Facultad de Ingeniería y Ciencias Agropecuarias

IMPLEMENTACIÓN DEL PROTOCOLO RADIUS EN UNA RED VIRTUAL PARA MEJORAR LAS SEGURIDADES INFORMÁTICAS

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el título de Ingeniero en Sistemas de Computación e Informática

Profesor Guía

Ing. Maritzol Tenemaza MSc.

Autor

Ramiro Xavier Escobar Pérez

Año

2012

DECLARACIÓN DEL PROFESOR GUÍA

"Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos para un adecuado desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación."

Ing. Maritzol Tenemaza MSc.

1706540638

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

Ramiro Xavier Escobar Pérez
1711861912

RESUMEN

El utilizar un servidor RADIUS, un protocolo reconocido como estándar en la industria de las Tecnologías de Información y Comunicación (TIC), para la gestión de los procesos de autenticación, contabilidad y acceso hacia los recursos de la red informática dentro de una organización, tiende a reducir las brechas de seguridad de la misma.

Mediante herramientas de virtualización se pretende diseñar la topología típica de una red y sobre ésta implementar una versión liberada de RADIUS denominada FreeRADIUS Server versión 2 en un servidor Linux, permitiendo la conectividad con los diferentes componentes que interactúan en una red.

Una vez integrado el protocolo RADIUS estará en capacidad de administrar el acceso a la red mediante procesos conocidos como “transacciones AAA” con dispositivos terminales que utilicen TCP/IP como protocolo de comunicación tales como: teléfonos inteligentes, PDAs, notebooks, iPods, etc.

ABSTRACT

Using a server through a protocol RADUIS, recognized as the industry standard in IT (Information Technology), to manage the processes of authentication, accounting and access to network resources within an organization tends to reduce the gaps Security of it.

By virtualization tools is to design the typical topology of a network and on the organization to implement a release called FreeRADIUS Server version 2 on a Linux server, allowing connectivity to the various components that interact in a network.

Once integrated RADIUS protocol will be able to manage access to the network via processes known as "AAA transactions" with terminal devices over TCP/IP such: as smart phones, PDAs, notebooks, iPods, etc.

INDICE.

1. Capítulo I: Introducción 1

1.1 Generalidades 1

1.2 Antecedentes 2

1.3 Objetivos 4

1.3.1 Objetivos específicos 4

2. Capítulo II: Aspectos técnicos 6

2.1 La arquitectura AAA 6

2.1.1 Un panorama del AAA 6

2.1.1.1 Autenticación 8

2.1.1.2 Autorización 8

2.1.1.3 Contabilidad 9

2.1.2 La estructura de autorización 9

2.1.2.1 Secuencias de Autorización 9

2.1.2.2 Roaming 12

2.1.2.3 Servicios Distribuidos 12

2.1.2.4 Políticas 14

2.1.2.5 Gestión de Recursos y Sesiones 14

2.2 RADIUS 15

2.2.1 Propiedades de RADIUS 16

2.2.2 Especificaciones de RADIUS 16

2.2.2.1 Utilizando UDP versus TCP 16

2.2.2.2 Formato de paquetes 17

2.2.2.3 Tipos de paquetes 19
2.2.2.4 Secretos Compartidos 21
2.2.2.5 Atributos y Valores 21
2.2.2.6 Métodos de autenticación 25
2.2.2.7 Reinos 27
2.2.3 Contabilización en RADIUS 27
2.2.3.1 Operación básica 28
2.2.3.2 El formato del paquete de contabilización 28
2.2.3.3 Tipos de paquetes de contabilización 30
2.3 LDAP 32
2.3.1 Lightweight 32
2.3.2 Directorio 33
2.3.3 Protocolo de acceso 35
2.3.4 Modelos LDAP 35
2.3.5 LDIF 37
2.3.5.1 ¿Qué es un atributo? 39
2.3.5.2 Autenticación 39
2.3.5.3 Directorios distribuidos 41
2.4 Arquitectura y modelos AAA para redes móviles e inalámbricas 43
2.4.1 Introducción 43
2.4.1.1 El modelo AAA en redes convergentes 45
2.4.2 Redes inalámbricas 47
2.4.2.1 Proceso de autenticación IEEE 802.11i 50
3. Capítulo III: Implementación 52
3.1 Antecedentes 52

3.1.1 Características del entorno 52
3.1.2 Riesgos en el uso de tecnologías WiFi 57
3.1.3 Protegiendo el acceso en entornos WiFi 58
3.2 Diseño de una red inalámbrica segura 59
3.2.1 Selección de los componentes de la solución 61
3.2.1.1 Servidor LDAP 61
3.2.1.2 Servidor AAA 65
3.2.1.3 Punto de Acceso 69
3.2.1.4 Clientes 71
3.3 Resumen de pasos a seguir 71
3.4 Instalando y configurando los componentes 72
3.4.1 Configurar el servidor de LDAP 73
3.4.2 Configuración del servidor Centos 5 y el servicio SAMBA 92
3.4.3 Instalación de FreeRADIUS y configuración del servicio 96
3.4.4 Configuración del cliente EAP 99
3.4.5 Configuración del suplicante y prueba de conexión 106
4. Capítulo IV: Conclusiones y recomendaciones 112
4.1 Conclusiones 112
4.2 Recomendaciones 113
5. Bibliografía 115
6. Glosario de términos 117

Tabla de Ilustraciones.

Ilustración 2-1 Relaciones independientes de confianza en una transacción salto-a-salto 7
Ilustración 2-2 La secuencia del agente 10
Ilustración 2-3 La secuencia de extraer 11
Ilustración 2-4 La secuencia de empujar 11
Ilustración 2-5 La secuencia del agente Roaming 12
Ilustración 2-6 Un modelo de servicios distribuidos 13
Ilustración 2-7 Una representación de la estructura del paquete de datos de RADIUS 18
Ilustración 2-8 El patrón de transmisión estándar AVP 22
Ilustración 2-9 X.500 sobre OSI versus LDAP sobre TCP/IP 33
Ilustración 2-10 Relaciones entre un cliente LDAP, un server LDAP y un repositorio de datos 34
Ilustración 2-11 LDAP requerimientos y respuestas 35
Ilustración 2-12 Ejemplo de un árbol de directorio LDAP 37
Ilustración 2-13 Un árbol de directorio LDAP 38
Ilustración 2-14 Detalle de la clase de objeto: person 40
Ilustración 2-15 Construyendo un directorio distribuido 42
Ilustración 2-16 Clase de objeto referenciado 43
Ilustración 2-17 Integración de RADIUS en redes móviles 47
Ilustración 2-18 Configuración del 802.1x 50
Ilustración 3-1 Establecimientos registrados en Ecuador según Censo Económico 2010 53
Ilustración 3-2 Equipamiento en hogares de Ecuador ENEMDU 2010 55
Ilustración 3-3 Utilización de Internet en Ecuador ENEMDU 2010 56
Ilustración 3-4 Componentes de una WLAN segura 60
Ilustración 3-5 Cuota de participación de Microsoft Windows dentro del mercado de sistemas operativos 64
Ilustración 3-6 Interfaz gráfica de inicio del sistema operativo Microsoft Windows 2008 Server edición estándar 65

Ilustración 3-7 Interfaz gráfica del sistema operativo Centos versión 5 69
Ilustración 3-8 WAP Cisco Aironet 1200 71
Ilustración 3-9 Dispositivos con conexión WiFi -computador portátil y teléfono inteligente 71
Ilustración 3-10 Interface para selección de parámetros iniciales en Windows Server 2008 73
Ilustración 3-11 Interfaz que confirma inicio del proceso de instalación 74
Ilustración 3-12 Interface para activación de Windows en línea 74
Ilustración 3-13 Validación de la clave de activación del producto 75
Ilustración 3-14 Interface que permite la selección de la versión de Windows Server 2008 75
Ilustración 3-15 Interface de aceptación de los términos del licenciamiento 76
Ilustración 3-16 Interface que permite seleccionar el tipo de instalación 76
Ilustración 3-17 Selección del disco destino 77
Ilustración 3-18 Indicador de progreso en el avance de la instalación 77
Ilustración 3-19 Alerta sobre reiniciación del equipo 78
Ilustración 3-20 Definición de la contraseña de administrador 78
Ilustración 3-21 Selección del menú “Server Manager” 79
Ilustración 3-22 Selección del rol del servidor 79
Ilustración 3-23 Resumen de consideraciones previo al proceso de selección de roles 80
Ilustración 3-24 Plantilla resumen del servicio del AD y consideraciones para su instalación 81
Ilustración 3-25 Confirmación del requerimiento de instalación del rol del Active Directory 81
Ilustración 3-26 Resumen del proceso de instalación y estatus de los mismos 82
Ilustración 3-27 Interfaz que muestra la presencia del rol de AD en el servidor 83
Ilustración 3-28 Activación del servicio del AD mediante el comando dcpromo.exe 83
Ilustración 3-29 Asistente de configuración para activación del servicio del AD 84

Ilustración 3-30 Declaración de compatibilidad de la versión del servicio del AD en Windows 2008 85
Ilustración 3-31 Interfaz para la creación de un nuevo dominio 85
Ilustración 3-32 Ventana que permite el ingreso del dominio a crear 86
Ilustración 3-33 Selección del nivel funcional del bosque 87
Ilustración 3-34 Selección de la opción de servidor DNS como rol adicional ... 87
Ilustración 3-35 Ventana que alerta sobre la instalación del servicio DNS y sus consideraciones 88
Ilustración 3-36 Definición de la ubicación de carpetas del sistema del AD 89
Ilustración 3-37 Definición de una clave para restauración del AD 89
Ilustración 3-38 Resumen sobre los parámetros definidos para la instalación del AD 90
Ilustración 3-39 Instrucción de reiniciar el sistema al término del proceso de instalación del AD 90
Ilustración 3-40 Interfaz que muestra el término del proceso de instalación del AD 91
Ilustración 3-41 Catálogo de usuarios del domino *udla.local* gestionado por el AD 92
Ilustración 3-42 Ajuste de la dirección IP en el servidor Centos 93
Ilustración 3-43 Componentes de SAMBA 3X para inter-operatividad con Windows 94
Ilustración 3-44 Parámetros de configuración de SAMBA mediante el archivo *smb.cof* 94
Ilustración 3-45 Iniciación del servicio SAMBA en el servidor Centos 95
Ilustración 3-46 Ejecución de comando net join que permite unión con el servidor Windows 95
Ilustración 3-47 Validación del usuario Windows en un entorno Linux mediante comando ntlm_auth 96
Ilustración 3-48 Instalación del paquete freeradius2 - 2.1.7-7.e15.i386 para Centos OS-5 97
Ilustración 3-49 Edición del archivo ntlm_auth para autenticación a través de Radius 97

Ilustración 3-50 Definición del método de autenticación vía comando ntlm_auth 98
Ilustración 3-51 Visualización del modo debug para el servicio Radius 98
Ilustración 3-52 Solicitud de autenticación de un usuario del AD desde el servidor Radius 99
Ilustración 3-53 Prueba de validación de un usuario del AD mediante el servicio Radius 99
Ilustración 3-54 Definición de parámetros del AP en el servidor RADIUS 100
Ilustración 3-55 Definición del método de autenticación entre el AP y Radius 101
Ilustración 3-56 Definición del protocolo MSCHAP para manejo de clientes Windows 101
Ilustración 3-57 Propiedades de Hyperterminal para conexión con el AP 102
Ilustración 3-58 Parámetros iniciales del AP 102
Ilustración 3-59 Ingreso de parámetros de dirección IP en el AP 103
Ilustración 3-60 Definición de la dirección IP del servidor Radius en el AP 103
Ilustración 3-61 Habilitación del método WEP para encripción en el AP 103
Ilustración 3-62 Creación de la red inalámbrica “radius-X” en el AP 104
Ilustración 3-63 Salida de los parámetros de configuración ingresados en los pasos anteriores en el AP 104
Ilustración 3-64 Interfaz de la aplicación “Intel PROSet/Wireless” para gestión de redes inalámbricas 106
Ilustración 3-65 Creación de un perfil personalizado para una red inalámbrica 107
Ilustración 3-66 Definición del nombre del perfil e identificador de la red inalámbrica 107
Ilustración 3-67 Interfaz para definición de parámetros de seguridad de la red inalámbrica en el lado del cliente 108
Ilustración 3-68 Interfaz para definición de parámetros de seguridad de la red inalámbrica en el lado del servidor 109
Ilustración 3-69 Interfaz que permite la selección de perfiles de redes inalámbricas y su conexión 109
Ilustración 3-70 Interfaz que permite hacer seguimiento de eventos 110

Ilustración 3-71 Visualización de los eventos de una conexión exitosa utilizando Radius 111

Índice de Tablas.

Tabla 2-1 Tipos de atributos y valores de los campos 24
Tabla 2-2 Ejemplo de archivo de texto utilizado como diccionario 25
Tabla 2-3 Estructura paquete:Requerimiento de contabilización 31
Tabla 2-4 Estructura paquete: Requerimiento de respuesta 31
Tabla 2-5 Comparación de redes celulares y WLAN 46
Tabla 3-1 Lista de denominaciones comerciales del protocolo LDAP según el proveedor 62
Tabla 3-2 Niveles de seguridad según calificación EAL 63
Tabla 3-3 Servidores especializados en RADIUS 67
Tabla 3-4 Resumen de los pasos de configuración y alineamiento con los objetivos 72

1. Capítulo I: Introducción

1.1 Generalidades

Siendo la actual, una era digital, la mayoría de la información se encuentra en formato electrónico y presentado en infinidad de aplicaciones que utilizan una red para transmitirla.

La exclusividad de ordenadores, servidores, impresoras y computadoras portátiles que eran los llamados a conectarse a una red utilizando el protocolo IP, hoy en día se ha multiplicado en billones de dispositivos inteligentes que dependen de la disponibilidad de esta conexión para gestionar la información que de manera ávida, los sistemas que interactúan con ellos y los usuarios están siempre consumiendo. La imagen de usuarios visualizando correos electrónicos en sus teléfonos inteligentes o utilizando navegadores para acceder hasta aplicaciones WEB desde un equipo que utiliza el concepto de la computación móvil como son los notebooks, netbooks, Tablet PCs y iPods son cada vez más cotidianas y familiares tanto para ámbitos empresariales, académicos, de entretenimiento y dentro de nuestros propios hogares.

Si adicionamos a lo arriba expuesto el auge de las aplicaciones que explotan el fenómeno de las redes sociales, como punta de lanza de la Web 2.0, entre otras herramientas de productividad. Han impreso entre sus consumidores la necesidad de estar “siempre conectados en línea” a fin de obtener un mejor beneficio. Esta combinación redunda en tener cada vez más usuarios demandantes de conexión hacia la red independiente del dispositivo y el medio a utilizar sea este a través de cable o inalámbrico.

Frente a esta realidad el tema de Seguridad Informática es un tópico que debe ser analizado con profundidad y mucho detenimiento por parte de los administradores a fin de mantener un entorno controlado evitando accesos no autorizados por parte de los usuarios, partiendo del principio irrefutable de que en toda organización el activo más importante que ésta dispone es la información y los recursos que utiliza para su diaria operatividad.

Aunque no existe un entorno totalmente seguro, son cuatro características que un sistema debe controlar y estas son:

- **Integridad:** La información sólo puede ser modificada por quien está autorizado y de manera controlada.
- **Confidencialidad:** La información sólo debe ser legible para los autorizados.
- **Disponibilidad:** Debe estar disponible cuando se necesita.
- **Irrefutabilidad** (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Aunque en un mundo ideal no debería existir la necesidad de autenticarse, es decir validar nuestra identidad a través de métodos que certifiquen que realmente somos quienes aseguramos ser, dentro del entorno empresarial esta condición es imperativa ya que constituye el único medio que permite gestionar las políticas de acceso que armonizan la interacción entre los usuarios y los recursos que éstos demandan, todo esto dentro del marco de los principios de seguridad arriba expuestos.

1.2 Antecedentes

Es realmente desafiante para un administrador de red, tomando en cuenta el actual entorno y la demanda de usuarios, el proveer las condiciones de seguridad necesarias para mantener un entorno controlado.

Ante esta realidad el grupo de trabajo formado por el Internet *Engineering Task Force* (IETF)[1] respondió con la arquitectura de un modelo denominado AAA cuyo acrónimo viene del inglés: "*Authentication, Authorization y Accounting*" (Autenticación, Autorización y Contabilidad).

Para hacer una analogía que facilite la comprensión del modelo propuesto, éste se desarrolla para responder a las siguientes interrogantes en la interacción con los usuarios:

[1] http://www.ietf.org/

- ¿Quién eres tú?
- ¿Qué permisos tengo permitido entregarte?
- ¿Qué hiciste o haces con mis servicios mientras los utilizas?

Previo a la introducción del modelo AAA cada máquina utilizaba un diferente método de autenticación de usuarios, ante la falta de un estándar formal, unos lo hacían mediante perfiles locales, otros habían utilizado el *Challenge/Handshake Authentication Protocol* (CHAP) y algunos más pequeñas bases de datos en SQL. El mayor problema que afrontaba éste modelo era la escalabilidad: el manejar el rastro de un usuario en un equipo no representaba mayor desafío, pero al incrementar la cantidad de dispositivos (donde cada uno manejaba su propio método de autenticación) interconectados rápidamente convirtió este reto en una pesadilla.

El grupo de trabajo a cargo del AAA creó una arquitectura funcional que pudiera direccionar las limitaciones de lo arriba expuesto. El primer paso era obvio y consistía en la necesidad de concentrarse en un equipo descentralizado que facilite su uso en redes heterogéneas y segundo, estandarizar la forma en la cual los usuarios: deben ser verificados, inician sesiones y son monitoreados a través de la red.

Pues bien existe un protocolo que permite hacer todo esto y es el: *Remote Access Dialin User Service*, o RADIUS.

A pesar de que existen otros protocolos que satisfacen plenamente los requerimientos de la arquitectura, RADIUS fue creado previamente a la aparición del modelo AAA y éste fue el primer protocolo real que exhibió la funcionalidad AAA y creció en la industria con amplia aceptación.

Si bien RADIUS está presente como solución desde la década de los noventa, ha sido desarrollado por empresas de código propietario que han hecho inaccesible esta solución para ciertos segmentos de la industria, especialmente para las Pymes (Pequeñas y medianas empresas) donde se requiere proteger el activo más importante de estas organizaciones que es la información, que ahora atraviesa la red en formato digital.

1.3 Objetivos

- Implementar el modelo AAA en una red virtual mediante el protocolo RADIUS para clientes que se conectan a la red vía inalámbrica.

- Desarrollar una topología de red típica dimensionada para el tamaño de una Pyme. Se utilizarán herramientas de virtualización para poner en producción aquellos componentes susceptibles de correr sobre esta plataforma como son: servidores, PCs de clientes, ruteadores y otros elementos. Minimizando el uso de equipos físicos a fin de permitir la portabilidad de la solución con fines didácticos.

- Integrar las funcionalidades y capacidades del servidor RADIUS a las prestaciones del protocolo LDAP, cuyo acrónimo en ingles corresponde a: Lightweight Directory Access Protocol. Quien será el encargado de administrar el catálogo de los objetos componentes de una red.

1.3.1 Objetivos específicos

- Configurar los elementos virtuales, físicos y lógicos que conforman la red.
- Gestionar transacciones AAA para equipos inalámbricos, centralizadas en el server *FreeRADUIS*[2] versión 2.1 sobre Linux.
- Disponer de un entorno que tenga en cuenta características de seguridad para clientes móviles.

Los fundamentos teóricos de los componentes involucrados en la consecución de los objetivos serán abordados en el desarrollo del Capítulo II. Se explicará en detalle los factores claves para el éxito del modelo AAA y se revisará el protocolo RADIUS observando con detenimiento la interacción que realiza con servidores LDAP y su posicionamiento en la industria a lo largo de estos años y el porqué de su vigencia. La seguridad de redes inalámbricas es un tópico a

[2] http://freeradius.org/

revisarse ya que es el medio nativo de conexión para equipos de computación móviles sin dejar de mencionar a los dispositivos inteligentes basados en IP y sus limitaciones frente a este entorno.

Contar con una guía detallada de la configuración del FreeRadius que permite la interacción con los elementos de la red es la propuesta del Capítulo III donde se incluirá además todas las consideraciones técnicas de la puesta en marcha de esta red virtual dentro del marco AAA.

Plantear conclusiones y recomendaciones en función del entorno construido en la red virtual y plasmarlos en el Capítulo IV, donde de manera práctica y objetiva se pondrán en consideración frente a entornos empresariales identificados como el segmento de las Pymes, que representan en número y aporte un grupo muy significativo en la economía del país que se integra cada día con mayor celeridad a la era digital para la gestión de sus negocios pero no siempre evaluando de manera detenida los riesgos en materia de seguridad informática.

2. Capítulo II: Aspectos técnicos

El desarrollo de este capítulo explora en forma detallada las características técnicas, estándares y especificaciones relevantes de los elementos claves que componen la arquitectura virtual a construir.

Los elementos que en su engranaje permitirán la puesta en marcha de esta propuesta y cuyos conceptos exploraremos son:

- El modelo AAA
- El protocolo RADIUS
- El protocolo LDAP
- Redes inalámbricas seguras

2.1 La arquitectura AAA

2.1.1 Un panorama del AAA

El Grupo de Trabajo a cargo del modelo AAA por encargo del Internet Research Task Force (IRTF) lo creó diseñado para trabajar en ambientes con variedad de requerimientos de usuarios e igual variedad de diseños de redes. En pocas palabras, la arquitectura AAA es un intento de trazar un diseño de la forma en la que las piezas AAA encajan, por ende una implementación AAA puede ser tan simple o compleja como ésta necesite ser.

Existen algunos elementos claves de este modelo que lo hacen posible.

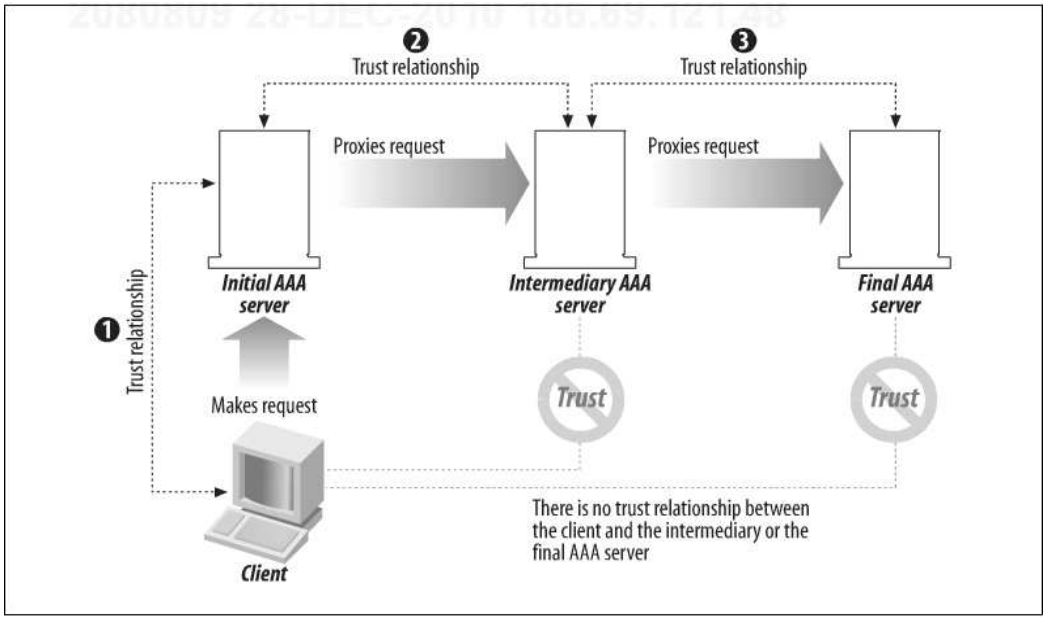
Primero el modelo AAA depende de la interacción cliente/servidor, en la cual un sistema cliente requiere de los servicios o recursos de un sistema servidor. En una implementación simple estos roles generalmente no son intercambiables es decir el servidor nunca actúa como cliente y viceversa. El ambiente cliente/servidor permite un buen diseño de balance de la carga en el cual la alta disponibilidad y el tiempo de respuesta son críticos, los servidores pueden ser distribuidos o centralizados a lo largo de la red. Contrasta esto al modelo de red opuesto, una red peer-to-peer (P2P). Con redes P2P todos los sistemas despliegan características tanto del cliente como del servidor, lo cual introduce

algunos procesos que corren como servicios o demonios en ambos lados y producen retardos e indisponibilidad.

Otro elemento relevante es la capacidad de Proxy, un servidor AAA puede ser configurado para autorizar un requerimiento o pasar éste a otro servidor AAA quien a su vez hará las provisiones necesarias o pasará el mismo nuevamente. En esencia se crea una cadena *proxy*, donde servidores AAA pueden realizar requerimientos ya sea como clientes o como servidores AAA donde una relación de confianza ha sido creada en cada salto cliente/servidor hasta que el requerimiento alcance al equipo encargado de provisionar los recursos demandados.

La capacidad de *Proxy* es un elemento muy útil en el modelo AAA y un factor clave para implementaciones distribuidas en entornos empresariales en la cual algunos equipos pueden ser configurados para siempre pasar requerimientos AAA hasta máquinas ubicadas en otras locaciones. La imagen adjunta trata de ejemplificar el proceso dentro de esta cadena.

Ilustración 2-1 Relaciones independientes de confianza en una transacción salto-a-salto



Fuente: (Hassell, October 8, 2002)

El modelo AAA se enfoca en tres aspectos cruciales del control de acceso de los usuarios: autenticación, autorización y contabilidad, respectivamente.

2.1.1.1 Autenticación

La autenticación es el proceso de verificar la identidad declarada por una persona o máquina.

El proceso mas común y conocido es aquel que utiliza un ID y un *password* en el que el conocimiento del *password* es la representación de la autenticidad del usuario. Los certificados digitales son una de las soluciones preferidas para la autenticación en Internet sobre todo por la demanda de los creadores de sitios que ofrecen servicios de *e-commerce* y otras transacciones financieras de disponer de métodos más fuertes y fiables de autenticación.

El aspecto clave de la autenticación es que ésta permite a dos objetos únicos establecer una *relación de confianza* donde los dos asumen ser usuarios válidos. La confianza entre los sistemas permite una funcionalidad clave, como son los servidores *proxy*, donde un sistema atiende un requerimiento a nombre de otro sistema y permite implementaciones AAA sobre redes heterogéneas soportando diferentes tipos de clientes y servicios.

2.1.1.2 Autorización

La autorización implica el uso de un conjunto de reglas o plantillas para decidir lo que un usuario autenticado puede hacer dentro del sistema, donde el administrador tiene la facultad de definir estas reglas.

Las denominadas “implementaciones inteligentes” de servidores AAA actuarán sobre la lógica de analizar un requerimiento y otorgar los accesos que pueda, siempre y cuando el requerimiento sea válido. Como ejemplo podemos citar el requerimiento de un cliente dial-up que solicita multienlace, un servidor genérico AAA simplemente denegaría la solicitud mientras que una implementación inteligente se fijaría con detenimiento en el requerimiento y solo permitiría una conexión mientras deniega las otras.

2.1.1.3 Contabilidad

La contabilidad completa el marco del modelo AAA, ésta se encarga de registrar y documentar los recursos utilizados por el cliente durante la conexión. Esto puede incluir el total de tiempo en el sistema o la cantidad de datos ya sean enviados o recibidos durante la sesión. La contabilidad se lleva a cabo para mantener estadísticas de inicios de sesiones, del uso de información y es utilizada para el control de autorización, facturación, análisis de tendencias, utilización de recursos y actividades asociadas a planear la capacidad.

2.1.2 La estructura de autorización

Se refiere a un subconjunto dentro del documento denominado *Request For Comment* (RFC) diseñado por el Grupo de trabajo AAA del IETF. Un documento de arquitectura esta diseñado como una hoja de ruta pero éste tiende a ser un poco más específico. La estructura diseña como los sistemas interactúan uno con otro, pero las estructuras se enfocan generalmente en modelos específicos de ciertos entornos como es un mayorista de Internet o un centro corporativo de *Virtual Private Network* (VPN) u otra situación similar.

La estructura de autorización introduce el concepto de un *User Home Organization* (UHO), la cual es una entidad que tiene una relación contractual directa con un usuario final. También está involucrado el *Service Provider* (SP) el cual mantiene y provisiona recursos tangibles de la red. El UHO y el SP no necesitan ser la misma organización pero para propósitos de ésta ilustración examinaremos en escenarios donde el UHO y el SP son la misma entidad.

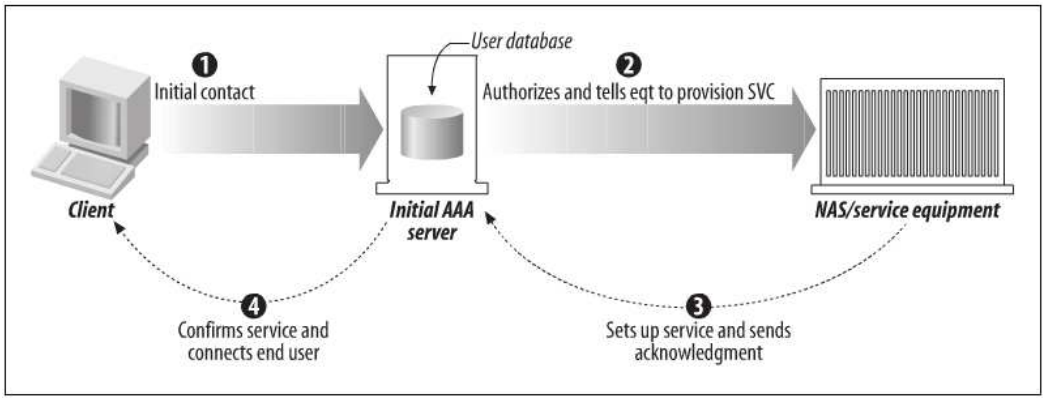
2.1.2.1 Secuencias de Autorización

Existen varios métodos distintos en los cuales el usuario final, el servidor AAA y el equipo de red se comunican durante la transacción. Específicamente existen tres secuencias diferentes en la que cada máquina es contactada.

