UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA ELECTRÓNICA Y REDES DE COMUNICACIÓN

"SERVIDOR AAA PARA VALIDACIÓN Y CONTROL DE ACCESO DE USUARIOS HACIA LA INFRAESTRUCTURA DE NETWORKING DE UN ENTE DEL MINISTERIO DE DEFENSA NACIONAL"

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTOR: Luis Carlos Plasencia Bedón

DIRECTOR: Ing. Carlos Vásquez

Ibarra, Julio 2012

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital Institucional determina la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información.

DATOS DEL CONTACTO	
Cédula de Identidad	1003332739
Apellidos y Nombres	Plasencia Bedón Luis Carlos
Dirección	Ejido de Caranqui
Email	electrolucho23@hotmail.com
Teléfono Móvil	080541766

DATOS DE LA OBRA	
Título	SERVIDOR AAA PARA VALIDACIÓN Y CONTROL DE ACCESO DE USUARIOS HACIA LA INFRAESTRUCTURA DE NETWORKING DE UN ENTE DEL MINISTERIO DE DEFENSA NACIONAL
Autor	Plasencia Bedón Luis Carlos
Fecha	11 de Julio de 2012
Programa	Pregrado
Título por el que se aspira	Ingeniero en Electrónica y Redes de Comunicación
Director	Ing. Carlos Vásquez

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Luis Carlos Plasencia Bedón, con cédula de identidad Nro. 1003332739, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior Artículo 143.

UNIVERSIDAD TÉCNICA DEL NORTE

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, **Luis Carlos Plasencia Bedón,** con cédula de identidad Nro. 1003332739, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, Artículos 4, 5 y 6, en calidad de autor del trabajo de grado denominado **"SERVIDOR AAA PARA VALIDACIÓN Y CONTROL DE ACCESO DE USUARIOS HACIA LA INFRAESTRUCTURA DE NETWORKING DE UN ENTE DEL MINISTERIO DE DEFENSA NACIONAL",** que ha sido desarrollado para optar por el título de **Ingeniero en Electrónica y Redes de Comunicación,** quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en el formato impreso y digital a la biblioteca de la Universidad Técnica del Norte.

_____

Firma
Nombre: Luis Carlos Plasencia Bedón
Cédula: 1003332739

DECLARACIÓN

Yo **LUIS CARLOS PLASENCIA BEDÓN** declaro bajo juramento que el trabajo aquí descrito es de mi autoría; y que éste no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo los derechos de propiedad intelectual correspondiente a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las leyes de propiedad intelectual, reglamentos y normatividad vigente de la Universidad Técnica del Norte.

_____

Luis Carlos Plasencia Bedón

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el estudiante: **LUIS CARLOS PLASENCIA BEDÓN,** bajo mi supervisión.

_____

Ing. Carlos Vásquez

DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

En primer lugar agradezco a Dios por darme la oportunidad de gozar de las maravillas de la vida.
A la Universidad Técnica del Norte por abrirme las puertas para mi formación profesional y permitirme ser parte de ella.

A mi director de tesis Ing. Carlos Vásquez por dedicarme su tiempo en la dirección de mi proyecto y por su paciencia durante la transición del mismo, de igual manera a mis profesores que compartieron sus conocimientos conmigo y que fueron el elemento principal para mi formación.

Al Ing. Hugo Chamba por brindarme su amistad, confianza, apoyo incondicional y ser una guía en la aplicación práctica de soluciones tecnológicas. Al Ente del Ministerio de Defensa Nacional por brindarme las facilidades necesarias para implementar el proyecto de tesis en sus instalaciones especialmente al Subs. Gonzalo Román y Sgop. César Quiña por su valiosa amistad y apoyo para el desarrollo del proyecto.

A mis amigos y personas que de una u otra manera me apoyaron para que el proyecto se lleve a cabo.

Carlos

DEDICATORIA

A mis padres Juan Plasencia y Pilar Bedón por darme la vida, su amor, su apoyo incondicional, educarme y estar a mi lado durante el transcurso de mi vida.

A mis hermanas Cecilia, Cristina y Alejandra por estar conmigo cuando las necesito y por el aliento que me brindan para seguir adelante.

A mi novia Paola por comprenderme, motivarme, amarme y por todo lo que comparte conmigo.

A mis familiares que me ayudaron cuando más necesitaba para desarrollar mi proyecto de tesis.

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

En los tiempos actuales la seguridad de la información es un tema de suma importancia para cualquier organización o institución, debido a las facilidades de las comunicaciones que se brinda a los usuarios a través de servicios internos y públicos (Internet) para el desarrollo de sus actividades laborales, por tal motivo no se debe descuidar la protección de los datos que circulan por la red. El presente proyecto mediante la implementación de un servidor AAA valida el acceso de los usuarios que ingresan a la infraestructura de networking del ente del Ministerio de Defensa Nacional con la finalidad de asegurar la conexión a la red sólo a usuarios autorizados y complementariamente a la solución se utiliza infraestructura UTM desarrollada sobre software libre que controla el acceso de usuarios a los recursos de red de la institución.

ABSTRACT

Today's the security information is an issue of paramount importance to any organization or institution, due to communications facilities provided to users through internal services and public (Internet) for the development of its work activities, for that reason we must not neglect the protection of data flowing through the network. The present project through the implementation AAA server validates the user access to enter the networking infrastructure of the entity of the Ministry of National Defense in order to secure the connection to the network only to authorized users and in addition to the solution UTM infrastructure developed using free software that controls user access to network resources of the institution.

CAPÍTULO I

ESTUDIO DE SITUACIÓN ACTUAL Y REQUERIMIENTOS DE ACCESO DE USUARIOS DEL ENTE DEL MINISTERIO DE DEFENSA NACIONAL

1.1 ANÁLISIS DEL ESTADO ACTUAL DE LA ENTIDAD

El ente del Ministerio de Defensa Nacional es el encargado de administrar y gestionar el backbone principal de las comunicaciones a nivel nacional, y en la actualidad no consta de métodos y esquemas que garanticen la confidencialidad, integridad y disponibilidad de la información que se maneja internamente en la red LAN (Local Area Network, Red de Area Local).

No existe control de los usuarios que acceden a los recursos de la red, pudiendo de esta manera existir intrusiones de sujetos con fines desconocidos que pueden perjudicar o comprometer la información que circula por la red.

La institución cuenta con dos infraestructuras, una de telefonía y otra de networking, las mismas que son administradas en los cuartos de telecomunicaciones ubicados en cada bloque del edificio. Tanto la infraestructura de telefonía como la de networking cuentan con su propio personal de administración, sin embargo, no poseen normas de control de acceso de los individuos que ingresan a dichos cuartos, creando una amenaza de seguridad. En este sentido las personas que acceden a los cuartos de telecomunicaciones, fácilmente pueden desconectar el cable de conexión de un usuario que se encuentre ausente y usurpar la información que se transmite por la red.

En la actual infraestructura no se cuenta con mecanismos de autenticación de usuarios para el acceso hacia los recursos de red tanto en la red cableada como en la red inalámbrica.

1.1.1 EQUIPAMIENTO *[1]*

La institución cuenta con infraestructura de red de características robustas para controlar a los usuarios que acceden a la infraestructura de red. Las características y prestaciones de los elementos de networking no son aprovechadas al máximo, y a la vez tienen problemas de rendimiento por la falta de control de tráfico de la red.

Los equipos que conforman la infraestructura de networking de la red se presentan en la *Tabla 1*:

Tabla 1. Infraestructura de Networking
Fuente: Carlos Plasencia

CANTIDAD	MARCA	MODELO	ESTADO
1	Switch 3Com	7750	Funcionando
1	Switch 3Com	5500-SI-24-ports	Funcionando
7	Switch 3Com	5500-EI-48-ports	Funcionando
1	Access Point 3Com	2780	Funcionando
1	Switch 3Com-Wirelees	WX1200	Funcionando
1	Modem ADSL	VisioNet	Funcionando
1	Switch 3Com	5500G	SIN USO
1	Router Cisco	3700	SIN USO
1	Switch D-Link	D-Link 16 ports	Funcionando

Los equipos de networking que forman el nivel de acceso son los siete switches 3Com 5500-EI-48-ports y el switch 3Com 5500-SI-24-ports los mismos que prestan servicio a la red cableada. Para el acceso a la red inalámbrica se cuenta con el Access Point 3Com 2780.

Los switches 3Com 5500 tienen funcionando la versión de IOS (Internetwork Operating System, Sistema Operativo de Interconexión de Red) 03.03.02 y las funcionalidades principales son las siguientes:

- Soporte de Capa 3: Filtran y enrutan paquetes basándose en direcciones MAC (Media Access Control, Control de Acceso al Medio) y de red.
- Políticas de seguridad y ACL (Access Control List, Listas de Control de Acceso).
- QoS (Quality of Service, Calidad de Servicio).
- Gigabit Ethernet y 10 Gigabit Ethernet.
- XRN[1] stack (eXpandable Resilient Networking, Red flexible apilable).
- Agregación de puerto
- VLAN (Virtual Local Area Network, Red de Area Local Virtual).
- DHCP (Dymamic Host Configuration Protocol, Protocolo de Configuración Dinámica de Host).
- Control de acceso basado en direcciones MAC
- Protocolos de enrutamiento estático, RIP (Routing Information Protocol, Protocolo de Información de Enrutamiento), OSPF (Open Shortest Path First, Primero el Camino más Corto).
- IGMP (Internet Group Management Protocol, Protocolo de Administración de Grupos de Internet).
- RSTP (Rapid Spanning Tree Protocol, Protocolo Rápido de Árbol Expandible).
- 802.1X[2]
- FTP (File Transfer Protocol, Protocolo de transferencia de ficheros).
- TFTP (Trivial File Transfer Protocol, Protocolo de Transferencia de Archivos Trivial).
- SNMP (Simple Network Management Protocol, Protocolo Simple de Gestión de Red).
- RMON (Remote Network Monitoring, Monitoreo Remoto de Red).
- SSH (Secure Shell, Intérprete de Órdenes Segura).

Los equipos que se utilizan en la red wireless, son puntos de acceso de la marca 3Com los cuales se conectan a través de un switch 3Com WX1200, el mismo que sirve para gestionar los puntos de acceso de la red.

---

[1] XRN.- Tecnología que permite administrar múltiples equipos de la misma marca, igual serie e igual versión de IOS como si fuera un solo equipo.
[2] 802.1X.- Es una norma del IEEE para el control de acceso a red basada en puertos.

A través de la red de la institución circula información referente a los siguientes servicios:

- DNS (Domain Name Service, Servicio de Nombres de Dominio) interno, para la resolución de Nombres de Dominio. La consulta de nombres de dominio se realiza a través del protocolo UDP (User Datagram Protocol, Protocolo de Datagrama de Usuario) por el puerto 53.
- Correo institucional, el acceso a la interfaz WEB es mediante HTTPS; envío de coreos a través del servicio SMTP (Simple Mail Transfer Protocol, Protocolo Simple de Transferencia de Correo).
- Portales WEB (acceso vía HTTP)
- Base de datos LDAP (Lightweight Directory Access Protocol, Protocolo Ligero de Acceso a Directorios), las consultas a la base de datos se realiza a través de protocolo TCP por el puerto 389.
- Sistema Controlador de Dominio (acceso a través de NETBIOS)
- Antivirus Kaspersky (para actualización desde los clientes hacia el servidor por los puertos 13000, 14000 y 15000)
- Servidor de Archivos
- Aplicaciones financieras, contables e internas que no se hacen mención en el presente proyecto por razones de confidencialidad, pero que son tratados en el proceso de control de acceso.

1.1.2 TOPOLOGÍA FÍSICA DE LA RED ACTUAL

La topología física actual de la red de la institución sirve para conocer la estructura de las conexiones de los equipos de networking, y la función que cumple cada uno dentro de la misma. Mediante la representación gráfica se conocerá si se tiene implementado algún modelo jerárquico o simplemente es una red plana.

En base a la topología de red actual se realiza el análisis y diseño de los esquemas de control de acceso del presente proyecto, los cuales mejoran el nivel de seguridad de la información que se maneja internamente.

La topología de red actual se presenta en la *Figura 1:*

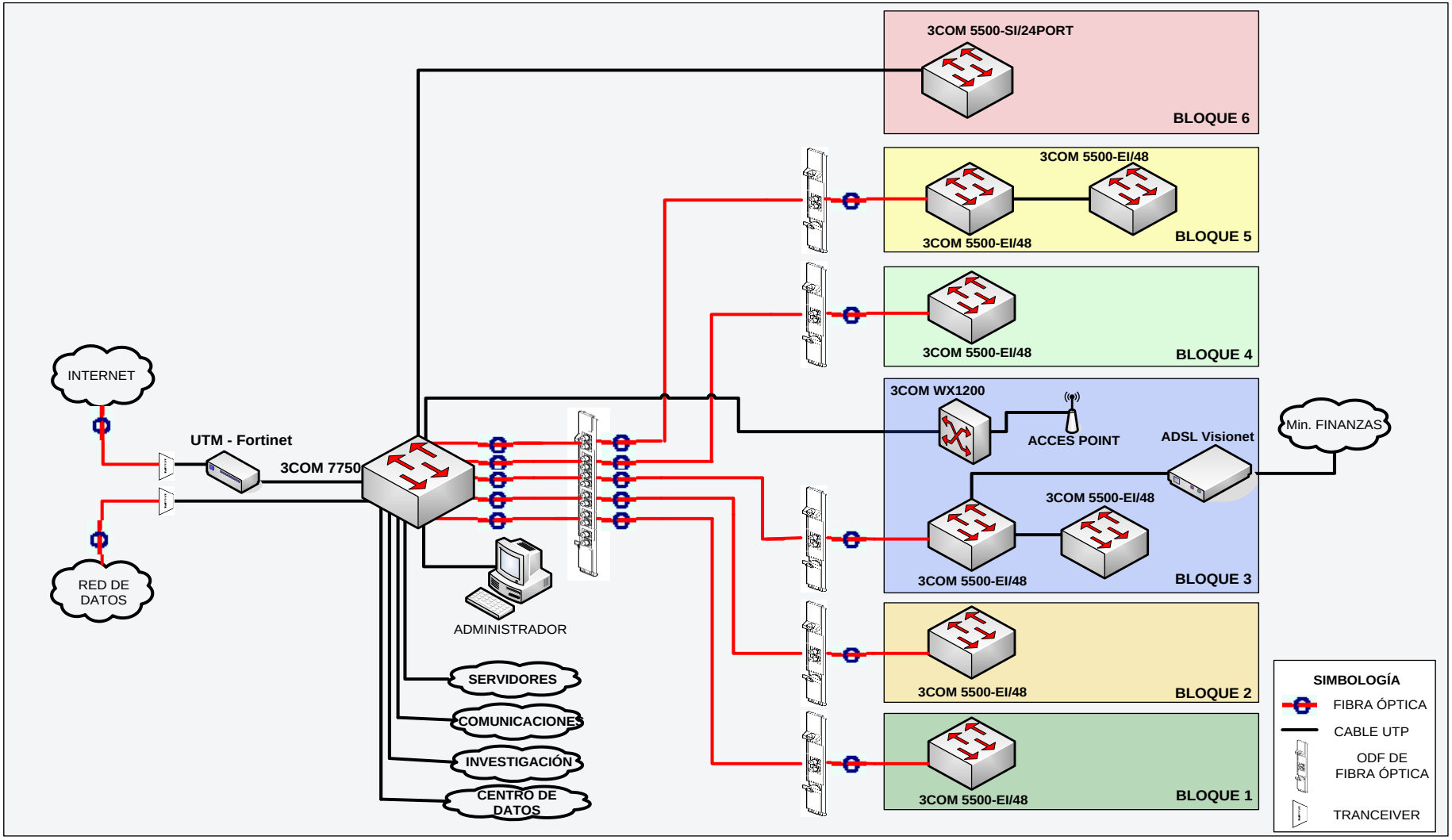


Figura 1. Topología física de la red
Fuente: Carlos Plasencia

1.1.2.1 Descripción de la topología Física *[2]*

Como se observa en la *Figura 1*, se distinguen dos capas: la capa de distribución conformada por el switch 3Com 7750 y la de acceso la cual tiene equipos en cada uno de los bloques del edificio para dar servicio a los usuarios. En todo el edificio existen aproximadamente 350 puntos de red en el cableado estructurado.

Los usuarios que acceden a través de la red wireless, usualmente son usuarios temporales que hacen uso del servicio cuando se tiene reuniones con los directores y además ciertos usuarios internos que poseen equipos personales.

El backbone principal de la red es de fibra óptica, la misma que llega a los ODFs (Optical-Fiber Distribution Frame, Distribuidor de Fibra Óptica) en cada cuarto de comunicaciones.

Los switches del bloque 3 y bloque 5 se encuentran apilados ya que soportan la tecnología XRN stack. Esta tecnología permite administrar hasta ocho switches de la misma marca, el mismo modelo y la misma versión de IOS, como si fuera un sólo equipo.

EL cableado estructurado del edificio es de categoría 5E, el mismo que tiene un tiempo de uso de aproximadamente 10 años, siendo el limite según la norma ANSI/EIA/TIA-568B[3] de cableado estructurado. El cableado soporta el servicio AAA (Authentication Authorization and Accounting, Autenticación Autorización y Contabilidad) a instalarse en la red, pero se debe tener en cuenta que para la implementación de nuevos servicios como voz IP, es necesario pensar en su remplazo por un cableado que soporte los servicios actuales y futuros que puedan implementarse.

En el switch del bloque 3 se encuentra conectado un Módem ADSL (Asymmetric Digital Subscriber Line, Línea de Abonado Digital Asimétrica)

[3] ANSI/EIA/TIA-568B.- Estándar para cableado estructurado para servicios de telecomunicaciones.

Visionet de CNT (Corporación Nacional de Telecomunicaciones) el cual es un canal dedicado para acceder a las páginas WEB del ministerio de finanzas.
Este canal al no ser filtrado por ningún equipo de seguridad como firewall, IDS/IPS (Intrusion Detection System and Intrusion Prevention System, Sistema de Detección de Intrusos y Sistema de Prevención de Intrusos) representa una vulnerabilidad en cuanto al tráfico que puede ingresar o salir a través de este enlace.

