capacidad física de un enlace de acuerdo al estándar Ethernet 100BASE-TX.

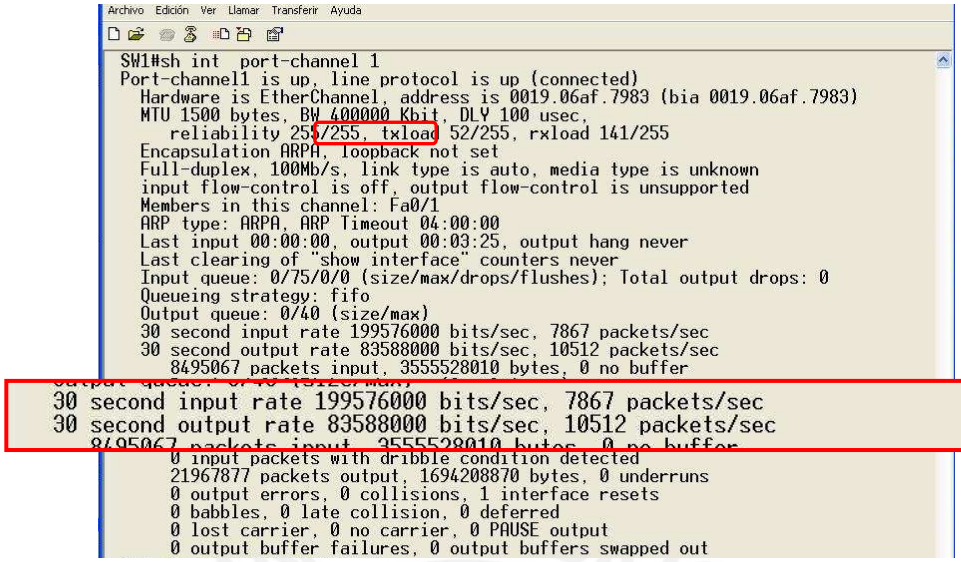

FIGURA 4- 21*: ANCHO DE BANDA EN PORT-CHANNEL CONFORMADO POR DOS ENLACES FISICOS*

Fuente: Elaboración propia

- Paso 3: Para probar la redundancia que se obtiene con la tecnología Etherchannel desconectamos uno de los enlaces físicos y el trafico continuó transportándose por el enlace restante. En la figura 4-21 se comprueba que la velocidad es menor a la que se tenía con ambos enlaces activos, en las pruebas de laboratorio se alcanzó una velocidad de 131.228 Mbps en suma de input y output.

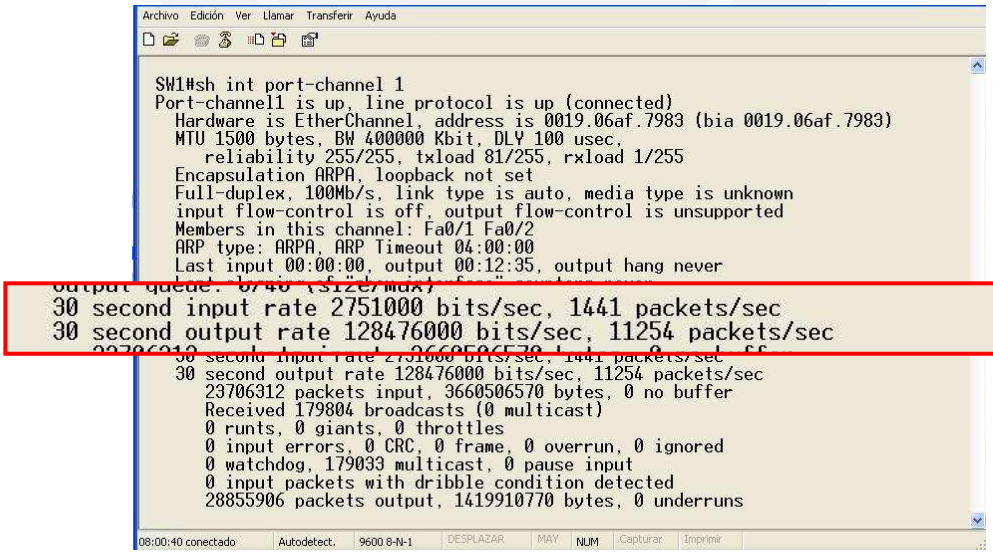

FIGURA 4- 22*: ANCHO DE BANDA EN PORT-CHANNEL CONFORMADO POR UN ENLACES FISICOS*

Fuente: Elaboración propia

Con el protocolo GLBP se puede optimizar el funcionamiento de la red gracias al balanceo de carga y redundancia de equipo.

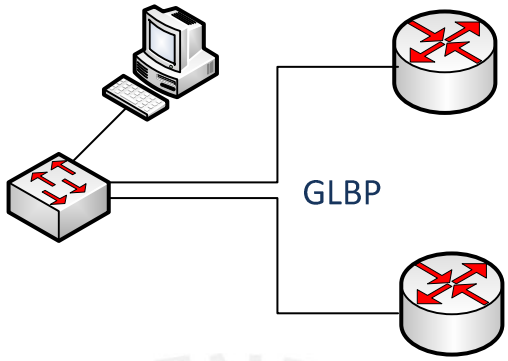

FIGURA 4- 23*: DIAGRAMA GLBP*

Fuente: Elaboración propia

Para probar esto nos ubicamos en la PC de un usuario de la VLAN de Marketing y se observaron las direcciones IPs que toma como Default Gateway y que toma como servidor DHCP. La dirección IP del Default Gateway es la configurada en la interfaz GLBP lógica de la Fast Ethernet 0/1 de ambos routers para esa VLAN (VLAN de Marketing) y el servidor DHCP toma la IP física del enlace Fast Ethernet 0/1 del router 1 (toma este por la prioridad configurada)

```
G:\Documents and Settings\Administrador>ipconfig -all

Configuración IP de Windows

   Nombre del host . . . . . : telecom6
   Sufijo DNS principal  . . . . . :
   Tipo de nodo. . . . . . . . . . . : híbrido
   Enrutamiento habilitado . . . . : No
   Proxy WINS habilitado . . . . . : No
   Lista de búsqueda sufijo DNS  : pucp.edu.pe

Adaptador Ethernet Conexión de área local 2:

   Sufijo conexión específica DNS:
   Descripción . . . . . . . . . . . : D-Link DGE-530T Gigabit Ethernet Adapter
   Dirección física. . . . . . . . . : 00-15-E9-A6-C9-A3
   DHCP habilitado . . . . . . . . . : No
   Autoconfiguración habilitada  : Sí
   Dirección IP. . . . . . . . . . . : 192.168.10.37
   Máscara de subred . . . . . . . . : 255.255.255.224
   Puerta de enlace predet. . . . : 192.168.10.36
   Servidor DHCP . . . . . . . . . . : 192.168.10.34
   Concesión obtenida. . . . . . . . : Domingo, 16 de Mayo de 2010 02:37:36 a.m.
   Concesión expira. . . . . . . . . : Lunes, 17 de Mayo de 2010 02:37:36 a.m.
```

FIGURA 4- 24*: DIRECCIÓN IP DEL DEFAULT GATEWAY Y DEL SERVIDOR DHCP – PRUEBA 1*

Fuente: Elaboración propia

Para probar la redundancia del servidor DHCP se apagó el router 1, se liberó la dirección IP que había sido asignada por el servidor DHCP 1(router 1) y se renovó la dirección IP.