La secuencia de agente

En esta secuencia el servidor AAA actúa como un intermediario de todo tipo entre el equipo que presta el servicio y el usuario final. El usuario final inicialmente contacta al server AAA el cual autoriza el requerimiento del usuario y envía un mensaje al equipo que presta el servicio notificando que inicialice el servicio y lo ponga disponible. El servidor ejecuta dicha tarea, notifica al server AAA y la notificación es pasada al usuario final quien entonces empieza a utilizar los servicios de la red. Esta secuencia es típicamente utilizada en aplicaciones de banda ancha en las cuales la calidad de servicio (QoS) es parte de un contrato existente.

Ilustración 2-2 La secuencia del agente

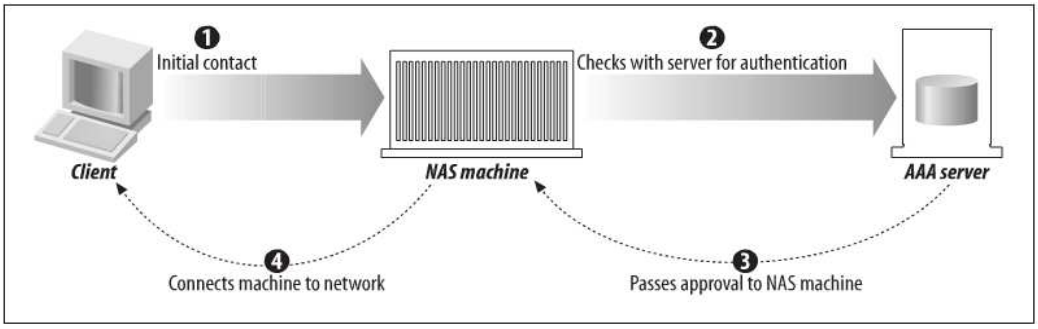


Fuente: (Hassell, October 8, 2002).

La secuencia de extraer

El usuario final se conecta directamente al equipo proveedor de servicios el cual entonces revisa con un server AAA sobre el análisis del requerimiento. El servidor AAA notifica al prestador de servicios sobre su decisión y éste procede a conectar o desconectar al usuario de la red.

Ilustración 2-3 La secuencia de extraer

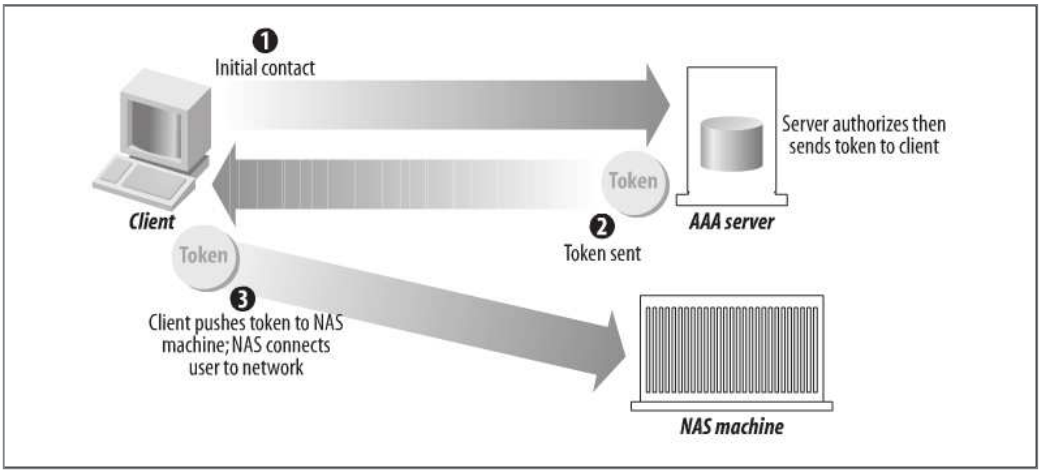


Fuente: (Hassell, October 8, 2002).

La secuencia de empujar

La secuencia de empujar altera la relación de confianza entre todas las máquinas en una transacción. El usuario primero se conecta a un server AAA y cuando el requerimiento al servidor es autorizado, el server AAA distribuye un tipo de autenticación de “recepción” (un certificado digital o un token firmado, tal vez) como respuesta al usuario final. El usuario final a continuación, empuja este token junto con su solicitud al equipo de servicio y el equipo trata a la entrada del servidor AAA como una luz verde a la prestación del servicio. La principal distinción es que el usuario actúa como el agente entre el server AAA y el equipo proveedor del servicio.

Ilustración 2-4 La secuencia de empujar



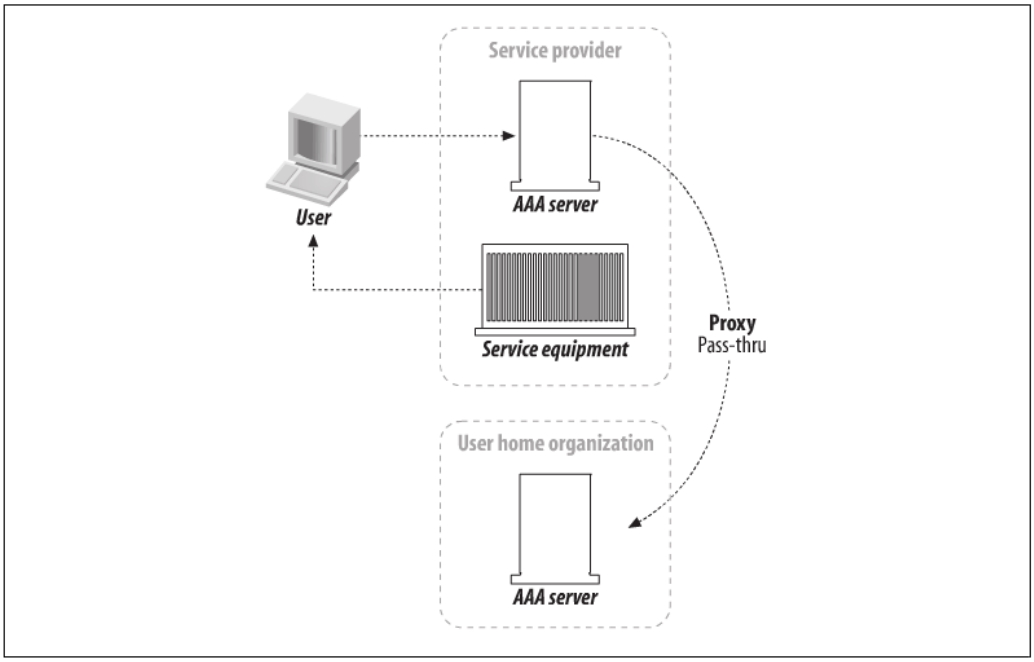
Fuente: (Hassell, October 8, 2002).

2.1.2.2 Roaming

Es el modelo en el cual no todos los elementos y servidores AAA están bajo el control y/o administración de una entidad o todos ellos son propiedad de una organización. Esta capacidad permite añadir un giro interesante al concepto de progresión en cuanto a los componentes de la red. El servicio de Roaming es bastante común actualmente ya que equipos terminales pueden conectarse al servicio utilizando la infraestructura de un proveedor que administra un dominio diferente.

Todas las secuencias de autorizaciones arriba descritas son posibles de combinar bajo este modelo y se ilustran en la siguiente figura:

Ilustración 2-5 La secuencia del agente Roaming



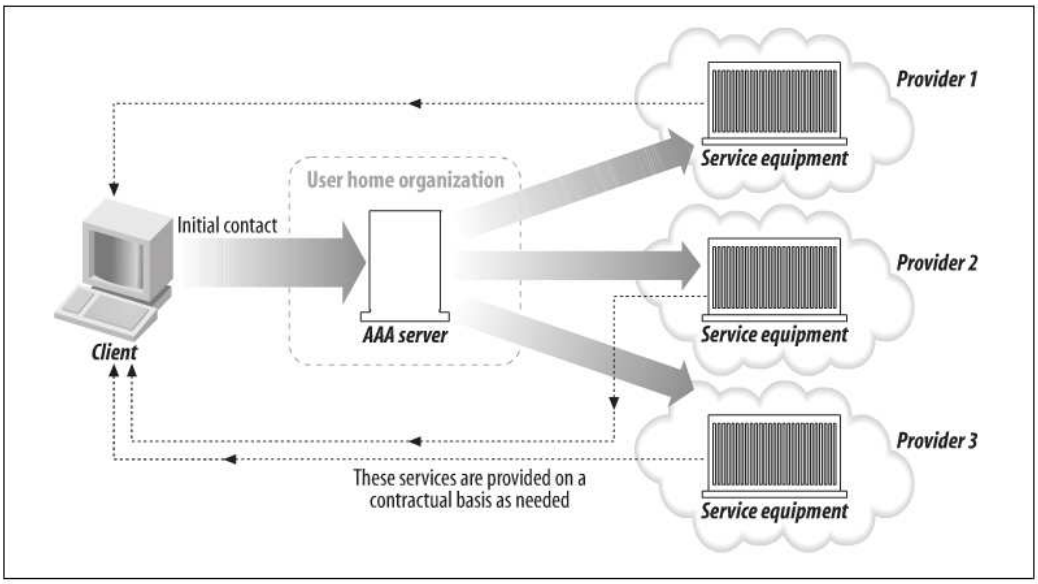
Fuente: (Hassell, October 8, 2002)

2.1.2.3 Servicios Distribuidos

Constituye la capacidad de especializar equipos y/o procesos como elementos que interactúan sobre protocolos basados alrededor del diseño AAA.

Las características de Servicios Distribuidos en conjunción con el Roaming han permitido la creación de nuevos negocios dentro de la infraestructura de IT. Así pueden existir de manera autónoma empresas dedicadas a proveer exclusivamente funciones de Autorización y Autenticación a diversas redes, actuando como "*broker* AAA" para ISP mayoristas y/o minoristas o siendo corporaciones de *outsourcing* de sus propios grupos de *Dial-Up*.

Ilustración 2-6 Un modelo de servicios distribuidos



Fuente: (Hassell, October 8, 2002)

Consideremos una situación donde un cliente contractualmente solicita a su ISP la provisión de cierto ancho de banda a lo largo de todo el país a sabiendas que éste no dispone de una cobertura completa en el territorio con su propia red. Bajo este escenario el ISP procederá a contratar con numerosos mayoristas la prestación de diversos servicios para cubrir las necesidades de sus clientes. En este caso la primera empresa proveedora actuará como cliente para establecer contratos que cubran las necesidades de establecer una política de QoS en equipos en todo el país, fuera de su red, que le permitan satisfacer su condición contractual con el cliente. Bajo esta condición éste último está utilizando un servicio distribuido.

2.1.2.4 Políticas

Se define como política el insumo que utiliza un servidor AAA para determinar luego de un análisis, sí una petición es válida y debe concederse.

El marco AAA prevé un conjunto de directivas que se extiende a través de múltiples dominios y entidades. Se enumeran tres tareas específicas para un servidor AAA en términos de la utilización de políticas, las mismas deben ser: recuperadas, evaluadas y cumplidas. La manera en que esto puede efectivizarse varía ampliamente dependiendo del entorno, incluso puede contener consultas hacia un directorio que utiliza un protocolo de directorio abierto como es el LDAP.

Cualquier servidor que reúna los requerimientos genéricos del AAA debe tener alguna forma de almacenar y retribuir información de políticas. Estas políticas están almacenadas en un repositorio, el mismo puede virtualmente ser de cualquier tipo que permita guardar información como: una base de datos, un archivo de texto plano u otro mecanismo de almacenamiento.

2.1.2.5 Gestión de Recursos y Sesiones

A continuación detallaremos qué son cada uno de estos componentes y cómo éstos pueden beneficiar a un protocolo que está basado en el modelo AAA.

Gestión de Recursos es básicamente la habilidad de monitorear los recursos que han sido previamente asignados. Un programa o un utilitario denominado “Gestor de Recursos” debería estar disponible para recibir y desplegar información sobre un recuso en tiempo real.

Gestión de Sesiones es la capacidad de un protocolo o parte de un equipo de notificar a un servidor AAA de un cambio en las condiciones e idealmente modificar una sesión existente. Ésta sesión podría ser cambiada, puesta en modo de espera o finalizada en base al cambio de condiciones registradas por el Gestor de Recursos.

La combinación de la Gestión de Recursos y Sesiones permite la implementación de complicadas políticas y provisionarlas de manera fácil a lo largo de una plataforma distribuida. La agilidad para adaptarse a una variedad de condiciones ha permitido al grupo de trabajo AAA profundizar en investigaciones, produciendo algunas alternativas de desarrollo.

2.2 RADIUS

Éste protocolo fue creado por un grupo de trabajo mucho antes que aparecieran los fundamentos y diseños del modelo AAA. Sin embargo las similitudes con éste último son destacables.

El modelo AAA es la base de la siguiente generación de protocolos para control de acceso remoto, sin embargo la amplia presencia de RADIUS y el bien ganado respeto en la industria hacen prever que aun tenga un futuro provisorio.

RADIUS nace como respuesta a una necesidad, en este caso la de tener un método de autenticación, autorización y contabilidad de usuarios que requieren acceder a recursos de computación heterogéneos.

El origen de RADIUS se remonta a 1991, con la empresa Merit Networks un gran operador que administraba una larga pila de recursos del tipo dial-up para acceso a Internet a lo largo de California. En su momento, los métodos de autenticación eran peculiares para específicas piezas de equipos, lo cual añadía una sobrecarga de trabajo y no permitía flexibilidad a la hora de la administración y generación de reportes. Ya que los usuarios dial-up crecían, la corporación decidió que necesitaban un mecanismo más flexible y expandible que les permitiera mantener sus operaciones, por lo tanto Merit envió un requerimiento de propuesta y la Empresa Livingston fue una de las primeras en responder. Los representantes de Merit y Livingston luego de varias reuniones y conferencias escribieron la primera versión de RADIUS. Steve Willins fue el desarrollador del software el cual corría sobre Unix y fue construido para operar sobre los equipos que construía Livingston y el servidor de RADIUS de Merit. En cierto momento la empresa Livingston se convirtió en Lucent así Merit y Lucent acordaron los pasos para la formalización y aceptación de la industria

de RADIUS como un protocolo. Ambas compañías ahora ofrecen un servidor RADIUS al público sin costo alguno.

2.2.1 Propiedades de RADIUS

Las especificaciones para el protocolo RADIUS presente en el documento que contiene los requerimientos para comentarios (RFC), dictan que:

- Está basado en el *User Datagram Protocol* (UDP), es decir que no utiliza conexiones directas.
- Utiliza un modelo de seguridad salto-por-salto.
- No tiene estado.
- Soporta autenticación mediante el *Password Authentication Protocol* (PAP) y el *Challenge-Handshake Authentication Protocol* (CHAP) mediante el *Point-to-Point Protocol* (PPP).
- Utiliza MD5 (*Message-Digest algorithm* 5) para algoritmos de ocultamiento de contraseñas.
- Provee hasta 50 pares de atributos y/o valores con la habilidad de crear pares acorde a la especificación del vendedor.
- Soporta el modelo de autenticación, autorización y contabilidad.

2.2.2 Especificaciones de RADIUS

Se describirán las características mas relevantes del RFC su tamaño original es de 80 páginas. Algunas partes del documento son anticuadas, están fuera de uso o simplemente no son relevantes.

2.2.2.1 Utilizando UDP versus TCP

Esto obedece netamente a requerimientos operacionales, fue seleccionado debido a que RADIUS tiene algunas propiedades inherentes que son características de UDP. RADIUS requiere que las consultas fallidas a un servidor primario de autenticación sean re-direccionadas a un servidor secundario y para lograr esto, una copia del requerimiento original debe existir por encima de la capa de transporte del modelo OSI. En efecto esto hace mandatorio la utilización de temporizadores.

Debido al requerimiento de que RADIUS no tiene estado, UDP luce como natural para esta tarea ya que el mismo tampoco lo tiene. Con TCP clientes y servidores deben tener un código especial o tareas administrativas para mitigar los efectos de perdida de energía, reiniciaciones, tráfico congestionado en la red y decomiso de sistemas. UDP previene esto ya que permite a una sesión abrirse y permanecer abierta a lo largo de la transacción.

Para permitir que sistemas pesados utilicen tráfico en el backend, con lo que algunas oportunidades retrasan las consultas por un tiempo mayor a 30 segundos, se determinó que RADIUS debería ser multiproceso. UDP permite a RADIUS diseminar y servir a múltiples requerimientos a la vez y cada sesión tiene total habilidad de comunicación entre el dispositivo de la red y el cliente, para esta tarea, UDP se ajustaba perfectamente.

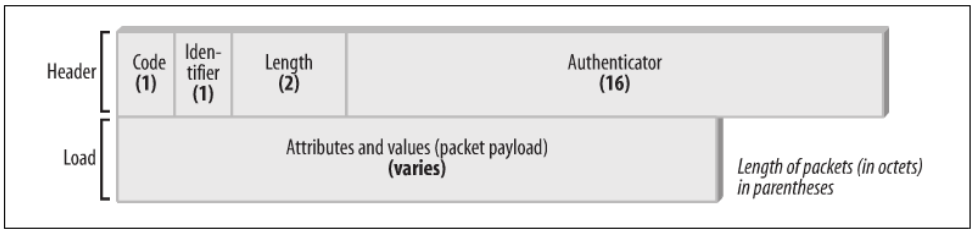
La única desventaja de utilizar UDP obedece a que los desarrolladores debieron crear y administrar los temporizadores por ellos mismos, siendo esta una capacidad incluida dentro de TCP. A pesar de aquello el grupo a cargo de RADIUS consideró que esta dificultad era menor versus la conveniencia y simplicidad del uso de UDP y así lo hicieron.

2.2.2.2 Formato de paquetes

El protocolo RADIUS utiliza paquetes UDP para pasar la transmisión entre el cliente y el servidor. El protocolo se comunica sobre el puerto 1812, el cual es un cambio del RFC original. La primera versión especificaba que la comunicación tenía que darse en el puerto 1645, pero posteriormente se encontró conflictos con el servicio “*Datametrics*”.

La estructura predecible del paquete que utiliza RADIUS para la comunicación, se muestra en la siguiente imagen:

Ilustración 2-7 Una representación de la estructura del paquete de datos de RADIUS



Fuente: (Hassell, October 8, 2002)

Código

Esta región tiene la longitud de un octeto y sirve para distinguir el tipo de mensaje RADIUS que está siendo enviado en el paquete. Aquellos paquetes con códigos inválidos son descartados sin enviar notificación.

Identificador

Con una longitud de un octeto este campo se lo utiliza para enhebrar o encadenar automáticamente los requerimientos iniciales y las réplicas subsiguientes. Los servidores de RADIUS pueden generalmente interceptar mensajes duplicados para examinar factores como la dirección IP origen, el puerto UDP original, el tiempo transcurrido del mensaje sospechoso y el campo del identificador.

Longitud

Es usado para especificar cuan largo un mensaje de RADIUS es, el valor en éste campo es calculado y resulta de la suma de los campos: código, identificador, longitud, autenticador y atributo, luego de su análisis. La longitud es de dos octetos y este campo es revisado cuando un servidor RADIUS recibe un paquete para asegurar su integridad. Los valores de longitud válida están en el rango entre 20 y 4096.

Autenticador

Con una longitud de 16 octetos es el campo en el cual la integridad de la carga útil del mensaje es inspeccionada y verificada. En este campo el octeto más

importante es transmitido antes que cualquier otro y este valor es utilizado para autenticar réplicas desde el servidor RADIUS. Este campo es utilizado también en el mecanismo de ocultar contraseñas. Existen dos tipos específicos de valores de autenticador, los de respuesta y de requerimiento.

2.2.2.3 Tipos de paquetes

Existen cuatro tipos de paquetes que son relevantes para las fases de autenticación y autorización de una transacción AAA y a continuación se detallan.

Requerimiento de Acceso

Este paquete es utilizado por el servicio del cliente cuando el mismo requiere un servicio en particular de la red. El cliente envía un paquete de requerimiento al servidor de RADIUS con una lista de los servicios requeridos. El factor clave en esta transmisión es el campo del código en la cabecera del paquete éste debe ser inicializado en 1, el único valor del paquete de requerimiento.

El campo de valores y atributos del paquete de Requerimiento de Acceso debería incluir el atributo del nombre de usuario para identificar a la persona que requiere acceder a los recursos de la red. Además se requiere de la dirección IP del equipo desde el cual se solicita el servicio, debe también incluir la contraseña, una contraseña basada en CHAP, o un identificador de estado, pero no los dos tipos de claves. La contraseña del usuario debe ser encriptado utilizando un método MD5[3].

Aceptación de Acceso

Estos paquetes son enviados por el servidor RADIUS al cliente como un acuse de recibo al requerimiento generado por el cliente. Sí todos los requerimientos contenidos en la carga útil del paquete son aceptados, entonces el servidor de RADIUS debe inicializar en el valor de 2 los paquetes de respuesta. El cliente, luego de recibir los paquetes de aceptación, coteja los paquetes de respuesta

[3] "En criptografía, MD5 (abreviatura de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado" (Wikimedia Foundation, Inc).

utilizando el campo del identificador. Aquellos paquetes que no siguen este estándar son descartados.

Para asegurar que los paquetes de requerimiento y aceptación son coincidentes, es decir, asegurarse que las respuestas de aceptación son enviadas en respuesta a los paquetes de requerimientos, el campo del identificador en la cabecera del paquete de aceptación de acceso debe contener un valor idéntico al campo del paquete de requerimiento de acceso.

El paquete de aceptación de acceso puede contener mucho más o un poco menos de información en el campo de atributos según necesiten ser incluidos. La mayoría de información sobre atributos en este paquete describirá los tipos de servicios que han sido autenticados y autorizados, así que el cliente puede inicializar estos servicios. A pesar de lo expuesto, si no se incluye información en los atributos, el cliente asume que todos los servicios requeridos han sido concedidos.

Acceso Rechazado

El servidor de RADIUS requiere enviar un paquete de Acceso Rechazado de vuelta al cliente sí es denegado cualquier servicio requerido en el paquete de Requerimiento de Acceso. La negación se puede basar en las políticas del sistema, privilegios insuficientes o cualquier otro criterio. El Acceso Rechazado puede ser enviado en cualquier momento durante una sesión, lo es ideal para forzar límites en el tiempo de conexión. A pesar de esto no todos los equipos soportan el receptar paquetes de Acceso Rechazado durante una conexión pre-establecida.

La carga útil de este tipo de paquete está limitada a dos atributos específicos: el mensaje de réplica y el estado del Proxy.

Acceso Desafío

En el caso de que un servidor reciba información conflictiva de parte de un usuario, requiera más información o simplemente desea minimizar el riesgo de una autenticación fraudulenta, éste puede emitir un paquete del tipo Acceso

Desafío al cliente. Al recibir el mismo el cliente debe emitir un nuevo paquete del tipo Requerimiento de Acceso incluyendo la información apropiada.

Es oportuno notar que algunos clientes no soportan procesos como estos desafío/respuesta, en este caso el cliente le da el tratamiento a un paquete Acceso Desafío como un paquete de Acceso Rechazado.

2.2.2.4 Secretos Compartidos

Para fortalecer la seguridad e incrementar la integridad de la transaccionalidad el protocolo RADIUS utiliza el concepto de secretos compartidos, éstos son valores generados de manera aleatoria y son conocidos por ambos tanto el servidor como el cliente -de ahí el término de secretos- se utilizan con todas las operaciones que requieren ocultar datos y conciliar valores. La única limitación técnica está dada porque los secretos compartidos deben tener un valor mayor a cero en la longitud, el RFC recomienda que el valor secreto sea de al menos 16 octetos. Un valor secreto es virtualmente imposible de craquear de una manera abrupta, el mismo conjunto de mejores prácticas que se establecen para el uso de contraseñas gobiernan la utilización de secretos por parte de RADIUS.

Los secretos compartidos (normalmente denominados “secretos”) son únicos y particulares a cada par de cliente y servidor de RADIUS. Para una instancia en la cual un cliente se suscribe a múltiples proveedores de servicios mediante discado telefónico, él indirectamente realiza requerimientos a múltiples servidores RADIUS. Los secretos entre el equipo del cliente en un ISP A, B y C que son utilizados para comunicarse con sus respectivos servidores RADIUS no deben coincidir.

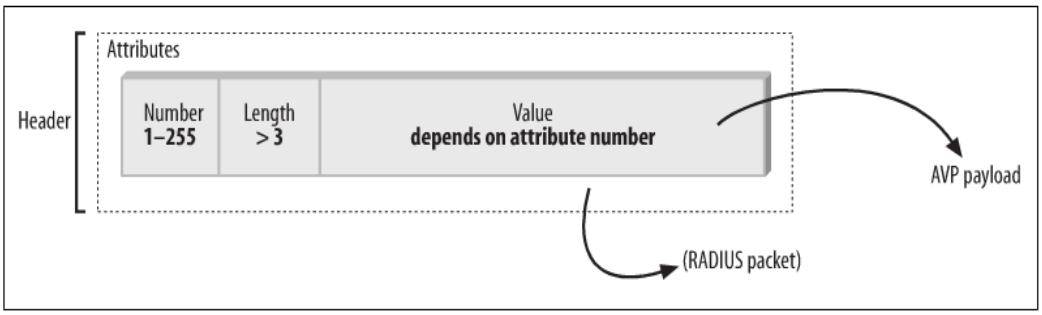
2.2.2.5 Atributos y Valores

Las transacciones en RADIUS se construyen sobre la base de pasar información entre el cliente y el servidor en pares de valores y atributos, su denominación en inglés AVP (*attribute-value pair*), que contienen virtualmente la totalidad de propiedades y características de una transacción AAA.

Para mejorar la seguridad RADIUS restringe algunos atributos que deben ser enviados en ciertos paquetes, siendo mas específicos el tiempo de duración de ciertos paquetes. Para prevenir que las contraseñas crucen por la red más de una vez para procesos de autenticación, el atributo de la contraseña nunca es permitido de ser enviado en un paquete de réplica desde el servidor hasta el cliente. Para ser más estrictos, el RFC previene que algunos atributos incluso estén presentes en ciertas transacciones mientras que otros pueden aparecer más de una vez y aún otros solamente una ocasión.

Los atributos en todos los paquetes siguen un formato de campos específicos, como se ilustra en la gráfica:

Ilustración 2-8 El patrón de transmisión estándar AVP



Fuente: (Hassell, October 8, 2002)

Número de Atributo

Este número denota el tipo de atributo presente en el paquete. El nombre del atributo no es pasado en el paquete, solamente el número. El rango de los números del atributo van del 1 al 255, con un número específico que sirve como enlace para clasificar a los proveedores que proveen sus propios atributos.

Longitud del Atributo

Este campo describe la longitud del campo del atributo el cual deber ser tres o mayor. Se comporta en muchas ocasiones en la misma forma como el campo longitud de la cabecera del paquete RADIUS.

Valor

Contiene la propiedad o característica del atributo, este campo es requerido por cada atributo presente incluso sí el valor es nulo. La longitud de éste varía en función de la naturaleza inherente del propio atributo.

Atributos

Describen un comportamiento o una propiedad de un tipo de servicio. Mientras la mayoría de atributos son incluidos para denotar un ajuste en particular para un tipo de servicio, la presencia de algunos atributos en el paquete informa al servidor de RADIUS que es lo que necesita conocer. Los atributos son transmitidos dentro del paquete RADIUS en un formato estándar predeterminado. La estructura AVP consiste en un conjunto continuo de bytes que contienen al menos tres octetos, el primer octeto es el tipo, el segundo la longitud y el octeto final el valor del mismo atributo.

Tipos de Atributos

Acorde al RFC la implementación de RADIUS está diseñada para buscar ciertos tipos de valores en el campo “valor” de un atributo en particular. Por ejemplo, no se esperaría encontrar números aleatorios en un atributo diseñado para pasar una fecha, tampoco se esperaría tener una dirección IP, consistente en números, en una cadena de caracteres aleatorios. Para facilitar la confusión se rodean valores de múltiples atributos que están siendo pasados en una transacción cada atributo corresponde a valores que han sido asignados a un cierto tipo. Simplemente describe que el valor es un número, una dirección IP, una fecha, etc. Existen 6 tipos que se indican en el RFC:

- Entero (INT)
- Enumerado (ENUM)
- Dirección IP (IPADDR)
- Cadena de caracteres (STRING)
- Fecha (DATE)
- Binario (BINARY)

Las anotaciones en mayúsculas que figuran entre paréntesis al lado de cada término, indican la abreviatura correcta de notación para cada uno de los tipos de atributos

Valores

Hay que recordar que todos los atributos deben tener valores aún si el valor del atributo es nulo. Los valores representan la información que cada atributo en particular fue diseñado para comunicar. Los valores deben estar conforme al tipo de atributos arriba descritos. La tabla a continuación ejemplifica cada tipo de atributo y los valores esperados para cada uno:

Tabla 2-1 Tipos de atributos y valores de los campos

Tipo de atributo	Longitud (en octetos)	Tamaño	Ejemplo
Entero (INT)	4	32 bits	6
			2432
			65284
Enumerado (ENUM)	4	32 bits	3 = Callback-Login
			4 = Callback-Framed
Cadena de caracteres (STRING)	1 – 253	Variable	“Suriname”
			“MyBolg.com”
			“593.2.2228830”
Dirección IP (IPADDR)	4	32 bits	0xFFFFFE
			0x0000B
Fecha (DATE)	4	32 bits	0xFFFFFE
			0xC0A80102
Binario (BINARY)	1	1 bit	1
			0

Elaborado por: Autor

Diccionarios

Estos pueden ser almacenados en archivos de texto plano, bases de datos o cualquier otro medio, la única restricción es que la información sea accesible para el servidor RADIUS ya que es la manera en la cual se corresponde un atributo con un número y el tipo de campo esperado. La siguiente tabla muestra un ejemplo común de un diccionario contenido en un archivo en formato texto:

Tabla 2-2 Ejemplo de archivo de texto utilizado como diccionario

Nro.	Nombre del atributo	Tipo
1	Nombre de usuario	STRING
2	Contraseña del usuario	STRING
3	Contraseña – CHAP	STRING
4	Dirección IP NAS	IPADDR
5	Puerto NAS	INT
6	Tipo de servicio	ENUM

Elaborado por: Autor

Cada implementación de RADIUS debe almacenar información referente a los atributos de cualquier vendedor específico en el diccionario.