En la entrada de los datos de Internet se encuentra ubicado un UTM (Unified Threat Management, Gestión Unificada De Amenazas) de la marca Fortinet, el mismo que tiene el firmware y aplicaciones desactualizadas por la caducidad de la licencia, y actualmente no cumple con las funciones de UTM, por lo cual es recomendable comprar la licencia para el equipo y reconfigurarlo adecuadamente para aprovechar su funcionalidad u optar por una solución para realizar el control del tráfico de internet.

Las conexiones tanto para la red de internet como para la red de datos son de fibra óptica.

En la red de datos no existe ningún dispositivo que controle el tráfico que ingresa o sale de ella, convirtiéndose en otra vulnerabilidad, teniendo en cuenta que la mayoría de ataques que se pueden producir, suele suceder por usuarios de la red de datos interna.

1.1.3 REQUERIMIENTOS DE USUARIOS

En la red LAN de la institución se tiene una subred de servicios y aplicaciones las mismas que son usadas por usuarios de la red interna para el desarrollo de sus actividades de acuerdo a la función que cumplen dentro de la institución.

En este sentido y rigiéndose a las normas, políticas y procedimientos especificados en el SGSI (Sistema de Gestión de Seguridad de la Información) de la institución se han aplicado políticas sobre la utilización de las aplicaciones y recursos.

Los usuarios que se encuentran conectados en la infraestructura de networking cableada necesitan acceder a los servicios y aplicaciones de la institución de manera segura, controlando el acceso de personas no autorizadas utilizando mecanismos de autenticación que garanticen el acceso sólo a usuarios que pertenecen a la institución.

Los usuarios que poseen laptops acceden a la red Wireless sin la utilización de mecanismos de autenticación, por lo cual, cualquier persona que se encuentre dentro de esta zona puede acceder a los servicios internos, provocando un punto de inseguridad. A través de esta conexión es sencillo obtener información de la red, tal como: direcciones IP (Internet Protocol. Protocolo de Internet) de servidores de aplicaciones, equipos de red, de usuarios, entre otros.

Para la utilización de la red inalámbrica de forma segura, se necesita la implementación de controles de acceso que garanticen la confidencialidad, integridad y disponibilidad de la información.

Como solución complementaria en la mejora de la seguridad de la información se toma en cuenta los siguientes aspectos:

- **Autenticación de usuarios:** Para que el usuario pueda hacer uso de los recursos de red, debe contar con su nombre de usuario y contraseña.

- **Control de la navegación de internet:** Es necesario conocer los privilegios de navegación que debe tener cada usuario dependiendo de las actividades laborales que realizan, para así determinar los permisos a asignarse a cada uno.

- **Control de Acceso a las Aplicaciones**: Para realizar este control se debe conocer cuáles son los usuarios que necesitan el acceso y a qué aplicaciones.

Actualmente no se cuenta con infraestructura para control de navegación de internet por lo que cada usuario puede utilizar este recurso sin medida, causando problemas de lentitud a otros que lo necesitan para desarrollar sus actividades laborales. De igual forma no existe control de los usuarios que acceden desde las redes LAN y de datos hacia aplicaciones internas como correo institucional, portales web, sistemas integrados, entre otros.

Una de las mayores debilidades en cualquier organización, es que los directivos se preocupan sólo de poseer el servicio de internet sin tomar en cuenta la optimización del recurso para el desempeño laboral, y tampoco piensan en lo peligroso que puede ser al no contar con esquemas de control de acceso del tráfico de internet, por lo que se vuelven vulnerables a ciertos ataques que puedan producirse desde el exterior de la red.

No se toma en cuenta que el internet es una nube a la que puede acceder cualquier persona desde cualquier parte del mundo a cualquier información que esté publicada.

Hay que tener en cuenta que el instalar un firewall por hardware o por software en la red LAN, no garantiza que la institución esté protegida, depende de la manera que está configurado y la función que desempeña dentro de la misma.

1.2 RECOMENDACIONES Y POLÍTICAS DEL SGSI AFINES AL CONTROL DE ACCESO DE USUARIOS *[3][4]*

El ente del ministerio de defensa Nacional posee un Sistema de Gestión de Seguridad de Información (SGSI) basado en la norma ISO-27001[4]. El SGSI es un documento que ayuda a las instituciones u organizaciones a establecer políticas, procedimientos y controles en relación a los objetivos de la razón de ser de la institución, con objeto de mantener siempre el riesgo por debajo del nivel asumible por la propia organización. Para los responsables de la entidad es una herramienta, alejada de tecnicismos, que les ofrece una visión global sobre el estado de sus sistemas de información, las medidas de seguridad que se están aplicando y los resultados que se están obteniendo de dicha aplicación. Todos estos datos permiten a la dirección una toma de decisiones sobre la estrategia a seguir.

Las principales recomendaciones y normas del SGSI relacionadas con el presente proyecto son:

1.2.1 RECOMENDACIONES

Esta sección detalla recomendaciones que se deben tener en cuenta para mejorar la confidencialidad de la información.

1.2.1.1 Sobre el acceso no autorizado

Para evitar el riesgo de accesos no autorizados hacia la información, se deben implementar medidas como las siguientes:

- Limitar el acceso a programas y archivos.
- Asegurar que los usuarios puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.

[4] ISO-27001.- Organización Internacional para la Estandarización de la seguridad de la información**.**

- Asegurar que se estén utilizando los datos, archivos y programas correctos con su respectivo procedimiento.
- Se debe implementar medidas de control de acceso.
- Se debe crear e implementar políticas de contraseñas.

1.2.1.2 Utilización de los recursos del sistema para fines no previstos

- Se debe definir el uso de los servicios públicos a aquellos usuarios autorizados.
- Los usuarios autorizados deberán recibir información complementaria sobre el uso de tales sistemas y las posibles amenazas que pueden presentar.
- Crear un reglamento que controle el uso correcto e incorrecto de la red y sus recursos, en el cual se establezcan las sanciones por incumplir el mismo.

1.2.2 POLÍTICAS

Las políticas son lineamientos a los cuales deben someterse los usuarios implicados en el uso de los recursos informáticos de la institución.

1.2.2.1 Contraseñas

- Capacitar a los usuarios en la forma que deben crear sus contraseñas.
- Se debe garantizar que las contraseñas cumplan con las características siguientes:
    - Utilizar al menos 8 caracteres.
    - Utilizar letras mayúsculas, minúsculas, símbolos y números.
    - Los usuarios deben cambiar las contraseñas cada 120 días.
    - Los administradores deben cambiar las contraseñas cada 90 días.
    - No deben re-utilizarse contraseñas.

1.2.2.2 Acceso a la información

- El personal que labora en la institución debe tener acceso sólo a la información necesaria para el desarrollo de sus actividades.

- En el caso de personas ajenas a la institución, la persona responsable de generar la información debe autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación. Este proceso debe ser documentado.
- Los proveedores o terceras personas solamente deben tener privilegios durante el período del tiempo requerido para llevar a cabo las funciones aprobadas.

1.2.2.3 Seguridad de la información

- Los usuarios son responsables de la información que manejan.
- Los usuarios deben cumplir los lineamientos generales y especiales dados por la Institución y por la Ley para proteger la información.
- Ningún personal de la institución debe suministrar cualquier información a ningún ente externo sin las autorizaciones respectivas.
- *"Todos los usuarios tienen la responsabilidad de velar por la integridad, confidencialidad y disponibilidad de la información que maneje, especialmente si dicha información ha sido clasificada con algún nivel distinto al ORDINARIO".* (SGSI de la institución, 2009)
- La persona que detecte el mal uso de la información está en la obligación de reportar el hecho.

1.2.2.4 Seguridad en recursos informáticos

Para cada recurso informático se debe tener la siguiente documentación:

- Manejo de claves: Establece como utilizar las claves. Está asociada a una política de gestión de contraseñas.
- Roles: Se Debe tener la capacidad de definir roles, así como las acciones permitidas a cada rol.

1.2.2.5 Control de acceso

- Cada usuario debe disponer de un nombre de usuario y contraseña única.
- Las contraseñas son responsabilidad de sus propietarios.
- Las contraseñas solo deben ser conocidas por su propietario.

- Los usuarios son responsables de las actividades llevadas a cabo con su nombre de usuario y/o contraseña.
- Las contraseñas deben tener una fecha de caducidad definida en base a la sensibilidad de la información a proteger. Para los sistemas de acceso a las estaciones de trabajo, se recomienda cambiarlas cada 60 o 90 días.
- Los nombres de usuario no deben estar basados en las funciones de trabajo. Los nombres de usuario identifican a personas específicas.
- Toda la información con un nivel de sensibilidad igual o superior a CONFIDENCIAL debe ser cifrada.

1.2.2.6 Seguridad para terceros usuarios

- Si es necesario que un usuario ajeno a la Institución acceda a algún recurso informático, se debe firmar un acuerdo de confidencialidad con dicho usuario.
- Si se requiere acceder a redes externas utilizando algún módem, el equipo que lo use no puede estar conectado simultáneamente a la red externa y a la red interna.
- La conexión entre sistemas de la Institución y sistemas externos debe ser aprobada y certificada por el personal de Seguridad Informática para no afectar la seguridad de la información interna.

1.2.2.7 Seguridad física

- Si un trabajador se encuentra a un visitante en un área restringida, el visitante debe ser cuestionado acerca de su propósito en el área y se debe informar a los responsables de la seguridad del edificio.
- El personal ajeno a la Institución no está autorizado a utilizar los recursos informáticos de la Institución.

1.2.2.8 Listado de Usuarios con acceso a redes de alcance global

- Se debe disponer de un Listado de Usuarios autorizados, especificando Nombre, Apellidos y Cargo que ocupa en la Institución, así como los Servicios para los que está autorizado.

CAPÍTULO II

INTEGRACIÓN DEL ESTANDAR IEEE 802.1X

2.1 IMPORTANCIA DEL CONTROL DE ACCESO EN LA SEGURIDAD DE LA INFORMACIÓN *[5] [6]*

Según Juan M. Chamorro (2005) en su artículo Consideraciones para la implementación de 802.1X en redes WLAN's (Wireless Local Area Network, Red de Area Local Inalámbrica) define que:

> El control de acceso, en sistemas de información, es la capacidad de controlar la interacción de un elemento activo (usuario, dispositivo, servicio) con un recurso informático (red de datos, sistema, servicio). Adicionalmente, el control de acceso implica procedimientos de identificación, autenticación y autorización para permitir o denegar el uso de los recursos así como para llevar un registro de este. (p. 3).

La seguridad es un tema importante en las redes tanto cableadas como inalámbricas, porque alrededor de la red local se encuentran personas que buscan obtener información confidencial para utilizarla con fines desconocidos que pueden perjudicar la seguridad de la información y la imagen de la institución. En la gran mayoría de instituciones y empresas se reciben ataques desde su propia red, generalmente efectuados por empleados que tienen desconocimiento en el uso de los sistemas informáticos o insatisfechos con intereses ocultos. Evitar que dichos ataques se lleven a cabo mejora la calidad de los procesos de seguridad de la institución.

Las evaluaciones periódicas de seguridad interna permiten a la institución conocer el nivel de acceso que tiene la información que circula y forma parte de la red, visto desde la perspectiva de un usuario malicioso con la configuración actual de sus equipos y dispositivos de red.

El gran desarrollo de la tecnología informática está ofreciendo un nuevo y amplio campo de acción a comportamientos antisociales y delictivos, presentados de formas inesperadas, permitiendo la realización de ataques tradicionales utilizando nuevos mecanismos que explotan las debilidades de los sistemas.

Al tratar de proteger la información, hay que identificar todos los elementos que participan en su manipulación, como son aplicaciones de software, medios de transmisión y medios de almacenamiento, y tratar de protegerlos de ataques o manipulaciones maliciosas.

En los tiempos actuales el empleo de mecanismos de seguridad tradicionales como el uso de candados o cerraduras ya no son suficientes para proteger la información, por su naturaleza, ésta puede ser vulnerada por otro medio (Ej. medios de transmisión por donde se transmiten los datos), lo que indica que para proteger la información, se deben considerar tanto los elementos físicos como lógicos que intervienen en los sistemas con el objetivo de dar una solución de seguridad adecuada y acorde con el sistema que se desea proteger.

2.2 CONCEPTOS DE SEGURIDAD DE INFORMACIÓN *[7][8]*

El objetivo de la seguridad de información es proteger los datos de la institución, se debe considerar tres aspectos muy importantes en la preservación de la misma, los cuales son la confidencialidad, integridad y disponibilidad.

Clara Baonza (n.d.) afirma que:

> La información es el principal patrimonio de cualquier organización, por lo que su protección y seguridad resulta imprescindible, máximo en un momento en el que Internet y las relaciones electrónicas se han establecido como la nueva forma de relacionarse, con las ventajas innegables, pero también con los riesgos que ello conlleva. (p. 1).

2.2.1 CONFIDENCIALIDAD

El objetivo de la confidencialidad, es permitir que la información esté autorizada y sea únicamente vista por las personas a quienes está destinada, es decir, se refiere a la privacidad de la información. Para este fin se utilizan mecanismos de encripción de los datos.

2.2.2 INTEGRIDAD

La integridad hace referencia a la habilidad de proteger la información, los datos o las transmisiones de alteraciones no autorizadas, no controladas o accidentales.

Asegurar la consistencia de la información y que atributos como el tiempo y la totalidad de la información sean consistentes con los requerimientos.

La integridad hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad, por ejemplo: la huella digital, firma digital, entre otros.

2.2.3 DISPONIBILIDAD

Hace referencia a que la red, hardware y software sean confiables, es decir se puedan recuperar rápido y completamente ante eventos de una interrupción.

Para poder lograr este objetivo se emplean generalmente mecanismos de redundancia de enlaces, hardware y software, con el fin de que en caso de que un evento interrumpa el funcionamiento de uno de estos elementos del sistema, el respaldo redundante solucione el problema lo más rápido posible.

2.3 ATAQUES Y VULNERABILIDADES *[9][10]*

Es importante conocer el por qué implementar esquemas o métodos de seguridad de información, y además, entender contra qué hay que tomar medidas de prevención.

- Un ataque es una técnica empleada para aprovechar alguna debilidad o falla de un sistema (vulnerabilidad), por ejemplo una amenaza podría ser el ataque de negación de servicio, siendo la vulnerabilidad el empleo de un esquema de seguridad diseñado sin considerar esta amenaza.
- Una amenaza es toda posible interrupción de operación, integridad, disponibilidad de la red o sistema, pudiendo ser la misma de origen natural, por negligencia, por intrusos, mala manipulación o por intenciones indebidas como los hackers.
- Una vulnerabilidad es una debilidad propia de los sistemas que permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones, causados por un error en el diseño, configuración o implementación de las redes o servicios.

El ataque es la acción misma, pero previo a esta acción existió una amenaza, por lo que se considera a la amenaza como el paso previo a la ejecución de un ataque. Por tal razón lo importante es encontrar las posibles amenazas con el objetivo de identificar vulnerabilidades y prevenir posibles ataques.

2.3.1 AMENAZAS HUMANAS

Los sistemas están al servicio de humanos, siendo una de las principales amenazas ya que la inquietud, curiosidad o desconocimiento puede ser el motivo para que se genere una amenaza humana.

- ***Personal interno***, ataques generados por personal interno de la misma organización, que pueden darse por falta de conocimiento en el manejo de los sistemas, intencionalmente o por inexistencia de normas básicas de seguridad. A este tipo de amenaza no se suele prestar la adecuada atención, ya que se piensa que ataques desde el interior de la institución no se dan, pero en realidad suceden con frecuencia. En la mayoría de las organizaciones la mayor parte de los ataques son causados por este tipo de usuarios. El administrador de los sistemas debe ser el encargado de aplicar normas y generar políticas basadas en la ingeniería social.

- ***Ex-empleados***, son ciertos casos cuando el personal de la institución tuvo que abandonar su lugar de trabajo en malos términos o fueron despedidos y no se firmó un acuerdo de confidencialidad, estos individuos se convierten en una amenaza al tener conocimiento del estado de la red y los niveles de seguridad que se aplica y mucho más cuando son los encargados de administrar los accesos remotos para la manipulación de equipos y aplicaciones desde el exterior de la institución. Para evitar este tipo de amenazas se recomienda firmar acuerdos de confidencialidad que garanticen la protección de la información después del despido del empleado.
- ***Curiosos,*** son los más habituales en cualquier organización ya que existen personas formándose en el campo de la informática y cada día tienen la necesidad de adquirir conocimiento en la administración y gestión de los sistemas de información.
- ***Crackers,*** Los entornos de seguridad media son un objetivo típico de los intrusos, ya sea para fisgonear, para utilizarlas como enlace hacia otras redes o simplemente por diversión. Generalmente las redes de grandes, medianas y pequeñas empresas y organizaciones son abiertas, y no se tiene en cuenta la seguridad de la información, por lo que, los sistemas conectados a estas redes provoca, que al menos algunos de sus equipos sean vulnerables y mediante la utilización de un scanner de un dominio cualquiera pueda explotar las debilidades para robar o dañar la información de la institución.
- ***Terroristas,*** ataques ocasionados por individuos u organizaciones que buscan a toda costa realizar un daño en la integridad de los sistemas o de los datos. Un ejemplo de esto puede ser el tratar de robar o modificar la información entre organizaciones competidoras. Algo adicional es que este tipo de ataques al momento ya son comercializados y generalmente empleados entre competidores de empresas para robar o destruir información de su contraparte. Este tipo de amenaza no se puede evitar pero si prevenir mediante la utilización de sistemas de seguridad perimetrales que protejan a la información de la institución.

2.3.2 AMENAZAS NATURALES

Son todas aquellas amenazas de origen natural, el efecto de las mismas puede ser mitigado considerando el daño que ocasionan en el proceso de diseño de los sistemas.