FIGURA 4- 25*: DIRECCIÓN IP DEL DEFAULT GATEWAY Y DEL SERVIDOR DHCP – PRUEBA 2*

Fuente: Elaboración propia

Se puede observar que la dirección IP del Default Gateway no ha cambiado ya que esta es lógica mientras que la asignada al servidor DHCP cambió por la IP asignada a la interfaz Fast Ethernet 0/1 del router 2.

Para probar que durante la caída de uno de los routers no se pierden paquetes, se envió un ping continuo a la IP configurada en la subinterfaz GLBP lógica de la VLAN Administrativa de los routers 1 y 2. Se observa que en el momento de la desconexión el tiempo de respuesta fue mayor pero no hubo pérdidas; luego de establecerse la comunicación con el segundo router el tiempo de respuesta se estabilizó.

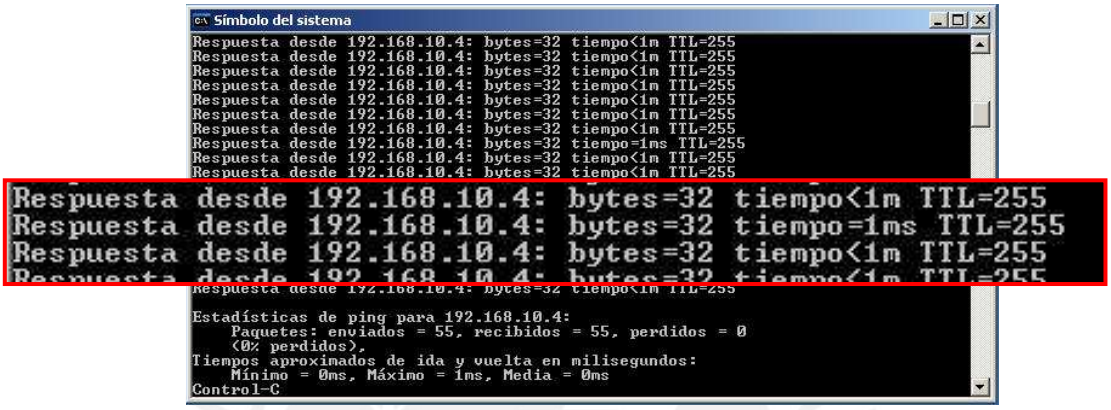

FIGURA 4- 26*: CONTINUIDAD DE PAQUETES LUEGO DE AVERIA DE UN ROUTER*

Fuente: Elaboración propia

Luego de configurar el protocolo GLBP podemos observar que debido a las prioridades asignadas el AVG (Active Virtual Gateway) es el Router 1 y el AVF (Active Virtual Forwarder) es el router 2. En la descripción del protocolo podemos confirmar que el "Active router" es el Router 1 y el "Standby route" es el router 2, además se ve el balanceo de carga que se está dando entre ambos routers

```
R2#sh glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby route
Fa0/1.1     2    -   100 Active   192.168.10.4    local           unknown

Fa0/1.1     2    1   7   Active   0007.b400.0201  local           -
Fa0/1.3     3    -   100 Standby  192.168.10.68   192.168.10.66   local

Fa0/1.3     3    1   7   Active   0007.b400.0301  local           -
Fa0/1.3     3    2   7   Listen   0007.b400.0302  192.168.10.66   -
Fa0/1.4     4    -   100 Standby  192.168.10.100  192.168.10.98   local

Fa0/1.4     4    1   7   Active   0007.b400.0401  local           -
Fa0/1.4     4    2   7   Listen   0007.b400.0402  192.168.10.98   -
Fa0/1.5     5    -   100 Standby  192.168.10.132  192.168.10.130  local

Fa0/1.5     5    1   7   Active   0007.b400.0501  local           -
Fa0/1.5     5    2   7   Listen   0007.b400.0502  192.168.10.130  -
Fa0/1.6     6    -   100 Standby  192.168.10.164  192.168.10.162  local

Fa0/1.6     6    1   7   Active   0007.b400.0601  local           -
Fa0/1.6     6    2   7   Listen   0007.b400.0602  192.168.10.162  -
Fa0/1.7     7    -   100 Standby  192.168.10.195  192.168.10.193  local

Fa0/1.7     7    1   7   Active   0007.b400.0701  local           -
Fa0/1.7     7    2   7   Listen   0007.b400.0702  192.168.10.193  -
```

Balanceo de Carga entre ambos

FIGURA 4- 27*: PROTOCOLO GLBP – BALANCEO DE CARGA*

Fuente: Elaboración propia

Si apagamos el router 1 el router 2 será el “Active Router”, no se conoce el “Standby Route” y no hay balanceo de carga pero el flujo de datos seguirá hacia el router 2

```
R2#sh glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby route
Fa0/1.1     2    -   100 Active   192.168.10.4    local           unknown

Fa0/1.1     2    1   7   Active   0007.b400.0201  local           -
Fa0/1.3     3    -   100 Active   192.168.10.68   local           unknown

Fa0/1.3     3    1   7   Active   0007.b400.0301  local           -
Fa0/1.3     3    2   7   Active   0007.b400.0302  local           -
Fa0/1.4     4    -   100 Active   192.168.10.100  local           unknown

Fa0/1.4     4    1   7   Active   0007.b400.0401  local           -
Fa0/1.4     4    2   7   Active   0007.b400.0402  local           -
Fa0/1.5     5    -   100 Active   192.168.10.132  local           unknown

Fa0/1.5     5    1   7   Active   0007.b400.0501  local           -
Fa0/1.5     5    2   7   Active   0007.b400.0502  local           -
Fa0/1.6     6    -   100 Active   192.168.10.164  local           unknown

Fa0/1.6     6    1   7   Active   0007.b400.0601  local           -
Fa0/1.6     6    2   7   Active   0007.b400.0602  local           -
Fa0/1.7     7    -   100 Active   192.168.10.195  local           unknown

Fa0/1.7     7    1   7   Active   0007.b400.0701  local           -
Fa0/1.7     7    2   7   Active   0007.b400.0702  local           -
```

Redundancia

FIGURA 4- 28*: PROTOCOLO GLBP - REDUNDANDIA*

Fuente: Elaboración propia

4.8 Resultados en la WLAN

Como se puede observar en la siguiente figura el usuario inalámbrico esta conectado a la red inalámbrica autenticándose con WPA. Para verificar que el certificado con el que se autentica pertenezca al dominio y verificar que haya sido emitido por el servidor de certificados ejecutaremos: certmgr.msc.