2.2.2.6 Métodos de autenticación

RADIUS soporta una variedad de diferentes mecanismos y protocolos para transmitir datos sensitivos de un usuario específico desde y hasta un servidor de autenticación. Los dos más comunes son el Protocolo de Autenticación de *Passwords* (PAP) y el CHAP. RADIUS también permite más atributos y métodos desarrollados por fabricantes de software incluyendo soporte para elementos peculiares a Windows 2000, Windows 2008 y otros populares sistemas operativos de red.

PAP

El atributo “Contraseña de usuario” en un paquete de requerimiento es la señal a un servidor de RADIUS que el protocolo PAP será utilizado para la transacción. Es importante notar que éste es el único campo mandatorio para este caso. El campo “Nombre de usuario” no tiene que ser incluido en el paquete de requerimiento y es muy probable que RADIUS a lo largo de una cadena de servidores Proxy cambie el valor del campo “Nombre de usuario”.

El algoritmo utilizado para esconder la contraseña original del usuario está compuesto de algunos elementos. Primero, el cliente detecta el identificador y el “secreto compartido” del requerimiento original y lo somete a una secuencia

hashing[4] MD5. La contraseña original del cliente es puesta a través de un proceso XOR[5] y el resultado que proviene de estas dos secuencias son ubicadas en el campo "contraseña del usuario". El servidor RADIUS que recibe, reversa estos procedimientos para determinar si se debe autorizar la conexión. La naturaleza misma de la contraseña oculta es un mecanismo que previene a un usuario determinar, cuando falla la autenticación, si fue causada por una contraseña incorrecta o un secreto inválido.

CHAP

Se basa en la premisa de que la contraseña nunca debería ser enviada en ningún paquete cruzando la red. CHAP dinámicamente encripta el ID y contraseña del usuario que solicita. La máquina del usuario a continuación, pasa a través de su procedimiento de inicio de sesión, habiendo obtenido una clave del cliente RADIUS del equipo de al menos 16 octetos de longitud. El cliente entonces obtiene un hash de esa clave y la envía de vuelta como un CHAP ID, una respuesta CHAP y el nombre de usuario al cliente de RADIUS. Habiendo recibido el cliente todo esto, ubica el CHAP ID dentro del campo apropiado que es el atributo "CHAP-*Password*" y entonces envía una respuesta. El valor de desafío originalmente obtenido es ubicado dentro del atributo "CHAP-*Challenge*" o en el campo autenticador en la cabecera, de esta manera el servidor puede acceder fácilmente al valor en orden de autenticar al usuario.

Para autenticar al usuario el servidor RADIUS utiliza el valor del atributo "CHAP-*Challenge*", el "CHAP ID" y la contraseña de registro para ese usuario en particular y los somete a otro algoritmo de *hashing* MD5. El resultado de este algoritmo debería ser idéntico al valor ubicado en el atributo "CHAP-*Password*". De no serlo el servidor debería denegar el requerimiento, caso contrario el requerimiento es concedido.

---

[4] "Hash se refiere a una función o método para generar claves que representen de manera casi unívoca a un registro" (Wikimedia Foundation, Inc).

[5] "En criptografía, el cifrado XOR es, como su nombre indica, un algoritmo de cifrado simple" (Wikimedia Foundation, Inc).

El hecho de que la contraseña en una transacción CHAP nunca cruce por la red es precisamente una de las razones por las que este protocolo es atractivo. Adicionalmente el protocolo soporta desafíos del cliente en cualquier momento durante la sesión del usuario, lo cual incrementa la probabilidad de mantener fuera del sistema usuarios no válidos.

2.2.2.7 Reinos

Se refiere a la capacidad que incorpora RADIUS para reconocer a un usuario en base a un identificador, el cual es ubicado previo al nombre del usuario y los dos son separados por un símbolo pre-configurado, los más comunes son: @, \ o /.

Por ejemplo el usuario “CarlosT” perteneciente a la compañía ADN podría identificarse de manera válida como: carlost@adn, adn\carlost o adn/carlost ante un servidor RADIUS. Mediante esta propiedad se puede establecer relaciones de confianza que permiten a RADIUS tener la flexibilidad para atender diferentes esquemas de infraestructura y modelos de negocios adaptados a numerosos esquemas de diseños de la red.

2.2.3 Contabilización en RADIUS

En RADIUS el diseño de la contabilización se basa en tres características principales:

- La contabilidad se basa en un modelo cliente servidor.

  El equipo que centraliza la contabilización de todos los dispositivos que cuentan con clientes es el servidor de RADIUS. El cliente envía la utilización de datos hasta el servidor para su proceso y éste envía un acuse de recibo exitoso de los datos.

- La comunicación entre dispositivos sería segura.

  Todos los datos que se intercambian entre el servidor de RADIUS y los clientes hacen uso de los “secretos compartidos”, los cuales nunca son transmitidos a través del cable.

- La contabilidad de RADIUS sería extensible.

  El formato para la contabilización de atributos es muy similar a los atributos de autorización y autenticación.

2.2.3.1 Operación básica

Todas las comunicaciones concernientes a la contabilización en RADIUS utilizan un paquete ¨Requerimiento de contabilización¨. Un cliente que está participando en el proceso generaría un paquete de “Inicio de contabilización” el cual es un tipo específico de paquete de ¨Requerimiento de contabilización¨. Este paquete incluye información sobre qué servicio ha sido provisionado y el usuario para el cual éste servicio ha sido provisto. Este paquete es enviado hasta un servidor de contabilización de RADIUS el cual retorna un acuse de recibo de los datos. Cuando el cliente ha finalizado con los servicios de la red, éste enviará al servidor de contabilización un paquete de ¨Contabilización detenida¨ el cual incluye el servido entregado, estadísticas de la utilización como el tiempo transcurrido, la cantidad de data transferida, el promedio de velocidad y otros detalles. Sí toda la información está correcta el servidor envía un acuse de recibo del paquete de ¨Contabilización detenida¨, en caso de que el servidor no pueda manipular el contenido del paquete, el servidor no está permitido de enviar un acuse de recibo al cliente.

Para esta instancia, el RFC recomienda que el cliente continúe enviando paquetes al servidor hasta cuando haya recibido una confirmación de que el paquete de “Requerimiento de contabilización¨ ha sido procesado. En la práctica, para redes distribuidas y grandes, es ideal contar con algunos servidores contabilizadores que actúen de una manera redundante para gestionar los casos de falla y necesidades de redundancia.

2.2.3.2 El formato del paquete de contabilización

Conforme lo previamente descrito, el protocolo RADIUS utiliza el fundamento de paquetes UDP para la transmisión entre, servidores, clientes y proxies. Las transacciones se llevan a cabo mediante el puerto 1813.

Los paquetes están seccionados en cuatro diferentes regiones, siendo estas:

Código

Esta región tiene una longitud de un octeto e indica el tipo de información contable a ser transmitida en el paquete, aquellos paquetes con códigos inválidos en este campo son descartados sin enviar notificación. Lo códigos válidos son:

4 Requerimiento de contabilización

5 Respuesta de contabilización

Identificador

Con una longitud de un octeto este campo es utilizado para realizar encadenamientos o enlaces automáticos de requerimientos iniciales y sus réplicas subsiguientes. Los servidores de contabilización de RADIUS pueden generalmente interceptar mensajes duplicados para examinar algunos factores como la dirección IP origen, el puerto UDP, el tiempo transcurrido del mensaje sospechoso y campo del identificador.

Longitud

Con un tamaño de dos octetos este campo se utiliza para especificar la longitud del mensaje de contabilización de RADIUS. El valor de este campo es calculado en base al análisis del código, el identificador, longitud, autenticador y los campos de atributos y se sumarizan, El campo longitud es revisado para asegurar la integridad cuando un servidor de contabilización recibe un paquete, el rango de valores válidos está entre 20 y 4095.

Autenticador

La región del autenticador, de hasta 16 octetos de longitud, es el campo en el cual la integridad de la carga del paquete es inspeccionada y verificada. En este campo, el octeto más importante es trasmitido antes que cualquier otro.

Existen dos tipos distintos de autenticadores: el de requerimiento y el de respuesta.

Los requerimientos autenticadores, consisten de 16 octetos MD5 de sumas de comprobación, son computados utilizando un hash generado desde el código, identificador, longitud, atributos, secretos compartidos y 16 octetos reducidos a ceros. El valor que retorna de este hash es ubicado dentro del campo autenticador.

El autenticador de respuesta se calcula de la misa manera que el requerimiento autenticador.

Fiabilidad de la contabilidad

Si bien las especificaciones de RADIUS son prometedoras, la experiencia muestra que los paquetes de contabilización no tiene una certeza del 100%. Si tomamos como ejemplo un cliente que envía paquetes de contabilización a un servidor pero no recibe acuse de recibo o respuesta, éste continuará enviando los mismos paquetes solo por un tiempo limitado, esto representa un problema con algunas sesiones en cuanto a la inconsistencia de registros que requieren operaciones que necesitan exactitud como el caso de la facturación.

2.2.3.3 Tipos de paquetes de contabilización

Existen dos tipos de paquetes de RADIUS que son relevantes para la fase de contabilización de una transacción AAA, estos son:

- Requerimiento de contabilización
- Respuesta de contabilización

A continuación se detalla la identidad y propiedades de estos paquetes específicos.

Requerimiento de contabilización

Tabla 2-3 Estructura paquete:Requerimiento de contabilización

CAMPO	ATRIBUTO
Tipo de paquete	Requerido
Código	4
Identificador	Único para cada requerimiento, cada transmisión o modificación de datos
Autenticador	Requerido
Datos del atributo	0 o más atributos

Elaborado por: Autor

Estos paquetes son enviados por el cliente hasta el servidor. El cliente envía el paquete con el campo inicializado en 4. Cuando el servidor recibe el paquete, éste es requerido a transmitir un acuse de recibo hasta el cliente, al menos que no pueda gestionar o procesar el paquete. En este caso, éste no puede transmitir nada hasta el cliente.

Con las excepciones de: Contraseña del usuario, Contraseña CHAP, Mensaje de réplica y Estado de atributos, cualquier otro atributo permitido en un paquete de “Requerimiento de acceso” o “Requerimiento de aceptación” puede ser utilizado dentro de un paquete “Requerimiento de contabilización”.

Respuesta de contabilización

Tabla 2-4 Estructura paquete: Requerimiento de respuesta

CAMPO	ATRIBUTO
Tipo de paquete	Respuesta
Código	5
Identificador	Idéntico al correspondiente Requerimiento de contabilización
Autenticador	Requerido
Datos del atributo	0 o más atributos

Elaborado por: Autor

Estos paquetes son diseñados principalmente como paquetes de acuse de recibo a ser enviados por el servidor de contabilización hasta el cliente, indicando que el requerimiento ha sido recibido y registrado. Sí el paquete en

efecto ha sido procesado y registrado exitosamente, el RFC ordena que el campo código del paquete de acuse de recibo sea inicializado en 5 para indicar una respuesta. Ya que el identificador del paquete de respuesta es idéntico al campo correspondiente “Requerimiento de contabilización”, el cliente puede fácilmente emparejar los dos paquetes para guardar el rastro de cuáles requerimientos han cumplido y los que están pendientes.

2.3 LDAP

El Lightweight Directory Access Protocol (LDAP) es un servicio de directorio de un tipo particular con el potencial de consolidar servicios existentes en un único repositorio y tiene la capacidad de localizar cierto tipo de información de una manera fácil, eficiente y rápida. Además a éste directorio pueden acceder clientes del LDAP de diversos vendedores y estos clientes pueden ser: navegadores de internet, servidores de correo o cualquier otra aplicación que requiera para su operatividad visualizar información del directorio.

El consolidar la información dentro de un único directorio no permite simplemente agrupar los contenidos de múltiples o pequeños repositorios en uno mucho más grande sino que al organizar permite pensar cuidadosamente acerca de información en común requerida por aplicaciones de clientes y poder reducir duplicidad de datos y carga de trabajo excesiva para su mantenimiento.

Una de las mejores formas de explicar qué es LDAP es examinando la composición de su nombre tomando como referencia el RFC 3377[6], así sus componentes son:

2.3.1 Lightweight

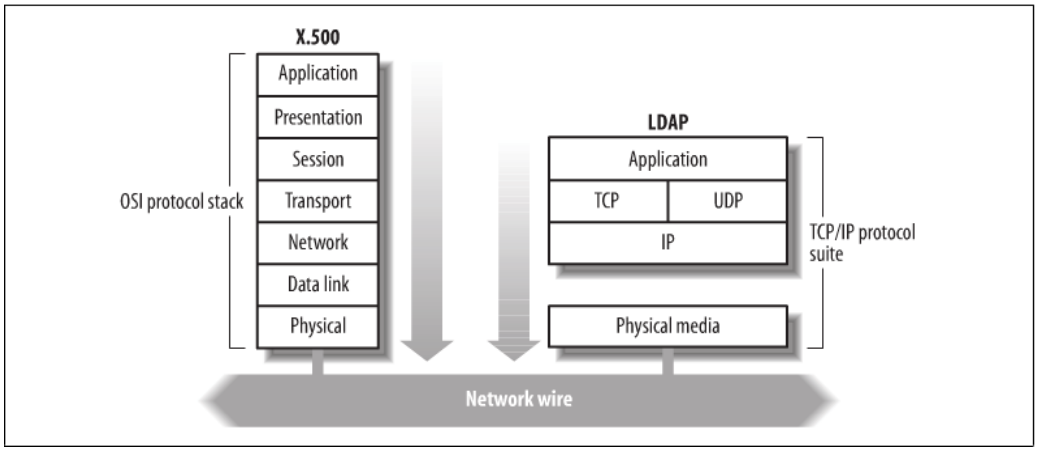
Para responder a la interrogante de por qué es ligero (Lightweight) es necesario revisar los inicios del LDAP ya que fue originalmente creado como un protocolo más ligero utilizado como enlace entre los requerimientos de

[6] http://tools.ietf.org/html/rfc3377

servidores X.500 y equipos de escritorio, sus raíces están estrechamente vinculadas al servicio de directorio X.500[7].

LDAP es más ligero comparado con el servicio de directorio del X.500 debido a que utiliza mensajes con baja sobrecarga que son mapeados directamente dentro de la capa TCP, en el puerto 389 por defecto, del protocolo TCP/IP. Debido a que X.500 fue un protocolo en la capa de aplicación, en términos del modelo OSI, los paquetes llevaban mucha más carga por los encabezados añadidos en cada capa que tenía que atravesar hasta que finalmente era transmitido por la red como se muestra en la siguiente figura:

Ilustración 2-9 X.500 sobre OSI versus LDAP sobre TCP/IP



Fuente: (Carter, LDAP System Administration, March 20, 2003)

LDAP también es considerado ligero ya que cuenta solamente con nueve operaciones centrales que proveen un simple modelo para programadores y administradores. Omitiendo muchas operaciones de X.500 que son raramente utilizadas.

2.3.2 Directorio

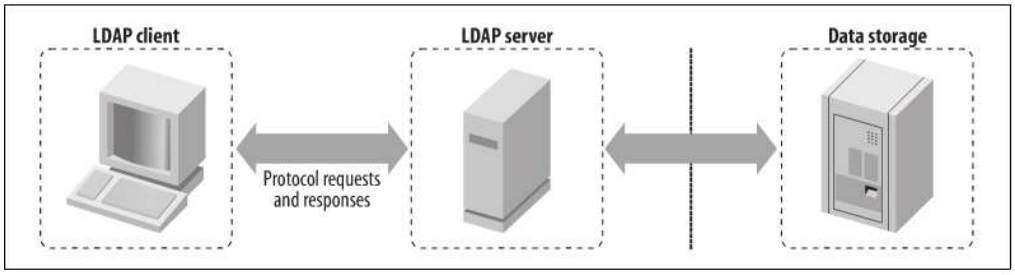
Es común que los servicios de directorio sean confundidos con una base de datos debido a que comparten características como son búsquedas rápidas y esquemas extendidos. Pero difieren en que un directorio está diseñado para ser mucho más leído que escrito, en contraste, una base de datos asume qué

[7] http://en.wikipedia.org/wiki/X.500

operaciones de lectura y escritura ocurren aproximadamente con la misma frecuencia. Esto no implica que soportar transacciones de bloqueo de escritura no sea esencial para un servicio de directorio como LDAP.

Es importante hacer una distinción entre LDAP y el repositorio utilizado para almacenar su data y vale recordar que LDAP es un protocolo, en esencia es un conjunto de mensajes para acceder a cierto tipo de datos. El protocolo no especifica nada sobre donde debe ser almacenada la data. Un proveedor de software en la implementación de un servidor de LDAP es libre de utilizar cualquier repositorio que desee, el rango puede partir desde archivos de texto plano hasta el otro extremo de una base de datos de alta escalabilidad, indexada y relacional. El punto es que un cliente nunca visualiza o está al tanto del mecanismo de almacenamiento de la data. Por esta razón una implementación compatible con LDAP provista por el vendedor A debería inter operar con un server LDAP compatible escrito por el vendedor Z.

Ilustración 2-10 Relaciones entre un cliente LDAP, un server LDAP y un repositorio de datos



Fuente: (Carter, LDAP System Administration, March 20, 2003)

Existen dos puntos de interés a resaltar sobre la función de LDAP:

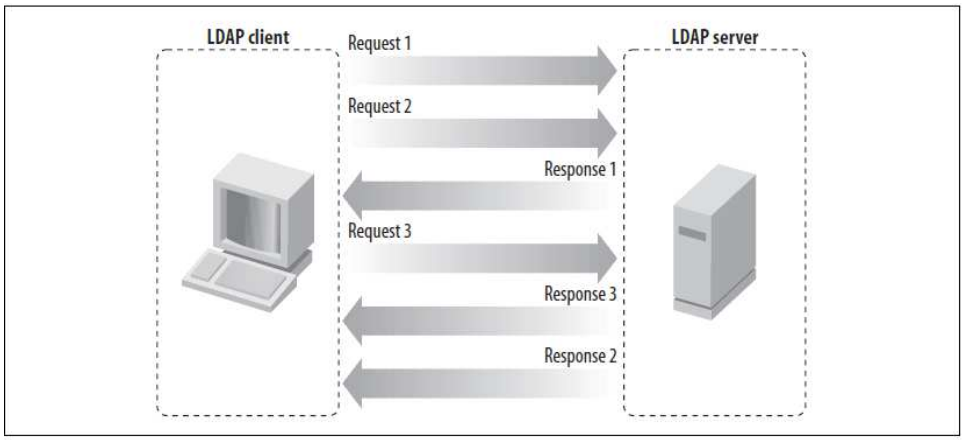
1. LDAP no constituye un reemplazo generalizado para directorios especializados como son sistemas de archivos (file systems) o DNS.
2. Si bien ciertos tipos de información binaria en un directorio pueden ser útiles como es el caso de fotos en JPEG, LDAP no tiene como propósito almacenar arbitrariamente una masa binaria de bits.

2.3.3 Protocolo de acceso

Por lo arriba expuesto sobre servicios de directorio y almacenamiento es fácil olvidar que LDAP es un protocolo y es común escuchar en algunos referirse a LDAP como un servidor ya que éste provee un árbol como modelo de visualización de los datos.

LDAP está definido en el RFC 2251[8] como un protocolo cliente servidor basado en mensajes y es asincrónico, lo que significa que un cliente puede promulgar múltiples requerimientos y las respuestas a los mismos pueden arribar en un orden diferente del cual estos fueron solicitados, esto se ejemplifica en la siguiente figura donde el cliente envía el requerimiento 1 y 2 previo a recibir una respuesta y la respuesta al requerimiento 3 es retornada antes que la respuesta al requerimiento 2.

Ilustración 2-11 LDAP requerimientos y respuestas



Fuente: (Carter, LDAP System Administration, March 20, 2003)

2.3.4 Modelos LDAP

Los modelos LDAP representan los servicios provistos por un servidor desde la perspectiva de un cliente. Éstos son modelos abstractos que describen varias facetas de un directorio LDAP. El RFC 2251 divide al directorio LDAP en dos componentes: el modelo del protocolo y el modelo de datos.

[8] http://tools.ietf.org/html/rfc2251

Sin embargo en el libro "*Understanding and Deploying LDAP Directory Services*" escrito por Timothy A. Howes, Mark C. Smith y Gordon S. Good (MacMillan), se definen cuatro modelos:

Modelo de Información

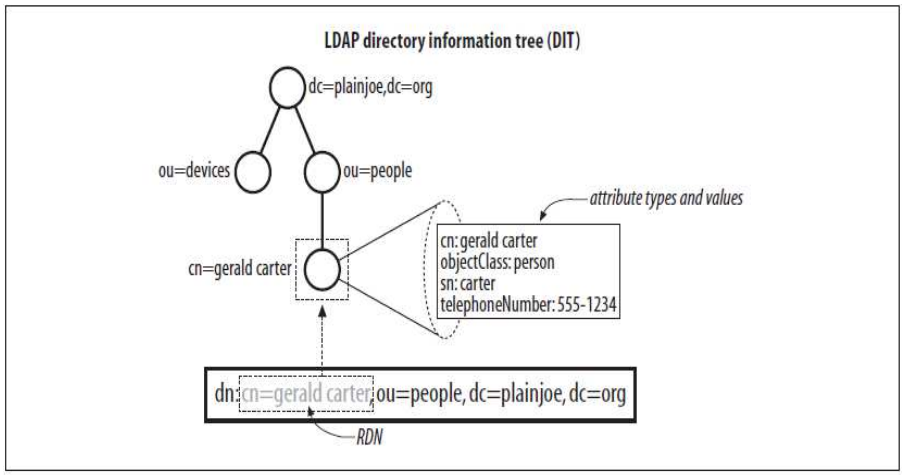
Este modelo provee las estructuras y tipos de datos necesarios para construir un árbol de directorio LDAP. Una entrada es la unidad básica en un directorio LDAP. Se puede visualizar una entrada ya sea como un nodo interior o exterior en el Árbol de Información del Directorio (DIT). Una entrada contiene información acerca de una instancia o de uno o más clases de objetos (objectClasses), estas clases de objetos tienen ciertos atributos requeridos u opcionales. Los tipos de atributos tienen definida una codificación y reglas de congruencia que gobiernan temas como el tipo de datos que el atributo puede almacenar y cómo comparar esta data durante una búsqueda.

Modelo de nomenclatura

Define cómo las entradas y los datos en el DIT son referenciados de manera única. Cada entrada tiene un atributo que es único de entre todos los hermanos de un solo padre. Este atributo único es denominado como el Nombre Relativo Distinguido (RDN). Se puede identificar de manera única una entrada en el directorio por los RDNs consecutivos de todas las entradas que conforman el camino que va desde el nodo deseado hasta la raíz del árbol. Esta cadena creada por la combinación de RDNs forma un nombre único que se denomina Nombre Distinguido (DN) del nodo.

En la Ilustración 2-12, la entrada del directorio marcada en el cuadrado con línea entrecortada tiene un RDN de: *cn=gerald carter*. El DN para este nodo debería ser: *cn=gerald carter, ou=people, dc=plainjoe, dc=org*.

Ilustración 2-12 Ejemplo de un árbol de directorio LDAP



Fuente: (Carter, LDAP System Administration, March 20, 2003)

Modelo funcional

El modelo funcional es el protocolo LDAP por sí mismo. Este protocolo provee los métodos para acceder a la data en el árbol del directorio. El acceso esta implementado por operaciones de autenticación, operaciones de consultas y operaciones de actualización.

Modelo de seguridad

El modelo de seguridad provee un mecanismo para clientes que prueban su identidad (autenticación) y para el servidor que controla el acceso de un cliente autenticado a la data (autorización).

2.3.5 LDIF

El Formato de Intercambio LDAP (LDIF), definido en el RFC 2849[9], es un archivo estándar en formato texto diseñado para almacenar información de la configuración LDAP y contenidos del directorio. En su forma más básica un LDIF es:

- Una colección de entradas separadas unas de otras por líneas en blanco.

[9] http://tools.ietf.org/html/rfc2849

- Una asignación de nombres de atributos a valores.
- Una colección de directivas que instruyen el análisis de cómo procesar la información.

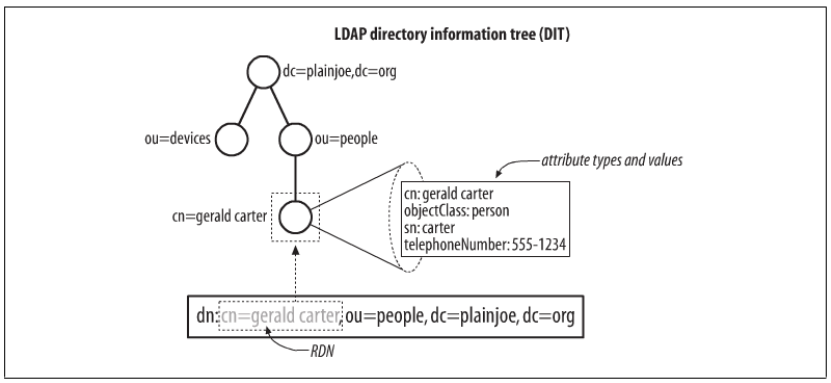
Las dos primeras características proveen exactamente lo que se necesita para describir el contenido de un directorio LDAP.

Los archivos LDIF a menudo son utilizados para importar nueva data dentro del directorio o realizar cambios a la data existente. Los datos dentro del archivo LDIF deben obedecer las reglas del esquema del directorio LDAP, se puede asociar al esquema como la definición de datos del directorio. Cada ítem que es añadido o cambiado en el directorio es revisado contra el esquema para guardar exactitud. Una violación al esquema ocurre si la data no corresponde a las reglas existentes.

La ilustración 2-13 muestra las entradas en el archivo LDIF que corresponden al DN: dc=plainjoe, dc=org. Asociadas al DIT utilizado para el ejemplo:

Ilustración 2-13 Un árbol de directorio LDAP

```
# LDIF listing for the entry dn: dc=plainjoe,dc=org
dn: dc=plainjoe,dc=org
objectClass: domain
dc: plainjoe
```



Fuente: (Carter, LDAP System Administration, March 20, 2003)

Se pueden realizar ciertas observaciones acerca de la sintaxis LDIF a partir de la ilustración 2-13:

- Los comentarios en un archivo LDIF comienzan con el caracter numeral (#) en la posición inicial y continua hasta el final de la línea.
- Los atributos son listados en la parte izquierda del símbolo de los dos puntos (:) y los valores son presentados en la parte derecha. El caracter de los dos puntos está separado del valor por un espacio en blanco.
- El atributo *dn* únicamente identifica a la entrada DN.

2.3.5.1 ¿Qué es un atributo?

Los tipos de atributos y las reglas de sintaxis asociadas son similares a las variables y a las declaraciones de tipos de datos encontradas en algunos lenguajes de programación. Los atributos son utilizados para almacenar valores. Las variables en programas desempeñan una tarea similar, éstas almacenan información.

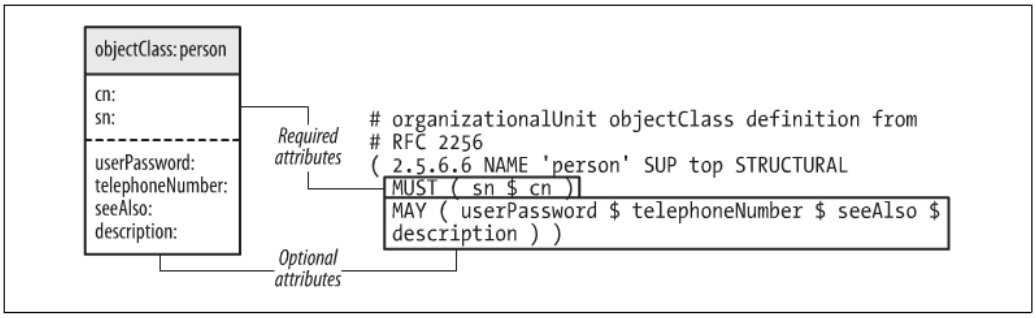
A diferencia de las variables, sin embargo, los atributos LDAP pueden ser multivalor. La mayoría de lenguajes de programación refuerzan la semántica de almacenar y reemplazar las asignaciones de una variable. Esto implica que cuando se asigna un nuevo valor a una variable, el valor anterior es reemplazado. Pero esto no es verdadero para LDAP; al asignar un nuevo valor a un atributo se añade el valor a la lista de valores del atributo ya existente.

2.3.5.2 Autenticación

La autenticación es el proceso utilizado para establecer los privilegios del cliente para cada sesión. Todas las consultas, búsquedas y demás son controladas por el nivel de autorización del usuario autenticado.

La ilustración 2-14 que describe a la clase de objeto persona (person) provee una idea de que otros atributos están disponibles para la entrada: cn=gerald carter, que se muestra en la ilustración 2-12. En particular se requiere definir el valor del atributo userPasword para explorar la autenticación LDAP.