Este tipo de amenazas pueden ser sobrellevadas, pero no evitadas, se consideran como amenazas naturales a los terremotos, inundaciones, incendios, entre otros. Para reducir el efecto cuando una amenaza de este tipo se produce, es tener un plan de contingencia efectivo, es decir, que haya sido probado de manera satisfactoria. Para esto se implementan data-centers alternos en sitios distintos con la finalidad de aumentar la disponibilidad del servicio.

2.3.3 AMENAZAS LÓGICAS

Son el tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (bombas lógicas[5], virus, software malicioso, también conocido como malware) o simplemente por error en el diseño del sistema (bugs[6] o agujeros).

2.3.4 ATAQUES

Los ataques son acciones que buscan causar daño a los sistemas de información, aplicaciones y servicios, con el fin de robar información o alterarla. Como se está hablando de información y de mecanismos de comunicación, es posible clasificar los ataques en función del modo como se abusa de los canales de comunicación, esta clasificación es la siguiente:

- Ataque por fuerza bruta, trata de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que se busca, y que permite el acceso al sistema, programa o archivo en estudio.
- Cartoneo (Trashing), generalmente, un usuario anota su user y contraseña en un papelito y luego, cuando lo recuerda, lo arroja a la basura. Este

[5] Bomba lógica.- Es una parte de código insertada intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones preprogramadas.
[6] Bug.- Es el resultado de un fallo o deficiencia durante el proceso de creación de programas de ordenador o computadora (software).

procedimiento por más inocente que parezca es el que puede aprovechar un atacante para hacerse de una llave para entrar al sistema. El Trashing puede ser físico o lógico, como analizar buffers de impresora y memoria, bloques de discos, entre otros.

- Fisgar, es la acción de copiar información sin autorización del propietario de la misma
- Hombre en el medio, es una situación donde un atacante supervisa (generalmente mediante un rastreador de puertos abiertos) una comunicación entre dos partes y falsifica los intercambios para hacerse pasar por una de ellos.
- Reenviar, consiste en capturar mensajes y reenviarlos más tarde, este ataque puede ser efectivo aun con mensajes encriptados. Es llevado a cabo por el autor o por un adversario que intercepta la información y la retransmite, posiblemente como parte de un ataque enmascarado.
- Denegación de servicio, consiste en inundar un canal o recurso con peticiones o mensajes falsos con el objetivo de que los usuarios que realmente requieren el canal o recurso no puedan hacer uso del mismo sobrecargando los recursos de los sistemas de la víctima.

2.4 ESTÁNDAR IEEE 802.1X *[11][12][13]*

Los estándares son un conjunto de especificaciones tecnológicas establecidas por un organismo controlador que en este caso es el Instituto de Ingenieros en Electrónica y Electricidad, conocidos con sus siglas en inglés como IEEE, para que los productores y desarrolladores de tecnología tengan una normativa que les permita lograr que los dispositivos puedan operar entre sí.

IEEE 802.1X permite implementar un acceso seguro, empleando medios de comunicación como Ethernet, Token Ring y LANs inalámbricas 802.11. El empleo del protocolo RADIUS (Remote Autentication Dial-Up Server, Servidor de Autenticación Remota Dial-In) es opcional dentro de IEEE 802.1X, la IEEE espera que varios autenticadores IEEE 802.1X funcionen como un cliente y servidor de autenticación a la vez.

El estándar IEEE 802.1X define el control de acceso a redes basadas en puertos, es decir, permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o evitando el acceso por ese puerto si la autenticación falla.
Gracias a él se exige autenticación antes de dar acceso a las redes ethernet. En el control de acceso a redes basadas en puertos se utilizan los elementos físicos que componen una infraestructura de conmutación de la red LAN para autenticar los dispositivos agregados al puerto de conmutación. No se pueden enviar ni recibir tramas en un puerto de conmutación ethernet si el proceso de autenticación ha fallado.

A pesar de que se diseñó para redes ethernet fijas, este estándar se ha adaptado para su uso en redes LAN inalámbricas con IEEE 802.11. Windows XP soporta la autentificación IEEE 802.1X para todos los adaptadores de red basados en redes LAN, incluyendo las ethernet y las inalámbricas.

IEEE 802.1X se apoya en el protocolo de autenticación EAP (Extensible Autentication Protocol, Protocolo de Autenticación Expandible), aunque en realidad es EAPoL (Extensible Autentication Protocolo over LAN, Protocolo de Autenticación Expandible sobre LAN) de forma que se puede usar en redes ethernet, 802.11, Token-Ring y FDDI (Fiber Distributed Data Interface) Interfaz de Datos Distribuida por Fibra).

802.1X trabaja en capa dos del modelo OSI, para autenticación y autorización de dispositivos en switches LAN y Puntos de Acceso Inalámbricos (WAP). Se asume un modelo punto a punto, esto indica que no es realmente proyectado para situaciones como conexiones múltiples de PCs conectadas a un switch vía un hub o un solo switch. Como ejemplo se puede mencionar puertos en los cuales el uso de autenticación puede ser requerida incluyendo puertos en base a su dirección MAC, y asociaciones entre estaciones y el punto de acceso en redes inalámbricas IEEE 802.11.

Cuando un nodo requiere tener acceso a otro recurso de una red LAN, el Access Point o switch de acceso pregunta la identidad de dicho nodo, el tráfico permitido entre el nodo y el punto de acceso o switch es EAP hasta que el nodo sea autenticado.

El estándar 802.1X se une con el protocolo de seguridad EAP empleado tanto en redes cableadas como inalámbricas, al ser un protocolo de autenticación genérico, puede trabajar con muchos tipos de mecanismos de autenticación, por ejemplo, EAP puede autenticar un usuario basado en un nombre y contraseña, empleando certificado digital, ticket kerberos o la información contenida en un impreso SIM (Subscriber Identity Module, Módulo de Identificación del Suscriptor). En redes inalámbricas, EAP ha remplazado otros mecanismos de autenticación de capa dos, como PAP (Password Authentication Protocol, Protocolo de Autenticación de Contraseña) y CHAP (Challenge Handshake Authentication Protocol, Protocolo de Autenticación por Desafío Mutuo). Las estaciones empleando 802.1X/EAP deberán autenticarse y asociarse al punto de acceso previo realizar la autenticación y asociación con 802.1X/EAP.

El proceso de autenticación 802.1X/EAP, consiste de tres elementos importantes, un suplicante (usuario), un autenticador (Access Point o switch) y un servidor de autenticación (FREERADIUS). El suplicante es el dispositivo que solicita acceso a la red generalmente el usuario. El autenticador es un dispositivo intermediario que pasa las tramas desde el usuario al servidor de autenticación, generalmente el punto de acceso inalámbrico o un switch de acceso. El servidor de autenticación es el dispositivo que actualmente autentica el usuario, generalmente el servidor FREERADIUS.

La *Figura 2* presenta el proceso de autenticación de forma detallada:

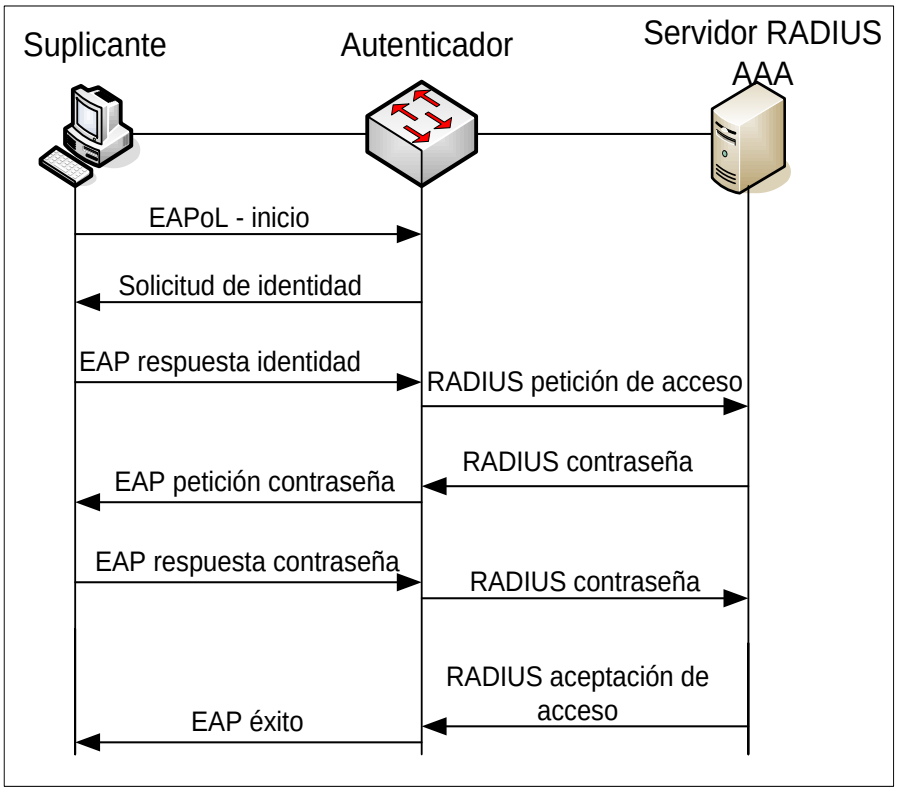


Figura 2. Autenticación 802.1X
Fuente: http://es.scribd.com/doc/65975381/34/Autenticacion-802-1x

- Primero el suplicante indica que desea realizar una autenticación EAP enviando una trama EAPoL-Inicio hacia el autenticador.
- El autenticador envía una trama EAP-requerimiento/identidad, solicitando al suplicante que provea algunos campos de información de identidad.
- La información específica depende del tipo de EAP que está siendo usado, por mencionar algunos, en EAP-MD5 será el nombre de usuario, mientras que en EAP-TLS la información requerida será un certificado digital.
- El siguiente paso es que una serie de tramas sean intercambiadas entre el suplicante y el servidor de autenticación, en este punto el autenticador solo actúa como un conmutador de tramas entre estos dos. Las tramas realizan el proceso de autenticación del usuario, y los datos llevados son específicos al tipo de EAP que está siendo usado.

Si la autenticación es exitosa, una trama EAP-exitoso es enviada al suplicante.

En caso de que el tipo de EAP soporte asignación de llaves de encripción dinámica, el siguiente paso para el suplicante y el servidor de autenticación es deducir la llave de encripción. Ellos realizan esta tarea en base a la información intercambiada en el proceso de autenticación, o basada en la información que es pre-configurada en las dos estaciones. Posterior a esto el suplicante y el servidor de autenticación conocen la llave de encripción que el suplicante usará, pero el autenticador no la conoce.

El autenticador solo conocerá la llave de encripción del usuario ya que con esta enviará mensajes al suplicante. El servidor de autenticación entregará la llave de encripción al autenticador en un campo atributo de la trama RADIUS, el cual se encripta usando la clave secreta que es conocida por el servidor RADIUS y el autenticador. En este momento la llave de encripción es conocida por las tres piezas del modelo 802.1X/EAP y la comunicación puede comenzar.
En redes wireless se utiliza el protocolo WPA para la asociación de los usuarios hacia la infraestructura de red.

WPA (Wi-Fi Protected Access) es un estándar de seguridad de redes inalámbricas que incluye TKIP (Temporal Key Integrity Protocol) y 802.1X con autenticación EAP. El estándar WPA define dos tipos de autenticación y administración de claves, ambos tipos emplean 802.1X/EAP para autenticar la estación, pero el primer tipo conocido como WPA requiere el uso de un servidor RADIUS, mientras que el segundo WPA-PSK[7] (Pre-Shared Key) no requiere de RADIUS.

En el caso de WPA empleando RADIUS la autenticación se realiza exactamente igual que 802.1X/EAP.
En el caso de WPA-PSK, una cadena ASCII es configurada en todos los puntos de acceso y estaciones, y esta cadena es usada para autenticar las estaciones.

[7] WPA-PSK.- Basa su seguridad en una contraseña compartida.

La PSK no es empleada en la encripción de las tramas, esta es empleada en la negociación para establecer la clave WEP (Wired Equivalent Privacy) dinámicamente a cada estación.

WPA-PSK no es tan segura como WPA empleando RADIUS, pero si es más segura que WEP.

2.4.1 TRAMAS 802.1X

En la autenticación se utiliza el protocolo EAP (especificado en el RFC-3748) para intercambiar información de autenticación entre el Suplicante y Servidor de Autenticación. EAP puede utilizar diversos mecanismos de autenticación tales como MD5, Kerberos, Encriptación con Clave Pública (PKE), Contraseñas de un solo uso (OTPs), entre otras. EAP consiste en un simple encapsulado que puede correr sobre diferentes niveles de enlace. Las tramas de autenticación deben ser transportadas entre el Suplicante y el Servidor de Autenticación. Para ello se ha elegido un protocolo que transporta EAP directamente sobre un servicio de Red de Area Local (EAPOL).

En la *Figura 3* se muestra la arquitectura 802.1X por capas:

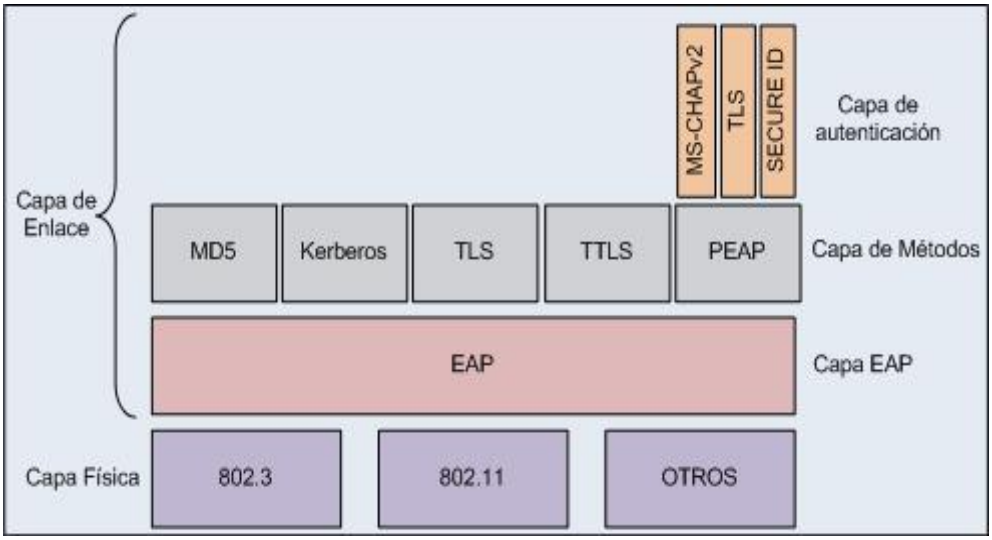


Figura 3. Arquitectura 802.1X
Fuente: http://blogs.technet.com/davidcervigon

EAP no tiene seguridad “built-in”. Los protocolos de autenticación deben implementar sus propios métodos de seguridad. El método de autenticación es elegido por los equipos durante la negociación de forma transparente al autenticador (equipos de acceso).

Las tramas a transmitirse se detallan a continuación:

- Para la red cableada las tramas a transmitirse se muestran en la *Figura 4*:

7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 - 1500 bytes	4 bytes
PREAMBULO	SDF	Dir. Destino	Dir. Origen	Tipo / Longitud	Datos + Relleno	FCS

Figura 4. Formato de la trama Ethernet
Fuente: http://es.wikipedia.org/wiki/IEEE_802.3

El contenido de cada campo de la trama se describe a continuación:

- **PREAMBULO.-** Sincronización de bits.
- **SDF.-** Delimitador de inicio de trama, es probable que el reloj del receptor no se sincronice inmediatamente, posiblemente tenga que perder algunos bits del preámbulo para lograrlo, entonces no se puede determinar cuántos bytes perdió y por lo tanto tampoco se sabe donde se termina el preámbulo y comienza los datos. Para resolver este problema se agrega otro byte que termina en “11”.
- **Dirección Destino.-** En este campo va colocada la dirección MAC del destinatario.
- **Dirección Origen.-** El sistema emisor que origina la trama coloca su propia dirección en este campo.
- **Tipo/Longitud.-** Según la IEEE 802.3 contiene el largo del paquete, según Ethernet se coloca el tipo de paquete.
- **Datos.-** Datos + Cabecera de transporte + cabecera de red. Es un campo que puede codificar entre 0 y 1500 bytes en donde se incluye la información de usuario procedente de la capa de red.
- **Relleno.**- La norma IEEE 802.3 específica que una trama no puede tener un tamaño inferior a 64 bytes, por tanto, cuando la longitud del campo de datos es muy pequeña se requiere rellenar este campo para completar una

trama mínima de al menos 64 bytes. Es un campo que puede tener una longitud comprendida entre 0 y 46 bytes, de modo que la suma total de la trama sea al menos de 64 bytes.

- **FCS.**- Secuencia de chequeo de trama. El trasmisor calcula el CRC de la trama que está enviando y también lo envía para que el receptor vuelva a calcularlo y comparando ambos, verifique que los datos llegaron correctamente.