FIGURA 4- 29*: USUARIO INALAMBRICO CONECTADO A WLAN*

Fuente: Elaboración propia

En la siguiente ventana se observa que el usuario inalámbrico tiene instalado el certificado de autenticación emitido por el servidor de certificados instalado en el Server 2003 como Prueba Tesis.

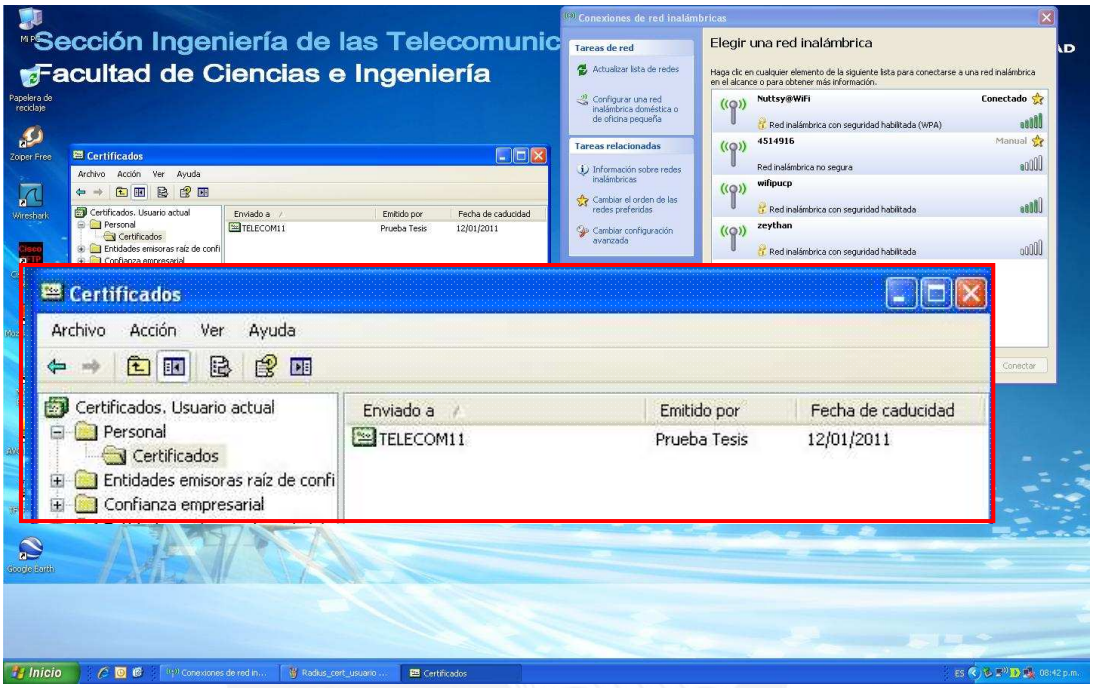

FIGURA 4- 30*: CERTIFICADO DE AUTENTICACIÓN ISNTALADO EN USUARIO INALAMBRICO*

Fuente: Elaboración propia

Para comprobar los pasos del proceso de autenticación IEEE 802.1x vistos en el capitulo 1 hicimos uso del sniffer Wireshark y se analizó las tramas obtenidas:

- Paso 1: El usuario inalámbrico (GemtekTE_f1:31:14) inicia el proceso de autenticación, enviando un mensaje 802.1x Authentication (de tipo Start) al Cliente RADIUS (AP D-Link_a3:c8:4d) por medio del protocolo de transporte EAP Over LAN.

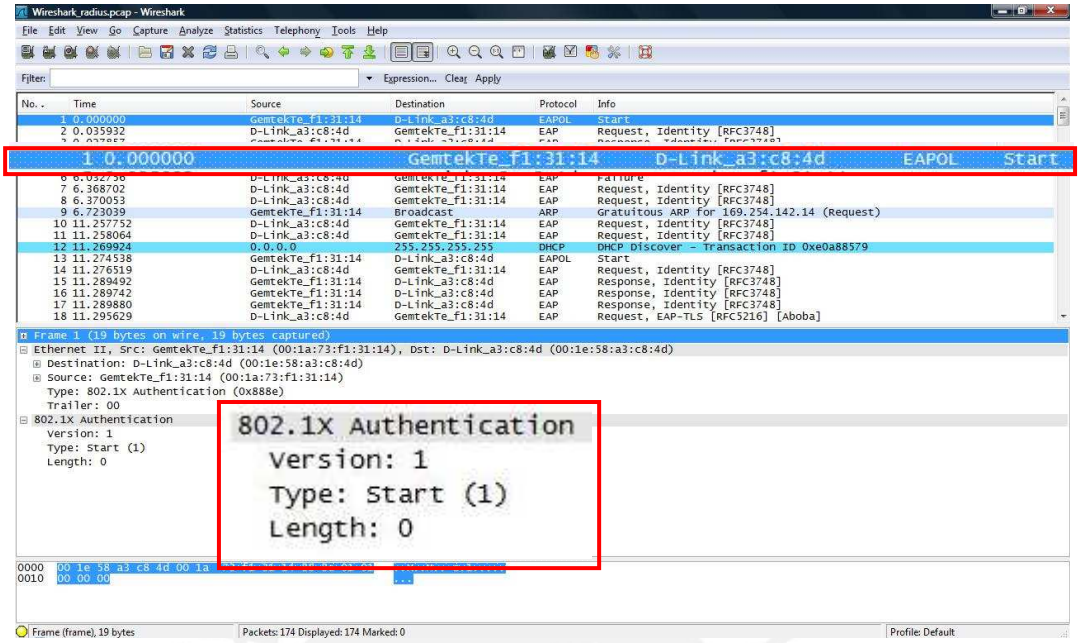

FIGURA 4- 31*: TRAMA WIRESHARK DE INICIO DE AUTENTICACIÓN*

Fuente: Elaboración propia

- Paso 2: El AP bloquea entrada a la red hasta que el usuario se autentique, para ello solicita identidad al usuario inalámbrico, esta solicitud es un mensaje del protocolo EAP.