Ilustración 2-14 Detalle de la clase de objeto: person



Fuente: (Carter, LDAP System Administration, March 20, 2003)

La representación LDIF para la versión expandida de cn=gerald carter, sería:

```
dn: cn=gerald carter,ou=people,dc=plainjoe,dc=org
objectCalss: person
cn: gerald carter
sn: carter
telephoneNumber: 555-1234
userPassword: {MD5}Xr4il0zQ4PCOq3aQObduaQ==
```

Se ha añadido un atributo denominado `userPassword`. Este atributo almacena una representación de credenciales necesarias para autenticar un usuario. El prefijo (`{MD5}`) describe cómo las credenciales son codificadas. El RFC 2307[10] define los prefijos de algunos algoritmos de encripción, algunos de los tipos más comunes son:

`{CRYPT}`

El *password* debería ser generado utilizando una función local del sistema, la cual es normalmente incluida en una librería estándar.

`{MD5}`

El *password* desmenuzado, codificado en base de 64 bits, de la función MD5 resultante de digerir la contraseña del usuario.

`{SHA} (Secure Hash Algorithm)`

El *password* desmenuzado, codificado en base de 64 bits, de la función SHA-1 (RFC 3174[11]) resultante de digerir la contraseña del usuario.

[10] http://tools.ietf.org/html/rfc2307
[11] http://tools.ietf.org/html/rfc3174

Las especificaciones de LDAPv3 definen algunos mecanismos para la autenticación de clientes:

- Autenticación anónima.
- Autenticación simple.
- Autenticación simple sobre SSL/TLS.
- Autenticación simple y capa de seguridad (SASL).

2.3.5.3 Directorios distribuidos

Existen algunas razones que determinen distribuir el árbol del directorio a lo largo de múltiples servidores. Las mismas pueden incluir, pero no estar limitadas a:

Rendimiento

En circunstancias donde una sección del árbol del directorio es con exceso utilizada. El ubicar solo ésta ramificación en un servidor, les permitirá a los clientes restantes del árbol acceder más rápidamente.

Ubicación geográfica

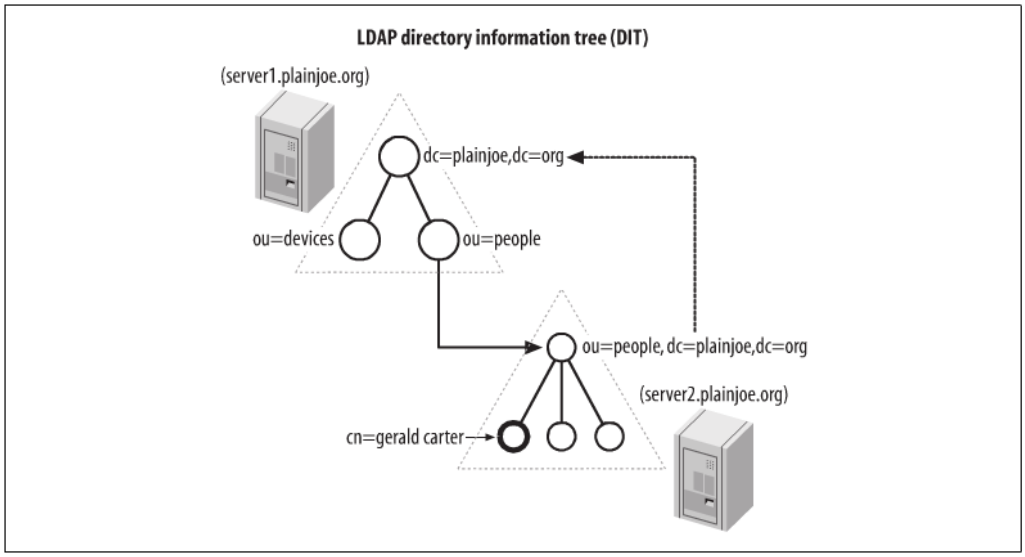
Sí todos los clientes acceden a una ramificación del árbol en particular y se encuentran en una misma locación, entonces tiene mas sentido el ubicar esta sección del directorio más cerca a los clientes que lo requieren. De esta manera se pueden evitar consultas que atraviesan la WAN y afectan su rendimiento.

Limitantes administrativas

En algunas ocasiones es más fácil delegar tareas administrativas del control de una ramificación del directorio ubicando la misma en un servidor controlado por un grupo responsable de la información en este nodo. De esta manera los operadores del servidor pueden tener acceso total a facilidades como son réplicas y procesos de respaldo sin interferir con el server principal.

Para dividir el árbol del directorio en dos servidores como lo muestra la Ilustración 2-15, se deben configurar dos enlaces entre el servidor del directorio principal y el servidor que hospeda al `ou=people`. Al hacer esto, se crea una referencia conocida como superior y subordinada.

Ilustración 2-15 Construyendo un directorio distribuido

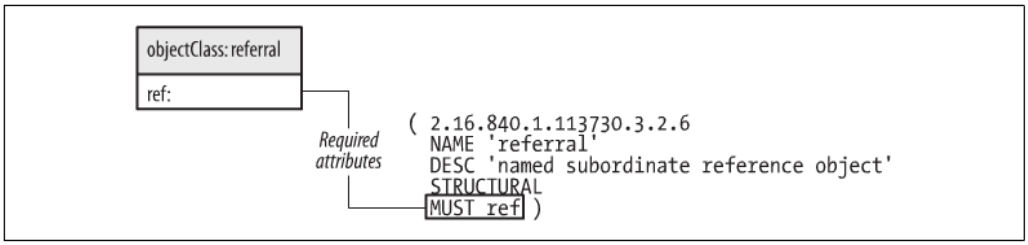


Fuente: (Carter, LDAP System Administration, March 20, 2003)

Un enlace denominado subordinado, o simplemente denominado referencia, lógicamente conecta un nodo dentro de un árbol de directorio con el nombre del contexto de otro servidor. Lo más frecuente es que el nombre del contexto del segundo servidor es una continuación del directorio. Para el ejemplo, el `people` ou en el directorio principal no tiene hijos debido a que todas las consultas referentes a las entradas en el `ou=people,dc=plainjoe,dc=org` del árbol deberían ser procesadas por el segundo servidor. La entrada `ou=people,dc=plainjoe,dc=org` en el servidor del directorio principal es ahora un puntero que contiene la referencia al actual servidor de directorio de ésta entrada. La Ilustración 2-16 muestra la definición para la clase de objeto referenciado, definido en el RFC 3296[12].

[12] http://tools.ietf.org/html/rfc3296

Ilustración 2-16 Clase de objeto referenciado



Fuente: (Carter, LDAP System Administration, March 20, 2003)

El objeto referenciado (`referral`) contiene solamente un simple atributo requerido: `ref`. Éste atributo almacena el Identificador Uniforme de Recursos (URI) que apunta al servidor que contiene el sub árbol. El formato de éste URI está definido en el RFC 2255[13] como:

```
ldap://[host:port]/[/dn[?attribute][?scope][?filter][?extensions]]
```

Por ejemplo, el LDIF listado para la nueva entrada `people ou`, es:

```
# LDIF listing for the entry ou=people,dc=plainjoe,dc=org
dn: ou=people,dc=plainjoe,dc=org
objectClass: referral
ref: ldap://server2.plainjoe.org/ou=people,dc=plainjoe,dc=org
```

2.4 Arquitectura y modelos AAA para redes móviles e inalámbricas

2.4.1 Introducción

Los entornos de computación están omnipresentes hoy en todos los ambientes, lo que representa nuevos retos en la provisión de servicios móviles. Se proyecta en el corto plazo que los usuarios estarán accediendo hacia redes convergentes. Esto significa, que una red será utilizada para entregar diferentes servicios, por ejemplo: difusión de señal de TV, telefonía e Internet. Compuesta de terminales móviles, redes inalámbricas y redes cableadas.

[13] http://tools.ietf.org/html/rfc2255

Estas redes ocultan la frontera entre el sector de las telecomunicaciones, la difusión de señal y las redes de computadores. Un servicio común habilita a terminales móviles acceder a todas las prestaciones independientemente de la tecnología de red utilizada.

El cambio del entorno involucra también modificar el plan de gestión de las redes de apoyo. Los proveedores que disponen de redes convergentes tienen que cambiar sus métodos de contabilización y facturación así como redefinir sus modelos de negocios. Investigaciones en el área del modelo AAA están enfocadas en proveer una base común que cubran los próximos servicios presentes en las redes convergentes.

Los métodos AAA empleados en las actuales redes fueron desarrollados para un único tipo de red, resultando en dos sistemas diferentes uno para sistemas de telecomunicaciones y otro para redes de computadores.

Las redes de computadores proveen un acceso unificado AAA y las investigaciones se centran en extender los actuales métodos para ser aplicables a los servicios de telecomunicaciones. La propuesta es la utilización de extensiones del protocolo RADIUS, actual estándar por defecto para autenticación de usuarios remotos, o el *Diameter*[14].

La mayoría de proveedores de telefonía celular 3G consideran la arquitectura de sistemas AAA como uno de los más importantes bloques funcionales para el éxito en la entrega de servicios. Típicamente los usuarios son autenticados cuando requieren un servicio y únicamente luego de un proceso de autenticación exitoso son autorizados para utilizarlo. Una vez que el usuario ha obtenido acceso al servicio, se generan en la red mensajes de contabilización acerca de la actividad del usuario. Actualmente RADIUS es el protocolo más ampliamente implementado en redes celulares para ejecutar tareas de suscripción.

Independientemente de las diferencias fundamentales de las redes de comunicaciones y de computadoras, la movilidad es el factor clave para los dos

[14] "Diameter es un protocolo AAA sucesor de RADIUS" (Wikimedia Foundation, Inc).

entornos. Los servicios de red no deberían ser solamente accesibles desde terminales móviles sino que estos necesitan ser adaptados a los requerimientos de calidad de servicio (QoS) de los enlaces, sean estos móviles o inalámbricos. Las mejoras en los métodos AAA son de fundamental importancia para la movilidad, proporcionando rápida transferencia, confiabilidad y comunicaciones seguras basadas en la protección de la privacidad y la facilidad de uso.

2.4.1.1 El modelo AAA en redes convergentes

Una red convergente acarrea varios tipos de tráfico y habilita el intercambio de información entre diferentes terminales sin tener en cuenta el medio de transporte. Para habilitar una red convergente AAA los trabajos de investigación se están sucediendo en diferentes áreas: habilitando la interoperabilidad entre redes WLAN[15] y redes móviles, mejorando la movilidad dentro de las redes inalámbricas de computadores y reduciendo los requerimientos de recursos en criptografía.

Interoperabilidad entre redes móviles e inalámbricas

La convergencia de redes es más significativa en entornos inalámbricos, medio que debe afrontar varias medidas de QoS sobre la interface de radio. Estos parámetros (QoS) son dependientes tanto del usuario como del terminal, enfatizando que un óptimo acceso debería utilizar todas la conexiones inalámbricas y móviles. En la siguiente tabla se provee en resumen las diferencias de estas redes.

[15] Wireless Local Area Network (WLAN)

Tabla 2-5 Comparación de redes celulares y WLAN

	Celular	**WLAN**
Cobertura	Nacional	Local
Seguridad	Fuerte	Dependiente de la configuración
Tasa de transmisión	Baja	Alta
Costo de implementación	Alto	Bajo
Costo de licenciamiento	Alto	No se requiere
Construcción	Difícil	Fácil
Soporte de movilidad	Alto	Pobre

Fuente: (Leu, 2006)

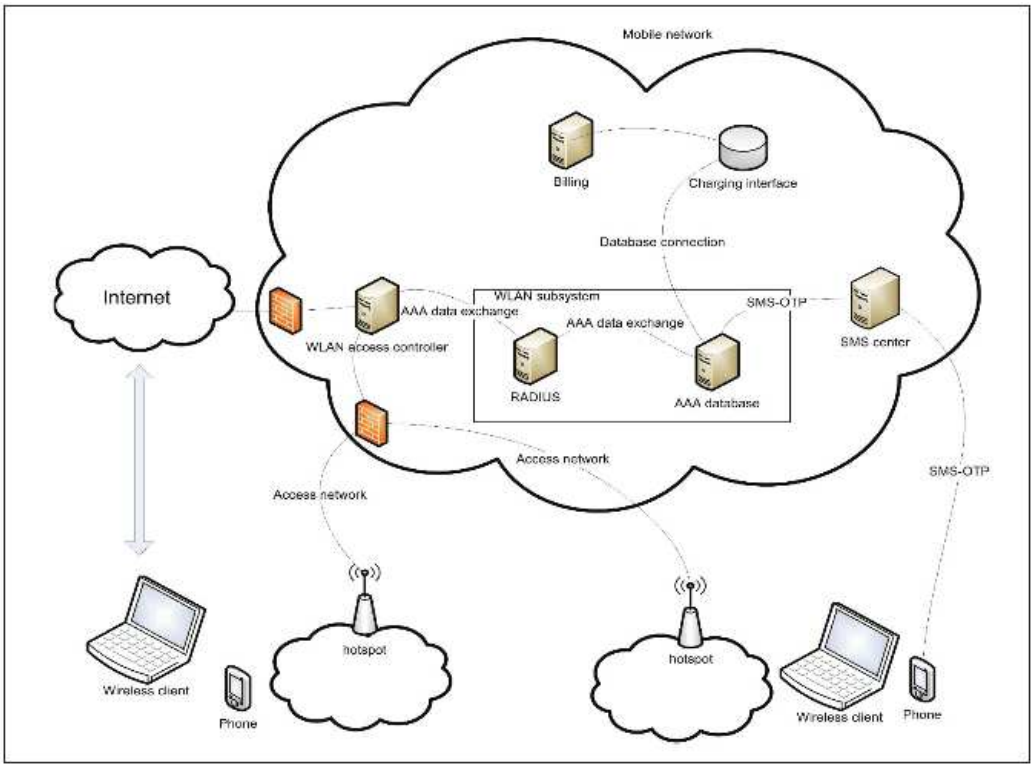
El incremento en la demanda ha mejorado la seguridad en los enlaces inalámbricos, obteniendo como resultado Accesos Protegidos Wi-Fi [16] (WPA) y WPA2 que son implementaciones del estándar IEEE 802.11i. Este estándar tiene como objetivo incorporar protocolos de la familia EAP, especialmente el de Transporte de la Capa de seguridad TLS -por sus siglas en inglés- y el SIM[17].

Un enfoque diferente consiste en ampliar la actual red de telefonía móvil con elementos adicionales para habilitar una red integrada AAA en un ambiente Internet. En la siguiente ilustración se muestra la integración de RADIUS a redes móviles para procesos de autenticación.

[16] El termino Wi-Fi en un dispositivo identifica al mismo con la capacidad de poder conectarse al Internet cuando está dentro de un rango cubierto por una red inalámbrica.

[17] Subscriber Identification Module (SIM) es un circuito integrado el cual almacena de manera segura las claves para identificar al suscriptor en un dispositivo de telefonía móvil.

Ilustración 2-17 Integración de RADIUS en redes móviles



Fuente: (Zhang, Zheng, & Ma, March 31, 2008)

2.4.2 Redes inalámbricas

Las redes inalámbricas de área local WLAN, por sus siglas en inglés, se han convertido rápidamente en una parte central dentro de la infraestructura de acceso de una empresa. El estándar IEEE 802.11 ha liderado la interoperabilidad entre proveedores y rápidamente ha reducido los precios de los dispositivos, haciendo el acceso inalámbrico una alternativa económicamente tentadora frente a las redes que utilizan cableado. Actualmente, las configuraciones en entornos empresariales incorporan elementos que soportan la movilidad entre los Puntos de Acceso (AP) así como también soluciones para la seguridad y el monitoreo.

La movilidad ha introducido una serie de nuevos problemas que no estaban presentes en una infraestructura cableada, debido a la transferencia que existe entre los puntos de acceso. Las implicaciones para la seguridad de la

comunicación recaen en el tema de transferirse frecuentemente hasta diferentes APs, el estándar IEEE 802.11 requiere que el Nodo Móvil (MN) tiene que someterse a un proceso completo de autenticación cada vez que desee conectarse a un nuevo AP. Ratificaciones de seguridad del IEEE han definido algunas remediaciones para las WLANs en el estándar IEEE802.11i.

De acuerdo a este estándar, los procesos completos de autenticación involucran la utilización del 802.1X una arquitectura de control basada en el acceso al puerto y provee mecanismos para el manejo de claves. Un servidor AAA como RADIUS es utilizado para la derivación de la autenticación y la clave. Luego de una autenticación satisfactoria, el MN y el AP se comprometen mediante un protocolo de cuatro vías para derivar materiales de encripción de claves. El material de claves generado de esta manera es entonces utilizado en sesiones de comunicación encriptadas entre el AP y el MN. Así, mediante el protocolo de cuatro vías, el cual no involucra a un servidor AAA, es una necesidad en cada asociación segura de un MN a un segmento controlado por un AP que no puede ser evitada.

Sin embargo, los procesos de autenticación sugeridos en el 802.11i ratifican la utilización del Protocolo Extensible de Autenticación (EAP) sobre la capa de transporte de seguridad (TLS) y pueden introducir significativas demoras debido a que involucra el intercambio de una serie de mensajes entre el MN y el servidor AAA vía el AP. Este tipo de demoras son aceptables para aplicaciones flexibles en cuanto al requerimiento de tiempo de respuesta. Más en programas de tiempo real, como son aquellas soluciones de voz sobre IP que tienen estrictos requerimientos en cuanto a retrasos, esta demora en la red y el manejo de los cortes, resultan perjudiciales para una exitosa provisión de aplicaciones populares en entornos inalámbricos.

Los inconvenientes arriba planteados provienen de dos direcciones: transferencias dentro del dominio y transferencia entre dominios. Por lo tanto se requieren soluciones para los dos casos. Si bien varias alternativas han sido presentadas para la primera dirección, resulta que las transferencias entre proveedores o dominios se están convirtiendo en un escenario común que

requiere de diferentes soluciones ya que involucra la autoridad de más de un administrador en gran parte de los casos.

En resumen el estándar IEEE 802.11x agrupa a una familia de protocolos provistos para comunicaciones inalámbricas que utilizan una frecuencia de radio como medio de transmisión. A continuación se lista la conformación de esta familia y sus características más destacables:

802.11 éste estándar define para la red inalámbrica un ancho de banda en la transmisión de 1Mbps o 2 Mbps utilizando el espectro de frecuencia de 2.4GHz e incorporando cualquiera de los siguientes métodos para la codificación de datos: *Frequency-Hopping Spread Spectrum* (FHSS) o *Direct-Sequence Spread Spectrum* (DSSS).

802.11a éste estándar provee para la red inalámbrica un ancho de banda en la transmisión de hasta 54Mbps utilizando el espectro de frecuencia de 5GHz y utiliza el método de codificación *Orthogonal Frecuency Division Multiplexing* (OFDM) en reemplazo del FHSS o el DSSS.

802.11b éste estándar provee un ancho de banda en la transmisión de hasta 11Mbps (con tasas de repliegue de 5.5, 2 y 1 Mbps) utilizando el espectro de frecuencia de 2.4GHz y utiliza únicamente el método de codificación DSSS.

802.11g éste estándar provee un ancho de banda en la transmisión de hasta 54Mbps utilizando el espectro de frecuencia de 2.4GHz. Si bien es cierto es capaz de obtener velocidades más rápidas, sufre de los mismos problemas de interferencia heredados de su estándar predecesor 802.11b al tener que compartir el espectro con otros dispositivos que utilizan la misma frecuencia.

802.11i éste estándar incorpora a su predecesor mejoras en el tratamiento de la seguridad haciendo particularmente énfasis en la autenticación. Con frecuencia se referencia a éste estándar como WPA2 que es el nombre otorgado por la alianza WiFi.

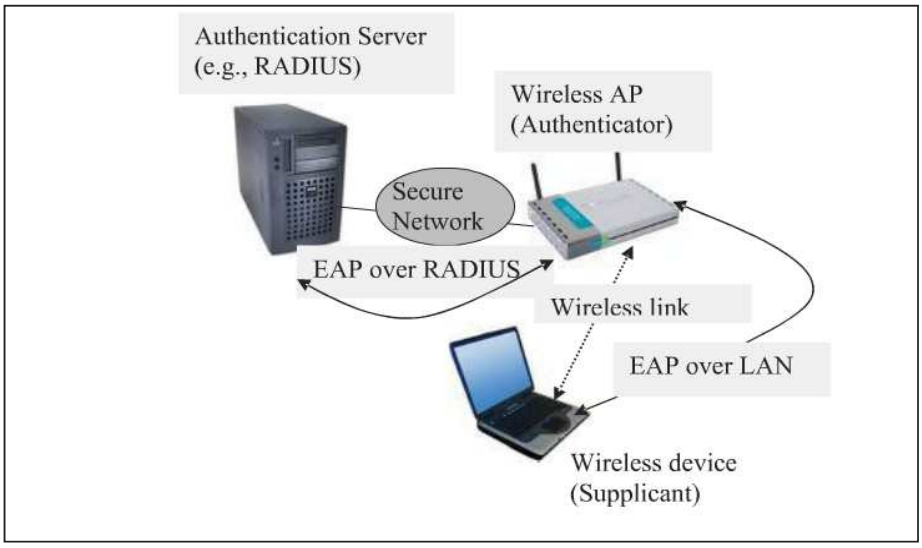
802.11n éste estándar proporciona anchos de banda que pueden llegar a hasta los 300Mbps en el espectro de frecuencia de los 5GHz y por temas de

compatibilidad también puede comunicarse a 2.4GHz. La ventaja de este estándar es que oferta altas velocidades en una frecuencia que no tiene mucha interferencia.

2.4.2.1 Proceso de autenticación IEEE 802.11i

Este proceso es un mecanismo de control de acceso basado en la autenticación, definida en el estándar IEEE 802.11. El IEEE 802.11i incluye la utilización de la arquitectura definida en el IEEE 802.1x[18] que es un estándar de control de acceso a la red basado en el puerto, aplicable para diferentes tecnologías de la capa de enlace como son: IEEE 802.3[19], FDDI[20], IEEE 802.11, etc. En éste estándar existen tres entidades involucradas en el proceso de autenticación: el suplicante o el dispositivo inalámbrico del usuario, el autenticador o el puerto de red (WAP[21]) y un servidor autenticador como es el caso de un servidor RADIUS. La siguiente ilustración muestra esta configuración.

Ilustración 2-18 Configuración del 802.1x



Fuente: (Zhang, Zheng, & Ma, March 31, 2008)

[18] Suplemento al ISO/IEC 15802-3:1998 (IEEE Std 802.1D-1998) provee la capacidad del control de acceso basado en el puerto (http://www.ieee802.org/1/pages/802.1x.html).
[19] Grupo de trabajo que desarrolla estándares para Ethernet basados en LANs (http://www.ieee802.org/3/)
[20] Fiber Distributed Data Interface (FDDI)
[21] Wireless Access Point (WAP)

Suplicante: Es un dispositivo de un usuario final en busca de conectividad a la capa de enlace de una red que le provea los servicios ofrecidos por la misma.

Autenticador: Es el AP inalámbrico que provee conexiones a la capa de enlace a los dispositivos de usuarios. Cuando el autenticador recibe un mensaje exitoso desde el servidor de autenticación, éste le permite al suplicante establecer la conexión hasta la capa de enlace.

Servidor de autenticación: Es un servidor central el cual ayuda al autenticador con las decisiones de autenticación en base a lo que conoce acerca del suplicante y la información suministrada por este último.

3. Capítulo III: Implementación

3.1 Antecedentes

La multiplicidad de dispositivos electrónicos con capacidad Wi-Fi utilizados en diversos ámbitos productivos, ha convertido el acceso hacia las redes inalámbricas en un servicio relevante dentro de la infraestructura tecnológica de toda organización. Ante esta creciente demanda por parte de los usuarios de estar siempre conectados mediante sus dispositivos, sean estos personales o de trabajo, la industria rápidamente ha inundado el mercado con una variada gama de equipos que simplifican su conexión, permitiendo su abaratamiento y fácil acceso. La mayoría de dispositivos utilizados como APs utilizan como método de seguridad el algoritmo WEP (*Wired Equivalent Privacy*), el cual puede ser fácilmente vulnerado.

Debido a la ausencia de un proceso de autenticación, autorización y registro por parte del usuario que solicita el servicio, cualquier dispositivo configurado adecuadamente podría acceder de manera anónima hacia la red interna de la organización, poniendo en riesgo tanto la información como la seguridad de la misma.

Por lo expuesto es necesario entonces contar con un entorno que viabilice la prestación de servicios tecnológicos de alta demanda como son las conexiones hacia redes inalámbricas, disponiendo de controles destinados a proteger la información de la empresa de accesos no autorizados y permitiendo a la organización beneficiarse de las actuales tendencias de seguridad sobre manejo de la información.

3.1.1 Características del entorno

Sí una unidad productiva está compuesta entre uno y nueve trabajadores y su facturación de ventas al año no sobrepasa los USD 100.000, entonces acorde al reglamento del Código de la Producción, esta entidad tiene la calificación de Microempresa.

En función de los resultados obtenidos del último Censo Económico que el Instituto Nacional de Estadísticas y Censos (INEC) llevo a cabo el 2010, el Ministerio de Industrias y Productividad plantea que de los 543.000 negocios registrados a escala nacional el 95% (515.000) corresponden al segmento denominado como Microempresas o Pequeñas y Medianas Empresas (MiPymes).

Ilustración 3-1 Establecimientos registrados en Ecuador según Censo Económico 2010

Fuente: (INEC)

Del gráfico que precede es fácil deducir que las MiPymes tienen una notable presencia en todas las industrias que componen la actividad económica del país y están jugando un rol importante como agentes productivos.

> *"Las pequeñas y medianas industrias (Pymes) de la región se afianzan en Latinoamérica. Según cifras de la Fundación para el Desarrollo Sostenible (Fundes) en la región existen 716 mil pequeñas empresas y 145 mil medianas, las mismas que*

> *generan el 88% del total de empleos y siempre relacionado con el sector comercial. Todo ello frente a un 10% que avivan las grandes compañías"* (Diario HOY, 2011).

Por la naturaleza propia de las MiPymes estas tienen la necesidad de adoptar con celeridad las innovaciones tecnológicas a fin de mantenerse competitivas y satisfacer las demandas del mercado.

> *"Un estudio realizado en conjunto por la Cámara de la Pequeña Industria de Pichincha (Capeipi) y la Pontificia Universidad Católica de Quito en el 2010, revela que el 26% de empresas pequeñas han realizado algún tipo de innovación, frente al 23% de las medianas empresas. Esto, de un universo de 1200 firmas que conforman el sector. De las cuales 950 son pequeñas y 250 medianas empresas.*
>
> *Para Ricardo Flor, presidente de la Capeipi, la innovación tecnológica comprende un mejor proceso e innovación en el producto, en la gestión organizacional y en el desarrollo comercial. Esto se traduce en "adquirir nueva maquinaria, generar procesos cortos que abaraten la producción, innovar productos, mejorar la gestión administrativa y realizar nuevas investigaciones", afirma el empresario."* (Revista Lideres, 2011).

Lo arriba expuesto se traduce como la respuesta del sector de las MiPymes ante el desafío de reducir la brecha tecnológica existente entre Ecuador y los países desarrollados. Siendo este esfuerzo parte de un proceso que pretende replantear las estrategias corporativas y permitan alinear su visión a las necesidades de un mundo globalizado.

El Instituto Nacional de Estadística Geográfica e Informática INEGI de México, sobre la base de un estudio realizado en algunos países de

América Latina y varios pertenecientes al denominado G7, ha logrado identificar algunos indicadores sobre la inversión en TIC que realizan las empresas, siendo estos:

- Gasto en tecnologías de información y comunicaciones.
- Número de computadoras personales.
- Usuarios de Internet.
- Servidores de Internet.
- Líneas telefónicas.
- Usuarios de telefonía móvil.

A continuación se muestra la evolución de algunos de estos indicadores en nuestro país desde el 2008 y según los datos publicados por el INEC en base al último censo nacional y económico llevado a cabo el 2010:

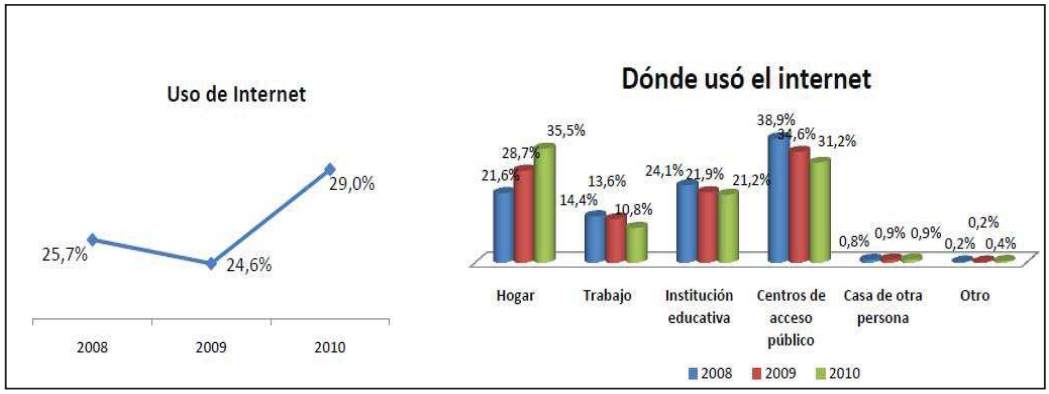
- En Ecuador el 27% de los hogares reporta la tenencia de al menos un computador y el 11.8% dispone de acceso al Internet. La cobertura de telefonía fija llega al 38.5% de la población mientras que la celular abarca al 80.1%.

Ilustración 3-2 Equipamiento en hogares de Ecuador ENEMDU 2010

Fuente: (INEC)

- El 29% de la población reporta que son usuarios de Internet, 3 de cada 10 ecuatorianos ha ingresado al internet en el 2010, accede principalmente desde el hogar o centros de acceso público, y más de la mitad de los usuarios lo hace de manera diaria.