A continuación se detalla los campos de las tramas 802.1X:

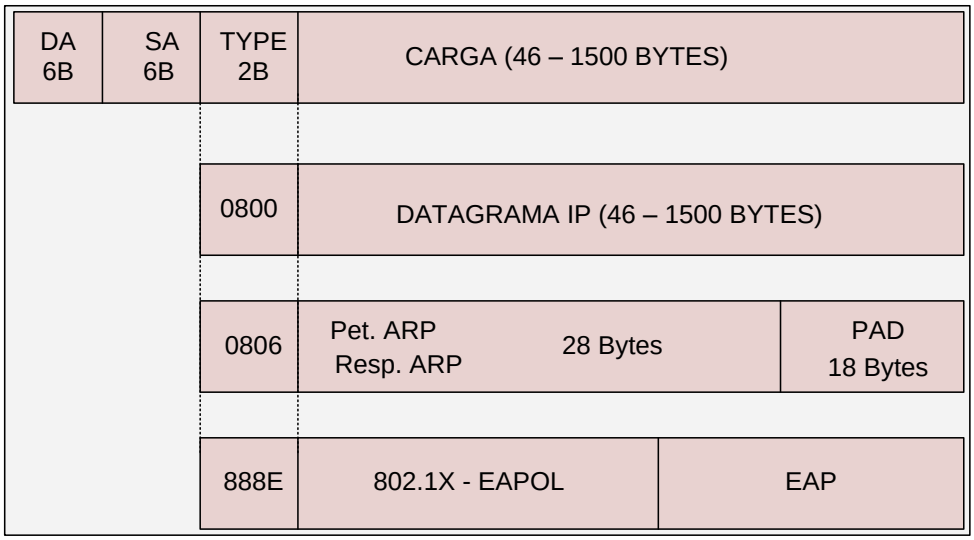


Figura 5. Tipos de tramas Ethernet
Fuente: http://blogs.technet.com/davidcervigon

Como se observa en la *Figura 5* los campos de Dirección MAC Destino y Dirección MAC Origen tienen un tamaño de 6 Bytes. El campo Type tiene un tamaño de 2 Bytes y soporta los siguientes valores:

- 0800 (decimal = 2048 - 0800 hex) – Datagrama IP
- 0806 (decimal = 2054 - 0806 hex) – ARP
- 8035 (decimal = 32821 - 8035 hex) – RARP
- 888E (decimal = 34958 - 888e hex) – 802.1x
- 8863 (decimal =34915 - 8863 hex) - Tramas de control PPPoE[8]
- 8864 (decimal = 34916 - 8864 hex) – Tramas de datos PPPoE

[8] PPPoE.- Point to Point Protocol over Ethernet

Para el presente proyecto se utilizará las tramas de tipo 888E por lo cual es necesario conocer sus campos detalladamente. A continuación se muestra la trama con los respectivos campos:

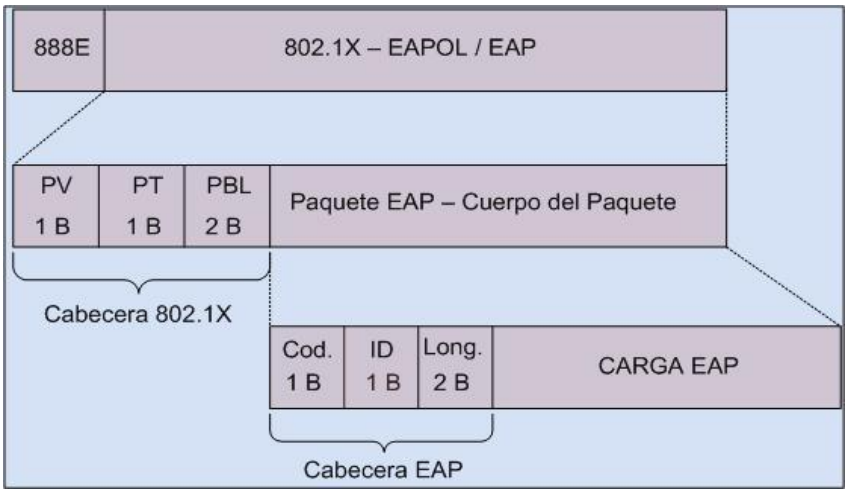


Figura 6. Campos de la trama 802.1X
Fuente: http://blogs.technet.com/davidcervigon

La cabecera EAPoL contiene 4 octetos:

- **Versión de Protocolo (1 Byte).-** Identifica la versión de EAPoL soportada por el remitente (valor 0000 0001)
- **Tipo de Paquete (1 Byte).-** paquete EAPoL (valor: 0000 0000), inicio EAPoL (valor 0000 0001), logoff EAPoL (valor 0000 0010), clave EAPoL (valor 0000 0011).
- **Longitud del cuerpo del Paquete (2 Bytes)**

La cabecera EAP contiene los siguientes elementos:

- Código (1 byte):
    - Código = 1 para petición
    - Código = 2 para respuesta
    - Código = 3 para EAP exitosa (estos mensajes no contienen datos en la carga EAP)
    - Código = 4 para EAP no exitosa (no datos en carga EAP)
- Identificador (1 byte): sirve para asociar una respuesta a una petición.
- Longitud (2 byte s)

El campo de datos EAP empieza con un campo Tipo (1 byte) que indica el tipo de protocolo de autentificación usado en la carga.

El tamaño máximo de un paquete EAP que se puede incluir dentro de una trama EAPoL dependerá del tamaño máximo de trama MAC soportado por el método MAC usado para transmitir la trama.

2.4.2 DEFINICIÓN DE SERVICIOS AAA *[14]*

Las siglas AAA significan Autenticación, Autorización y Contabilidad (en inglés Authentication, Authorization, Accounting).

Los niveles de confidencialidad, integridad y disponibilidad de la información se complementan con niveles adecuados de autenticación, mecanismos de control de acceso, definición de niveles de acceso a servicios o perfiles y control del tiempo que los usuarios permanecen conectados durante el desempeño de sus labores.

2.4.2.1 Autenticación

Garantiza que la identidad del individuo que se valida corresponda a su propietario.

Cada usuario que intente acceder a la red de datos o servicios de la misma, posee un distintivo único que es su identidad, por lo que, para poder acceder a los servicios de red deberá autenticarse con sus respectivas credenciales. En este caso las credenciales serán el nombre de usuario y contraseña, pues a través de éstas se define si el usuario cuya identidad se quiere verificar es quien dice ser.

2.4.2.2 Autorización

La autorización es la asignación de recursos adicionales, que permite tener un control de acceso por usuario después de la autenticación.

Permite realizar un control de acceso de un usuario a determinados servicios de la red, en función de un perfil prestablecido, el cual será aplicado en base a la identidad del usuario que fue autenticado.

2.4.2.3 Contabilidad

La contabilidad se refiere a llevar el registro de toda la actividad realizada por un usuario desde el momento que accedió a la red hasta que finalizó su sesión, es decir, permite llevar un control de uso del sistema en base a la identidad de quién accedió, a que accedió y por cuánto tiempo permaneció dentro del sistema.

Este tipo de control adicional, sirve de ayuda en el caso de realizar una auditoría del uso de la red, o en el caso de que se suscite un inconveniente a causa del mal uso por parte del usuario sea este con o sin intensión.

2.4.3 PROTOCOLO RADIUS *[15] [16]*

RADIUS (Remote Authentication Dial-In User Server) es un protocolo que permite gestionar la “autenticación, autorización y contabilidad” de usuarios sobre un determinado recurso.

El protocolo RADIUS proporciona un servicio de acceso centralizado. Por este motivo, uno de los principales usos de RADIUS se encuentra en empresas que proporcionan acceso a Internet o grandes redes corporativas, en un entorno con diversas tecnologías de red incluyendo módems, xDSL, VPN (Virtual Private Network, Red Privada Virtual) y redes inalámbricas.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y duración de la sesión; los datos se pueden utilizar con propósitos estadísticos.
Para comprender el funcionamiento de este protocolo es necesario conocer los mensajes que se intercambia entre los elementos de autenticación (cliente, autenticador y servidor de autenticación).

2.4.3.1 Mensajes RADIUS

Los mensajes RADIUS se envían como mensajes de datagramas de usuario UDP. El puerto UDP 1812 se utiliza para los mensajes de autenticación RADIUS y el 1813 para los mensajes de administración de cuentas RADIUS. La carga UDP de un paquete RADIUS sólo incluye un mensaje RADIUS.

- ***Access-Request*** (solicitud de acceso)
  Enviado por un cliente RADIUS para solicitar autenticación y autorización de un intento de conexión, y contiene información que el servidor RADIUS utiliza para determinar si a dicho usuario se le permite o no el acceso.
  Los atributos que mínimo debe contener este paquete son los siguientes:
  - *User-Name.-* El atributo User-Name debe llegar al servidor RADIUS de cliente como: usuario@dominio
  - *User-Password.-* Contraseña del usuario
- ***Access-Accept*** (aceptación de acceso)
  Enviado por un servidor RADIUS como respuesta a un mensaje Access-Request. En él se informa al cliente RADIUS de que se ha autenticado y autorizado el intento de conexión.
- ***Access-Reject*** (rechazo de acceso)
  Enviado por un servidor RADIUS como respuesta a un mensaje Access-Request. En él se informa al cliente RADIUS de que se ha rechazado el intento de conexión. Un servidor RADIUS envía este mensaje si las credenciales no son auténticas o si no se ha autorizado el intento de conexión.
- ***Access-Challenge*** (desafío de acceso)
  Enviado por un servidor RADIUS como respuesta a un mensaje Access-Request. Este mensaje es un desafío al cliente RADIUS que exige una respuesta.
- ***Accounting-Request*** (solicitud de administración de cuentas)
  Enviado por un cliente RADIUS para especificar información de administración de cuentas de una conexión que se ha aceptado.

- ***Accounting-Response*** (respuesta de administración de cuentas)

  Enviado por el servidor RADIUS como respuesta a un mensaje de Solicitud de administración de cuentas. En este mensaje se confirman la recepción y el procesamiento correctos del mensaje de Solicitud de administración de cuentas.

El servidor de autenticación (a veces llamado *NAS*, que significa *Servicio* de autenticación de red o Servicio de acceso a la red) puede aprobar la identidad del usuario transmitida por el controlador de la red y otorgarle acceso según sus credenciales. Además, este tipo de servidor puede almacenar y hacer un seguimiento de la información relacionada con los usuarios, por ejemplo, estas características le permiten al administrador conocer cuánto tiempo estuvo conectado un usuario o cuántos datos transfirieron.

Los datos entre el cliente y el servidor son intercambiados en paquetes RADIUS. Cada paquete contiene la siguiente información:

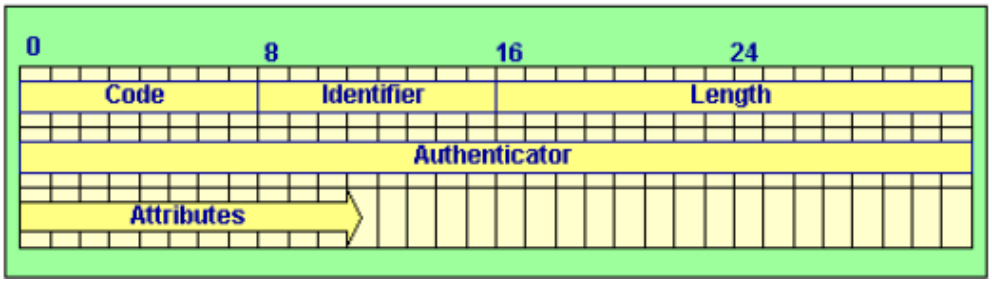


Figura 7. Formato de paquete RADIUS
Fuente: http://es.scribd.com/doc/65975381/34/Autenticacion-802-1x

Los campos en un paquete RADIUS son:

- *Code (Código).* Un octeto que contiene el tipo de paquete.

Tabla 2. Tipo de paquete RADIUS
Fuente: http://tools.ietf.org/html/rfc2865

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

- *Identifier (Identificador).* Un octeto que permite al cliente RADIUS relacionar una respuesta RADIUS con la solicitud adecuada.
- *Length.* Longitud del paquete (2 octetos).
- *Authenticator (Verificador).* Valor usado para autenticar la respuesta del servidor RADIUS. Es usado en el algoritmo de encubrimiento de contraseña.

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

Tabla 3. Tipo de atributos RADIUS
Fuente: http://tools.ietf.org/html/rfc2865

Valor del campo	Tipo de atributo	Valor del campo	Tipo de atributo
1	User-Name	23	Framed-IPX-Network
2	User-Password	24	State
3	CHAP-Password	25	Class
4	NAS-IP-Address	26	Vendor-Specific
5	NAS-Port	27	Session-Timeout
6	Service-Type	28	Idle-Timeout
7	Framed-Protocol	29	Termination-Action
8	Framed-IP-Address	30	Called-Station-Id
9	Framed-IP-Netmask	31	Calling-Station-Id
10	Framed-Routing	32	NAS-Identifier
11	Filter-ID	33	Proxy-State
12	Framed-MTU	34	Login-LAT-Service
13	Framed-Compression	35	Login-LAT-Node
14	Login-IP-Host	36	Login-LAT-Group
15	Login-Service	37	Framed-AppleTalk-Link
16	Login-TCP-Port	38	Framed-AppleTalk-Network
17	(unassigned)	39	Framed-AppleTalk-Zone
18	Reply-Message	40-59	(reserved for accounting)
19	Callback-Number	60	CHAP-Challenge
20	Callback-ID	61	NAS-Port-Type
21	(unassigned)	62	Port-Limit
22	Framed-Route	63	Login-LAT-Port

2.5 PROTOCOLOS EAP

Algunos de los mecanismos de autenticación EAP, se presenta con una breve descripción de cada uno:

- *EAP-MD5*, MD5-Challenge requiere nombre de usuario y contraseña, es equivalente a CHAP, poco empleado en autenticación en ambientes inalámbricos.
- *Lightweight EAP (LEAP)*, envía un nombre de usuario y contraseña al servidor de autenticación, es protocolo propietario desarrollado por CISCO y es considerado no seguro por lo que se está dejando fuera LEAP para emplear PEAP.
- *EAP-TLS*, crea una sesión TLS (Transport Layer Security) dentro de EAP, entre el suplicante y el servidor de autenticación, siendo necesario en el servidor y el cliente un certificado digital y una infraestructura PKI (Public Key Infraestructure, Infraestructura de Clave Pública), esta autenticación es bidireccional. Asumiendo que se empleen procedimientos adecuados de mantenimiento de los certificados, EAP-TLS es una de las formas más seguras de EAP, pero también es la que conlleva mayores requerimientos de mantenimiento.

  Hay que considerar que en ambientes donde se va a realizar cambios constantes en la red inalámbrica no sería aplicable este método pues hay que instalar certificados tanto en el cliente como en el servidor para poder ser autenticado.
- *EAP-TTLS*, se establece un túnel encriptado TLS para transporte de datos de autenticación, dentro de este túnel TLS otros métodos de autenticación se pueden emplear.
- *PEAP* (Protected EAP, EAP Protegido), emplea como EAP-TLS un túnel encriptado TLS, los certificados de suplicante para EAP-TTLS y EAP-PEAP son opcionales, pero los certificados del servidor de autenticación son necesarios.
- *EAP-MSCHAPv2*, requiere un nombre de usuario y contraseña, y en resumen es encapsulamiento EAP de MS-CHAP-v2.

2.6 PROTOCOLOS UTILIZADOS EN LA IMPLEMENTACIÓN

Para la implementación del servidor AAA es importante conocer los protocolos que intervienen y la función que cumple en el desarrollo del proyecto.

2.6.1 PROTOCOLO SSH

SSH (Secure Shell) es un programa para ingresar a servidores o computadores a través de la red, para poder ejecutar comandos desde otro computador de forma remota y poder realizar configuraciones, modificar, mover y crear archivos desde o hacia el computador remoto, siendo esta comunicación de forma segura empleando mecanismos de autenticación a través de una red insegura.

Emplea mecanismos de encripción para proteger la integridad de la información, permitiendo re-direccionar los puertos TCP/IP sobre un canal encriptado. A diferencia de rlogin o telnet, SSH encripta la sesión de registro imposibilitando que alguien pueda obtener una contraseña de texto. No servirán de nada los intentos de falsificar la identidad de cualquiera de los dos lados de la comunicación, ya que cada paquete está cifrado por medio de una clave conocida sólo por el sistema local y el remoto.

Los clientes autentican al servidor el momento de establecer la comunicación, permitiendo controlar ataques de hombre en la mitad y de igual manera el servidor autentica al usuario antes de permitir la conexión.

La idea de emplear el protocolo SSH es que sea fácil de emplear para un usuario convencional y además permita crear conexiones seguras entre dos sistemas. Los problemas puntuales que soluciona SSH son, intercepción de la comunicación entre dos sistemas y personificación de un determinado host, considerando las ventajas que brinda este protocolo y la seguridad que emplea tanto en el establecimiento de las comunicaciones como en el intercambio de datos en una conexión ya establecida, se consideró conveniente emplear este protocolo para la administración remota de los servidores.

2.6.2 PROTOCOLO SCP *[17]*

Secure Copy o SCP es un medio de transferencia segura de archivos informáticos entre un host local y otro remoto o entre dos hosts remotos, usando el protocolo Secure Shell (SSH).

En el protocolo SCP los datos son cifrados durante su transferencia, para evitar que potenciales packet sniffers extraigan información útil de los paquetes de datos. Sin embargo, el protocolo mismo no provee autenticación y seguridad; espera que el protocolo SSH lo asegure.

El modo SCP es un protocolo simple que deja al servidor y al cliente tener múltiples conversaciones sobre una TCP normal. Este protocolo está diseñado para ser simple de implementar.

El servicio principal de este protocolo es el control del dialogo entre el servidor y el cliente, administrando y agilizando sus conversaciones. Para realizar la subida, el cliente le proporciona al servidor los archivos que desea cargar y opcionalmente puede incluir otros atributos (permisos, fechas, etc.) Esto es una ventaja sobre el protocolo FTP (File Transfer Protocol, Protocolo de Transferencia de Archivos).

Para descargar, el cliente envía una solicitud por los archivos que desea obtener. Este proceso está dirigido por el servidor y es el que se encarga de la seguridad del mismo.

La sintaxis es la siguiente:

Copia el cliente del servidor

```
scp usuario@host:directorio/ArchivoOrigen ArchivoDestino
```

Copia desde el servidor al cliente

```
scp ArchivoOrigen usuario@host:directorio/ArchivoDestino
```

2.7 SELECCIÓN DEL SISTEMA OPERATIVO PARA LA IMPLEMENTACIÓN DEL SERVICIO AAA *[18] [19]*

En el mercado actual existe un sinnúmero de sistemas operativos para todos los gustos, para todas las aplicaciones, para todo el mundo, y en el momento de elegir tal o cual sistema operativo el usuario elige el que se preste más a las necesidades.