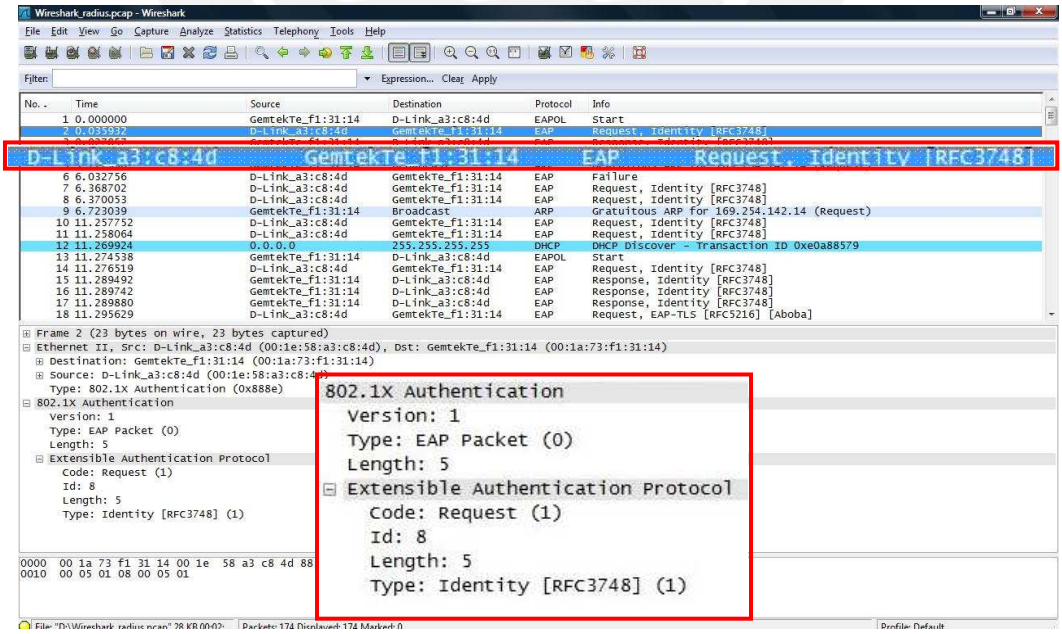

FIGURA 4- 32*: TRAMA WIRESHARK EAP REQUEST*

Fuente: Elaboración propia

- Paso 3: Usuario inalámbrico envía su identidad indicando que pertenece al grupo mindtek.com creado en el Active Directory (qaqo@mindtek.com) con un mensaje EAP.

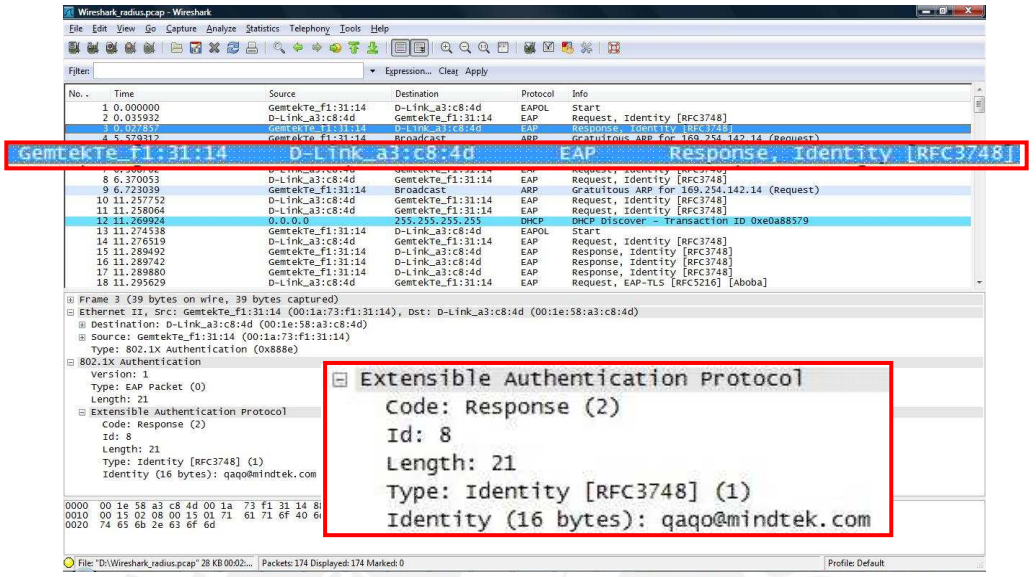

FIGURA 4- 33*: TRAMA WIRESHARK EAP RESPONSE*

Fuente: Elaboración propia

- Paso 4: AP pide autenticación del usuario a través mensajes del método elegido en la configuración. En esta implementación se pide un certificado por medio del protocolo TLS.

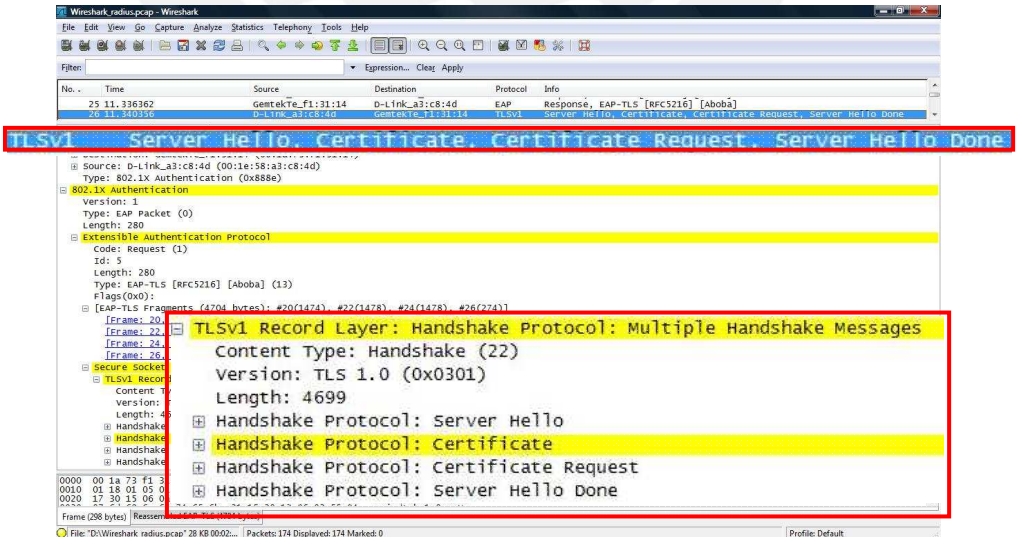

FIGURA 4- 34*: TRAMA WIRESHARK EAP-TLS ENVIADA POR ACCESS POINT*

Fuente: Elaboración propia

- Paso 5: El usuario envía la credencial al servidor RADIUS a través del AP.