Ilustración 3-3 Utilización de Internet en Ecuador ENEMDU 2010



Fuente: (INEC)

En base a las estadísticas que anteceden sobre el entorno, se identifica claramente el peso tecnológico que cada componente que confluye en una MiPyme lleva consigo: colaboradores que para el desempeño de su rol demandan de información digital ya que la misma es parte de su normal comportamiento – sea esta de una fuente interna o externa-, consumiendo la misma en una amplia gama de dispositivos -con capacidad inalámbrica de preferencia y cada vez mas creciente- y la necesidad de mantener a la organización competitiva en un mercado globalizado. Hace que las MiPymes deban estar preparadas para responder de una manera ágil y efectiva a las nuevas realidades que les plantea el ambiente donde deben desenvolverse.

Por ello este trabajo de titulación propone como alternativa la adopción de un mecanismo seguro para la gestión de la comunicación inalámbrica de la red LAN, entre los elementos autorizados, mediante la adopción del protocolo RADIUS.

3.1.2 Riesgos en el uso de tecnologías WiFi

Los indicadores arriba descritos sobre el uso del Internet, computadores y telefonía móvil -donde los denominados teléfonos inteligentes tienen una tendencia al crecimiento- muestran la relevante incidencia de la globalización (conformado por procesos tecnológicos, culturales, económicos y sociales) en nuestra población y por ende en las empresas.

En nuestro país existe una amplia gama de dispositivos electrónicos que manejan información en formato digital y están certificados para trabajar en ambientes WiFi y su pronta adopción es la respuesta que las empresas dan para mantenerse competitivas e impactar positivamente en su necesidad de solucionar aspectos relevantes en su gestión como son: producción, administración y relación con los clientes sean estos internos o externos.

Tomando en cuenta que por definición una microempresa emplea de uno a diez trabajadores no es difícil imaginar que existen pocas oportunidades de contar con especialistas en cada área, excepto en aquella relacionada al propósito de la actividad productiva. Por lo tanto éste empresario debe ser poli-funcional y sus conocimientos deben abarcar todos los procesos.

La reducción en el costo que implica la instalación de un sistema de cableado estructurado en una MiPyme y la opción de brindar a los empleados mayor flexibilidad para realizar sus labores en el lugar de trabajo han sido factores que ha alentado la rápida aparición de entornos WiFi en las empresas.

No sería extraño entonces encontrar escenarios donde MiPymes que a pesar de contar en su infraestructura con servicios de conexión inalámbrica para atender la demanda de dispositivos de última generación con capacidad WiFi (Laptops, Tablet PCs, Smartphones, etc.) adquiridos bajo la premisa de optimizar sus procesos internos estén expuestos a los siguientes riesgos:

- Accesos no autorizados
- Degradación del servicio
- Perdida de información

Los accesos no autorizados se presentan debido a la debilidad del proceso de autenticación y autorización utilizado para brindar el servicio de conexión hacia la red inalámbrica de la empresa. En algunos casos los APs están configurados de manera abierta y atienden todas las solicitudes de conexión de cualquier cliente sin restricción alguna. Otros poseen métodos de restricción mediante la asignación de una clave, que es administrada mediante el mecanismo de autenticación WEP que fue originalmente introducido como estándar del protocolo IEEE 802.11 definido para la protección de sistemas WiFi, la misma que puede ser descifrada con cierta facilidad por diferentes aplicaciones o el mecanismo de difusión y control del código de acceso suele escapar al control de la organización.

La degradación del servicio se debe a la debilidad del mecanismo de autenticación WEP que permite la conexión hacia la red de dispositivos con capacidad WiFi de uso personal de manera ilimitada en detrimento de aquellos equipos y usuarios que utilizan la conexión inalámbrica con fines productivos.

La incapacidad de mantener a salvo la privacidad en la red inalámbrica mediante WEP deja abierta una brecha que puede ser aprovechada por personas ajenas al entorno que por diversas motivaciones (como son: juego, revancha, espionaje o ego) ponen en riesgo la información de la empresa.

3.1.3 Protegiendo el acceso en entornos WiFi

La alternativa para una MiPyme en Ecuador, cuya necesidad es contar una infraestructura de red inalámbrica más segura y eficiente, es la adopción de las recomendaciones del estándar IEEE 802.11i mediante el cual se pretende regular el acceso hasta los servicios de la red inalámbrica solo para aquellos usuarios autorizados.

Tal como se mencionó en el capítulo anterior, en el tema de ¨Redes inalámbricas", a parir del año 1999 donde se definió el estándar IEEE 802.11 para entornos WLAN, debido a la vulnerabilidad que representa el uso de WEP, se realiza una revisión del mismo que deriva en el aparecimiento del IEEE

802.11i donde se analizan con profundidad los tópicos de seguridad y se plantea una nueva arquitectura.

En esta nueva propuesta de organización aparece el rol del servidor autenticador, a cargo de la gestión de transacciones AAA (Autorización, Acceso y Contabilidad) de los suplicantes, liberando de esta responsabilidad al tradicional WAP, quien sigue siendo el encargado de otorgar o denegar el acceso al cliente pero en función de la respuesta de servidor autenticador.

3.2 Diseño de una red inalámbrica segura

Partiendo del hecho de que no existe un entorno cien por ciento seguro, en el área de provisión de servicios de conexión inalámbrica y en el ámbito de las TICs en general, el modelo que a continuación se desarrolla hace énfasis en la utilización de un mecanismo de gestión de transacciones del tipo AAA, que implican procesos de autenticación, autorización y contabilización -registro de los recursos utilizados durante la conexión- al que serán sometidos los usuarios que solicitan acceso hasta la red inalámbrica a diferencia de aquel que solo valida la identificación del suplicante y es el método tradicionalmente presente en las MiPymes.

De esta manera se trata de dar cumplimiento a un principio muy simple pero básico que es permitir el acceso a usuarios autorizados y denegarlo para aquellos que no lo son.

La infraestructura de la red inalámbrica segura, que se propone para dar cumplimiento al objetivo planteado de contar con un modelo AAA, implica la participación armónica de los protocolos, estándares y arquitecturas que en detalle se abordaron en el capítulo anterior, siendo estos:

Servidor LDAP que será el encargado de administrar el catálogo de los recursos de la red, entre otros los usuarios autorizados para acceder a los recursos disponibles.

Servidor AAA que gestionará las transacciones de autenticación y autorización, previa consulta con el servidor LDAP, y mantendrá el registro

contable de todos los recursos utilizados durante la conexión del usuario. Además será el encargado de administrar la base de datos de los puntos de acceso inalámbrico que formen parte de la infraestructura.

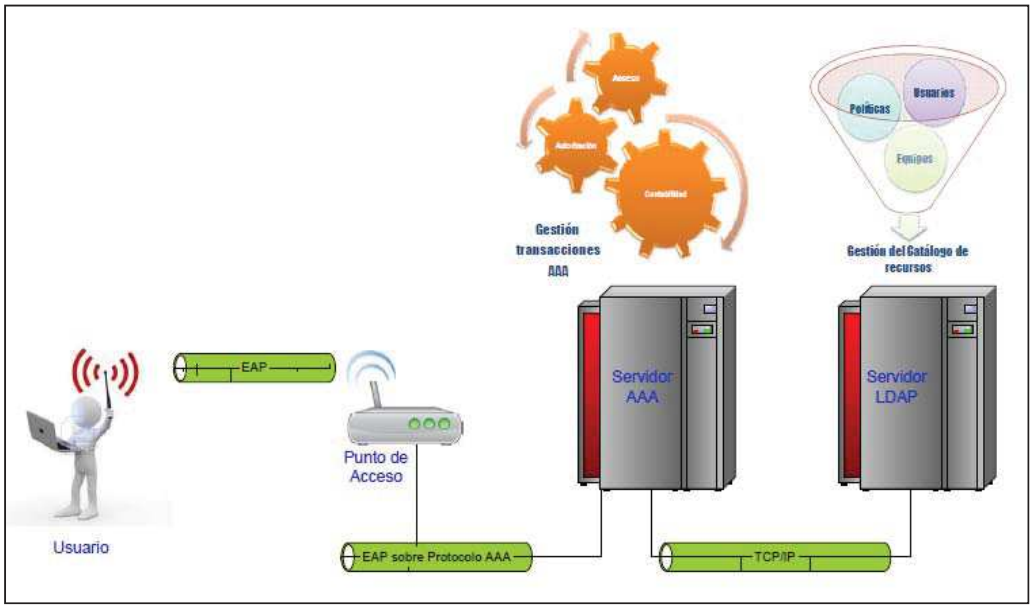
Protocolo AAA que será el utilizado para la interacción entre los servidores LDAP y AAA para el intercambio de información.

Puntos de acceso inalámbrico son aquellos dispositivos electrónicos encargados de expandir los recursos de la red LAN hacia los clientes que utilizan como medio de conexión el espectro de radio frecuencia, compatibles con el estándar IEEE 802.11i, cuyo registro conste en la base de datos de dispositivos autorizados por el servidor AAA y gestionen entre ellos la comunicación bajo el protocolo EAP en la capa de transporte.

Equipos terminales o clientes compatibles con el estándar IEEE 802.11i que serán los dispositivos a utilizar por los usuarios autorizados para conectarse a la red inalámbrica.

El siguiente gráfico muestra la interacción existente entre los elementos arriba descritos para lograr el objetivo de contar con una WLAN segura:

Ilustración 3-4 Componentes de una WLAN segura



Elaborado por: Autor

3.2.1 Selección de los componentes de la solución

El diseño arriba propuesto será implementado a través de herramientas de virtualización y en cumplimiento de uno de los objetivos específicos planteados en la sección “1.3.1 Objetivos específicos”, en un esfuerzo de reflejar las características de una MiPyme en Ecuador, utilizando tecnologías de información y comunicación accesibles en nuestro entorno.

A continuación se presenta en detalle el análisis y los criterios de evaluación utilizados en el proceso de selección de cada uno de los elementos integrales del diseño propuesto y que fueron calificados como idóneos para poder simular un ambiente de producción.

3.2.1.1 Servidor LDAP

Tal como se explicó en el Capitulo II, LDAP ha sido un protocolo que desde su aparición ha demostrado ser una herramienta que en la práctica ha facilitado las tareas que los administradores de red deben afrontar en la gestión de sus recursos (usuarios, grupos, computadores, servidores, impresoras, perfiles, políticas, etc.). Su estructura le ha permitido fácilmente ser adoptada en cualquier arquitectura de red de computadores, independiente del tamaño de la organización, en consecuencia la mayoría de sistemas operativos existentes, que se comercializan bajo el esquema de licenciamiento o código abierto, lo incluyen como parte sus especificaciones. A continuación se muestra una tabla que lista algunos de los nombres comerciales con el que los diferentes fabricantes identifican a este protocolo dentro del sistema que ofertan:

Tabla 3-1 Lista de denominaciones comerciales del protocolo LDAP según el proveedor

Nombre comercial	Fabricante
CP Directory Server	Critical Path Inc., San Francisco
eTrust Directory	Computer Associates International Inc., Data
DC-Directory	Connection Ltd., London
SecureWay Directory	IBM
Active Directory	Microsoft Corp.
Nexor Directory	Nexor Inc., Falls Church, Va
eDirectory	Novell Inc.
Oracle Internet Directory	Oracle Corp.
iPlanet Directory Server	Sun Microsystems Inc.
Global Directory System	Syntegra (USA) Inc., Arden Hills, Minn.
DirX	Siemens AG, Munich, Germany
OpenLDAP	Linux open source

Elaborado por: Autor

Ya que el protocolo LDAP será parte integral del sistema operativo del servidor que tendrá a cargo una tarea crítica dentro de la operatividad de la organización, como es la gestión del catálogo de los recursos, el sistema operativo debe ser considerado de confianza y satisfacer un nivel de seguridad apropiado para su misión.

Mediante un acuerdo internacional, que involucra la participación de varios países, se establecen las bases técnicas para calificar la seguridad en las tecnologías de información y para ello se ha logrado determinar tanto Criterios Comunes (CC[22]), así como una Metodología Común de Evaluación (CEM). Un producto recibe una Certificación Común de Reconocimiento del Acuerdo (CCRA) una vez que satisface las bases arriba detalladas y se le asigna un nivel de Aseguramiento de la Evaluación (EAL) acorde a los resultados obtenidos.

Existen siete niveles en los que puede recaer una calificación EAL, la siguiente tabla muestra en detalle los mismos:

[22] Portal que mantiene los registros de lo productos certificados (http://www.commoncriteriaportal.org)

Tabla 3-2 Niveles de seguridad según calificación EAL

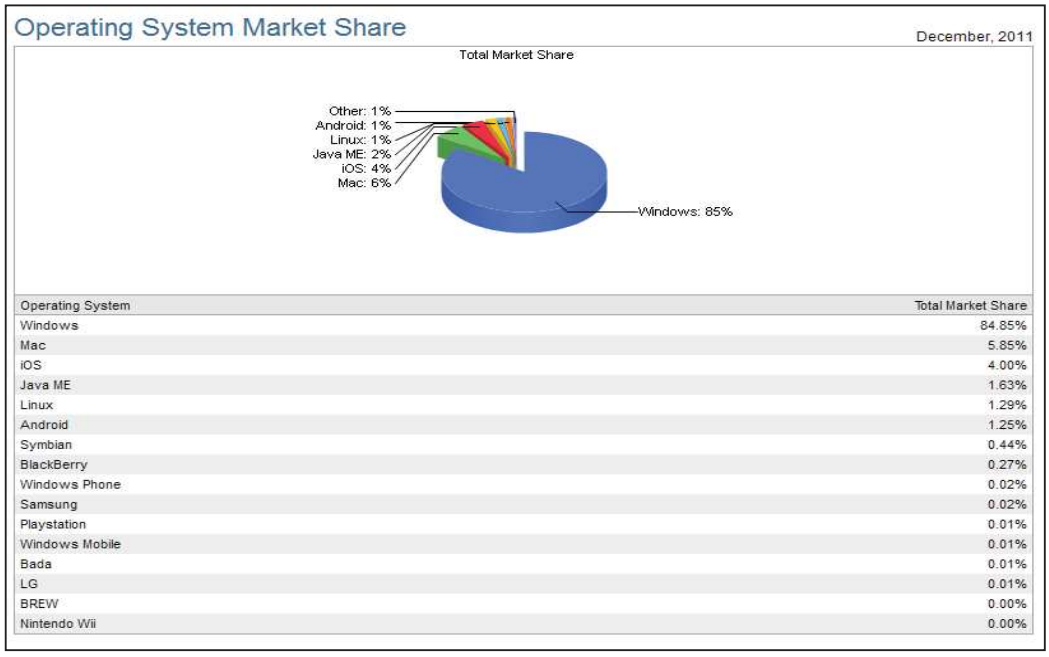
Nivel	Descripción de la calificación de la seguridad
1	Primaria, utilizada cuando un usuario quiere asegurarse que el sistema opere adecuadamente pero el tratamiento a la seguridad no es visualizado como un tema serio.
2	Requiere que los desarrolladores del producto utilicen buenas prácticas de diseño. La seguridad no es considerada una alta prioridad en esta certificación
3	Requiere consientes esfuerzos de los desarrolladores para proveer moderados niveles de seguridad.
4	Requiere de positiva ingeniería de seguridad en base al desarrollo de buenas prácticas comerciales. Se espera que éste sea el nivel de seguridad referente para los sistemas comercializados.
5	Tiene como objetivo garantizar que la ingeniería de seguridad ha sido implementada en el producto desde las tempranas fases del diseño. Su objetivo es garantizar altos niveles de seguridad.
6	Provee altos niveles de aseguramiento de ingeniería especializada en seguridad. Esta certificación indica que se han implementado altos niveles de seguridad que sirvan de protección frente a riesgos significativos. Los sistemas con éste nivel de certificación serían altamente seguros ante los intentos de penetración de atacantes.
7	Destinado a niveles extremadamente altos de seguridad. Esta certificación requiere un extenso plan de pruebas, métricas y un completo conjunto de pruebas a través de un grupo independiente para cada componente del sistema.

Elaborado por: Autor

El EAL reemplaza a las certificaciones ITSEC (Information Technology Security Evaluation Criteria) y TCSEC (Trusted Computer Systems Evaluation Criteria) populares en Europa y Estados Unidos, respectivamente, antes de lograr el acuerdo de los CC. El nivel recomendado de certificación para sistemas comerciales es el EAL 4.

Según el portal Net Market Share (http://marketshare.hitslink.com) por primera vez el fabricante Microsoft Corp. ha reducido su cuota de participación de mercado, usualmente mayor al 90%, al cerrar el 2011 en un rango del 85% en el terreno de los sistemas operativos a nivel mundial con su producto Windows, tal como lo muestra el gráfico a continuación:

Ilustración 3-5 Cuota de participación de Microsoft Windows dentro del mercado de sistemas operativos



Operating System	Total Market Share
Windows	84.85%
Mac	5.85%
iOS	4.00%
Java ME	1.63%
Linux	1.29%
Android	1.25%
Symbian	0.44%
BlackBerry	0.27%
Windows Phone	0.02%
Samsung	0.02%
Playstation	0.01%
Windows Mobile	0.01%
Bada	0.01%
LG	0.01%
BREW	0.00%
Nintendo Wii	0.00%

Fuente: (NetMarketShare)

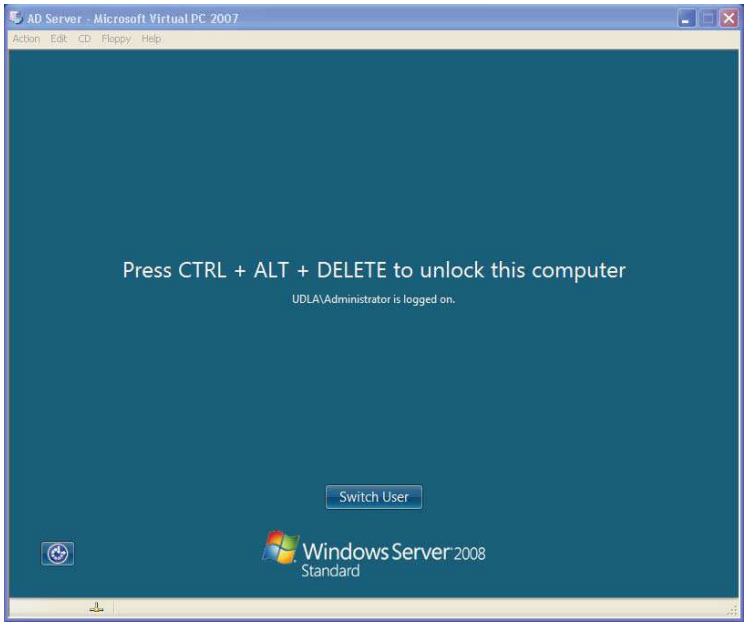
Ecuador no es un país que este al margen de esta realidad mundial, por ello es fácil inferir que exista una relación similar en nuestro mercado, siendo Windows el sistema operativo predominante en el sector de las MiPymes.

Tomando en consideración los antecedentes arriba expuestos y dando cumplimiento al primer objetivo detallado en la sección “1.3 Objetivos” de contar con un servidor que gestione el protocolo LDAP y el primer objetivo específico de la sección “1.3.1 Objetivos específicos” de hacerlo sobre un elemento virtual. Se ha determinado que el sistema operativo sobre el cual se implementará esta configuración es Windows 2008 R2 del fabricante Microsoft Corp., ya que sus características satisfacen plenamente las siguientes condiciones:

- ✓ Incorpora a LDAP como un componente del sistema operativo bajo la denominación de “*Active Directory*”.

- ✓ La versión Windows 2008 R2 cuenta con un certificado EAL 4+ de seguridad[23].
- ✓ El fabricante Microsoft tiene una amplia presencia en el mercado de MiPymes en Ecuador y está en lineamiento con el segundo objetivo de la sección "1.3. Objetivos", de contar con una solución portable para fines didácticos.

Ilustración 3-6 Interfaz gráfica de inicio del sistema operativo Microsoft Windows 2008 Server edición estándar



Elaborado por: Autor

3.2.1.2 Servidor AAA

Tal como se muestra en la ilustración 3-4, acorde a la definición del estándar IEEE 802.1X, es necesaria la participación de un servidor externo AAA (*Authentication, Authorization, Accounting*) para la implementación de un método que valide las credenciales tanto del usuario como del servidor y lleve el registro de las transacciones que el protocolo AAA tiene la capacidad de generar. Un servidor AAA tiene la capacidad de entender el protocolo EAP que es el lenguaje que permite su comunicación con los dispositivos que se utilizan

[23] Acorde el portal http://www.commoncriteriaportal.org/products/

como Puntos de Acceso (AP) vía inalámbrica, dentro de este esquema estos dispositivos viene a ser clientes del servidor AAA o autenticadores. El servidor AAA cumple funcionalidades de intermediario entre los APs y la base de datos de usuarios que reside en el servidor LDAP. Los APs se comunican directamente con los clientes, que dispongan del estándar IEEE 802.1X, independientemente que operen un computador u otro dispositivo compatible. La autenticación en el 802.1X se fundamenta en puertos. Esto significa que cuando existe un intento de autentificación a la red se apertura un puerto virtual para el paso de las credenciales, que se utilizan para el inicio de la sesión, y solamente sí el proceso de autenticación es exitoso se procede a transferir mediante un método seguro las claves de encripción, hasta los dispositivos de los clientes, permitiéndoles a los usuarios finales un total acceso a los recursos de la red.

En el capítulo II se describen los orígenes de RADIUS quien fue el primer protocolo AAA en aparecer a inicios de la década de los noventa y tuvo una rápida difusión entre los ISP que prestaban servicios de conexión mediante discado por líneas telefónicas y posteriormente su adaptación a los medios y redes de conexión vigentes.

Dada la vigencia del protocolo, por más de 20 años, es común asociar la figura de un servidor AAA con un servidor RADIUS y aunque en los inicios de la adopción del estándar IEEE 802.1x los servidores de RADIUS no estaban optimizados para este tipo de autenticación hoy en día existen servidores específicamente diseñados para la gestión de transacciones AAA en entornos WiFi basados en el protocolo RADIUS. La siguiente tabla muestra aquellos mas destacados en el mercado:

Tabla 3-3 Servidores especializados en RADIUS

Nombre comercial	Fabricante	Costo
Elektron	Periodic Labs LLC., California	USD 750 por servidor
ClearBox Enterprise Server	XPerience Technologies, Rusia	USD 599 por servidor
TekRADIUS	Yasin Kaplan, Turquía	USD 149 por servidor
Radiator	Open System Consultants, Australia	USD 1080 por servidor
FreeRADIUS	FreeRadius Server Project	Gratis bajo el esquema Open Source

Elaborado por: Autor

El RFC 3588[24] define a *Diameter* como un protocolo que cuenta con el marco necesario para gestionar transacciones AAA y nace en 1998 como una iniciativa que pretende superar las limitaciones de RADIUS. Destinado a trabajar tanto en ambientes locales como entornos donde los usuarios utilizan un perfil del tipo *Roaming*[25].

De hecho toma su nombre al asociar que el diámetro es el doble de un radio y su arquitectura le ha permitido al IETF identificarlo como la próxima generación de servidores AAA y sus requerimientos están siendo definidos por el grupo de trabajo TR45.6 denominado “Mobile IP RAOMOPS (*Roaming Operations*)”.

Según el sitio MarketResearch.com[26], se visualiza una coexistencia a largo plazo de la siguiente generación de RADIUS y *Diameter*. Por un lado RADIUS dispone de un diseño muy bien definido para la gestión de procesos AAA y algunos fabricantes tiene la capacidad de crear una nueva generación de este protocolo sin la necesidad de adoptar *Diameter*. Mientras que algunas ventajas del protocolo *Diameter* están siendo adoptadas y explotadas por otros segmentos de mercado como es su uso en redes de servicio de llamadas de voz.

Las previsiones sobre RADIUS indican que del mercado calculado en USD 886.4 millones en el 2008 alcance una participación de USD 1.7 billones para el

[24] http://tools.ietf.org/html/rfc3588
[25] Concepto introducido por Microsoft, en su sistema operativo, que permite a un usuario mediante el uso de sus credenciales iniciar una sesión en cualquier máquina de un dominio y presentarle el mismo entorno de trabajo que utiliza en su equipo primario.
[26] http://www.marketresearch.com/

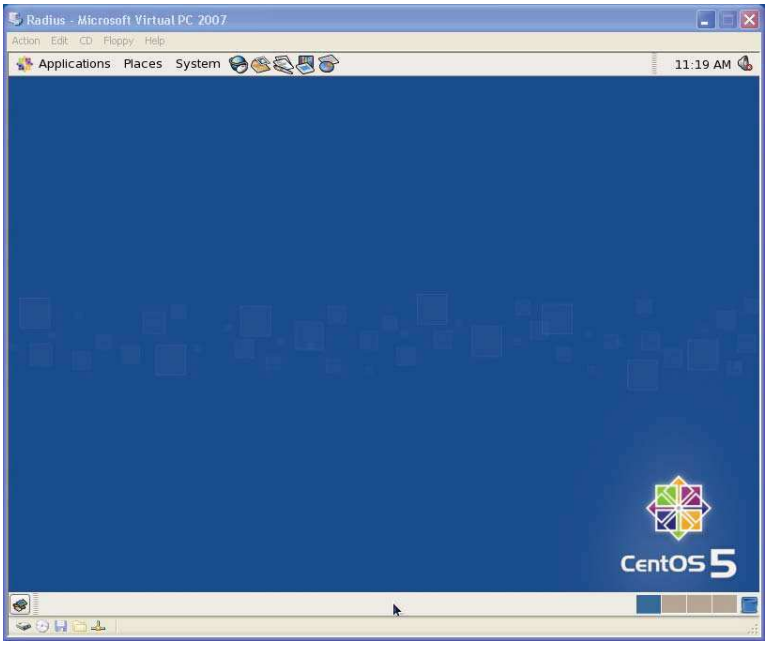
2015. Según el estudio realizado por WinterGreen Research, Inc.[27] bajo el título "AAA Radius and Diameter Server Market Shares, Strategies, and Forecasts, 2009 to 2015 ".

En base a los antecedentes descritos se ha optado por la elección de RADIUS tanto como protocolo así como servidor a cargo de gestionar las transacciones AAA. Con esta selección se cumple plenamente el primer objetivo específico, que implica la virtualización de los elementos susceptibles de tal acción para simular el entorno de una PyME. Las siguientes consideraciones justifican esta selección e identifican algunas características que definen la composición de este servidor:

- ✓ RADIUS desde su aparición ha gozado de alta aceptación y su adopción por los fabricantes de *networking* avizoran su permanencia en el mercado a mediano y largo plazo.
- ✓ FreeRADIUS en su versión 2.1.12 es la alternativa de mercado mas económica, ver tabla 3-3, su vigencia esta respalda por el grupo a cargo de mantener el producto que acorde una encuesta realizada en 2006[28] se estiman unos 10 millones de usuarios que se autentican utilizando FreeRADIUS y su adopción permite alinearse al segundo objetivo específico que implica la utilización de FreeRADIUS como el gestor de transacciones AAA.
- ✓ Centos versión 5, un sistema operativo basado en Linux, consta dentro de la lista de compatibilidad con FreeRADIUS y será el encargado de hospedar a FreeRADIUS. Además, la capacidad de configurar este servidor sobre una plataforma virtual está en lineamiento con el primer objetivo específico que es contar con elementos virtualizados.

[27] http://www.marketresearch.com/Wintergreen-Research-v739/
[28] http://freeradius.org/press/survey.html#others

Ilustración 3-7 Interfaz gráfica del sistema operativo Centos versión 5



Elaborado por: Autor

3.2.1.3 Punto de Acceso

Tal como se muestra en la ilustración 3-4 el AP es el dispositivo encargado de interactuar entre los clientes finales y el servidor AAA mediante el protocolo EAP. La mayoría de fabricantes de *networking* han incorporado dentro de sus especificaciones la compatibilidad con este protocolo.

Acorde al sitio de investigación de la compañía ABI *Research*[29], realizado en junio del 2010, Cisco sigue manteniendo un 50% de la cuota de mercado de dispositivos compatibles con WiFi para entornos empresariales que durante el primer trimestre del 2010 alcanzó la producción de un total de 800.000 unidades y se proyecta que para el 2015 existirá una demanda de 11.6 millones.

Posterior al anuncio por parte de *Hewlett Packard* (HP) de la adquisición de la empresa 3Com, ha dejado a éste fabricante junto a Motorola y Aruba como los principales jugadores de este segmento de la industria. Esta tendencia se

[29] http://www.abiresearch.com/

ratifica con la presencia de Cisco con una cuota de mercado equivalente al 68.5% en el segmento de *switches* en capa 2 y 3 así como un 54.2% a nivel de ruteadores, esto según el reporte "HP, *Cisco Dispute Meaning Of Latest Networking Market Share Numbers*" publicado en julio del 2011 por el portal Netwok Computing[30].

Tomando en cuenta la cuota de mercado que poseen los fabricantes de APs a nivel global, del cual Ecuador no es una excepción, para la instrumentación de la solución propuesta se utilizará un equipo marca Cisco modelo Aironet 1200 como el punto de acceso inalámbrico para la conexión de los clientes WiFi ya que es un objetivo de esta tesis brindar un entorno seguro para la conexión inalámbrica de dispositivos móviles. Tal como se muestra en la Ilustración 3-4, éste elemento es una pieza clave y juega un rol relevante dentro del esquema de conexión.

Se detallan a continuación los criterios que justifican esta selección:

- ✓ El fabricante Cisco y su modelo Aironet 1200 consta como parte de la lista de equipos compatibles con FreeRADIUS.
- ✓ Tiene la flexibilidad para trabajar con clientes que son compatibles con el estándar IEEE 802.11 en sus diferentes versiones: a y g.
- ✓ Diseñado para operar en entornos de espacios abiertos como: fábricas, almacenes y al aire libre.
- ✓ Permite experimentar altas prestaciones en temas de seguridad al permitir encripción asistida mediante hardware (AES[31]) sin disminuir su rendimiento.