2.7.1 ANÁLISIS Y SELECCIÓN DE LA PLATAFORMA PARA LA IMPLEMENTACIÓN DEL SERVIDOR AAA

Para la implementación del servicio AAA se analizarán dos sistemas operativos que lo soporten y de acuerdo a las necesidades de la institución se realizará la respectiva selección.

Los sistemas operativos a analizarse son:

- GNU/Linux RED-HAT
- GNU/Linux DEBIAN

2.7.1.1 GNU/Linux RED-HAT *[20]*

Desde la introducción de Red Hat Linux en 1994, Linux y Red Hat han dado pasos de gigante. Actualmente se certifica el soporte para cualquier tipo de plataforma hardware, mayor fiabilidad del sistema y el uso creciente de Linux por parte de muchísimas empresas en todo el mundo.

Linux sigue siendo un sistema operativo desarrollado por muchas personas en todo el mundo incluso Linus Torvalds continua formando parte de este proyecto. Red Hat continua teniendo su base operativa en Carolina del Norte, donde sigue desarrollando aplicaciones para hacer que el uso de Linux sea más sencillo.

Red Hat Enterprise Linux proporciona soporte para las aplicaciones tanto nuevas como existentes, productos de middleware[9] más recientes, arquitecturas de software en la nube y estructuras de tiempo de ejecución nuevas. Pero Red

[9] Middleware.- es un software de conectividad que ofrece un conjunto de servicios que hacen posible el funcionamiento de aplicaciones distribuidas sobre plataformas heterogéneas.

Hat ofrece muchos más que una interfaz universal para aplicaciones. Red Hat Enterprise Linux es un entorno con tendencia dominante básico para el desarrollo de servicios, procedimientos y políticas de centros de datos. Red Hat Enterprise Linux permite el gobierno y gestión de identidades, es una pila de aplicaciones web con gran capacidad de respuesta, flexible y completa y, además, garantiza una gestión eficaz de las puntuaciones de los servidores y el almacenamiento masivo.

Red Hat es posiblemente la distribución más popular de Linux disponible para el mercado del servidor. Red Hat es instalado con un ambiente gráfico llamado Anaconda, diseñado para facilitar el uso a usuarios que no tienen experiencia en este tipo de sistema operativo. También incorpora una herramienta llamada Lokkit para configurar las capacidades de Cortafuegos.

Es una distribución Linux creada por Red Hat, que fue una de las más populares en los entornos de usuarios domésticos.

Algunos fabricantes sólo tienen garantía que su software en Linux funcione en esas distribuciones.

2.7.1.1.1 Características

- Las numerosas mejoras del instalador simplifican la configuración del sistema.
- Programa de actualización basado en Yum/Pup para Red Hat Network.
- Las mejoras de escritorio brindan herramientas actualizadas de configuración, aplicaciones y soporte de laptop.
- Soporte multimedia integrado.
- Network Manager brinda una configuración de red automática con cables (wired) y sin cables (wireless).
- Amplia variedad de soporte para hardware nuevo.
- Soporte para procesadores multi-core.
- Soporte a la virtualización y herramientas de administración KVM virt-manager y libvirt/virsh. Para el funcionamiento de KVM mínimo se debe contar con 2 GB de memoria RAM para la interacción de los host húesped con el kernel y 10 GB de disco duro para almacenamiento.

- Las suscripciones para máquinas virtuales se contrata individualmente o paquetes de 4 y 100 hosts huéspedes según la necesidad.
- Sistema-RPM de empaquetado integrado.
- Los requerimientos mínimos para la instalación son: Procesador X86_64, memoria RAM 512 MB, disco duro 5 GB.

2.7.1.2 GNU/Linux DEBIAN *[21]*

Debian fue creado por Ian Murdock en 1993, inicialmente bajo el patrocinio del proyecto GNU (GNU's Not Unix, GNU no es Unix) de la FSF (Free Software Fundation, Fundación de Software Libre). En la actualidad, los desarrolladores de Debian consideran su trabajo como un descendiente directo del proyecto GNU.
Debian GNU/Linux, también es base para otras múltiples distribuciones de Linux como Knoppix, Linspire, MEPIS, Xandros y la familia Ubuntu. Además, Debian es conocido por su sistema de gestión de paquetes (especialmente APT[10]), por sus estrictas políticas con respecto a sus paquetes y la calidad de sus lanzamientos.
Estas prácticas permiten fáciles actualizaciones entre lanzamientos, y una instalación y desinstalación sencilla de paquetes. Es desarrollado por voluntarios de todo el mundo, y apoyado por donaciones a través de la "Software in the Public Interest", una organización sin fines de lucro para el apoyo de proyectos de software libre.

2.7.1.2.1 Características

- Completo: Debian incluye más de 15180 paquetes de software en la actualidad. Los usuarios pueden seleccionar qué paquetes instalar de acuerdo a su necesidad; Debian provee una herramienta para ese fin. Este sistema operativo posee una lista de los paquetes actualmente disponibles con las descripciones en cualquiera de sus sitios réplica.
- Libre para utilizar y redistribuir: No se requiere ninguna clase de cuota para ser socio de ningún consorcio, ni pago solicitado para participar en su distribución y desarrollo. Todos los paquetes que formalmente son parte de Debian GNU/Linux son libres para ser redistribuidos, normalmente bajo los términos especificados por la Licencia Pública General de GNU.

[10] APT.- Advanced Packaging Tool

Los archivos FTP de Debian también tienen aproximadamente 220 paquetes de software en los directorios non-free y contrib de los archivos FTP, los cuales se distribuyen bajo términos específicos que se incluyen con cada paquete.

- Los requerimientos mínimos de instalación sin entorno gráfico son: Procesador X86_64, memoria RAM 128 MB, disco duro 1 GB.
- Dinámico: Con alrededor de 1570 voluntarios constantemente contribuyendo con código nuevo y mejorado, Debian continua evolucionando constantemente. Se planea realizar nuevas entregas cada varios meses, y los archivos FTP se actualizan diariamente.
- Soporte de virtualización utilizando XEN-Hypervisor, el mismo que necesita mínimo 512 MB para la interacción entre máquinas virtuales y el kernel, y 3 GB de almacenamiento para alojamiento de huéspedes.

Debian GNU/Linux en sí mismo es software libre además de ser una base sobre la cual se pueden construir distribuciones de Linux con valor añadido. Al proveer un sistema base completo y fiable, Debian proporciona a los usuarios de Linux un alto grado de compatibilidad y permite a los creadores de distribuciones de Linux eliminar la duplicación de esfuerzos y enfocar su trabajo en aquellas cosas que hacen especial su distribución.

2.7.1.2.2 Diferencias con otras distribuciones Linux

- El sistema de mantenimiento de paquetes de Debian: todo el sistema, o cualquier componente individual, puede actualizarse sin reformatear, sin perder los ficheros de configuración con las personalizaciones, y en la mayoría de los casos sin reiniciar el sistema. La mayoría de las distribuciones de Linux disponibles en la actualidad tienen alguna clase de sistema de mantenimiento de paquetes; el sistema de paquetes de Debian es único y particularmente robusto.

- Desarrollo abierto: Mientras que otras distribuciones son el producto del desarrollo de individuos, pequeños grupos cerrados, o vendedores comerciales, Debian es la única distribución de Linux que está siendo

desarrollada cooperativamente por muchos individuos a través de Internet, en el mismo espíritu de Linux y otros paquetes de software libre.

Más de 1570 voluntarios encargados de mantener paquetes trabajan en más de 15400 paquetes y mejoran Debian GNU/Linux. Los desarrolladores Debian no escriben nuevo software en la mayoría de los casos, sino que contribuyen empaquetando software existente de acuerdo a las normas del proyecto, comunicando los informes de bugs a los desarrolladores originales, y suministrando soporte a los usuarios.

- El Sistema de Seguimiento de Bugs: La dispersión geográfica de los desarrolladores Debian requiere de herramientas sofisticadas y de una comunicación rápida de los bugs y sus enmiendas para acelerar el desarrollo del sistema. Cuando se presenta algún inconveniente, los usuarios envían los bugs a la comunidad, y los mismos se hacen fácilmente accesibles a través de archivos en la WEB o mediante correo electrónico.

- Las normas de Debian: Solamente Debian dispone de especificaciones extensivas de sus estándares de calidad, las normas de Debian (Debian Policy). En ese documento se encuentran definido las calidades y estándares bajo las cuales se mantienen los paquetes Debian.

2.7.1.3 Tabla comparativa entre los sistemas operativos propuestos

En la *Tabla 5* se realiza un análisis comparativo de los sistemas operativos propuestos para la implementación del presente proyecto.

Tabla 4. Comparación de sistemas operativos
Fuente: Carlos Plasencia

Característica	GNU/Linux RED HAT	GNU/Linux DEBIAN
Memoria mínima	512 MB	256 MB
Capacidad de disco mínimo	5 GB	1 GB
Soporte de hardware certificado	SI	NO
Instalación sencilla	SI	SI
Licencia de suscripción	SI	NO
Virtualización	KVM	XEN
Memoria mínima para virtualización	2 GB	512 MB
Disco mínimo para virtualización	10 GB	3 GB
Licencia por cada host huésped	SI	NO
Soporte para Bugs	Compania	Contribuyentes

De la tabla analizada entre el sistema operativo RED HAT y el sistema operativo Debian se concluye que los dos sistemas operativos tienen similares características, con la diferencia que RED HAT Linux posee licencias de suscripción para reportes de bugs y actualizaciones además de certificación de hardware.

Para el presente proyecto se ha optado por el sistema operativo GNU/LINUX DEBIAN para la implementación tanto del servidor AAA como los firewalls de seguridad debido a las siguientes características:

1. Del sistema Operativo:
    - Instalación sencilla.

- Posee una gran cantidad de elementos de software diferentes (paquetes).
- Es una distribución totalmente free[11].
- Código fuente abierto.
- Fácil de actualizar.
- Seguimiento de actualizaciones.
- Estabilidad.
- Rápido y ligero en memoria.
- Buena seguridad del sistema.
- Software de seguridad.
- Posee drivers para compatibilidad con el hardware.
- El soporte es apoyado por la comunidad a nivel mundial.
- Soporta Virtualización.
- XEN es muy rápido y necesita pocos recursos.
- No se necesita de entorno gráfico para los servicios a instalarse.

2. De los usuarios:
   - Con el fin de manejar un estándar de software libre.
   - Equipos robustos requieren software robusto.
   - Seguridad de la información.
   - Por el decreto nacional 1014 para el uso de software libre.

2.7.2 FREERADIUS *[22]*

FreeRadius es un servidor RADIUS de código abierto, rápido, flexible, configurable, con soporte de protocolos de autenticación y gran cantidad de plataformas. Además, permite autenticar usando su base propia de usuarios o puede usar bases externas como mysql, LDAP o postgresql. Este servidor fue liberado bajo GNU/GPL (General Public License, Licencia General Pública), lo que quiere decir que este software es libre de ser descargado e instalado por

[11] Free.- De código Abierto y totalmente gratuito.

cualquier persona. En este proyecto se integrará con una base de datos externa LDAP.

RADIUS es uno de los protocolos más ampliamente utilizados para realizar la gestión del acceso a redes de área extensa, sobre todo en el ámbito de los ISP (Internet Service Provider, Proveedor de Servicio de Internet). Sin embargo, en la actualidad es una herramienta robusta para el control de acceso a redes wireless. En el presente proyecto se utiliza para controlar el acceso de usuarios tanto a la red cableada como a la red wireless y está centrado principalmente en el uso de EAP-PEAP como protocolo de autenticación y en la definición básica de usuarios.

FreeRADIUS es un producto compuesto tanto por una base de datos de usuarios como por un servidor capaz de atender peticiones de autenticación realizadas por otros elementos de la red.

2.7.3 VIRTUALIZACIÓN *[23]*

El hardware de computadores y servidores vienen diseñados para ejecutar un solo sistema operativo y una única aplicación lo que hace que sus recursos estén subutilizados. La virtualización permite la ejecución de múltiples máquinas virtuales sobre una máquina física, con cada una compartiendo los mismos recursos (como memoria RAM, disco duro, interfaces de red) del equipo físico. Diferentes máquinas virtuales pueden ejecutar múltiples aplicaciones sobre el mismo equipo físico.

Existen dos formas de virtualizar:

1. Virtualización completa.- Cada servidor virtual se ejecuta aislado de los demás haciendo uso de sus recursos asignados.
2. Paravirtualización.- Las instrucciones de la máquina virtual se ejecutan directamente en el procesador físico ya que comparten el mismo kernel y por tanto las instrucciones se ejecutan más rápido consumiendo menos recursos.

2.7.3.1 Funcionamiento

Mediante la utilización software especial es posible virtualizar los recursos de un equipo (incluyendo CPU, RAM, discos duros e interfaces de red) para crear una máquina virtual completamente funcional que pueda ejecutar su propio sistema operativo y aplicaciones tal como una computadora “real”. Cada máquina virtual está completamente aislada de las demás y disociada del host subyacente por una fina capa de software conocida como el hypervisor. Esto permite que cada máquina virtual ejecute diferentes sistemas operativos y aplicaciones. Debido a que las máquinas han sido disociadas del hardware del host subyacente, pueden moverse desde un servidor físico a otro sin inconvenientes facilitando el proceso de clonación y migración.

2.7.3.2 Ventajas y desventajas

Ventajas

- Ahorra reinicio del hardware en caso de que se tenga que reiniciar una máquina virtual.
- Permite lanzar varios sistemas operativos diferentes en una misma máquina física si es virtualizada completamente o múltiples máquinas virtuales con el mismo sistema operativo en el caso de la paravirtualización.
- Facilita la administración de los sistemas operativos virtualizados ya que se tiene una administración centralizada.
- Se puede implementar máquinas virtuales de prueba sin interrumpir el funcionamiento de las máquinas que están en producción.
- Migración dinámica de aplicaciones y servicios.
- Ahorro de costes de Hardware y alojamiento de equipos.
- Mantenimiento independiente de cada servidor. Si una máquina falla las demás siguen funcionando normalmente.
- Aprovechamiento de recursos.
- Ahorro en consumo de energía.

- Flexibilidad al poder crear las máquinas virtuales con las características de CPU, memoria, disco y red que sea necesario, sin necesidad de comprar un equipo con esas características.
- Agilidad al momento de crear una máquina virtual, porque es un proceso muy rápido, básicamente la ejecución de un comando. Por tanto, si se necesita un nuevo servidor se lo puede tener casi al instante.
- Recuperación rápida en caso de fallo, si se dispone de una copia de los ficheros de configuración de la máquina virtual, en caso de desastre la recuperación será muy rápida, simplemente arrancar la máquina virtual con los ficheros de configuración guardados. No es necesario reinstalar, recuperar backups y otros procedimientos largos que se aplican en las máquinas físicas.

Desventajas

- Reduce el performance del equipo ya que se aumenta una capa más de software para la virtualización (hypervisor).
- Compatibilidad de hardware, si el equipo no es soportado por el hypervisor, no puede ser virtualizado.
- Mala administración, crear máquinas innecesarias consumen recursos.
- Daños de hardware, si falla cualquier componente físico interrumpe el trabajo de todas las máquinas alojadas sobre el servidor.
- El sistema operativo base se vuelve crítico, por lo que la seguridad de este es vital, así como evitar reinicios innecesarios que hace que todas las máquinas virtuales que se alojan puedan quedar fuera de servicio. El reiniciar ya no es la solución, como quizás muchas veces lo es.

Como se pudo ver en la sección anterior existen muchas ventajas frente a pocas desventajas, entonces, una opción para aprovechar los recursos es la virtualización, pero no hay que olvidar los riesgos que conlleva la implementación.

2.8 IMPORTANCIA DE LA ALTA DISPONIBILIDAD *[24]*

Actualmente, los servicios asociados a fallas de las TI (Tecnology Infraestructure, Infraestructura Tecnológica) pueden tener consecuencias en la interrupción de la operación normal de las actividades de los usuarios, por lo que es fundamental contar con arquitecturas que incorporen el concepto de alta disponibilidad.

La alta disponibilidad (High Availability) es una arquitectura de diseño del sistema y la implementación está asociada a asegurar la continuidad operacional de los servicios. La disponibilidad se refiere a: continuidad de acceso a sistemas y poder realizar nuevos trabajos, actualizar o alterar trabajos existentes o recoger los resultados de trabajos previos. Si un usuario no puede acceder al sistema, se dice que está no disponible, el servicio se encuentra interrumpido. El término tiempo de inactividad (downtime) es usado para definir cuándo el sistema no está disponible y es un parámetro que sirve para definir los tiempos de recuperación del servicio.

La falla de un sistema o servicio puede producir pérdidas en la productividad de los procesos gestionados por la institución. Por esta razón es necesario identificar los servicios críticos para establecer los medios y medidas para evitar incidentes o restablecer el servicio en caso de producirse un evento inesperado que interrumpa la operación normal en el tiempo mínimo.

La alta disponibilidad ofrece la continuidad de operación sobre los recursos de información por la mayor cantidad de tiempo posible, reduciendo los tiempos de interrupción de servicio.

2.8.1 CAUSAS PARA LA INTERRUPCIÓN DE SISTEMAS O SERVICIOS

Las interrupciones de un servicio o sistema pude producirse por las siguientes causas:

- Físicas (de origen natural o delictivo)
    - Desastres naturales (inundaciones, terremotos, incendios)
    - Ambiente (condiciones climáticas adversas, humedad, temperatura)
    - Fallas materiales
    - Fallas de la red
    - Cortes de energía
    - Falla de hardware

- Humanas (intencionales o accidentales):
    - Error de diseño (errores de software, aprovisionamiento de red insuficiente).
    - Desconocimiento en el manejo del servicio o sistema.
    - Con intenciones perjudiciales

- Operativas
    - Errores en el software
    - Falla del software

2.8.2 BENEFICIOS DE LA ALTA DISPONIBILIDAD

El esquema de alta disponibilidad en TI brinda beneficios como los siguientes:

- Mantener la continuidad de servicio ante fallas en el equipamiento y bajas programadas.
- Balancear la carga de los usuarios prestando un mejor servicio en condiciones operacionales.
- Cumplir con la continuidad del servicio ante desastres o eventos que afecten su operación normal, principalmente evitando la pérdida o retraso de la ejecución de procesos.
- Reduce las posibles bajas del servicio, reduciendo la pérdida de confianza por parte de los usuarios.