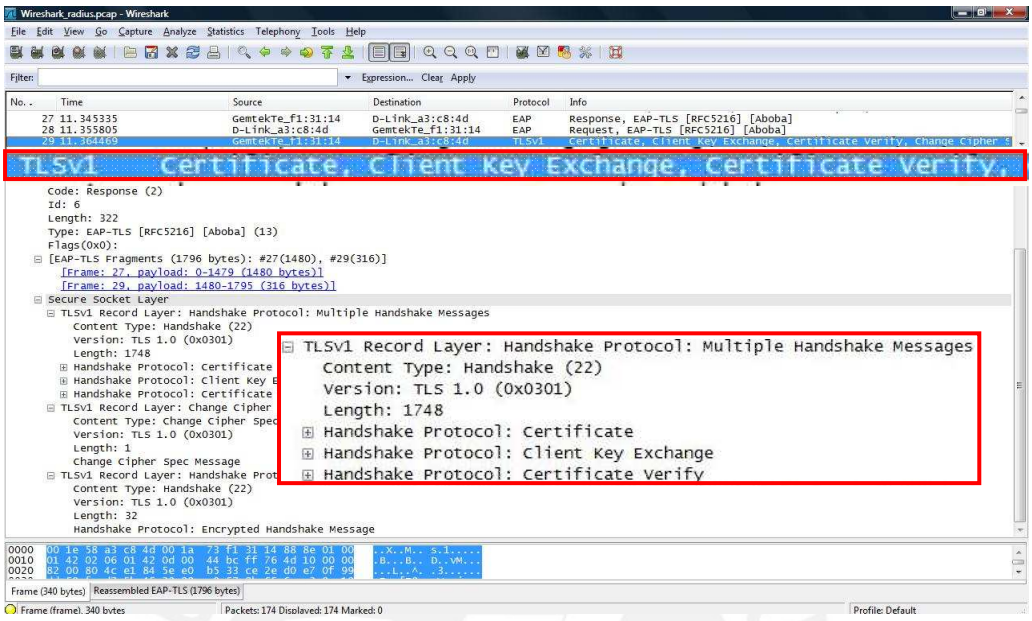

FIGURA 4- 25*: TRAMA WIRESHARK EAP-TLS ENVIADA POR USUARIO INALÁMBRICO*

Fuente: Elaboración propia

- Paso 6: Una vez autenticado el servidor distribuye la Master Key(MK).

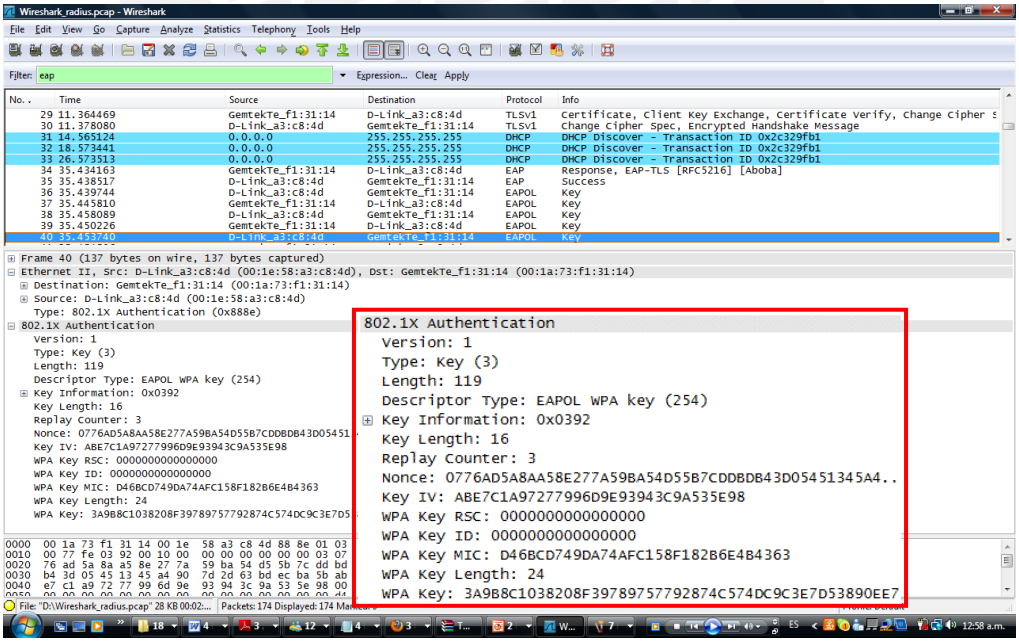

FIGURA 4- 36*: TRAMA WIRESHARK EAP – WPA KEY*

Fuente: Elaboración propia

- Paso 7: El proceso de autenticación IEEE 802.1x finaliza cuando el AP envía un mensaje “EAP Success”.

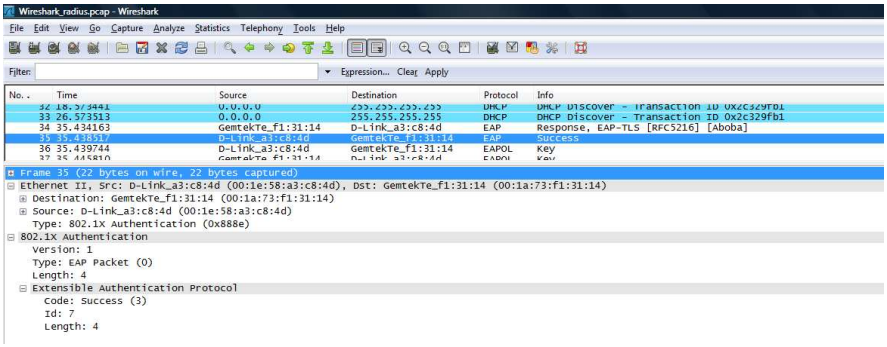

FIGURA 4- 37*: TRAMA WIRESHARK EAP - SUCCESS*

Fuente: Elaboración propia

Una vez que el usuario inalámbrico se encuentre en la red pedirá una dirección IP al servidor DHCP, que en esta implementación se trata de un router CISCO. Este le asignara una dirección IP del pool de direcciones destinadas para esa VLAN.