[30] http://www.networkcomputing.com
[31] Hardware-Assisted AES Encryption

Ilustración 3-8 WAP Cisco Aironet 1200

Elaborado por: Autor

3.2.1.4 Clientes

Son todos aquellos dispositivos con capacidad WiFi que tengan integrado un cliente que soporte autenticación mediante el protocolo IEEE 802.1x con autenticación tipo PEAP y protocolo de autenticación MS-CHAP-V2 que proveerá las credenciales del cliente a ser validadas.

Ilustración 3-9 Dispositivos con conexión WiFi -computador portátil y teléfono inteligente

Elaborado por: Autor

3.3 Resumen de pasos a seguir

A fin de disponer de una infraestructura de red inalámbrica segura. En la tabla que se muestra a continuación se listan, a modo de resumen, los pasos que de manera secuencial se deben seguir y permiten configurar cada elemento identificado en la sección de diseño (3.2) de la solución.

Tabla 3-4 Resumen de los pasos de configuración y alineamiento con los objetivos

	Descripción del paso	Objetivo general	Objetivo específico
1	Instalar y configurar un servidor Windows 2008 estándar que contenga un Directorio Activo.	Contar con un servidor LDAP.	Configurar elementos virtuales y lógicos.
2	Instalar Centos 5 y configurar el servicio de SAMBA para la integración con el servidor Windows 2008.	Lograr la interelación entre LDAP y RADIUS.	Configurar elementos virtuales y lógicos.
3	Instalar y configurar FreeRADIUS sobre el servidor Centos 5 y configurar los clientes.	Implementar un modelo AAA mediante RADIUS.	Gestionar transacciones AAA.
4	Configurar el Access Point Cisco Aironet 1200 bajo el protocolo EAP.	Integrar al modelo AAA elementos de una Pyme.	Disponer de un ambiente seguro para clientes móviles.
5	Configurar los suplicantes que requieren acceso inalámbrico	Integrar al modelo AAA elementos de una Pyme.	Disponer de un ambiente seguro para clientes móviles.
6	Realizar pruebas de conectividad	Integrar al modelo AAA elementos de una Pyme.	Disponer de un ambiente seguro para clientes móviles.

Elaborado por: Autor

3.4 Instalando y configurando los componentes

El disponer de una guía práctica y detallada de los pasos que se deben ejecutar para disponer de una red WLAN segura ha sido un factor considerado como relevante desde el inicio en la elaboración de este trabajo de titulación. Ya que la misma constituye la evidencia del cumplimiento del primer objetivo específico identificado en este trabajo de titulación que es el configurar los elementos virtuales, físicos y su lógica. Que en su conjunto representan a una red típica en ambientes MiPymes.

Por lo arriba expuesto, para cada uno de los componentes que forman parte de la solución propuesta, se muestran en detalle los parámetros de configuración seleccionados y el criterio utilizado que justifica esta acción.

Los elementos correspondientes al diseño propuesto para una WLAN segura que se muestra en la Ilustración 3-4, susceptibles de ser virtualizados, son los

servidores LDAP y AAA. Para lograr este objetivo, descrito en la sección “1.3”, se ha optado por utilizar la herramienta de virtualización Microsoft Virtual PC versión 6.0.192.0. Esto obedece a cuestiones de compatibilidad ya que el equipo que servirá de host utiliza como sistema operativo la versión Windows XP Profesional del mismo fabricante.

3.4.1 Configurar el servidor de LDAP

Un requisito previo, para la ejecución de estos pasos, es que las características de hardware del servidor a utilizar satisfagan las especificaciones de que se encuentran en la lista de compatibilidad de hardware que dispone Microsoft para este producto. Para la elaboración de esta guía se ha utilizado una versión que permite la evaluación del producto por un máximo de 180 días.

Al término del proceso que a continuación se detalla conseguiremos alcanzar el tercer objetivo planteado en la sección “1.3” que implica: contar con un elemento virtualizado y sobre el mismo configurar un servidor LDAP para la gestión del catálogo de los componentes de la red. Los pasos que permiten alcanzar este cometido son:

1. Arrancar el equipo con el CD de instalación de Windows Server 2008. Seleccionar el idioma para la instalación, en este caso escoger el idioma Inglés y dar clic sobre el botón “*Next*”.

Ilustración 3-10 Interface para selección de parámetros iniciales en Windows Server 2008

Elaborado por: Autor

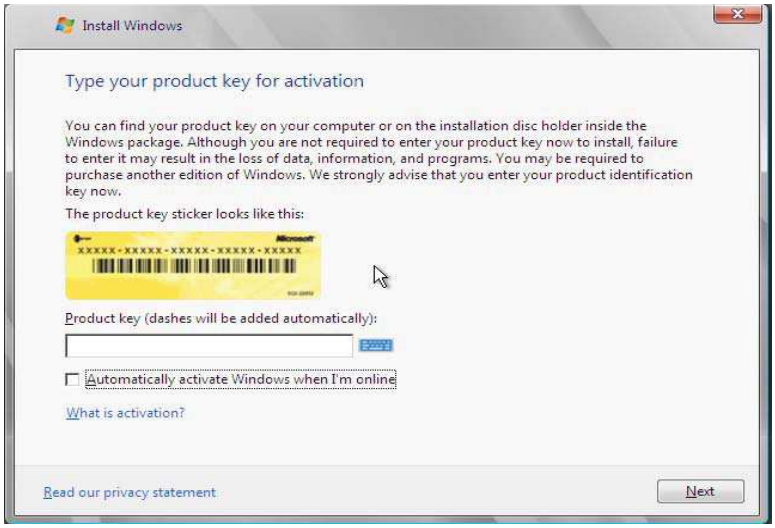
2. En la siguiente interface se espera la confirmación del usuario para proseguir con la instalación. Dar clic en ***Install Now***.

Ilustración 3-11 Interfaz que confirma inicio del proceso de instalación

Elaborado por: Autor

3. Al ser una versión de evaluación se requiere la desactivación de la opción "*Automatically activate Windows when I'm online*". Luego de desmarcar esta opción dar Clic en ***Next***.

Ilustración 3-12 Interface para activación de Windows en línea



Elaborado por: Autor

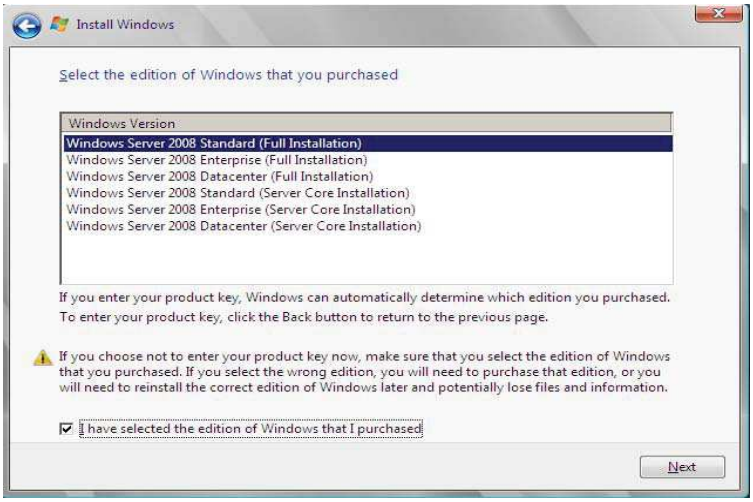
4. Considerando que se trata de una versión de evaluación optamos por seleccionar ***No*** en la ventana que solicita ingresar una clave de producto.

Ilustración 3-13 Validación de la clave de activación del producto

Elaborado por: Autor

5. Seleccionar la versión a instalar, en este caso escoger "*Windows Server 2008 Standard (Full Installation)*". Y marcamos la opción "*I have selected the edition of Windows that I purchased*". Clic en ***Next***.

Ilustración 3-14 Interface que permite la selección de la versión de Windows Server 2008



Elaborado por: Autor

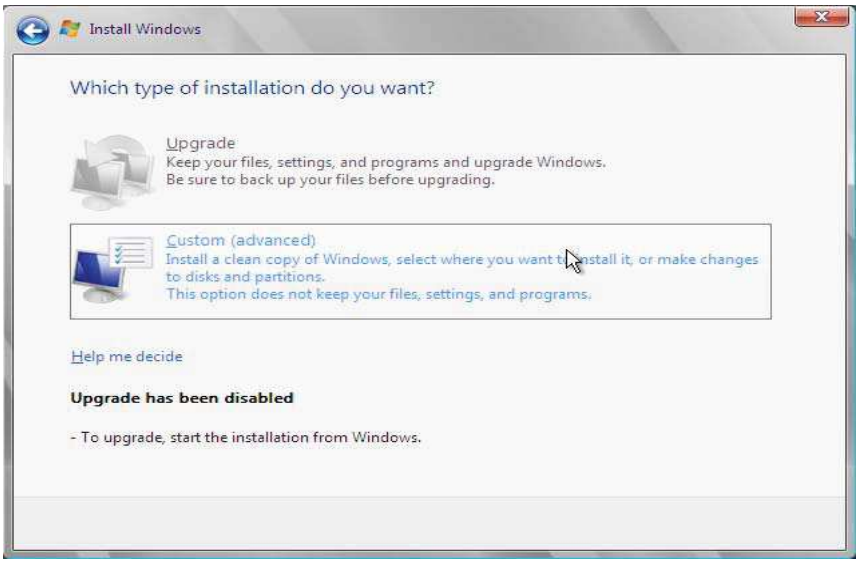
6. Leer los términos de Licencia y aceptar los mismos activando la casilla de aceptación. Clic en ***Next***.

Ilustración 3-15 Interface de aceptación de los términos del licenciamiento

Elaborado por: Autor

7. Ya que debemos personalizar ciertas características como la carpeta destino del sistema, se debe dar clic sobre la opción ***Custom (advanced)*.**

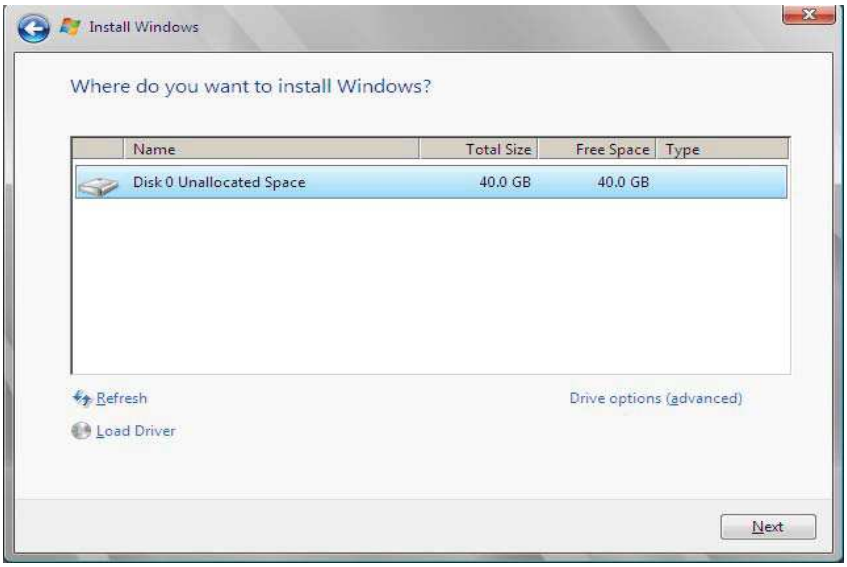
Ilustración 3-16 Interface que permite seleccionar el tipo de instalación



Elaborado por: Autor

8. Seleccionar el disco donde se va a instalar Windows. Clic en ***Next***.

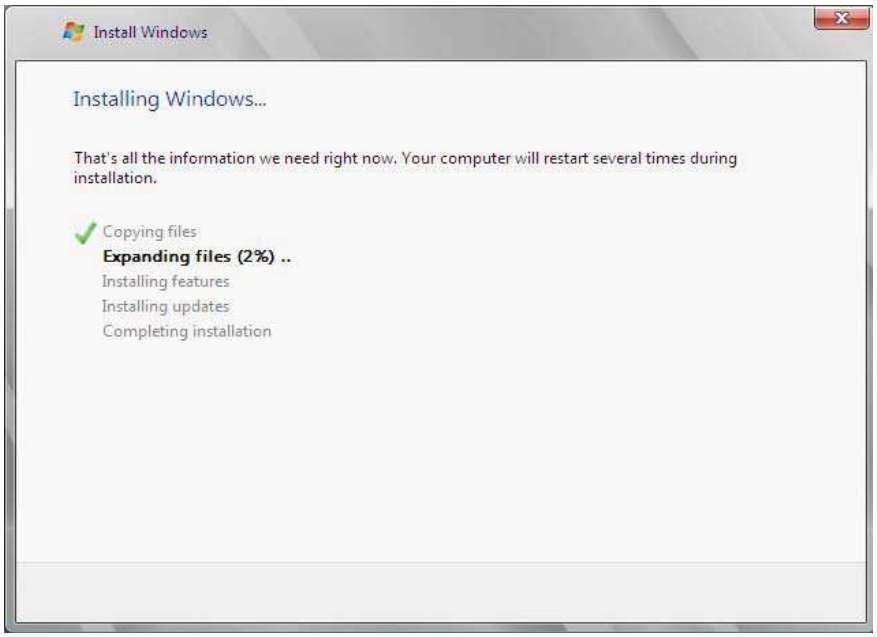
Ilustración 3-17 Selección del disco destino



Elaborado por: Autor

9. Se inicia el proceso de instalación, mostrando el avance de cada fase.

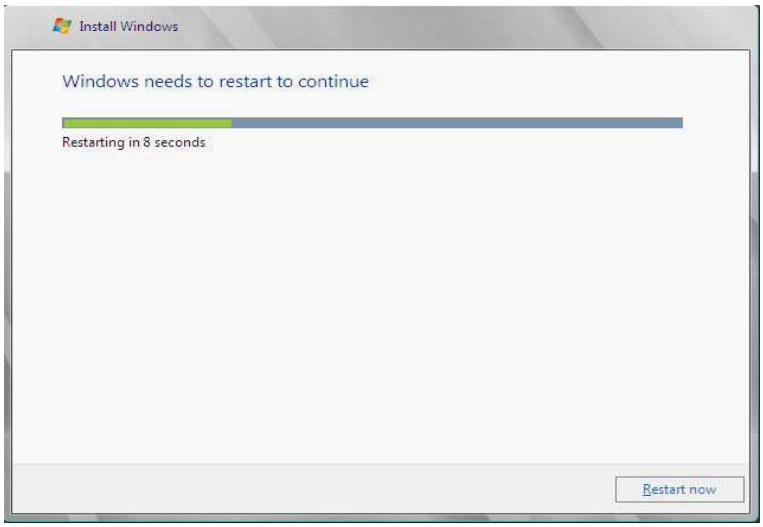
Ilustración 3-18 Indicador de progreso en el avance de la instalación



Elaborado por: Autor

10. Al completarse el proceso de instalación, se reinicia el equipo.

Ilustración 3-19 Alerta sobre reiniciación del equipo



Elaborado por: Autor

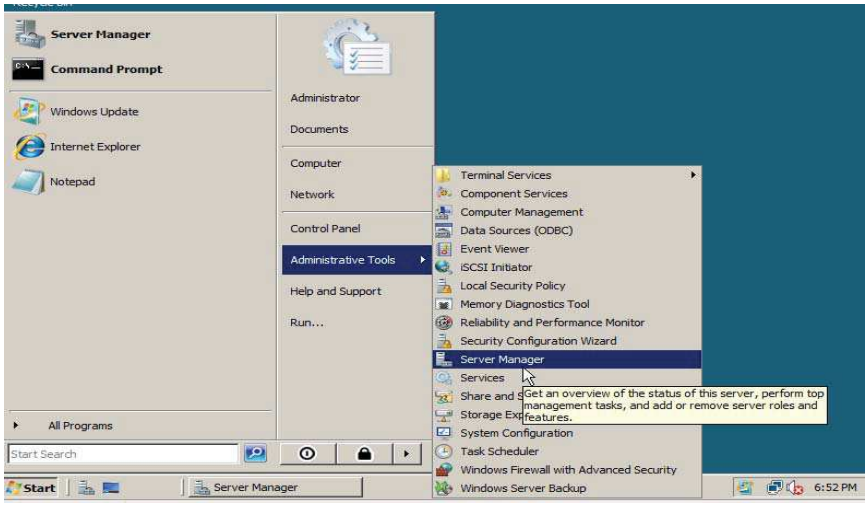
11. Al reiniciar el equipo dar clic, sobre el botón ¨*OK*¨ para configurar la contraseña del usuario *Administrator*. Esta clave es muy importante recordarla ya que es la única que permitirá tener un completo acceso al sistema.
12. Ingresar una contraseña para el usuario *Administrator* y presionar *Enter*.

Ilustración 3-20 Definición de la contraseña de administrador

Elaborado por: Autor

13. Una recomendación de Microsoft en el proceso de configurar el Directorio Activo (AD), por primera vez, es que la dirección IP del servidor del AD sea la misma del servidor de DNS. Abrimos el menú de "Server Manager" desde *Start*, *Administrative Tools*, *Server Manager*.

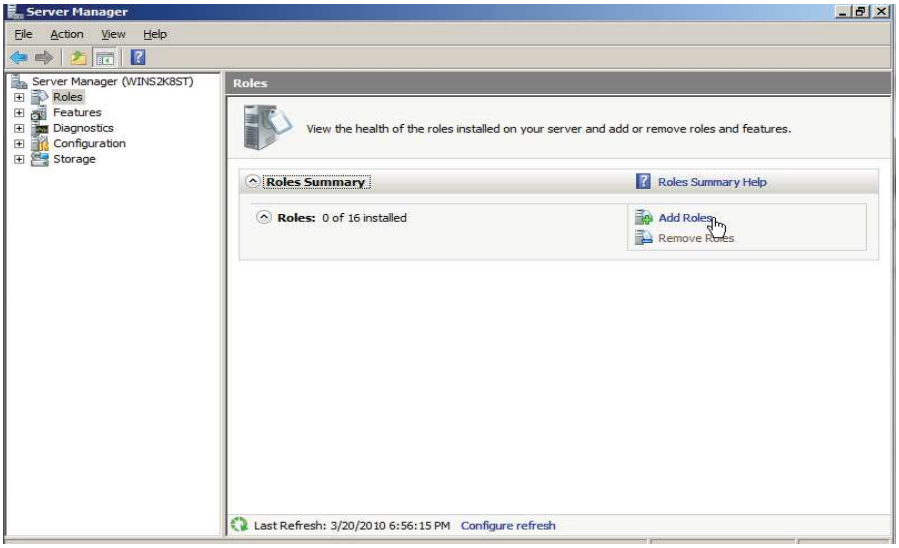
Ilustración 3-21 Selección del menú "Server Manager"



Elaborado por: Autor

14. Dentro del menú del Server Manager, en el panel Izquierdo dar clic sobre Roles. En el panel derecho seleccionar la opción: ***Add Roles***.

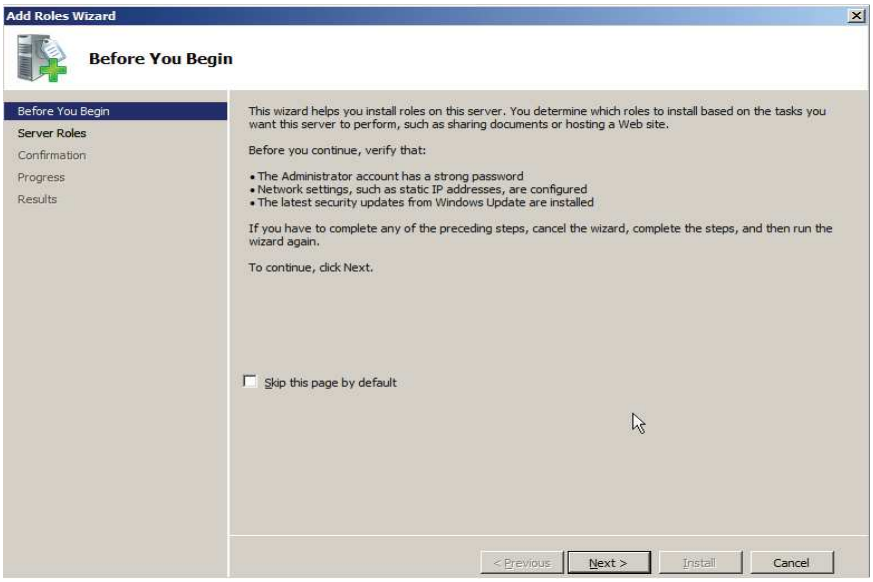
Ilustración 3-22 Selección del rol del servidor



Elaborado por: Autor

15. Aparece una ventana que resume las recomendaciones a considerar antes de iniciar el proceso, Dar clic en el botón ***Next***.

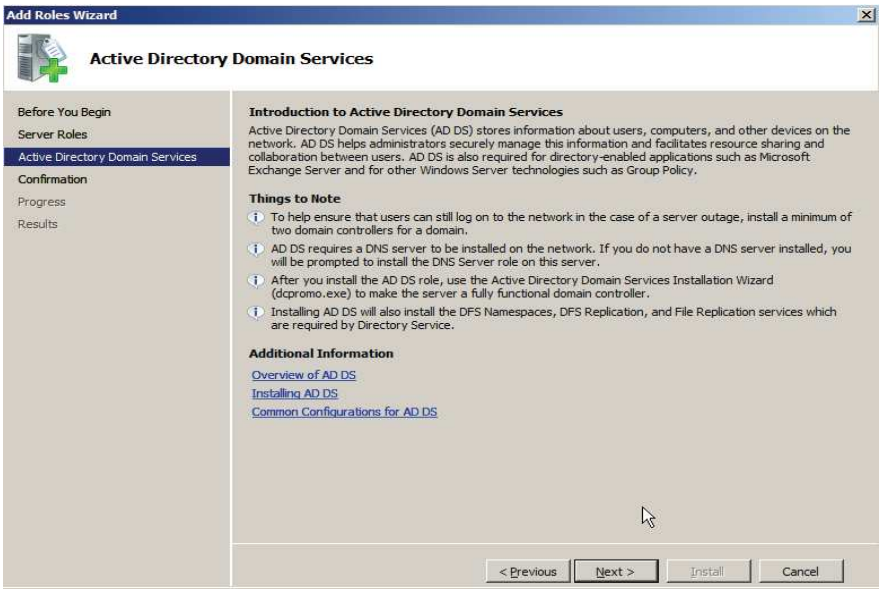
Ilustración 3-23 Resumen de consideraciones previo al proceso de selección de roles



Elaborado por: Autor

16. En la ventana *"Select Server Roles",* se muestran todos los roles que el servidor Windows 2008 puede ejecutar, seleccionar *Active Directory Domain Services*. Clic en ***Next***.
17. El rol de "*Active Directory Domain Services*" es la versión de LDAP que oferta Microsoft para la gestión del catálogo de la red en un dominio, luego de tomar nota sobre las consideraciones del vendedor sobre el proceso a seguir dar Clic en el botón ***Next***.

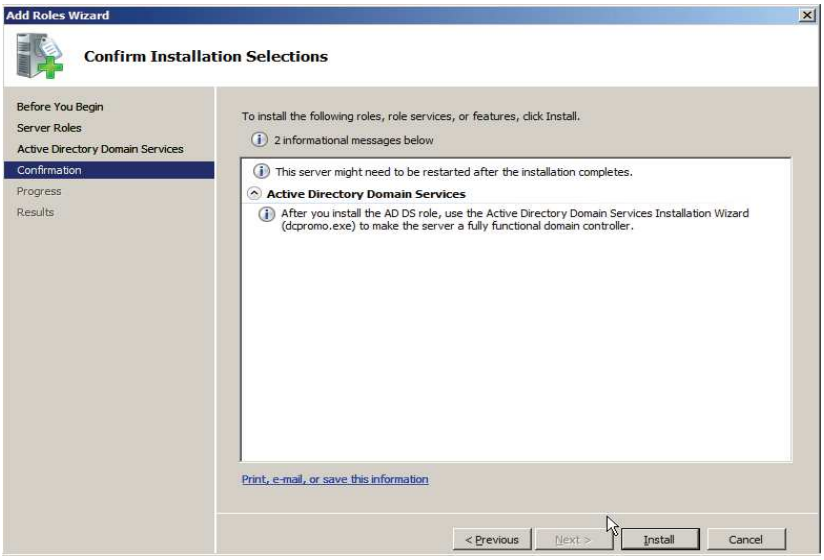
Ilustración 3-24 Plantilla resumen del servicio del AD y consideraciones para su instalación



Elaborado por: Autor

18. En la siguiente ventana el sistema espera recibir por parte del usuario la confirmación del rol elegido, por lo que se muestra la descripción del mismo, para ello se debe dar Clic sobre ***Install***.

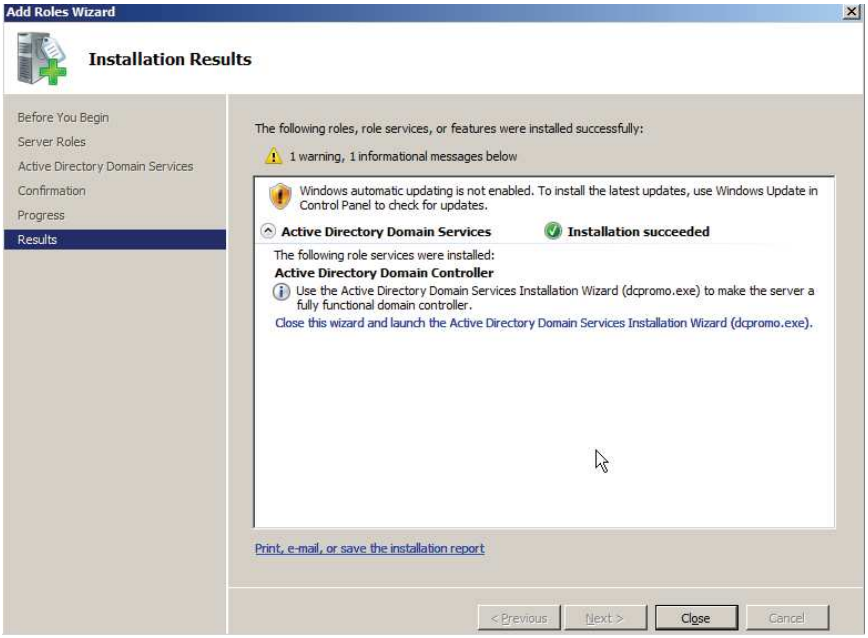
Ilustración 3-25 Confirmación del requerimiento de instalación del rol del Active Directory



Elaborado por: Autor

19. Luego de concluir el proceso de descompresión de archivos e instalación del servicio, se muestra una interfaz que resume los pasos ejecutados de este proceso y su estatus, en caso de ser exitoso dar clic en ***Close***.

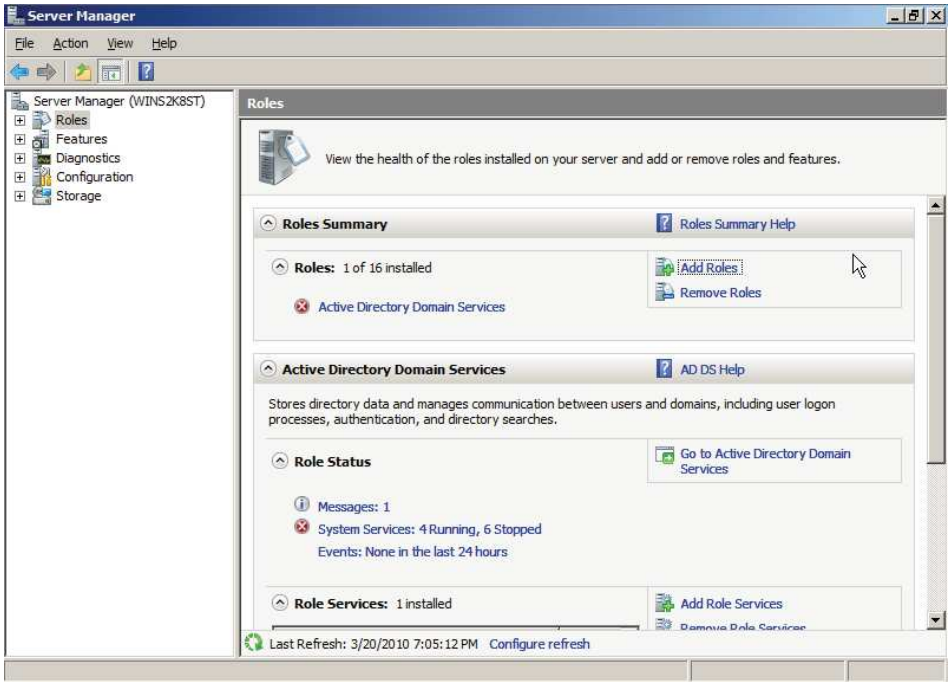
Ilustración 3-26 Resumen del proceso de instalación y estatus de los mismos



Elaborado por: Autor

20. Para confirmar el éxito del paso anterior, dentro del Server Manager, se puede observar que aparece Instalado el rol "*Active Directory Domain Services*", pero aparece deshabilitado con una cruz roja previo a su descripción.

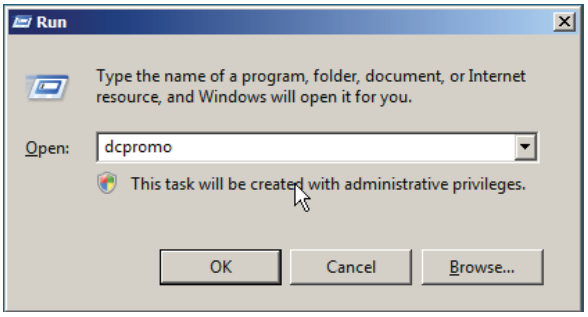
Ilustración 3-27 Interfaz que muestra la presencia del rol de AD en el servidor



Elaborado por: Autor

21. La manera de activar el rol del *Active Directory*, que es la implementación del protocolo LDAP a cargo de la gestión del catálogo de objetos de la red (concepto desarrollado en el capítulo 2.3), es mediante la ejecución del comando *dcpromo*. Para ello debemos ir al menú *Start*, *Run,* en la línea de comandos escribir ***dcpromo.exe*** y dar clic sobre el botón OK.