CAPÍTULO III
DISEÑO DEL SERVIDOR AAA

3.1 DISEÑO DE LA SOLUCIÓN

De acuerdo a las necesidades de la institución y sus debilidades, la solución que se plantea pretende mejorar los niveles de seguridad.
La seguridad total es inalcanzable, pero se puede reducir al máximo las vulnerabilidades.

3.1.1 CONTROL DE ACCESO DE USUARIOS

Debido a la inexistencia de esquemas de control de acceso de los usuarios que acceden a la red, la solución implementada ha tomado en cuenta algunos aspectos importantes como:

- Los equipos de parte activa son de la marca 3Com y soportan el estándar 802.1X.
- El uso del sistema operativo Microsoft Windows XP en los usuarios de la institución es estándar. Esta característica facilita la integración de la solución ya que IEEE 802.1X es nativo para este sistema operativo.
- La institución cuenta con una base de datos centralizada de usuarios LDAP.
- La institución dispone de hardware para la implementación de servicios.

El control de acceso de los usuarios hacia la infraestructura de networking se realiza mediante la utilización del estándar 802.1X. En el siguiente esquema se presenta la integración de la solución AAA implementada en la red interna de la institución:

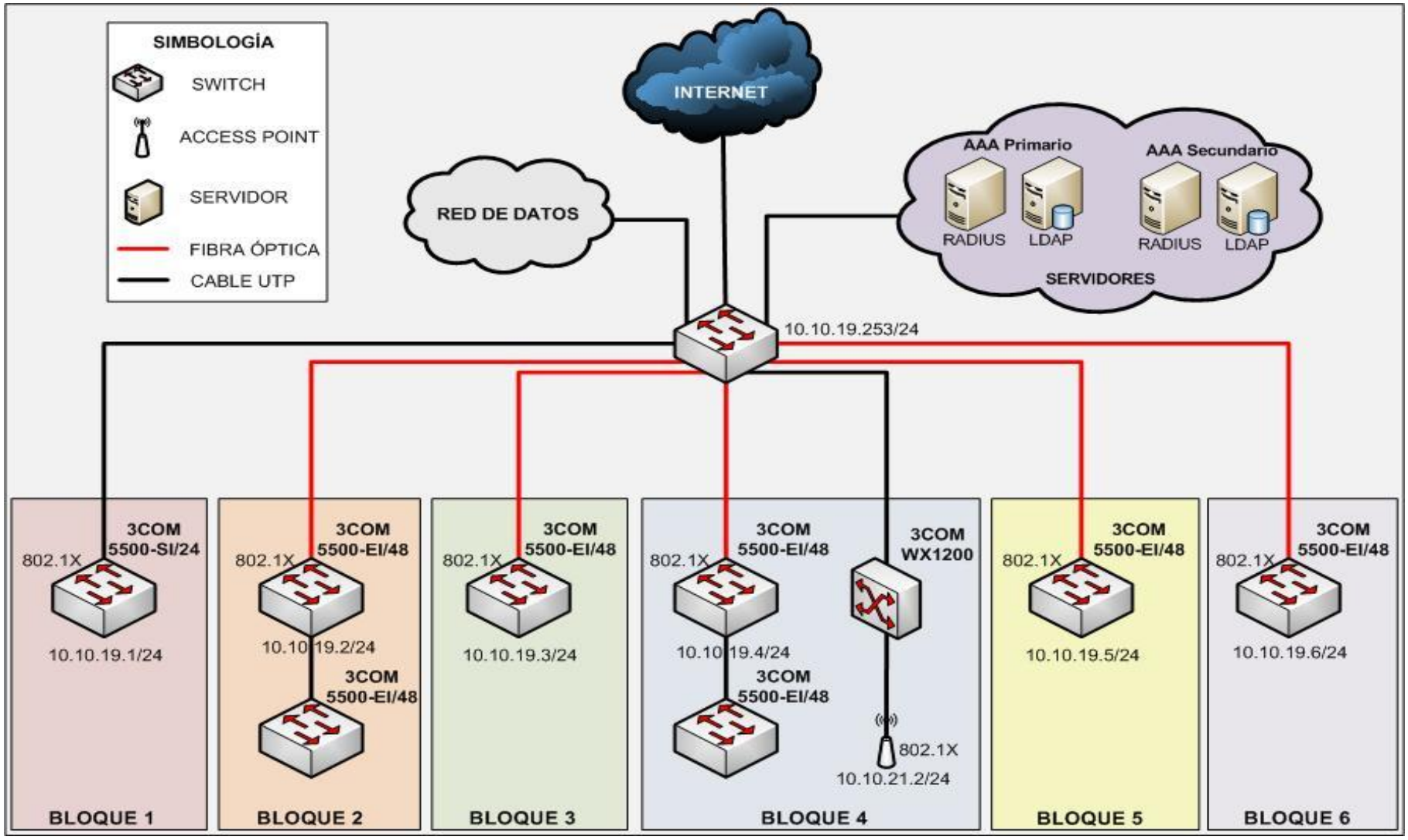


Figura 8. Integración del servidor AAA en la red LAN
Fuente: Carlos Plasencia

3.1.1.1 Descripción

Como se puede observar en la *Figura 8*, el diseño implementado consta de un servidor AAA primario y de un servidor AAA secundario, cada servidor cuenta con su propia base de datos de autenticación de usuarios LDAP. El servidor AAA primario autentica contra la base de datos LDAP-Master y el servidor AAA secundario autentica contra la base de datos LDAP-Slave. Estas bases de datos se encuentran sincronizadas y todos los cambios que se realice en el LDAP-Master se replican automáticamente hacia el LDAP-Slave. Se debe tomar en cuenta que los datos se pueden modificar sólo en el LDAP-Master porque solamente éste tiene privilegios de escritura sobre la base, mientras el LDAP-Slave tiene privilegios sólo de lectura.

Al tener el esquema Master-Slave de la base de datos se evita que exista inconsistencia en los datos.

El Protocolo Ligero de Acceso a Directorios es visto como un repositorio en donde se guarda información que posteriormente se accede a consultarla. Este tipo de Base de datos se utiliza para centralizar información como por ejemplo: usuarios, contraseñas, certificados digitales, cuentas de correo, etc.

En el presente proyecto se utiliza el LDAP existente de la institución para acceder a realizar las consultas de nombres de usuarios y contraseñas para habilitar el acceso mediante el servidor AAA.

El LDAP existente tiene almacenado alrededor de 300 usuarios y contraseñas utilizados para la autenticación del servicio de correo y de la mesa de servicios (Help-desk). El esquema con el que trabaja el LDAP está basado en atributos samba, dado a que ciertas máquinas pertenecen a un Dominio que está controlado por un PDC (Primary Domain Controller, Controlador Primario de Dominio).

La estructura del LDAP es la siguiente:

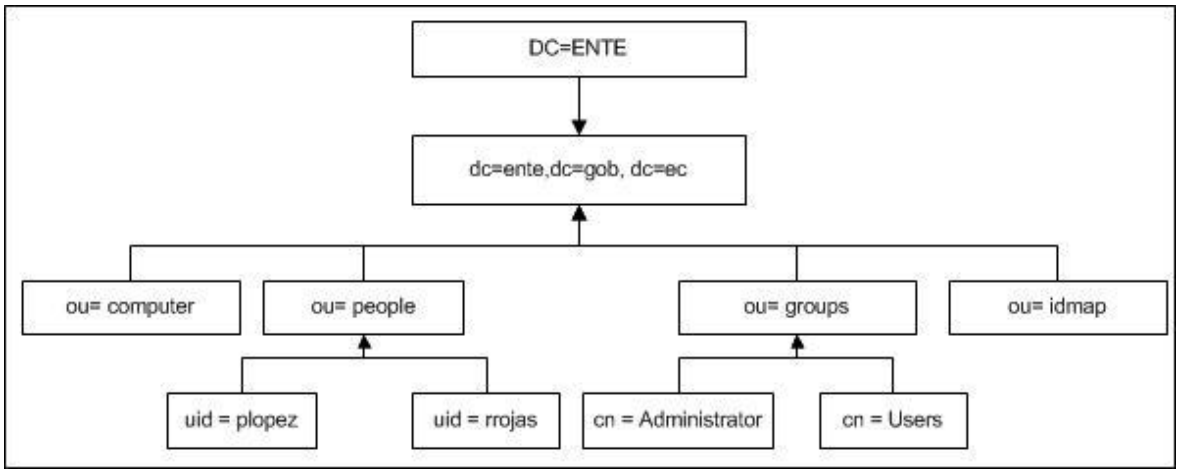


Figura 9. Estructura del LDAP de la institución
Fuente: Carlos Plasencia

Componentes de la base de datos LDAP:

- dc.- Componente de dominio. El nombre del reino LDAP de la institución está compuesta por: dc=ente,dc=gob,dc=ec.
- ou.- Unidad organizativa. Son subdominios de la estructura LDAP.
- uid.- ID de usuario. Parámetro de identificación única de los usuarios.
- cn.- Nombre Común.

Las contraseñas de los usuarios están encriptadas mediante el algoritmo MD5 por lo tanto se evita que se guarden en claro y no sea legible para el usuario que accede a la Base.

El formato de las contraseñas se ajusta de acuerdo a las políticas del SGSI mencionadas en el capítulo I en la sección 1.2.2.1.

La información del usuario consiste en el mapeo entre sus números de identificación y sus nombres. La consulta de los recursos es manejada por el subsistema del Servicio de Conmutación de Nombres (NSS, Name service Switch). La autenticación, es el chequeo de las contraseñas, ésta es manejada por el subsistema PAM (Plugable Authentication Module, Módulo flexible de

autenticación). Estos dos subsistemas se configuran de forma separada, pero son necesarios para trabajar con LDAP.

La lista de usuarios de la institución existentes en la base LDAP se presenta en el ANEXO 1.

Los servidores AAA se instalarán en la zona de servidores debido a lo siguiente:

- Para la autenticación de los clientes, simplemente es necesario que exista la interacción entre el autenticador (equipos de acceso) y el servidor AAA, y entre el suplicante y el servidor AAA.
- Para aprovechar la infraestructura BLADE, es la más robusta en la actualidad por el ahorro de energía, utilización de poco espacio y capacidad de aumentar servidores (cuchillas) según la capacidad (14 o 16).
- El ambiente en el que se desarrollará el servidor es virtualizado, para optimizar al máximo los recursos de hardware.

El esquema de implementación es redundante ya que es uno de los servicios más críticos de la institución. Si por algún motivo el servidor AAA primario no estuviese disponible, ningún usuario de la red interna LAN podría acceder a los servicios de red, y por lo tanto causaría la interrupción en la operación de sus actividades.

El estándar 802.1X se configura en el equipo cliente para que los usuarios se autentiquen con el nombre de usuario y contraseña luego de iniciar la sesión.

En los switch 3Com 5500 que conforman la capa de acceso a la red se configura el estándar 802.1X para interactuar entre los usuarios y el servidor AAA de autenticación. En todos los equipos de acceso se configura tanto la dirección IP del servidor AAA primario como la dirección IP del servidor AAA secundario para obtener alta disponibilidad del servicio.

3.1.2 ARQUITECTURA 802.1X IMPLEMENTADA EN LA INSTITUCIÓN

Los atributos de las tramas que se utilizan en el proceso de autenticación de los usuarios de la institución se muestran en el siguiente grafico:

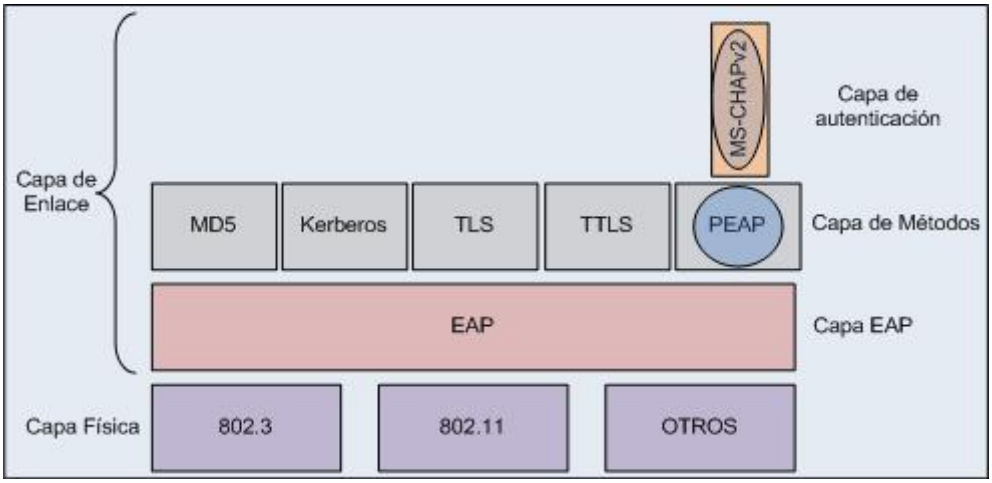


Figura 10. Arquitectura implementada
Fuente: http://blogs.technet.com/davidcervigon

El método EAP que se utiliza para realizar la autenticación de los usuarios es PEAP.

3.1.2.1 Protocolo EAP-PEAP *[25]*

El Protocolo de autenticación extensible protegido (PEAP) es miembro de la familia de protocolos de EAP. PEAP utiliza Seguridad de nivel de transporte (TLS) para crear un canal cifrado entre un cliente de autenticación PEAP, como un switch de acceso o un equipo inalámbrico, y un servidor de autenticación PEAP, como un servicio RADIUS. PEAP no especifica un método de autenticación, sino proporciona seguridad adicional para otros protocolos de autenticación de EAP, como EAP-MSCHAPv2, que pueden operar a través del canal cifrado de TLS que proporciona PEAP.

Para mejorar los protocolos EAP y la seguridad de red, PEAP proporciona:

- Protección de la negociación del método EAP que se produce entre el cliente y el servidor mediante un canal TLS. Esto ayuda a impedir que un intruso inserte paquetes entre el cliente y el servidor de autenticación. El canal TLS cifrado también ayuda a evitar ataques de negación de servicio

contra el servidor RADIUS ya que para cada intercambio de tramas maneja un campo identificador.

- Autenticación mutua entre el servidor RADIUS y clientes inalámbricos que tienen capacidad de autenticar al servidor.
- Protección contra la implementación de un equipo de acceso no autorizado cuando el cliente EAP autentica el certificado que proporciona el servidor RADIUS y la verificación del secreto compartido.

Comunicación autenticada por EAP

El servidor RADIUS autentica al usuario y al equipo cliente con el método que determina el tipo de EAP que se ha seleccionado para utilizar en PEAP (EAP-TLS o EAP-MS-CHAPv2). El cliente sólo reenvía mensajes entre el usuario y el servidor RADIUS; el cliente (o una persona que lo supervise) no puede descifrar estos mensajes porque no es el extremo TLS.

Implementaciones con PEAP

Se puede elegir entre dos tipos de EAP para usar con PEAP: EAP-MS-CHAPv2 o EAP-TLS. EAP-MS-CHAPv2 usa credenciales (nombre de usuario y contraseña) para la autenticación de usuarios, y un certificado del almacén de certificados del equipo servidor para la autenticación del servidor. EAP-TLS utiliza los certificados instalados en el almacén de certificados del equipo cliente o una tarjeta inteligente para la autenticación de usuarios y equipos cliente, y un certificado del almacén de certificados del equipo servidor para la autenticación del servidor.

PEAP con EAP-MS-CHAPv2

PEAP con EAP-MS-CHAPv2 (PEAP-EAP-MS-CHAPv2) es más sencillo implementar que EAP-TLS porque la autenticación de usuarios se realiza con credenciales basadas en contraseñas (nombre de usuario y contraseña) en lugar de certificados o tarjetas inteligentes; sólo es necesario que el servidor RADIUS tenga un certificado.