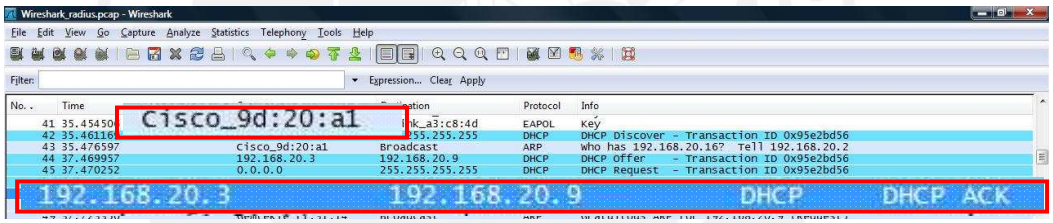

FIGURA 4- 38*: TRAMA WIRESHARK CON MENSAJES DHCP*

Fuente: Elaboración propia

Para probar conectividad del usuario con la red se enviaron algunos mensajes ICMP (ping) uno al servidor DHCP y otro al servidor RADIUS, ambos con respuesta exitosa.

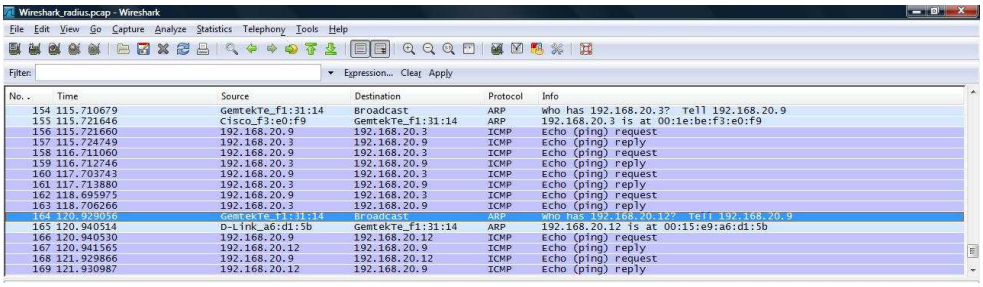

FIGURA 4- 39*: TRAMA WIRESHARK ICMP*

Fuente: Elaboración propia

Capítulo 5

Análisis económico del proyecto

5.1 Análisis Económico

En el análisis económico del proyecto se consideró los costos de implementación y operación y mantenimiento, con estos resultados se generó el flujo de caja y se medió la rentabilidad del proyecto con los métodos financieros TIR y VAN.

5.1.1 CAPEX

Los gastos que se generaron en la inversión inicial del proyecto se dividieron en:

Diseño: Realizado por un equipos de ingenieros.

TABLA 5- 1: PAGO TOTAL A INGENIEROS POR DISEÑO

Tiempo (día)	Horas	Número de Ingenieros	Costo/horas (S/.)	Costo Total (S/.)
15	120	2	60	14400

Fuente: Elaboración propia

Implementación: Realizado por un equipos de ingenieros y técnicos.

Ingenieros

TABLA 5- 2: PAGO TOTAL A INGENIEROS POR IMPLEMENTACIÓN

Tiempo (día)	Horas	Número de Ingenieros	Costo/horas (S/.)	Costo Total (S/.)
15	120	3	120	43200

Fuente: Elaboración propia

Técnicos

TABLA 5- 3: PAGO A TÉCNICOS POR IMPLEMENTACIÓN

Tiempo (día)	Horas	Número de Técnicos	Costo/horas (S/.)	Costo Total (S/.)
15	120	2	35	8400

Fuente: Elaboración propia

Los gastos de Hardware empleado en el proyecto se detallan en la siguiente tabla:

TABLA 5 4: INVERSIÓN EN HARDWARE PARA LA IMPLEMENTACIÓN

Producto	Descripción	Cantidad	Costo por unidad ($)	Costo Total ($)
Switch	Catalyst 2960 48 10/100 + 2 T/SFP LAN Base Image	4	2237.72	8950.86
Cable de Energía AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	4	0	0
Router	CISCO 2811 Security Bundle,Adv Security,128F/512D	2	3044.91	6089.82
Tarjeta HWIC-2T	2-Port Serial WAN Interface Card	2	1255.63	2511.26
Cable de Energía AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	2	0	0
Kit de accesorios para Router	CISCO2811 Green Accessory Kit - Cables, Quick-start Removed	2	0	0
Fuente de Poder	Cisco 2811 AC power supply	2	0	0
Up-grade de memoria RAM	256 to 512MB DDR DRAM factory upgrade for the Cisco 2811	2	0	0
CD de Configuración	Cisco Config Professional on CD, CCP-Express on Router Flash	2	0	0
Up-grade de memoria RAM	64 to 128 MB CF Factory Upgrade for Cisco 2800 Series	2	0	0
Access Point	DWL-3200AP	1	246.99	246.99
PC Core 2 Duo	PC – Core 2 Duo	2	650	1300

Fuente: Elaboración propia

Calcularemos los gatos de hardware con la relación de cambio Dólar/Nuevo Sol actual.

Total ($)	19098.93
Relación de cambio (Dólar/Nuevo Sol)	2.70
Total (S/.)	51567.12

Software

TABLA 5-5: INVERSION EN SOFTWARE PARA LA IMPLEMENTACION

Producto	Descripción	Cantidad	Costo por unidad ($)	Costo Total ($)
Licencia ACS - TACACS+	CiscoSecure ACS 4.2 for Windows	1	8995	8995
Licencia Microsoft Windows Server 2003	Windows Server 2003 Standard	2	1029	2058

Fuente: Elaboración propia

Calcularemos los gastos de software con la relación de cambio Dólar/Nuevo Sol actual.

Total ($)	11053
Relación de cambio (Dólar/Sol)	2.70
Total (S/.)	29843.10

Para este proyecto se considero un margen de ganancia del 15% en equipos, software y servicios profesionales de implementación.

TABLA 5- 6*:* PRECIO FINAL DE IMPLEMENTACIÓN CONSIDERANDO MARGEN DE GANACIA

	Gasto (S/.)	Margen de ganancia (%)	Precio (S/.)
Equipos	51567.12	15	59302.18
Software	29843.10	15	34319.57
Servicios de Implementación	66000.00	15	75900.00

Fuente: Elaboración propia

5.1.2 OPEX

Los costos de operación y mantenimiento están ligados a los servicios que se ofrecen:

Mantenimiento Preventivo (Babysitting) se pondrá un ingeniero junior en horario de oficina que estará en la sede del cliente los días laborables del mes.