Ilustración 3-28 Activación del servicio del AD mediante el comando dcpromo.exe



Elaborado por: Autor

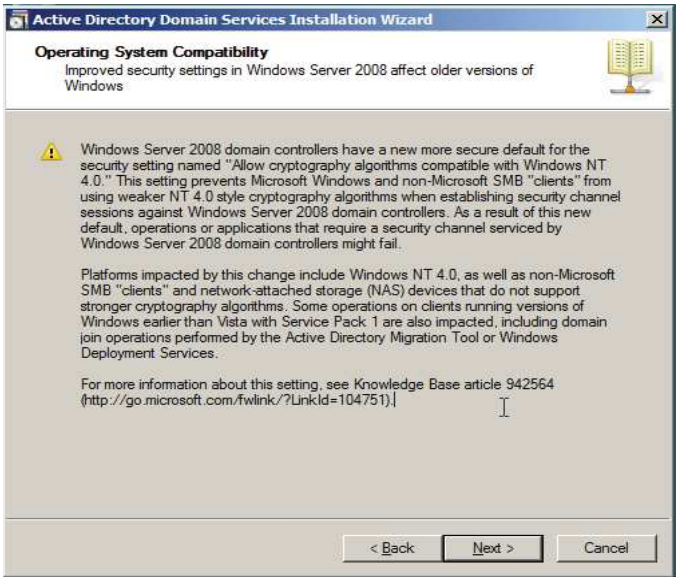
22. Se muestra una ventana que pertenece al asistente de configuración del proceso de activación del servicio, luego de leer su contenido, dar clic en ***Next***.

Ilustración 3-29 Asistente de configuración para activación del servicio del AD

Elaborado por: Autor

23. Se muestra la compatibilidad que el servicio del Active Directory en la versión de Windows 2008 Server presenta versus sus predecesoras, luego de familiarizarse con las mismas, dar Clic en ***Next***.

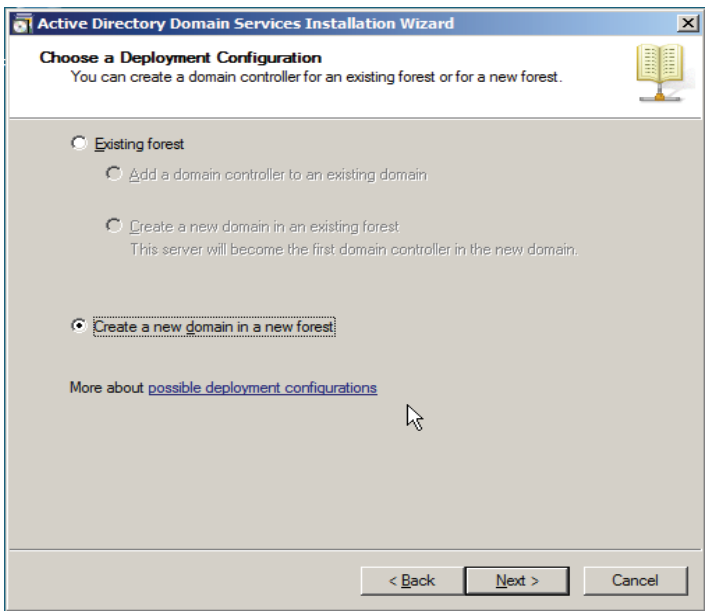
Ilustración 3-30 Declaración de compatibilidad de la versión del servicio del AD en Windows 2008



Elaborado por: Autor

24. Al ser el primer servidor del dominio a crear se debe seleccionar la opción "*Create a new domain in a new forest"* al ser el primer dominio en el nuevo bosque. Dar clic sobre el botón ***Next***.

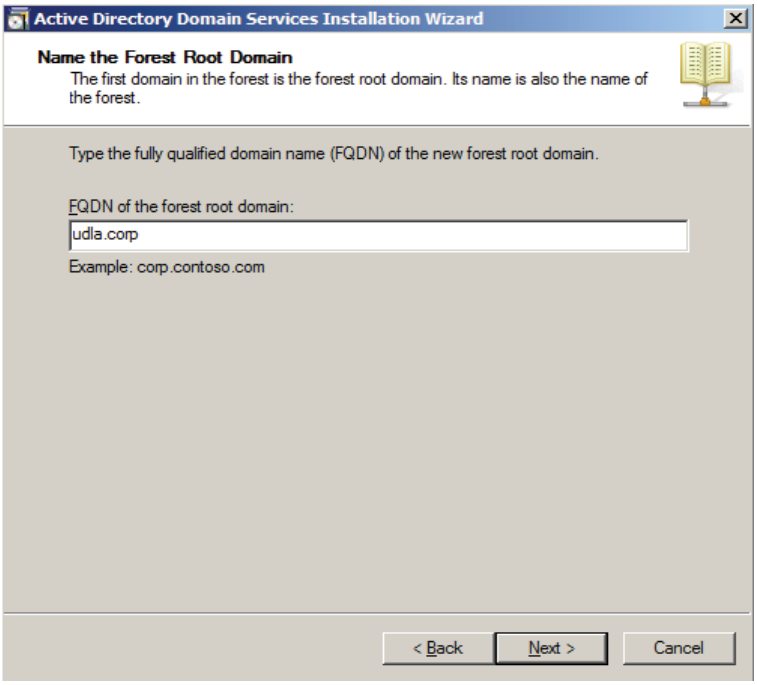
Ilustración 3-31 Interfaz para la creación de un nuevo dominio



Elaborado por: Autor

25. A continuación se muestra una ventana que permite ingresar el nombre que identifica al dominio creado, en este: *udla.corp*. clic en ***Next***.

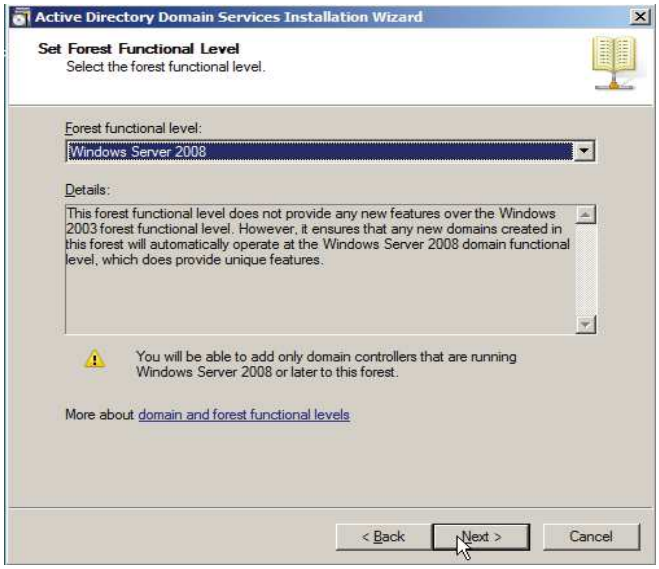
Ilustración 3-32 Ventana que permite el ingreso del dominio a crear



Elaborado por: Autor

26. Una característica a tomar en cuenta en el proceso de configuración es la compatibilidad de la versión a instalar con otros servidores que serán parte del dominio. Para este caso en particular seleccionar el Nivel Funcional de Bosque: *Windows Server 2008*, ya que será el único que lo conforma -varía la opción acorde al entorno-, luego de su selección se debe dar Clic en el botón ***Next***.

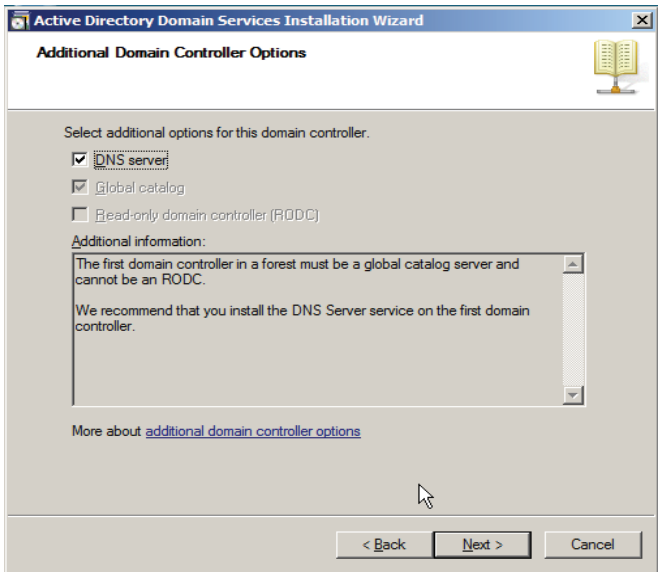
Ilustración 3-33 Selección del nivel funcional del bosque



Elaborado por: Autor

27. Tomando en cuenta una de las recomendaciones que se muestran en el paso 17, proceder a seleccionar la opción de *DNS Server*, como rol adicional del controlador de dominio y continuar luego de dar clic en el botón ***Next***.

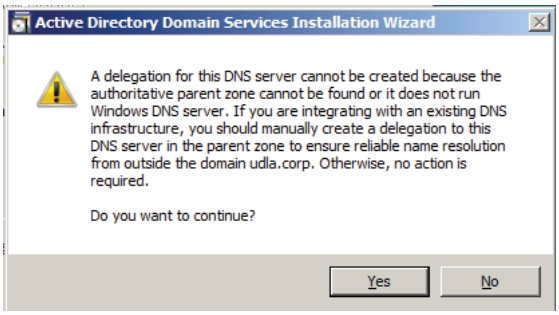
Ilustración 3-34 Selección de la opción de servidor DNS como rol adicional



Elaborado por: Autor

28. Se muestra una ventana que alerta sobre la inexistencia de una zona de DNS, no es necesaria acción alguna al no ser el caso porque la estamos creando, para continuar el proceso se debe dar clic sobre ***Yes***.

Ilustración 3-35 Ventana que alerta sobre la instalación del servicio DNS y sus consideraciones

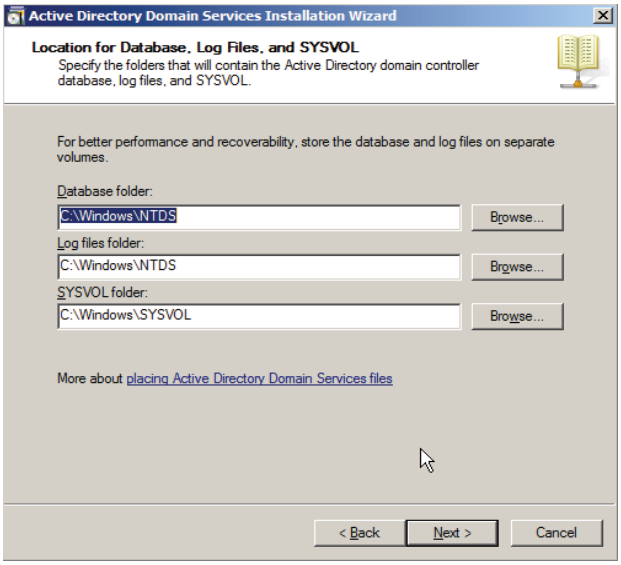


Elaborado por: Autor

29. En la ventana siguiente especificar la ubicación donde residirán los archivos componentes del Active Directory como son: la base de datos, los archivos de registro (log) y el Sysvol[32]. Al ser el único servidor del dominio utilizaremos las carpetas que aparecen por defecto. Clic en ***Next.***

[32] Acrónimo utilizado por Microsoft que proviene del termino ***System Volume*** (Sysvol) y se refiere a un conjunto de archivos y carpetas que residen en el disco duro local de cada servidor y será replicado entre los controladores de domino.

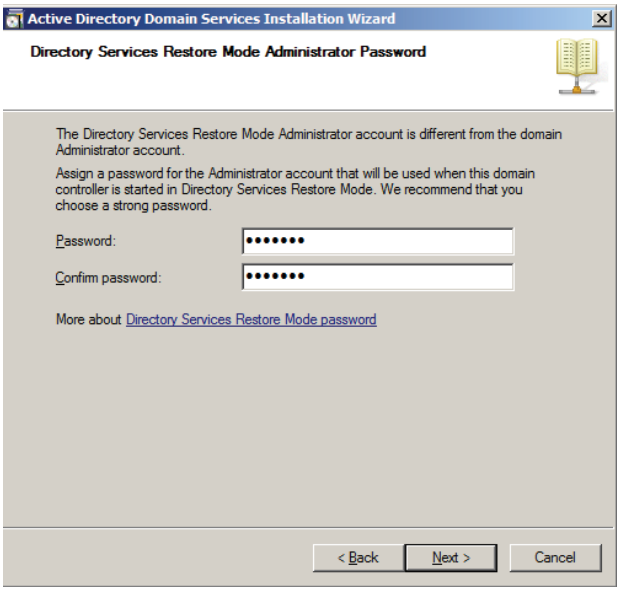
Ilustración 3-36 Definición de la ubicación de carpetas del sistema del AD



Elaborado por: Autor

30. Ingresar una contraseña de administrador para los servicios de directorio. Esta es una contraseña alterna a la del usuario "*administrator*" de Windows y útil para procesos de recuperación.

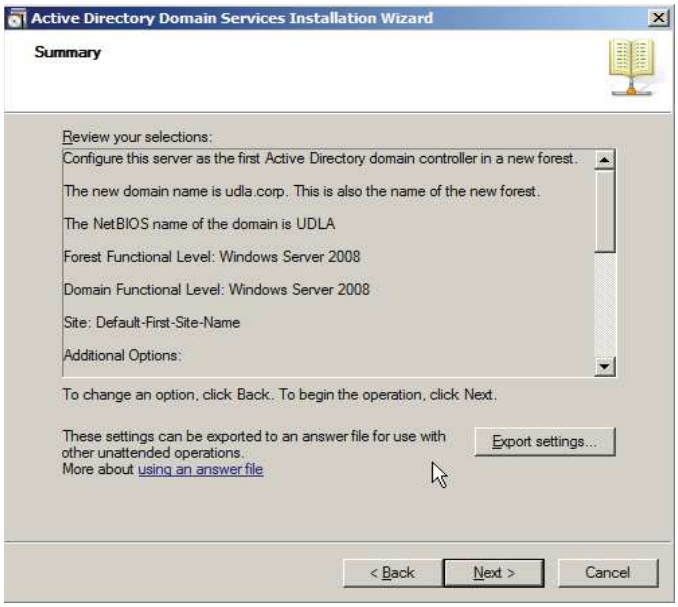
Ilustración 3-37 Definición de una clave para restauración del AD



Elaborado por: Autor

31. Se presenta la ventana *Sumary* donde se puede observar un resumen del proceso a ejecutar y los componentes a instalar. Clic en ***Next***.

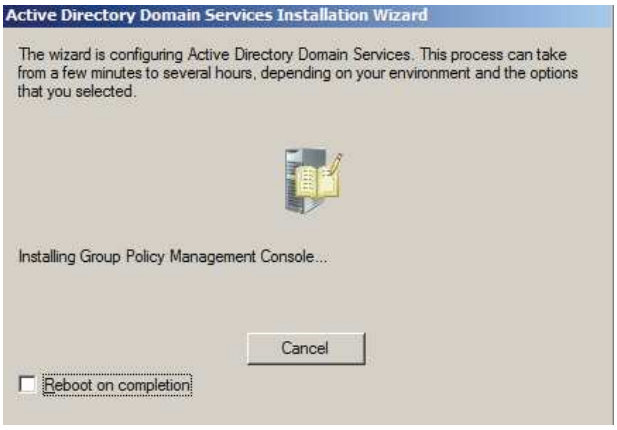
Ilustración 3-38 Resumen sobre los parámetros definidos para la instalación del AD



Elaborado por: Autor

32. Como parte del proceso de instalación se recomienda reiniciar el sistema, por ello se debe seleccionar la opción "*Reboot on completition*", luego dar clic en ***Next***.

Ilustración 3-39 Instrucción de reiniciar el sistema al término del proceso de instalación del AD



Elaborado por: Autor

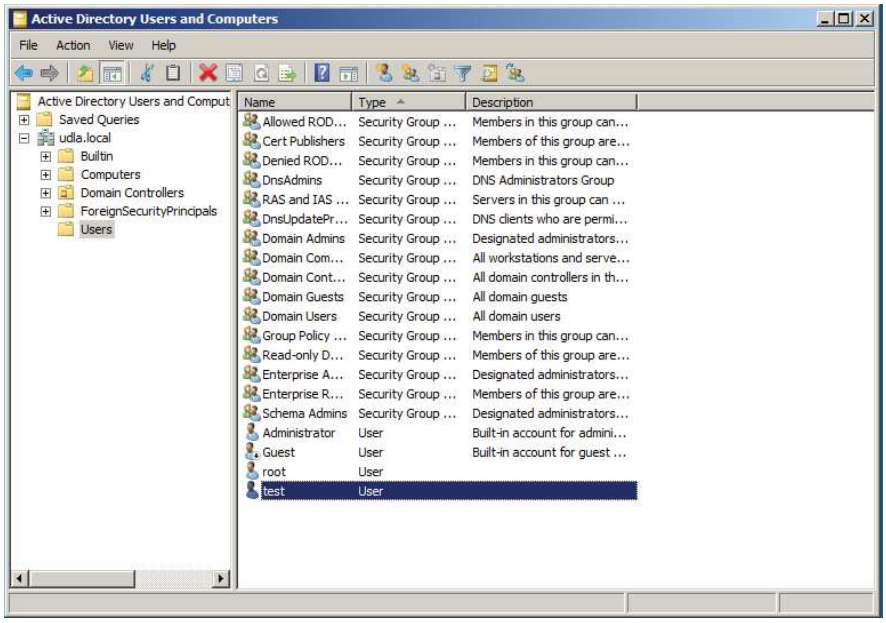
33. Una vez concluida la instalación, para que se ejecute el proceso de reiniciación del sistema, se debe dar clic en ***Finish***.

Ilustración 3-40 Interfaz que muestra el término del proceso de instalación del AD

Elaborado por: Autor

34. Una vez reiniciado el equipo el servicio del *Active Directory* se muestra como disponible en el servidor virtual.
35. La primera tarea en ejecutar es la creación de los usuarios que tendrán acceso a la red vía inalámbrica. La creación de estos objetos en el catálogo permite la consecución del objetivo planteado en la sección "1.3" que propone la necesidad de delegar estas tareas al protocolo LDAP. Para ello mediante la interfaz gráfica del Directorio Activo, nos ubicamos bajo el contenedor de "*Users*¨ y en el menú "*Action*" seleccionamos añadir nuevo usuario, luego de completar el asistente con las parámetros básicos que lo identifiquen (*Test user*), éste se muestra como parte del catálogo de usuarios de nuestro dominio (*udla.local)*. Tal como se aprecia en la imagen siguiente.

Ilustración 3-41 Catálogo de usuarios del domino *udla.local* gestionado por el AD



Elaborado por: Autor

3.4.2 Configuración del servidor Centos 5 y el servicio SAMBA

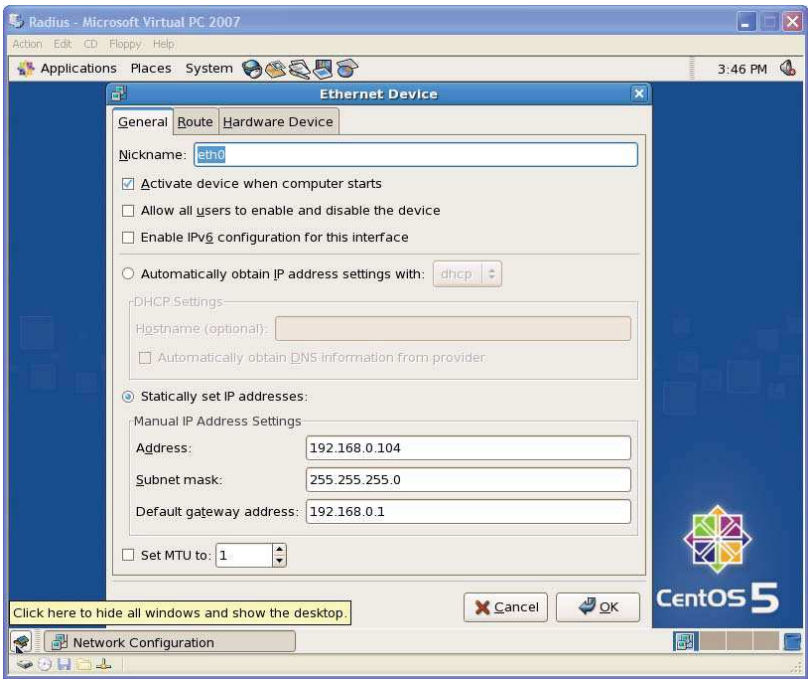
Mediante la ejecución del procedimiento que a continuación de detalla, se logra el cumplimento de los siguientes objetivos específicos:

- El contar con un elemento virtualizado como es el servidor RADIUS conforme el objetivo específico planteado en al Capítulo I.
- Configurar elementos lógicos cuyo encadenamiento permite la interacción entre el servidor Windows 2008 y Centos 5.
- Introducir en el entorno de conectividad actores necesarios en la aplicación de un modelo AAA y el estándar IEEE 802.X, de acuerdo a lo explicado en el Capítulo II en la sección correspondiente a cada tema, y brinde un ambiente seguro a los clientes móviles.

Se procede a configurar una imagen ya existente con el sistema operativo Centos 5 en el idioma inglés instalado en una máquina virtual y se detallan los pasos tendientes a afinar su configuración al entorno requerido:

1. Asignar la dirección IP correspondiente a la red, mediante la interfaz gráfica, luego de elegir del menú la opción “System/ Administration/ Network”.

Ilustración 3-42 Ajuste de la dirección IP en el servidor Centos

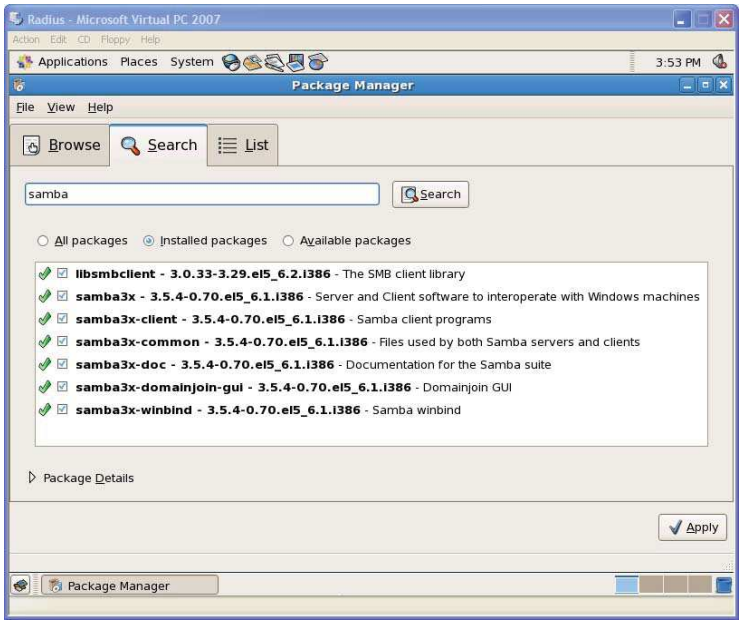


Elaborado por: Autor

2. Es necesario instalar el servicio Samba[33] para permitir la comunicación con el servidor Windows. La versión más actual de este servicio corresponde a SAMBA 3X, para su instalación, en el menú principal de la interfaz inicial navegar en el menú hasta “*Aplications / Add&Remove Software*”. Seleccionar todos los componentes que forman parte de esta versión, debido a que cada uno es complementariamente necesario, tal como se muestran en la figura. Luego dar clic sobre ***Apply***.

[33] Samba es un conjunto de programas diseñados para correr en entornos Linux y Unix que permiten la inter-operatividad con sistemas Windows.

Ilustración 3-43 Componentes de SAMBA 3X para inter-operatividad con Windows



Elaborado por: Autor

3. Una vez instalado el servicio de Samba proceder a editar el archivo **smb.cof** y modificar la sección `[global]` para direccionarla hasta el servidor de Windows 2008, allí incluir el nombre del host así como el dominio acorde las siguientes imágenes.

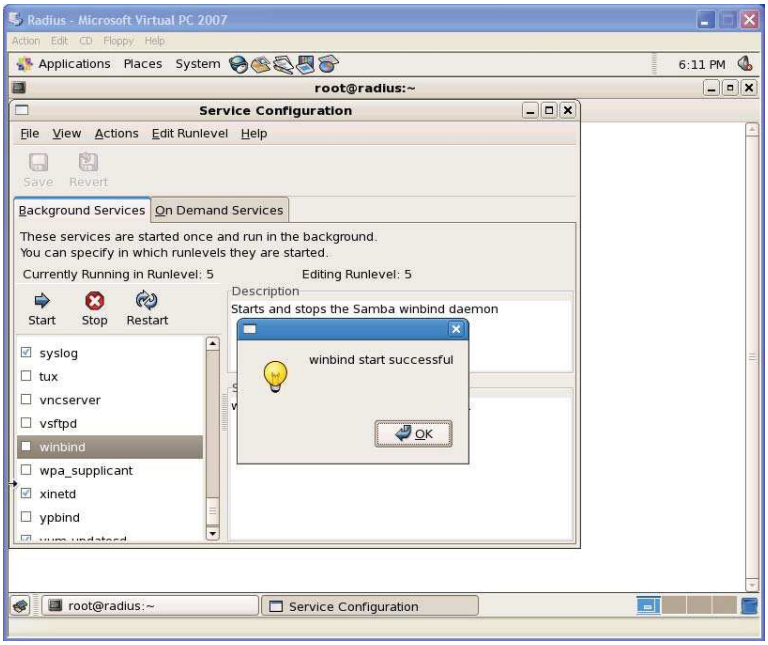
Ilustración 3-44 Parámetros de configuración de SAMBA mediante el archivo *smb.cof*


```
# Hosts Allow/Hosts Deny lets you restrict who can connect, and you can
# specifiy it as a per share option as well
#
        workgroup = UDLA
        server string = Samba Server Version %v

;       netbios name = MYSERVER

        security = ads
;       passdb backend = tdbsam
        realm = UDLA.LOCAL

;       password server = <NT-Server-Name>
```

Elaborado por: Autor

4. Es necesario arrancar el servicio SAMBA y tomen efecto los parámetros definidos en el paso anterior, para ello ir en el menú hasta "*System / Administration/ ServerSettings/ Services*" y luego sobre el servicio "winbind" dar clic en el botón ***Start.***

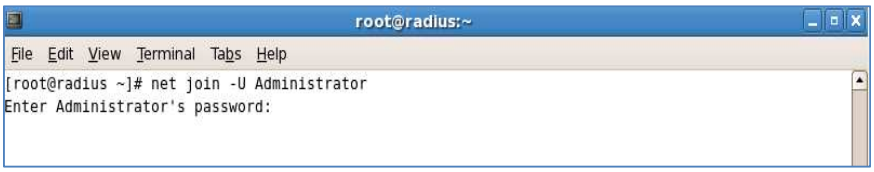
Ilustración 3-45 Iniciación del servicio SAMBA en el servidor Centos



Elaborado por: Autor

5. Proceder a unir el servidor Centos al dominio UDLA definido en el servidor Windows 2008, para ello con el perfil de root abrir una sesión del terminal e invocar el comando `netjoin -U Administrator` y luego suministrar la clave del servidor Windows.

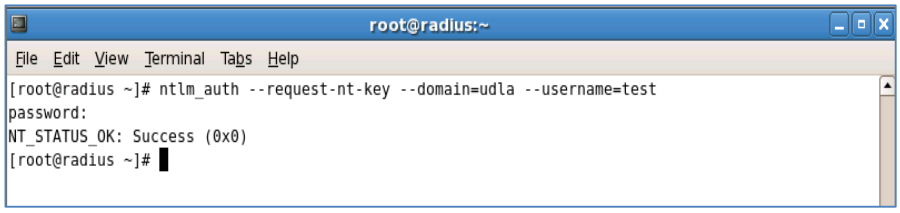
Ilustración 3-46 Ejecución de comando net join que permite unión con el servidor Windows



Elaborado por: Autor

6. Se valida la autenticación del usuario test@udla creado en Windows bajo el entorno de Centos, mediante una sesión del terminal ejecutar el comando `ntlm_auth –request-nt-key –domain=udla –username=test`. La salida exitosa, que muestra la ejecución de este comando, nos permite demostrar la integración conseguida entre el servidor LDAP bajo un entorno Windows -donde se creo el objeto usuario- y el servidor Centos que hospedará al protocolo RADIUS. Es precisamente esta integración la evidencia que demuestra la consecución del tercer objetivo general planteado en el Capítulo I.