A continuación se muestra la arquitectura 802.1X usada para la red wireless:

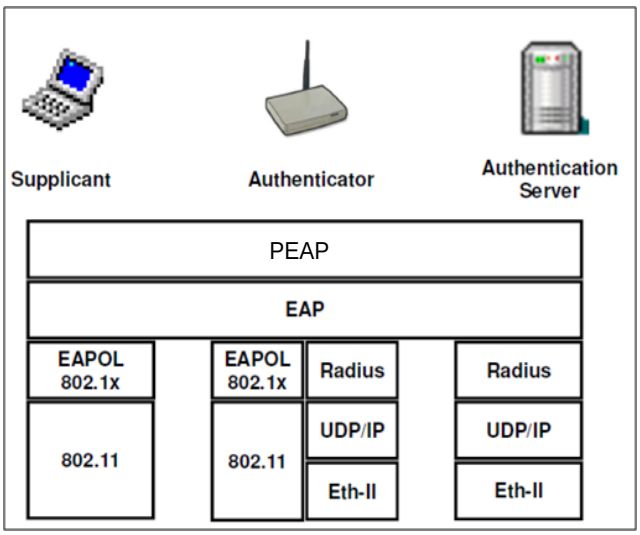


Figura 11. Arquitectura EAP en la red wireless
Fuente: http://www.tlmat.unican.es/siteadmin/submaterials/518.pdf

3.1.3 FUNCIONAMIENTO DE LA IMPLEMENTACIÓN

El esquema de funcionamiento se muestra en la *Figura 12*:

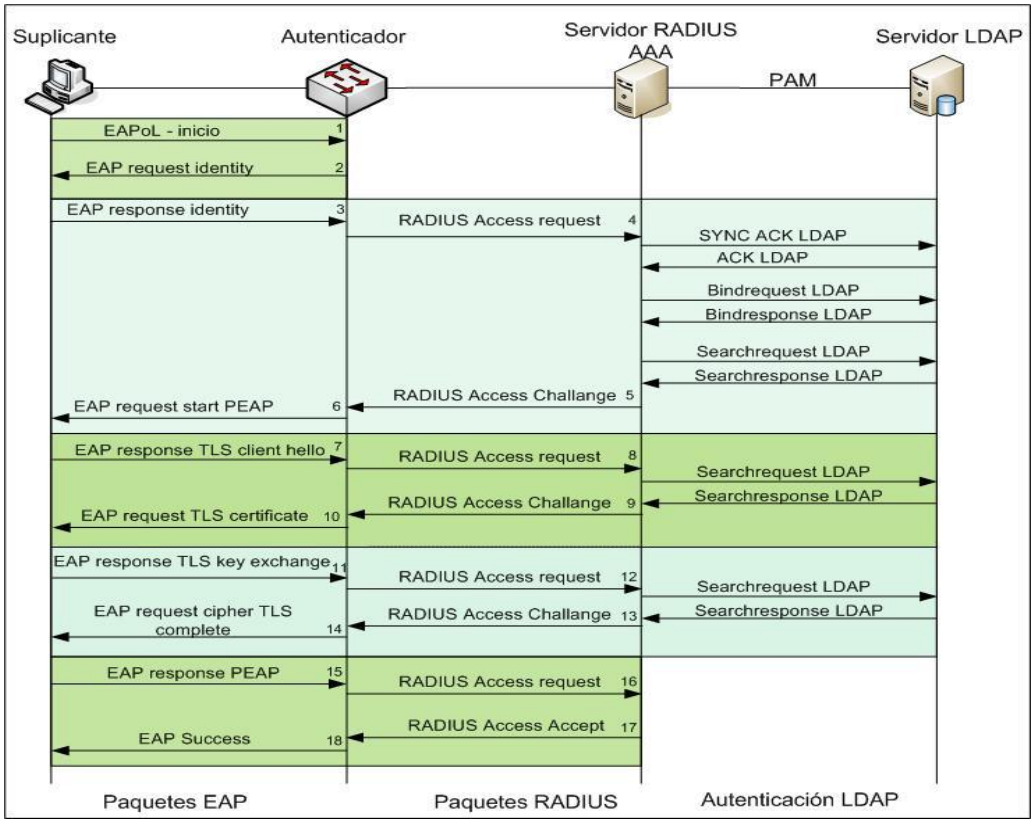


Figura 12. Funcionamiento del Sistema AAA
Fuente: Carlos Plasencia

1. El suplicante inicia solicitando conexión de red. Para darle acceso al usuario se iniciará el proceso de autenticación enviando un mensaje EAPoL de inicio hacia el equipo de acceso (Switch o AP).

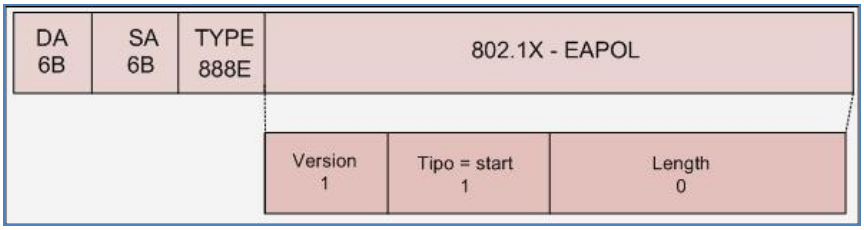


Figura 13. Trama EAPoL de inicio
Fuente: Capturas con wireshark

2. El autenticador envía un mensaje de solicitud de identidad al usuario.

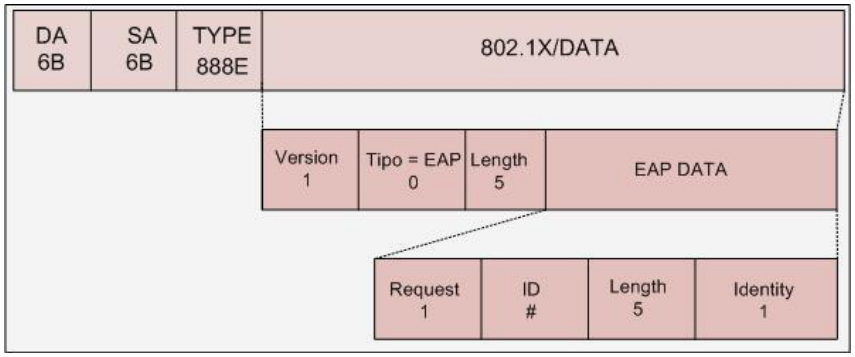


Figura 14. Trama EAP request identity
Fuente: Capturas con wireshark

3. El usuario envía un EAP de identidad al autenticador.

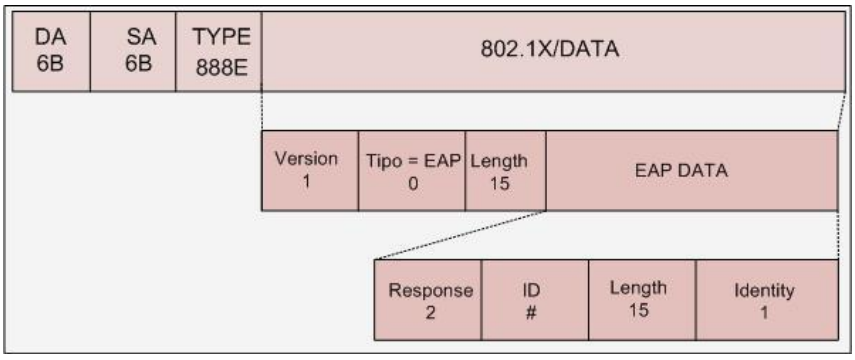


Figura 15. Trama EAP response identity
Fuente: Capturas con wireshark

4. La trama EAP response identity se encapsula en un mensaje RADIUS y el autenticador envía un mensaje de petición de acceso al servidor RADIUS.

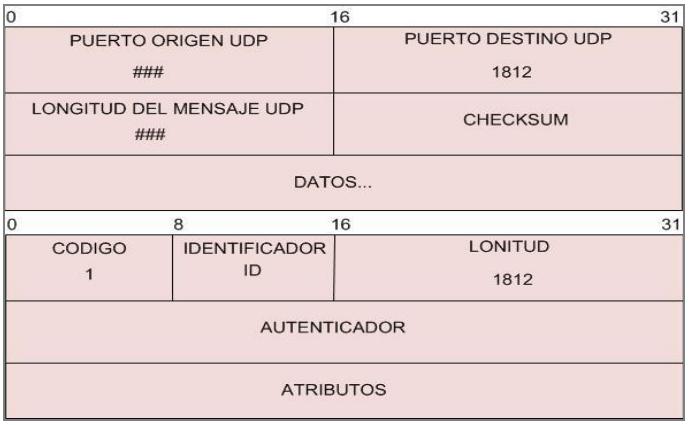


Figura 16. Mensaje RADIUS-Request
Fuente: Capturas con wireshark

Una vez que llega el mensaje RADIUS-request al servidor, la identidad del usuario es consultada en la base de datos LDAP mediante conexiones TCP al puerto 389. Para que el servidor RADIUS pueda consultar la base primero se autentica con las credenciales de la cuenta configurada en el módulo LDAP de RADIUS (bindrequest[12]/bindresponse[13]) y luego se procede a realizar comandos de búsqueda para verificar la autenticidad del usuario (searchrequest[14]/searchresponse[15]).

5. El servidor RADIUS inicia la negociación del método EAP que se utilizará para el establecimiento del canal seguro enviando una trama RADIUS Access-challenge.

[12] Bindrequest.- Solicitud de autenticación al servidor LDAP.
[13] Bindresponse.- Respuesta satisfactoria o fallida de autenticación.
[14] Searchrequest.- Petición de búsqueda en la base LDAP.
[15] Searchresponse.- Respuesta satisfactoria o fallida de la búsqueda.

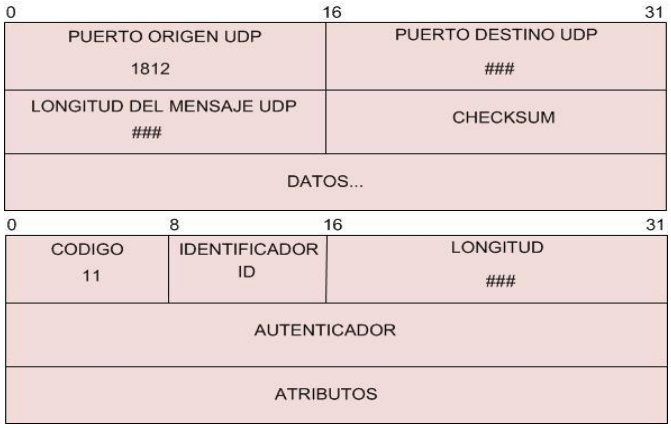


Figura 17. Mensaje RADIUS-Challenge
Fuente: Capturas con wireshark

6. El autenticador envía al usuario un EAP con petición de establecimiento de canal con EAP de tipo PEAP.

Figura 18. Trama de establecimiento del método PEAP
Fuente: Capturas con wireshark

7. El usuario negocia el método de la conexión y envía al autenticador un EAP de respuesta con el saludo para establecimiento del canal TLS (client hello).

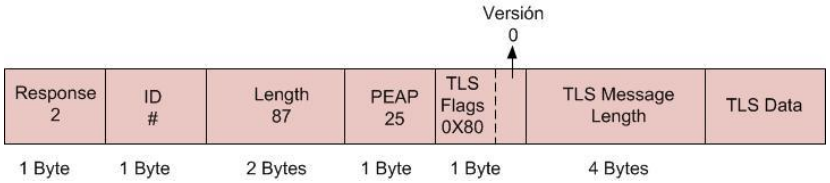


Figura 19. Trama EAP-Response TLS
Fuente: Capturas con wireshark

8. EL autenticador encapsula el mensaje EAP-Response en un mensaje RADIUS-request y lo envía al servidor (*Figura 16*).

9. EL servidor verifica el mensaje enviado por el usuario y le responde con su certificado en un mensaje RADIUS-Challenge. El mensaje contiene un server hello[16] + server certificate[17] + server hello done[18] (*Figura 17*).

10. El autenticador recibe el mensaje RADIUS y envía el certificado del servidor al usuario en un EAP-request TLS de credencial del usuario.

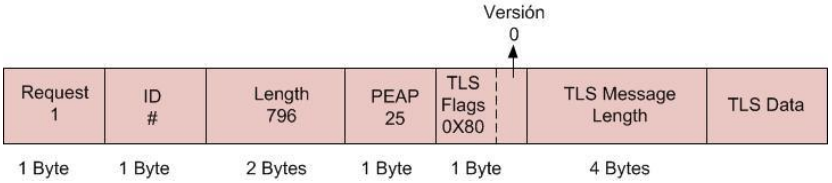


Figura 20. Trama EAP-Request TLS
Fuente: Capturas con wireshark

11. El usuario responde un mensaje EAP intercambiando la contraseña en el canal cifrado. El mensaje EAP-response TLS contiene el client key Exchange[19], change cipher spec[20] y encrypted handshake message[21].
12. La trama EAP-Response TLS se encapsula en un mensaje RADIUS-Request y se envía al servidor RADIUS, el mensaje llega encriptado con la contraseña del usuario y es verificada en la base de datos LDAP.

13. El servidor responde
    a. Si la contraseña del usuario es correcta el servidor responde con un mensaje RADIUS-Challange para finalizar el establecimiento del canal TLS.
    b. Si las credenciales no son correctas rechaza la conexión (RADIUS-Reject) y el puerto del switch al que se conecta el usuario se pone en estado down.
14. El autenticador recibe un RADIUS-Challange para finalizar de establecer el canal TLS y le envía al usuario un EAP-Request de canal cifrado completo.

[16] Server hello.- Saludo del servidor en respuesta de un client hello.
[17] Server certificate.- Certificado del servidor.
[18] Server hello done.- Fin del saludo del servidor. Termina la primera fase del dialogo.
[19] Client key Exchange.- Intercambio de clave del cliente.
[20] Change Cipher Spec.- Existe para señalar transiciones en estrategias de codificación.
[21] Encrypted handshake message.- Negociación de mensaje encriptado.

15. El usuario envía un mensaje EAP-PEAP de respuesta y solicita acceso a la red.

16. La solicitud de acceso a la red es enviara al servidor mediante un mensaje RADIUS-request.

17. El servidor responde con un mensaje de RADIUS-ACCEPT hacia el autenticador.

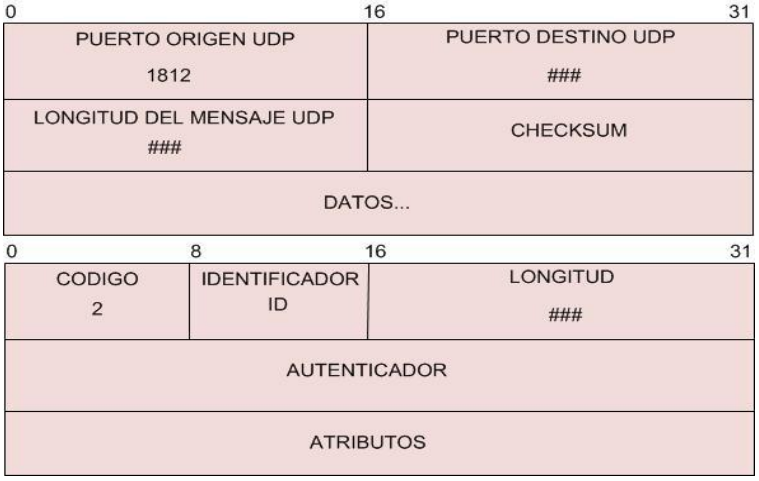


Figura 21. Mensaje RADIUS-ACCEPT
Fuente: Capturas con wireshark

18. El autenticador envía un mensaje EAP-Succsess y el usuario ya se encuentra habilitado para usar los recursos de la red.

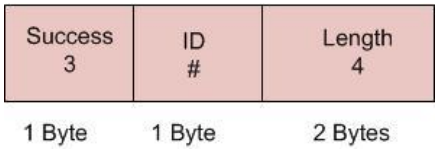


Figura 22. Trama EAP satisfactoria
Fuente: Capturas con wireshark

3.1.4 REQUISITOS DEL SISTEMA PARA LA IMPLEMENTACIÓN 802.1X

Los elementos que conforman la arquitectura de funcionamiento de la integración del servidor AAA con la infraestructura de la institución son:

- Cliente: Windows XP con Service Pack 2 o 3, el uso de éste sistema operativo se encuentra estandarizado en todo el edificio.
- Servicio de autenticación: servidor RADIUS desarrollado en software libre.

- Método de autenticación: EAP-PEAP
- Cifrado usado con PEAP: MSCHAPv2
- Base de datos de autenticación de usuarios: LDAP
- Clientes para autenticación: Switch 3Com 5500-EI
- Clientes para autenticación inalámbrica: AP con soporte del estándar 802.1X.

3.1.5 3Com y 802.1X

La infraestructura 3Com de la capa de acceso de usuarios tiene la capacidad de funcionar como servidor AAA y como cliente. En el presente proyecto todos los switches de acceso serán configurados para trabajar como autenticadores, esto es, la arquitectura AAA está conformada por los suplicantes (usuarios) los que requieren autenticación, autenticadores (switch o AP de acceso) los que interactúan entre el suplicante y el servidor AAA y el Servidor de autenticación en este caso el Servidor AAA (FREERADIUS) el encargado de validar la autenticidad de usuarios que requieren ingresar a la infraestructura de networking.

802.1x define el protocolo para control de acceso a red basado en puerto y sólo define la conexión punto a punto entre el dispositivo de acceso y el puerto de acceso. El puerto puede ser físico o lógico. El entorno de aplicación típico es el siguiente:

1. Cada puerto físico del switch LAN sólo se conecta a la estación de trabajo de usuario (basado en el puerto físico)
2. El entorno de acceso de LAN inalámbrica definidos por el estándar IEEE 802.11 (basado en el puerto lógico).

Los switches de la familia 5500 no solo soportan la autenticación basada en puerto sino también basado en su Dirección MAC, en el presente proyecto se ha implementado basado en puerto.

Una característica importante en estos equipos es que permiten la autenticación de múltiples usuarios por un puerto físico, pero se debe tener en

cuenta que cuando se maneja la asignación dinámica de VLAN, éste método no es práctico ya que el puerto sólo puede pertenecer a una determinada VLAN y no a múltiples VLAN. Por defecto en la configuración del switch viene permitida hasta un máximo de autenticación de 255 usuarios por cada puerto.

Para el presente proyecto los switches de acceso están configurados con las siguientes características:

- 802.1X global habilitado.
- Método de autenticación EAP.
- Método 802.1X basado en puerto para cada interfaz.
- Configuración de servidor AAA primario y secundario.
- Autenticación y autorización mediante el puerto UDP 1812 y Contabilidad a través del puerto UDP 1813 (no aplicada).

3.1.6 DISEÑO DE LA INFRAESTRUCTURA DEL SERVIDOR DE AUTENTICACIÓN

Para la implementación del servidor de autenticación AAA primario se dispone de una cuchilla Intel HS-22 y HS-21 de la infraestructura BLADE, las mismas que tienen las siguientes características:

- Procesador: Intel XEON 3.2 GHz
- Memoria: 32 GB
- Disco Duro: 2 x 140 GB configurados en RAID[22] 1
- Interfaces de red: 2 (10/100/1000)

Las especificaciones técnicas de las cuchillas Intel HS-21 y HS-22 se muestran en el ANEXO2.

[22] RAID.- Redundancy Array of Inexpensive Disks, muestra varios discos físicos como uno lógico.

Esta cuchilla está instalada el sistema operativo Debian la versión estable (Lenny 5.0), y se encuentra paravirtualizada utilizando el hypervisor XEN.

La instalación de un servidor con XEN requiere por lo menos un equipo físico x86, y será dedicado únicamente para hospedar y ejecutar las máquinas virtuales y se recomienda que se dedique el sistema exclusivamente para la ejecución de XEN ya que cualquier otra operación podría afectar tanto el rendimiento del sistema base como de las máquinas virtuales.