TABLA 5- 7*:* PAGO MENSUAL INGENIERO POR MANTENIMIENTO PREVENTIVO

Tiempo (día)	Horas	Número de Ingenieros	Costo/horas (S/.)	Costo Total (S/.)
30	160	1	40	6400

Fuente: Elaboración propia

Mantenimiento Correctivo (Bolsa de Horas) el cliente cuenta con una bolsa de horas que podrá utilizar cuando surjan emergencias a cualquier hora, el cliente requirió una bola de 40 horas al mes.

TABLA 5 - 8*:* PAGO MENSUAL INGENIERO POR MANTENIMIENTO CORRECTIVO

Tiempo (día)	Horas	Número de Ingenieros	Costo/horas (S/.)	Costo Total (S/.)
1	40	1	100	4000

Fuente: Elaboración propia

Soporte de Emergencia (24x7) el cliente cuenta con soporte remoto las 24 horas del día los 7 días de la semana.

TABLA 5 - 9: PAGO MENSUAL INGENIERO POR SOPORTE DE EMERGENCIA

Tiempo (día)	Horas	Número de Ingenieros	Costo/horas (S/.)	Costo Total (S/.)
30	5040	1	40	201600

Fuente: Elaboración propia

De igual manera, para el servicio de Operación y Mantenimiento, se consideró un margen de ganancia del 15%, en la siguiente tabla se detalla el precio por mes.

TABLA 5-10*:* PRECIO FINAL DE OPERACIÓN Y MANTENIMIENTO CONSIDERANDO MARGEN DE GANACIA

	Gasto (S/.)	Margen de ganancia (%)	Precio (S/.)
Mantenimiento Preventivo	6400.00	15	7360.00
Mantenimiento Correctivo	4000.00	15	4600.00
Mantenimiento de Emergencia	201600.00	15	231840.00

Fuente: Elaboración propia

5.1.3 Flujo de Caja

El flujo de caja de cada año se obtuvo de acuerdo a los precios fijados con el cliente y la inversión se recuperó en el primer año.

TABLA 5 - 11: FLUJO DE CAJA

	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
Ingresos por HW y SW	0.00	89551.24	0.00	0.00	0.00	0.00
Ingresos por Diseño e implementación	0.00	36960.00	0.00	0.00	0.00	0.00
Ingresos por Operación y Mantenimiento	0.00	573024.00	573024.00	573024.00	573024.00	573024.00
Egresos por HW y SW	-81410.22	0.00	0.00	0.00	0.00	0.00
Egresos por Diseño e Implementación	-33600.00	0.00	0.00	0.00	0.00	0.00
Egresos por Operación y Mantenimiento	0.00	-531840.00	-531840.00	-531840.00	-531840.00	-531840.00
Flujo de Caja	-115010.22	167695.24	41184.00	41184.00	41184.00	41184.00
Flujo de Caja con IGV (18%)	-115010.22	137510.09	33770.88	33770.88	33770.88	33770.88

Fuente: Elaboración propia

La Tasa de rentabilidad interna (TIR) se haya cuando el tipo de actualización del valor del capital se hace cero. En la gráfica se ve como se llega al valor luego de una iteración desde el valor inicial del capital S/.147410.22 hasta S/. 0, obteniendo como valor de TIR 282%.

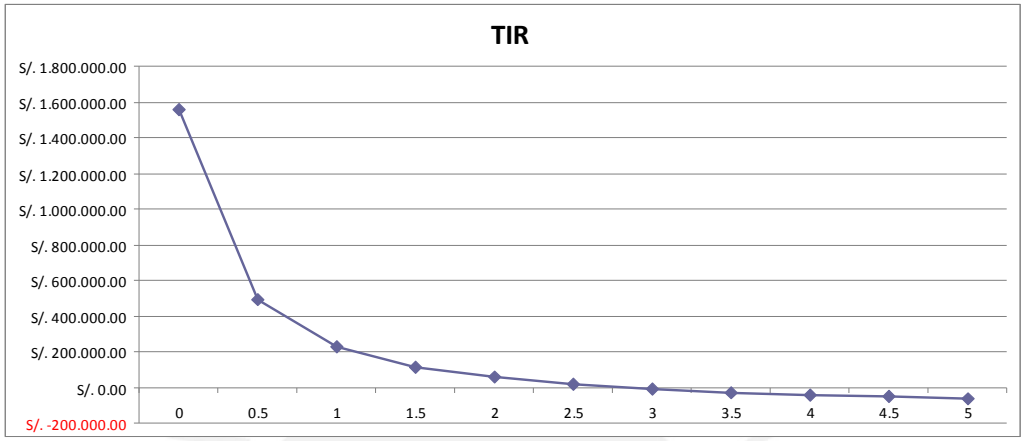

FIGURA 5- 1*: TASA DE RETORNO INTERNA*

Fuente: Elaboración propia

El Valor Neto Contable (VAN), mide el rendimiento de los flujos positivos y negativos originados por la inversión del proyecto durante el periodo de duración del proyecto. Con el flujo de caja y el TIR hallado para los 5 primeros años se obtiene un VAN de S/. 1 022 395.72.

Con ayuda de la curva de retorno podemos observar que la inversión se recupera en el primer año y se obtienen ingresos en los próximos 5 años por servicios de operación y mantenimiento

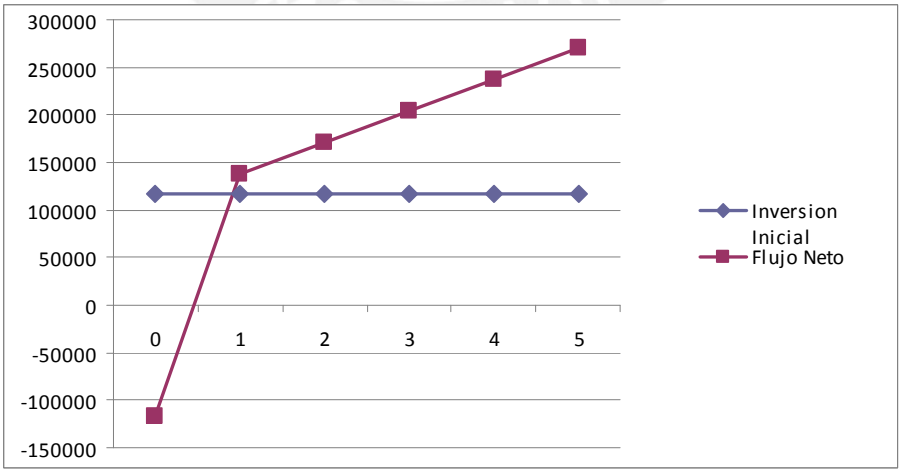

FIGURA 5- 2*: CURVA DE RETORNO DE LA INVERSIÓN*

Fuente: Elaboración propia

Con el TIR > 10% (10% representa el costo de oportunidad) y VAN > 0 la inversión genera ganancias superiores a la rentabilidad exigida, del análisis se obtiene que el VAN tiene un valor de S/. 88 403.02 nuevos soles y el TIR es de 61%, con estos resultados se concluye que el proyecto es rentable y la inversión se recupera en el primer año.