Ilustración 3-47 Validación del usuario Windows en un entorno Linux mediante comando ntlm_auth



Elaborado por: Autor

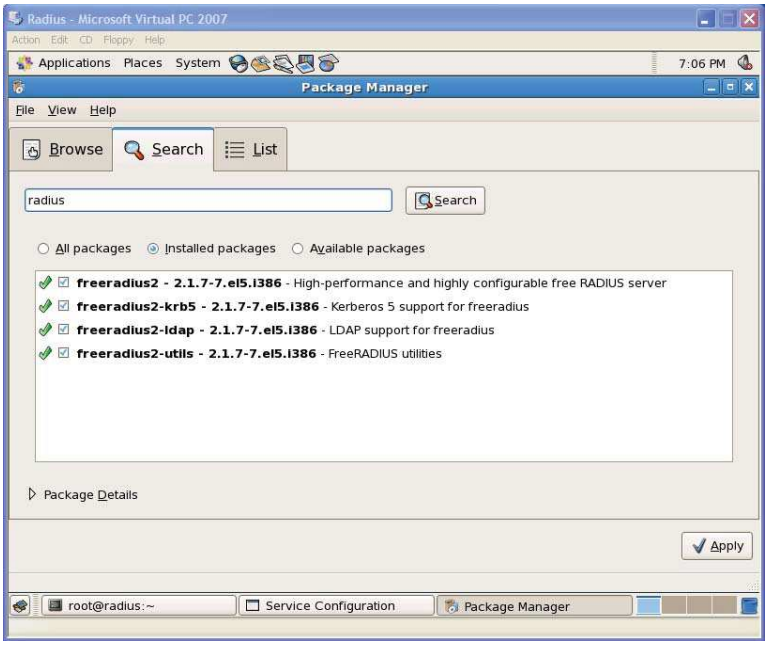
3.4.3 Instalación de FreeRADIUS y configuración del servicio

1. Para la instalación de RADIUS sobre el sistema operativo CentosOS-5 utilizaremos el paquete FreeRadius2 versión 2.1.7 *release* 7.e15[34]. Para lograr ese cometido en la interfaz gráfica de Centos, elegir del menú la opción "*Aplications/Add&Remove Software*", hacer una búsqueda para el servicio "radius" y marcar los siguientes componentes:
    a. Freeradius2: Que contiene el protoclo RADIUS como tal.
    b. Freeradius-krb5: Servicio que permiten la interconexión con Windows.
    c. Freeradius-ldap: Aplicación que permite la integración con LDAP.
    d. Freeradius-utlis: Utilitarios adicionales de la suite

[34] FreeRadius2-2.1.7-7.e15.i386 es una suite de programas que permiten disponer de un servidor RADIUS de alto rendimiento y sumamente configurable compatible con CentosOS-5 y liberado por el Proyecto FreeRADIUS Server (http://freeradius.org) bajo un licenciamiento tipo GPL.

Tal como se muestran en la Ilustración 3-49 y luego dar clic sobre el botón ***Apply***.

Ilustración 3-48 Instalación del paquete freeradius2 - 2.1.7-7.e15.i386 para Centos OS-5



Elaborado por: Autor

2. Configurar el servicio de Radius para que permita la autenticación de usuarios mediante el comando `ntlm_auth` definido en la sección previa. Crear mediante la consola el archivo `etc/raddb/modules/ntlm_auth` y editar su contenido según la imagen abajo detallada.

Ilustración 3-49 Edición del archivo ntlm_auth **para autenticación a través de Radius**

```
exec ntlm_auth{
        wait = yes
        program = "/usr/bin/ntlm_auth --request-nt-key --domain=udla --username=%{mschap:User-Nam
e} --password=%{User-Password}"
}
```

Elaborado por: Autor

3. Tal como se explicó en el Capítulo II el modelo AAA se basa en procesos de Autenticación, Autorización y Contabilidad. Acorde al diseño propuesto las tareas de autenticación corren por cuenta del servidor

LDAP y para lograr este cometido, que los usuarios se validen contra la base de definida en el AD, se requiere parametrizar ciertos valores en el servidor FreeRADIUS que corre sobre Centos. Para esto mediante un editor de texto se debe incluir el comando `ntlm_auth` en las secciones definidas como `authenticate` de los archivos `etc/raddb/sites-enabled/default` y `etc/raddb/sites-enabled/inner-tunel`. Al término de este proceso habremos cumplido con el objetivo de integrar la capacidades del LDAP y RADIUS bajo un modelo AAA tal como fue planteado en la sección "1.3".

Ilustración 3-50 Definición del método de autenticación vía comando ntlm_auth

```
authenticate {
        #
        #  PAP authentication, when a back-end database listed
        #  in the 'authorize' section supplies a password.  The
        #  password can be clear-text, or encrypted.
        ntlm_auth
        Auth-Type PAP {
                pap
        }

        #
        #  Most people want CHAP authentication
        #  A back-end database listed in the 'authorize' section
        #  MUST supply a CLEAR TEXT password.  Encrypted passwords
        #  won't work.
        Auth-Type CHAP {
                chap
        }
```

Elaborado por: Autor

4. Iniciar el servicio Radius en modo debug[35] mediante el comando `radiusd -X`, al final de la ejecución se debe mostrar la línea "`Ready to process request.`" y es la señal de que el servicio se ha iniciado correctamente con los parámetros hasta ahora definidos.

Ilustración 3-51 Visualización del modo debug para el servicio Radius

```
Listening on authentication address 192.168.0.104 port 1812
Listening on accounting address 192.168.0.104 port 1813
Listening on command file /var/run/radiusd/radiusd.sock
Listening on proxy address 192.168.0.104 port 1814
Ready to process requests.
```

Elaborado por: Autor

[35] Modo debug es un termino utilizado en el ambiente de programación que habilita la visualización de los mensajes que genera un sistema, servicio o aplicación y permite su depuración.

5. Proceder a realizar una prueba de validación del usuario test@udla con clave “myp@ssw0rd” mediante el servicio Radius. Abrir una nueva consola del terminal y ejecutar el siguiente comando: `radtest test myp@ssw0rd 192.168.0.104 0 testing123`, siendo la salida esperada de este comando la siguiente:

Ilustración 3-52 Solicitud de autenticación de un usuario del AD desde el servidor Radius

```
[root@radius ~]# radtest test myp@ssw0rd 192.168.0.104 0 testing123
Sending Access-Request of id 254 to 192.168.0.104 port 1812
        User-Name = "test"
        User-Password = "myp@ssw0rd"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 0
rad_recv: Access-Accept packet from host 192.168.0.104 port 1812, id=254, length
=20
[root@radius ~]#
```

Elaborado por: Autor

6. Si el paso anterior es exitoso entonces solo resta configurar FreeRADIUS para que acepte MS-CHAP [36] mediante el comando `ntlm_auth`. Editar el archivo `etc/raddb/modules/mschap` y en la sección correspondiente a `mschap` incluir una entrada como abajo se detalla.

Ilustración 3-53 Prueba de validación de un usuario del AD mediante el servicio Radius

```
ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --username=%{mschap:User-Name:-
None} --domain=%{%{mschap:NT-Domain}:-UDLA} --challenge=%{mschap:Challenge:-00}
--nt-response=%{mschap:NT-Response:-00}"
}
```

Elaborado por: Autor

3.4.4 Configuración del cliente EAP

Los objetivos a ser cubiertos, al término de este proceso son:

[36] Acrónimo que viene del inglés Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) y corresponde a un protocolo de autenticación de contraseñas mediante cifrado por desafío mutuo, propio del fabricante Microsoft.

- Configuración del elemento físico, identificado en el diseño, como es el Punto de Acceso bajo un esquema que permita gestionar transacciones AAA.
- Brindar a los clientes que utilizan dispositivos móviles un ambiente WLAN seguro.

Para la consecución de los objetivos arriba planteados se deben seguir las siguientes acciones:

1. Ingresar las características que identifican al equipo Cisco Aironet 1200 como cliente del servidor FreeRADIUS. Para ello editar en el servidor el archivo `etc/raddb/clients.conf` y al final del mismo se incluye el siguiente registro:

Ilustración 3-54 Definición de parámetros del AP en el servidor RADIUS

```
client 192.168.0.10{
        secret  =       keye@p
        ipaddr  =       192.168.0.10
        shortname       =       192.168.0.10
        nastype =       cisco
}
```

Elaborado por: Autor

   El contenido del campo `secret` es una clave a ser compartida entre el servidor FreeRADIUS y el Access Point, el `ipaddr` corresponde a la dirección IP y el `nastype` especifica la marca del fabricante del equipo.

2. Especificar en el servidor FreeRADIUS el método de autenticación a ser usado, para este caso seleccionar PEAP ya que el mismo permite el manejo de MSCHAPv2, que es el protocolo de autenticación utilizado por el Directorio Activo de Windows. Proceder a editar el archivo `etc/raddb/clients.conf` para aplicar los siguientes cambios:
   a. Reemplazar la línea "`default_eap_type = md5`" por "`default_eap_type = peap`".

Ilustración 3-55 Definición del método de autenticación entre el AP y Radius

```
#  If the EAP-Type attribute is set by another module,
#  then that EAP type takes precedence over the
#  default type configured here.
#
default_eap_type = peap
```

Elaborado por: Autor

b. Ubicar la sección `peap` y proceder a eliminar los comentarios a excepción de línea donde se identifica a MSCHAP como el tipo por defecto.

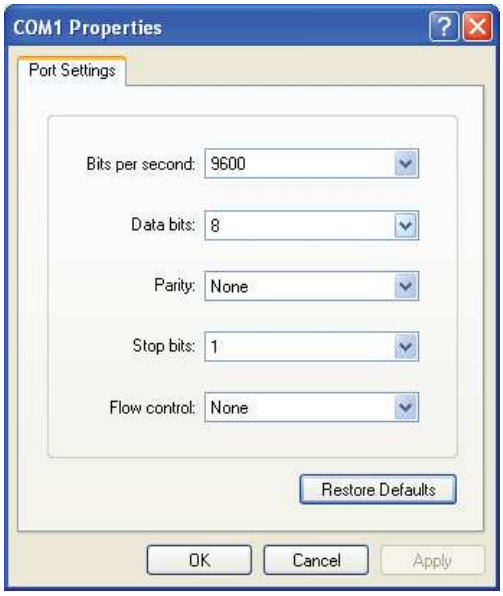
Ilustración 3-56 Definición del protocolo MSCHAP para manejo de clientes Windows

```
peap {
        #  The tunneled EAP session needs a default
        #  EAP type which is separate from the one for
        #  the non-tunneled EAP module.  Inside of the
        #  PEAP tunnel, we recommend using MS-CHAPv2,
        #  as that is the default type supported by
        #  Windows clients.
        default_eap_type = mschapv2
```

Elaborado por: Autor

3. Mediante la interface de línea de comandos, proceder a configurar el dispositivo Cisco Aironet 1200 que cuenta con el IOS 12.3.7(JA5) y las claves de acceso por defecto configuradas.
    a. Conectar el puerto serial de la computadora a la consola del equipo.
    b. Iniciar una sesión de “Hyperterminal” en Windows y configurar los parámetros de conexión del puerto serial como a continuación se detalla.

Ilustración 3-57 Propiedades de Hyperterminal para conexión con el AP



Elaborado por: Autor

c. Ingresar parámetros básicos como son el nombre del equipo "wrap[37]" y fecha.

Ilustración 3-58 Parámetros iniciales del AP

```
AP>enable
Password:
AP#clock set 21:11:25 1 June 2011
AP#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)#hostname wrap
wrap(config)#exit
wrap#_
```

Elaborado por: Autor

d. Asignar a la interface Ethernet 0 la dirección IP: 192.168.0.10 y el Gateway como IP: 192.168.0.1

[37] Acrónimo que proviene del inglés Wireless Router Access Point (WRAP)

Ilustración 3-59 Ingreso de parámetros de dirección IP en el AP

```
wrap#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
wrap(config)#interface fas
wrap(config)#interface fastEthernet 0
wrap(config-if)#ip add
wrap(config-if)#ip address 192.168.0.10 255.255.255.0
wrap(config-if)#no shutdown
wrap(config-if)#end
wrap#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
wrap(config)#ip default-gateway 192.168.0.1
```

Elaborado por: Autor

e. Definir la dirección del servidor de autenticación AAA para la comunicación EAP entre los dos equipos e ingresar la clave compartida a utilizar entre el AP y el FreeRADIUS definida en el primer punto del paso (3).

Ilustración 3-60 Definición de la dirección IP del servidor Radius en el AP

```
wrap#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
wrap(config)#aaa group server radius rad_eap
wrap(config-sg-radius)#server 192.168.0.104 auth-port 1812 acct-port 1813
wrap(config-sg-radius)#exit
wrap(config)#aaa new-model
wrap(config)#aaa authentication login eap_methods group rad_eap
wrap(config)#$er host 192.168.0.104 auth-port 1812 acct-port 1813 key keye@p
wrap(config)#end
wrap#_
```

Elaborado por: Autor

f. Ahora proceder a habilitar el método de encripción para la comunicación inalámbrica, para este ejemplo utilizar WEP.

Ilustración 3-61 Habilitación del método WEP para encripción en el AP

```
wrap#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
wrap(config)#interface dot11radio 0
wrap(config-if)#encryption mode wep mandatory
wrap(config-if)#end
wrap#
```

Elaborado por: Autor

g. Crear la identificación de la red inalámbrica “radius-X” y asignar a la misma los métodos de autenticación previamente definidos.

Ilustración 3-62 Creación de la red inalámbrica "radius-X" en el AP

```
wrap#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
wrap(config)#interface dot11radio 0
wrap(config-if)#ssid radius-X
wrap(config-if-ssid)#authentication open eap eap_methods
wrap(config-if-ssid)#authentication network-eap eap_methods
wrap(config-if-ssid)#end
wrap#
```

Elaborado por: Autor

h. Finalmente guardar la configuración mediante el comando "`wrap#copy running-config startup-config`". Revisar la configuración del Access Point con el comando "`wrap#show running-config`" y su salida debe ser similar a la siguiente:

Ilustración 3-63 Salida de los parámetros de configuración ingresados en los pasos anteriores en el AP

```
Building configuration...

Current configuration : 1981 bytes
!
! Last configuration change at 23:17:35 UTC Wed Jun 1 2011
! NVRAM config last updated at 12:37:47 UTC Sat May 28 2011
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname wrap
!
no logging console
enable secret 5 $1$Kxth$NAc1Ca9N8eR.KTYE1S5Do0
!
ip subnet-zero
!
!
aaa new-model
!
!
aaa group server radius rad_eap
server 192.168.0.104 auth-port 1812 acct-port 1813
!
aaa authentication login eap_methods group rad_eap
aaa session-id common
!
dot11 ssid radius-X
   authentication open eap eap_methods
   authentication network-eap eap_methods
!
!
!
```

```
username Cisco password 7 123A0C041104
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode wep mandatory
 !
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0
36.0 48.0 54.0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 ip address 192.168.0.10 255.255.255.0
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 192.168.0.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.0.1
ip http server
no ip http secure-server
ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface FastEthernet0
!
radius-server host 192.168.0.104 auth-port 1812 acct-port 1813 key 7
020D01420E261F
radius-server key 7 06100E2D5F4F0C0B0304
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
 transport preferred all
 transport output all
line vty 0 4
 transport preferred all
 transport input all
 transport output all
line vty 5 15
 transport preferred all
 transport input all
 transport output all
!
end
```

Elaborado por: Autor

3.4.5 Configuración del suplicante y prueba de conexión

Para la prueba de conexión de un cliente móvil, que requiere acceso hasta la red inalámbrica que en el paso anterior se denominó “radius-X”, se utiliza una laptop con sistema operativo Windows XP que cuenta con la aplicación Intel(R) PROSet/Wireless WiFi Software 13.2.1.0 encargado de gestionar las conexiones del adaptador Intel mediante la creación de perfiles.

1. En la sesión de Windows ir hasta “*Start/All Programs/Intel PROSet Wireless*” y hacer clic sobre “WiFi *Connection Utility*” para abrir la aplicación.
2. Para crear el perfil “radius-X” dar clic en el botón “*Profiles*…”

Ilustración 3-64 Interfaz de la aplicación “Intel PROSet/Wireless” para gestión de redes inalámbricas

Elaborado por: Autor

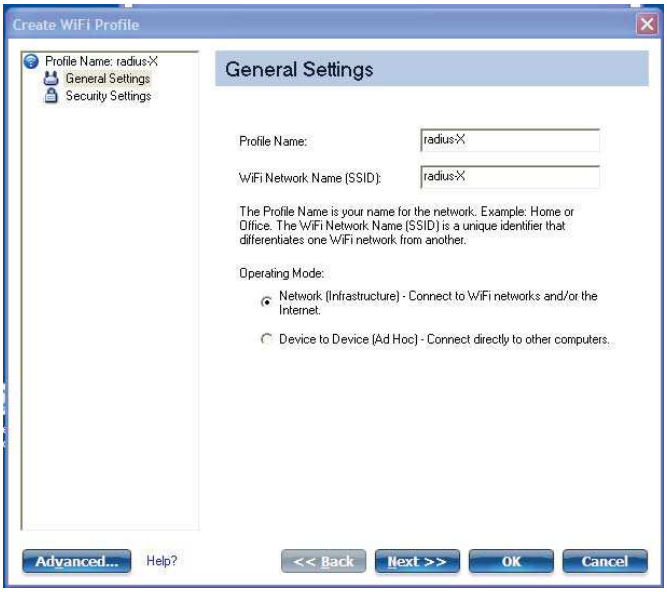
3. Clic sobre el botón “*Add*…”

Ilustración 3-65 Creación de un perfil personalizado para una red inalámbrica

Elaborado por: Autor

4. Ingresar el nombre del perfil y el SSID, para los dos casos es “radius-X” y seleccionar bajo la sección de “Operating Mode” la opción de “Network (Infraestructure) – Connect to WiFi networks and/or the Internet”.

Ilustración 3-66 Definición del nombre del perfil e identificador de la red inalámbrica



Elaborado por: Autor

5. Seleccionar ***Enterprise Security***.
6. Seleccionar **WEP** en el campo asociado a ***Data Encryption***.
7. Elegir **PEAP** en el campo asociado a ***Authentication Type*** luego de marcar ***Enable* 802.1X**.
8. En ***Authentication Protocol*** seleccionar **MS-CHAP-V2**.
9. En el campo ***User Credentials*** ubicar ***Use the following***.
10. Para el campo ***User Name*** ingresar ***test***.
11. Para el campo ***Domain*** ingresar **udla**.
12. En los campos asociados al *password* digitar la clave del usuario: test@udla, seguido de clic sobre ***Next***.

Ilustración 3-67 Interfaz para definición de parámetros de seguridad de la red inalámbrica en el lado del cliente

Elaborado por: Autor

13. Para este ambiente de pruebas se ha deshabilitado en el servidor de FreeRADIUS la utilización de Certificados de Autoridad (CA) por lo que es necesario no seleccionar la opción ***Validate Server Certificate*** y luego clic sobre ***OK***.

Ilustración 3-68 Interfaz para definición de parámetros de seguridad de la red inalámbrica en el lado del servidor

Elaborado por: Autor

14. Ahora que el perfil está disponible seleccionarlo y dar clic en el botón de ***Connect***.

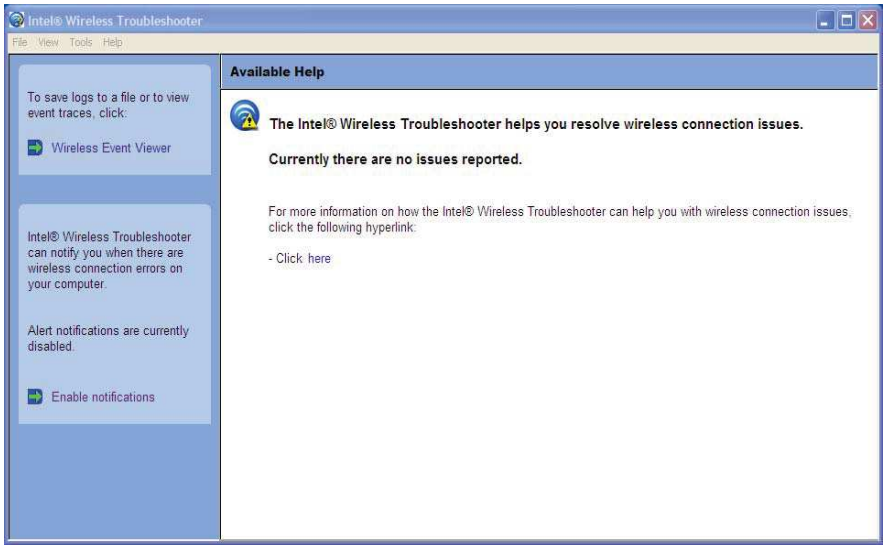
Ilustración 3-69 Interfaz que permite la selección de perfiles de redes inalámbricas y su conexión

Elaborado por: Autor

Al término de este proceso si el usuario test@udla existe en el Directorio Activo del servidor Windows 2008 y el *password* ingresado es válido entonces, el Access Point habrá provisionado el servicio de conexión al cliente de Windows XP.

15. Para revisar los pasos seguidos en el proceso de autenticación ejecutados desde el cliente seleccionar del menú la opción: "**Tools/Intel Wireless Troubleshooter…"**
16. En el panel izquierdo dar clic sobre ***Wireless Event Viewer*.**

Ilustración 3-70 Interfaz que permite hacer seguimiento de eventos

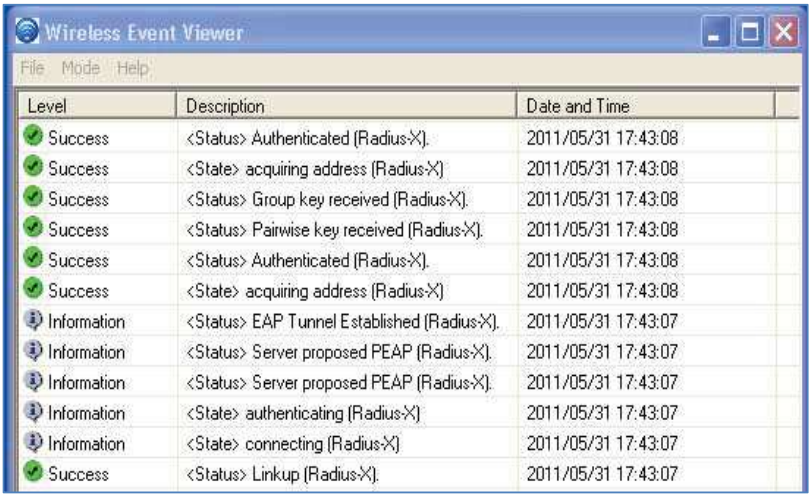


Elaborado por: Autor

17. El registro detallado o Contabilidad de la secuencia de los eventos registrados en el proceso de Autenticación y Autorización que se muestra en la Ilustración 3-72 correspondiente al exitoso proceso iniciado por el usuario definido en el servidor LDAP para obtener acceso hasta la red inalámbrica y se constituye en la evidencia que denota la interoperabilidad que se llevo a cabo entre todos los elementos del diseño y permitieron gestionar transacciones del tipo AAA en un ambiente seguro. Y precisamente la armónica interacción que se ha logrado entre estos componentes permiten afirmar que tanto los

objetivos generales así como aquellos específicos, motivo de este trabajo de titulación, han sido alcanzados completamente.

Ilustración 3-71 Visualización de los eventos de una conexión exitosa utilizando Radius



Elaborado por: Autor

4. Capítulo IV: Conclusiones y recomendaciones

4.1 Conclusiones

- Disponer de una red que gestione transacciones del tipo AAA es muy viable ya que el protocolo RADIUS por su vigencia y amplia difusión es compatible con la mayoría de equipos que son de habitual uso en entornos empresariales, sean estos: terminales, clientes y/o servidores de los más variados fabricantes.

- El mayor desafío para lograr el engranaje del servidor de AAA en un entorno ya existente, se centra en la elección adecuada de los parámetros de configuración del servidor FreeRADIUS, que debe responder a las características de los elementos relevantes del entorno correctas como es el servidor que maneja la autenticación así como de cada AP que conforma la arquitectura de la solución.

- Al ser FreeRADIUS una aplicación del tipo código abierto al igual que el sistema operativo donde reside, hace que su costo sea significativamente reducido en cuanto a temas de licenciamiento y derechos de propiedad.

- Las tareas de administración de usuarios que acceden al servicio de red inalámbrico se facilitan al concentrar su gestión en herramientas existentes como es el Directorio Activo de Windows 2008, sin sacrificar la seguridad ya que la misma está garantizada por los protocolos y servicios que corren entre los equipos que forman parte de infraestructura sugerida.

- La solución presentada cumple con la condición de simplificar al usuario final la tarea de autenticación ya que utiliza las mismas credenciales tanto para acceder al servicio inalámbrico así como a servicios de la red,

mientras que de forma transparente se ejecutan procesos de validación de su identidad.

- La implementación de una política adecuada en el Directorio Activo del servidor Windows 2008 que refuerce la complejidad y longitud de las claves, la limitación en cuanto a conexiones concurrentes y la concientización a los usuarios del manejo adecuado de claves son medidas preventivas que permiten minimizar la presencia de conexiones no deseadas.

4.2 Recomendaciones

- Habilitar los modos de depuración tanto en los clientes como el servidor ya que son herramientas poderosas para poder seguir el rastro de un inconveniente al momento de realizar la configuración.

- Prestar mucha atención y cuidado al momento de modificar los parámetros en los archivos de configuración ya que los mismos son del tipo texto que no permite una validación previa de su contenido.

- Una medida preventiva que pretende garantizar una alta disponibilidad de la red inalámbrica para los usuarios finales es la planificación de esquemas de redundancia tanto para los servidores AAA como los de gestión de LDAP, manteniéndolos en un entorno que brinde seguridades físicas adecuadas y así como continuidad del servicio.

- La creación de VLANS dedicadas, una para el segmento de Intranet cuya autenticación sea gestionada por el servidor AAA y otra para usuarios que solo tengan salida hasta el Internet con limitados recursos del canal de comunicación, es una alternativa viable para aquellos usuarios cuyos dispositivos móviles no dispongan de clientes capaces

de gestionar conexiones mediante el protocolo de autenticación PEAP y MSCHAPv2 o solo requieran conexión hacia el Internet.

- El mantener versiones actualizadas tanto de los sistemas operativos, de las aplicaciones que controlan los servicios así como del firmware de todos los dispositivos que forman parte de la infraestructura es una medida preventiva que tiende a reducir la indisponibilidad del servicio.

- Para ambientes de producción es necesario habilitar y gestionar adecuadamente, tanto en los servidores como todos los clientes, los Certificados de Autoridad (CA) adecuados que reflejen en ellos los parámetros y características que se ajusten a la realidad de cada entorno.

5. Bibliografía

Libros:

Bhaiji, Y. C. (s.f.). *CCIE Professional Development Series Network Security Technologies and Solutions.* Cisco Press.

Carter, G. (March 20, 2003). *LDAP System Administration.* O'Reilly Media, Inc.

Carter, G., Ts, J., & Eckstein, R. (January 23, 2007). *Using Samba, Third Edition.*

Hassell, J. (October 8, 2002). *RADIUS.* O'Reilly Media, Inc.

Sankar, K., Sundaralingam, S., Balinsky, A., & Miller, D. (November 15, 2004). *Cisco Wireless LAN Security.*

Zhang, Y., Zheng, J., & Ma, M. (March 31, 2008). *Handbook of Research on Wireless Security.* IGI Global.

Revista:

Leu, J.-S. L.-H.-I.-K. (2006). Running cellular/PWLAN services :Practical considerations for cellular/PWLAN.

Documentos de Internet:

Cisco. (s.f.). *Cisco Systems, Inc.* Recuperado el Febrero de 2011, de http://www.cisco.com/en/US/docs/wireless/access_point/12.3_7_JA/configuration/guide/s37cli.html

Cisco. (s.f.). *Debug Authentications.* Recuperado el Abril de 2011, de Document ID: 50843: http://www.cisco.com/en/US/products/hw/wireless/ps430/products_tech_note09186a008024aa4f.shtml

Deploying RADIUS Partnerships. (s.f.). *Deploying RADIUS:The book*. Obtenido de http://deployingradius.com/

Diario HOY. (15 de Feb de 2011). *Las Pymes generan 88% de empleos en América Latina.* Obtenido de http://www.hoy.com.ec/noticias-ecuador/las-empresas-pequenas-compiten-en-la-ue-458599.html

INEC. (s.f.). *Instituto Nacional de Estadísticas y Censos*. Obtenido de http://www.inec.gob.ec

Lideres, R. (s.f.). Obtenido de http://www.revistalideres.ec

NetMarketShare. (s.f.). Obtenido de http://marketshare.hitslink.com/.

Revista Lideres. (30 de 05 de 2011). *www.revistalideres.ec.* Obtenido de http://www.revistalideres.ec/2011-05-30/Informe.aspx

The FreeRADIUS Server Project. (s.f.). *FreeRADIUS The world's most popular RADIUS Server.* Obtenido de http://freeradius.org/

Wikimedia Foundation, Inc. (s.f.). *Wikipedia*. Recuperado el Octubre de 2010, de http://en.wikipedia.org/wiki/Main_Page

6. Glosario de términos

3G	3rd generation mobile telecommunications
AAA	Authentication, Authorization and Accounting
AP	Access Point
AVP	Attribute Value Pair
CA	Certificados de Autoridad
CHAP	Challenge/Handshake Authentication Protocol
DIT	Árbol de Información del Directorio
DN	Nombre Distinguido
EAP	Protocolo Extensible de Autenticación
FDDI	Fiber Distributed Data Interface
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Protocolo de Internet
IRTF	Internet Research Task Force
ISP	Internet Service Provider
IT	Tecnologías de Información
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format
MD5	Message-Digest algorithm 5
MN	Nodo Móvil
MS-CHAP-V2	Microsoft CHAP V2
OSI	Open System Interconnection
P2P	Peer to Peer
PAP	Password Authentication Protocol
PC	Personal Computer
PDA	Personal Digital Assistant
PPP	Point-to-Point Protocol
PyME	Pequeña y Mediana Empresa
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Serve
RDN	Nombre Relativo Distinguido
RFC	Request For Comment
SASL	Simple Authentication and Security Layer
SIM	Subscriber Identification Module
SP	Service Provider
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Protocolo de Control de Transmisión y Protocolo de Internet

TIC	Tecnologías de Información y Comunicación
TLS	Transport Layer Security
UDP	User Datagram Protocol
UHO	User Home Organization
URI	Identificador Uniforme de Recursos
VLAN	Virtual LAN
VPN	Virtual Private Network
WAP	Wireless Access Point
WEB	World Wide Web
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access ver. 2