Conclusiones

- Se comprobó que los protocolos AAA RADIUS y TACACS+ tienen diferentes características en el manejo de autenticación y autorización. El protocolo RADIUS maneja ambos servicios de manera combinada, mientras que el protocolo TACACS+ los ofrece como servicios independientes. A pesar de ello fueron implementados en una misma red y coexisten para brindar una red con sistema de control de acceso robusto.

- Se demostró que con ayuda de adecuados protocolos y técnicas de red se puede optimizar el uso de recursos de la misma y hacer que esta sea más robusta frente a averías que pueda sufrir. En esta tesis usamos la técnica Etherchannel para implementar redundancia de enlace, demostrándose que el tiempo de respuesta ante una caída de enlace será menor a 1 ms. Asimismo se utilizó la técnica Etherchannel para balancear la carga entre los enlaces resultando en la ampliación del ancho de banda. También se usó el protocolo GLBP para implementar redundancia de equipos y balanceo de carga entre ellos.

- Al culminar con la implementación del presente proyecto se pudo concluir que, gracias al servidor RADIUS, un usuario inalámbrico puede autenticarse e ingresar a la red; asimismo, el servidor TACACS+, teniendo como base el nivel de privilegio del usuario, permite a este ingresar o no a los equipos de red para realizar configuraciones en los equipos.

- Se diseño una solución teniendo en cuenta las características mas valoradas por los usuarios finales: continuidad de servicio, rapidez en el intercambio de datos y seguridad de la información.

- Luego de finalizar el análisis económico, con ayuda de los métodos financieros: TIR y VAN, se determinó que este proyecto es rentable y la inversión se recupera durante el primer año.

Observaciones, Recomendaciones y Trabajos Futuros

- Se recomienda que si el número de usuarios es más grande al planteado en el escenario real de esta tesis, se implemente un directorio activo en una base de datos externa a los servidores. Y se trabaje con un solo directorio para ambos tipos de autenticación, esto ayuda a optimizar los tiempo de respuesta de las peticiones dentro de la red.

- Si se tuviera que implementar el sistema de autenticación en una empresa con diversas sedes, se recomienda usar los servidores en modo Proxy para equilibrar la carga de tráfico de solicitudes de autenticación y conmutar a otro servidor si uno falla.

- Se recomienda que los servidores DHCP sean instalados en los routers de salida, pues como el diseño de estos es redundante y con balanceo de carga se podría aprovechar este escenario para tener al servidor DHCP con redundancia, sin tener que instalarlo en dos servidores Windows server o en dos servidores Linux

- La infraestructura inicial de la empresa ya cuenta con cableado horizontal y vertical implementados, es por ello que la tesis no contempla dicho despliegue.

Bibliografía

[CHA2006] Chaparro Vargas, R. A. (2006) Análisis de desempeño y evaluación de requerimientos AAA en protocolos de seguridad sobre redes inalámbricas IEEE 802.11. Tesis publicada de Ciencias e Ingeniería, Universidad Militar Nueva Granada – Nueva Granada, Bogota. Colombia. Recuperado el día 5, Mayo, 2009, de http://dialnet.unirioja.es/servlet/articulo?codigo=2293131

[CIS2009] Cisco (2009). Terminal Access Controller Access System (TACACS+). Recuperado el día 19, Junio, 2009. de http://www.cisco.com/en/US/docs/ios/11_3/security/configuration/guide/sctplus.html

[CRA2004] Craig Brian. (2004) Security Protocols Used for AAA Services. CCNP BCRAN Exam Certification Guide. Pg. 402. Recuperado el día 8, Junio, 2009, de http://books.google.com/books/CCNP+BCRAM+Exam+Certification+Guide

[DLI2009] D-link (2009). DWL-3200AP 802.11g Managed Access Point. Recuperado el día 5, Octubre, 2009, de http://www.dlink.com/products/?pid=396

[LEH2006] Lehembre Guillaume. Seguridad Wi-Fi - WEP, WPA y WPA2. 2006. Francia. Recuperado el día 4, Mayo, 2009, de http://www.zero13wireless.net/wireless/seguridad

[LOP2008] López Mori, J. a. (2008). Diseño e Implementación de un Sistema de Gestión de Accesos a una red Wi-Fi Utilizando Software Libre. Tesis publicada de Ingeniería de Telecomunicaciones, Pontificia Universidad Católica del Perú – Lima, Lima. Perú

[MED2009] Mediavilla Didac. (2009). Seguridad en WLAN IEEE 802.11: Evaluación de los mecanismos de cifrado y autenticación. Tesis de maestria del Departamento de Telemática, Universidad Politecnica de Cataluña, Barcelona. España. Recuperado el día 25, Mayo, 2009, de http://upcommons.upc.edu/pfc/handle/2099.1/6762

[MIC2009] Microsoft (2009). Active Directory. Recuperado el día 14, Noviembre, 2009, de http://technet.microsoft.com/es-es/library/cc782657%28WS.10%29.aspx

[MIC2009] Microsoft (2009). Servicios de Certificate Server. Recuperado el día 16, Noviembre, 2009, de http://technet.microsoft.com/es-es/library/cc783511%28WS.10%29.aspx

[MIC2009] Microsoft (2009). Servicios de Certificate Server. Recuperado el día 12, Noviembre, 2009, de http://technet.microsoft.com/es-es/library/cc787275%28WS.10%29.aspx

[PIN2009] Pino, Carlos (2009). Material Pedagógico: Seguridad avanza de Wi-Fi. Perú: Pontifica Universidad Católica del Perú

[RFC2000] RFC (2000). Remote Authentication Dial In User Service. Recuperado el día 7, Mayo, 2009, de http://www.ietf.org/rfc/rfc2865.txt

[TEC2008] TECSUP. Sistema de Autenticación y Cifrado. 2008

[WIF2009] Wi-fi. (2009). WPA2.Recuperado el día 28, Junio, 2009, de http://www.wi-fi.org