Cuando se instala el hypervisor XEN en sistemas x86 de 32-bit (i386) se limita a solo ejecutar VMs de 32-bit. En el presente proyecto el servidor tiene arquitectura de 64-bits, por lo tanto se implementará el Hypervisor XEN de 64-bits, el mismo que tiene soporte para ejecutar máquinas virtuales tanto en 32-bit y 64-bit dependiendo de la necesidad.

Las recomendaciones de Debian para la asignación de uso de memoria RAM es de 512 MB de RAM mínimo para el Domain0 ya que requiere recursos para realizar las operaciones de I/O y comunicación entre el hypervisor y las máquinas virtuales. El servidor disponible cuenta con 32 GB de memoria RAM y por tanto la memoria libre (memoria total menos memoria asignada a VMs) será utilizada por el Domain0 según necesite.

La asignación de disco se recomienda que se dedique por lo menos 20 GB de espacio para el sistema operativo del Domain0, ya que se va a ejecutar XEN en un sistema Linux y no va a usar demasiado espacio, 4GB serían suficientes, sin embargo, se recomienda agregar más espacio para los logs de sistema, archivos de imágenes de sistemas operativos, imágenes ISO, directorio para almacenar el estado (RAM) de las máquinas virtuales, etc.

La configuración de red para el servidor XEN influenciara en el modo de conexión de las máquinas virtuales, la mayoría de modos y dispositivos de red disponibles en un kernel Linux es soportado por XEN, desde interfaces de red

100M/s, 1GB o 10GB Ethernet, Bonding[23] (*Link Aggregation*), VLANs y otros esquemas conocidos pueden ser configurados en el Domain0 para proveer entornos compartidos, seguros y aislados de red para las máquinas virtuales. En este caso se utiliza la interfaz de red eth0 en modo bridge para todas las máquinas virtuales. La interfaz restante queda disponible en caso que se requiera aislar una VM o implementar esquemas de alta disponibilidad mediante la utilización de clústers.

El esquema implementado es el siguiente:

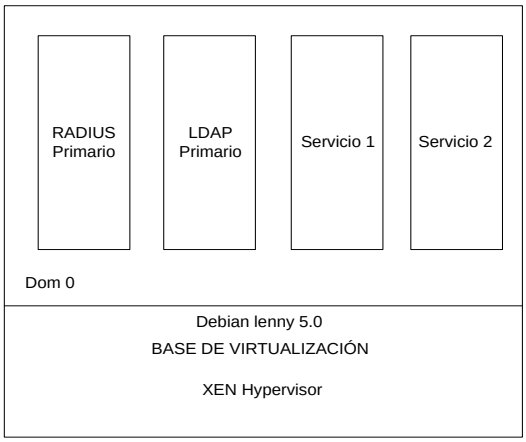


Figura 23. Esquema del Servidor virtualizado para el servicio AAA Primario
Fuente: Carlos Plasencia

La máquina virtual que ejecuta el servicio LDAP tiene asignada los siguientes recursos:

- Memoria: 256 MB son los requerimientos mínimos para funcionar un sistema Debian Lenny, pensando en un crecimiento a gran escala de la base de usuarios se asigna 512 MB.
- Espacio en Disco: Debido a que la base de datos se escribe en archivos de texto plano, los datos de usuarios que se agregan no ocupan mucho espacio, por tal motivo 20 GB son suficientes pensando en crecimientos futuros.

La máquina virtual que ejecuta el servicio RADIUS primario tiene asignado los siguientes recursos:

[23] Bonding.- Configuración de dos interfaces de red para que trabajen como una sola produciendo redundancia con balanceo de carga y tolerancia a fallos en la interface.

- Memoria: los requerimientos básicos para ejecutar una máquina virtual con sistema operativo Debian Lenny es de 256 MB. Los usuarios que se controlan en la institución crecen constantemente, por tal razón está asignada 1 GB de memoria RAM.
- Espacio en Disco: este servidor almacena los registros de los usuarios que acceden a la red, por lo tanto tiene asignado 20 GB de disco.

La implementación del servidor de autenticación AAA secundario se realiza sobre una cuchilla Intel HS-21. Esta cuchilla de igual forma tiene instalado el sistema operativo Debian la versión estable (Lenny 5.0), y también está paravirtualizada.

El esquema de la cuchilla es el siguiente:

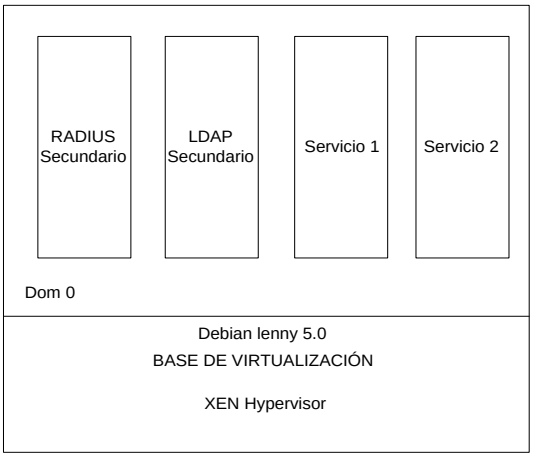


Figura 24. Esquema del Servidor virtualizado para el servicio AAA secundario
Fuente: Carlos Plasencia

Los recursos asignados a las máquinas virtuales que forman parte de la solución RADIUS secundario y LDAP secundario son similares a los servidores LDAP primario y RADIUS primario, estimando que, llegara el momento de entrar en funcionamiento, deberán soportar la misma carga.

3.1.7 CONTROL DE ACCESO A APLICACIONES

Una vez que los usuarios son autenticados y autorizados ya pueden hacer uso de los recursos de la red. Hasta este momento ya se conoce que los usuarios que ingresan a la red son sólo aquellos que están autorizados en la institución, pero se debe tomar en cuenta que no se está teniendo control del acceso hacia las aplicaciones y servicios institucionales.

A lo que se hace referencia es que, desde cualquier máquina de algún usuario por ejemplo, se puede acceder a la administración de cualquier servidor, incluso, desde la red de datos que conforman todos los entes del ministerio se puede acceder sin control alguno.

Si se llevara a cabo una intrusión en uno de los entes del ministerio, fácilmente se vería comprometida la información de la institución.

Con la implementación de un servidor UTM interno que controle el tráfico desde los entes externos hacia los servicios internos de la institución se reduce la posibilidad de obtención de información de manera no autorizada, además se controla el acceso de los usuarios hacia las aplicaciones necesarias para el desarrollo de sus actividades, de igual manera a los usuarios de la red LAN hacia servicios públicos.

Otro de los aspectos importantes en cualquier organización es el control de acceso a internet, y como ya se mencionó en el primer capítulo, en la institución no existe control alguno sobre la navegación, causando problemas de lentitud en la velocidad de conexión ya que los usuarios pueden usar dicho recurso de manera desmedida.

Para mejorar el control de acceso a internet se realiza el remplazo del UTM Fortinet actual por un servidor en software libre (UTM 01 externo), el mismo que tiene la capacidad de controlar el tráfico entrante y saliente hacia internet, además, filtrando la navegación a través del servicio proxy y detectando intentos de ataques de códigos maliciosos a través de un IDS/IPS.

El UTM externo además de controlar el acceso de los usuarios hacia internet, controla el acceso desde internet hacia la DMZ en donde se publican los servicios que se ofrecen a la WEB.

En base a la necesidad de la protección de los recursos internos de la institución se implementa el siguiente esquema:

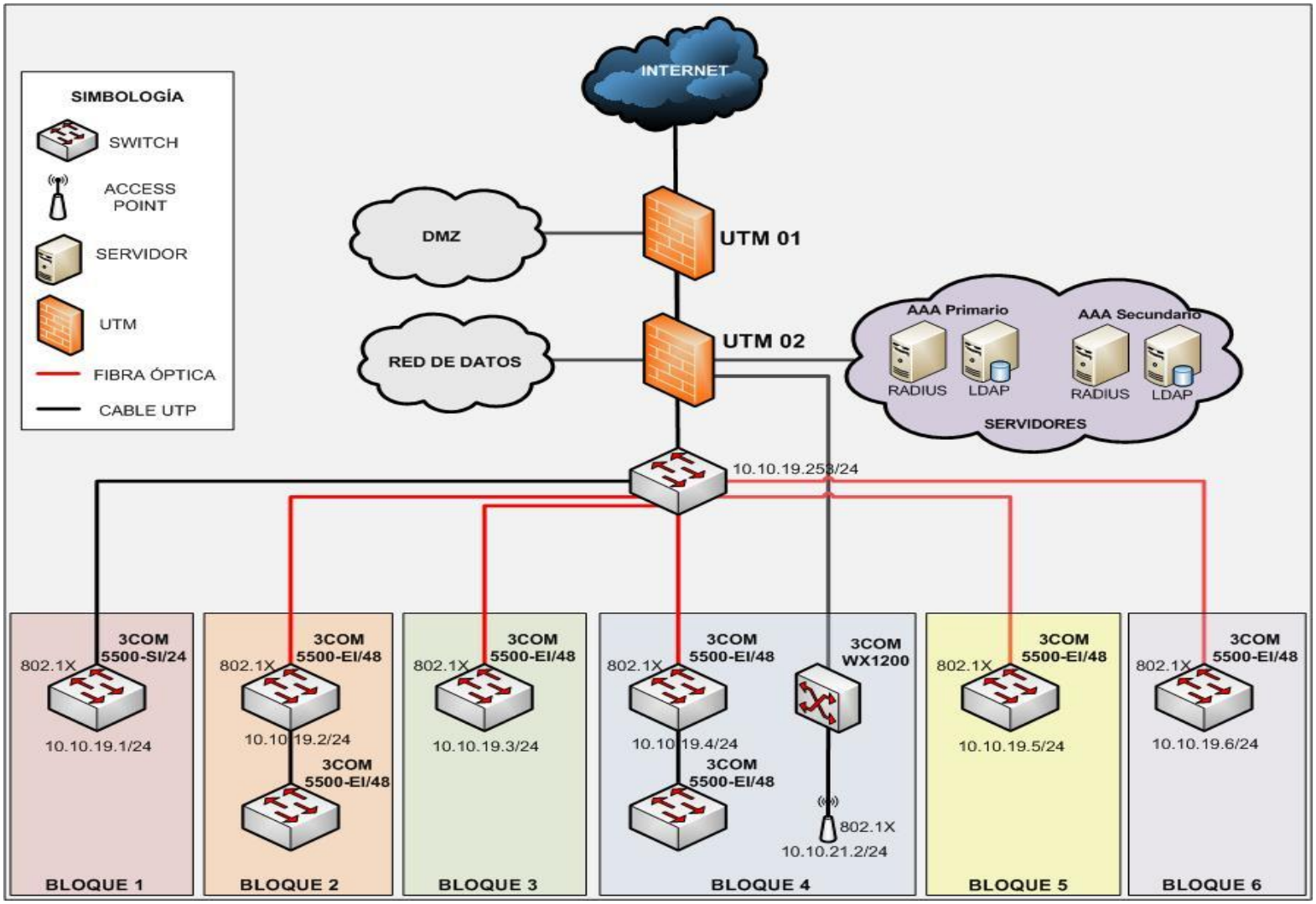


Figura 25. Esquema de seguridad implementado en la red LAN
Fuente: Carlos Plasencia

3.1.7.1 Descripción del UTM interno

Como se observa en la *Figura 25* el UTM 02 se encuentra integrado en la zona perimetral de la red interna LAN, y es el encargado de filtrar el tráfico tanto entrante como saliente desde y hacia la red interna, permitiendo o denegando las comunicaciones en función de los criterios del administrador de red y de esta forma se generan las políticas y reglas implementadas en el firewall.

Lógicamente el UTM interno (UTM 02) se encuentra limitando cinco zonas las mismas que se entienden de la siguiente manera:

- *Eth0: Zona LAN.-* Es la red interna LAN del edificio en donde se encuentran todos los usuarios.
- *Eth1: Zona Internet.-* Es la conexión que controla el tráfico desde la red interna LAN hacia el UTM externo (UTM 01).
- *Eth2: Zona Red de Datos.-* Es la conexión hacia los demás entes del ministerios y repartos de todas las fuerzas a nivel nacional.
- *Eth3: Zona Servidores.-* Es muy importante que esta zona se encuentre tras el firewall para poder controlar el acceso tanto de usuarios internos como de usuarios externos a la institución.
- *Eth4:* Zona Wireless.- Esta zona se la independiza para poder controlar todo el tráfico desde y hacia la subred inalámbrica ya que se debe tener en cuenta que al ser una red de acceso sin cables no se tiene control de los usuarios que intentan acceder de esta manera, solamente se controla a los usuarios que utilizan el mecanismo de autenticación implementado en el presente proyecto. Cuando se habla de seguridad se debe asumir el criterio de un atacante y suponer que éste puede romper el mecanismo de autenticación y logre conectarse, entonces se analiza el acceso hacia qué información se tiene desde dicha red.

No se debe olvidar que el servicio AAA necesita la comunicación a través de los puertos UDP 1812 y 1813 entre la red LAN y los servidores AAA de autenticación para no alterar su funcionamiento en la red.

Por la red de datos acceden todos los entes del ministerio incluidos los repartos, a ciertas aplicaciones que se encuentran en la zona de servidores, por lo cual se debe conocer exactamente quienes necesitan acceder y hacia qué servicios para establecer las políticas y reglas en la configuración del firewall.

Mediante la integración del firewall se mejora el control de acceso a las aplicaciones y en caso de ser necesario el acceso desde redes externas hacia la red interna LAN de la institución.

3.1.7.2 Descripción del UTM externo

El UTM externo (UTM 01) es el encargado de controlar el tráfico desde y hacia las zonas:

- *Eth0: Zona Internet.-* Es la conexión con el proveedor del servicio de Internet.
- *Eth2: Zona DMZ.-* Subred en la que están los servicios de acceso público.
- *Eth3: Zona red interna.-* Subredes de la red LAN interna, subred de servidores y redes de los entes del ministerio externos a la institución.

El servidor maneja un proxy para control y filtrado de la navegación de usuarios que pertenecen a la red LAN, las restricciones de las páginas web son aplicadas de acuerdo a las labores que desempeña cada grupo de usuarios.

El servidor tiene habilitado la función de IDS/IPS para la detección y prevención de ataques de código malicioso en las aplicaciones que se encuentran publicadas en la WEB o hacia la red interna.

CAPÍTULO IV
IMPLEMENTACIÓN DEL SERVIDOR AAA EN LA RED INTERNA DEL ENTE DEL MINISTERIO DE DEFENSA NACIONAL

4.1 PREPARACIÓN DEL SISTEMA BASE

De acuerdo al diseño presentado en el capítulo anterior, primero se procede a preparar el equipo sobre el cual se instalará el servidor de autenticación AAA.

El proceso de instalación del sistema base que se virtualiza para soporte de los servicios propuestos en el diseño es:

4.1.1 VIRTUALIZACIÓN DE SERVIDORES *[26]*

Sobre las cuchillas HS-21 y HS-22 se instala el sistema operativo base Debian Lenny 5.0 y luego se procede a paravirtualizar las dos cuchillas. El proceso en las dos cuchillas es similar, por este motivo se explica la configuración básica sobre la cuchilla Intel HS-21.

Un requisito previo a la instalación de los servidores es la asignación de direcciones IP para los servidores y máquinas virtuales. El direccionamiento IP asignado a los servicios se muestra en la tabla del ANEXO 3.

Los pasos fundamentales para la paravirtualización del servidor y la creación de las máquinas virtuales para la implementación de los servidores RADIUS y LDAP son:

Instalar los paquetes necesarios para realizar la paravirtualización:

- *apt-get update # Actualiza los repositorios de debian*
- *apt-get install xen-utils xen-tools xen-docs-3.2 xen-linux-system-2.6.26-2-xen-amd64 xen-hypervisor-3.2-1-amd64 # Instalar paquetes para soporte de xen*

Por defecto la virtualización con xen soporta la creación de hasta 4 máquinas virtuales, por esta razón, antes de reiniciar el equipo para que arranque con el

kernel xen se debe modificar la opción loop del fichero /etc/modules para permitir crear hasta 64 máquinas virtuales de la siguiente manera:

- *nano /etc/modules # Editar el fichero modules*

La opción *loop* cambiarla por *loop max_loop=64*

Guardar los cambios y salir.

Lo siguiente que se configura es el modo de acceso a la red, en este caso se configurará para que todas las máquinas virtuales compartan la interfaz de red física del servidor en modo bridge, para activar este modo se realiza lo siguiente:
Modificar el fichero xend-config.sxp con el comando:

- *nano /etc/xen/xend-config.sxp*
    - Localizar la línea ***(network-script network-bridge)*** y descomentarla.
    - **Encontrar la línea *(network-script network-dummy)*** y comentarla.
    - Verificar que la línea *(vif-script vif-bridge)* esté descomentada.

Realizados los cambios antes indicados se reinicia el servidor ejecutando el comando:

- *reboot*

Al arrancar nuevamente el sistema operativo, ya inicia con el kernel xen.

Lo siguiente que se configura son los parámetros que tendrán por defecto las máquinas virtuales. El fichero que se modifica es el siguiente:

- *nano /etc/xen-tools/xen-tools.conf*

Las opciones que se modifican son:

- *dir* = */home/xen* # Directorio en el que se crea la VM[24].
- *size* = *20 Gb* # Tamaño de la imagen del disco duro de la VM.
- *memory* = *1 Gb* # Tamaño de la memoria asignado a la VM.
- *swap* = *2 Gb* # Tamaño del swap de la VM.
- *fs* = *ext3* # Formato del sistema de ficheros de la VM.
- *gateway* = *10.10.20.1* # Puerta de enlace de la VM.

[24] VM.- Virtual Machine, Máquina Virtual

- *netmask* = *255.255.255.0* # Máscara de red de la VM
- *nameserver* = *10.10.20.4* # DNS para la VM.
- *passwd* = *1* # Solicitud de contraseña al finalizar la creación de la nueva VM.
- *kernel* = */boot/vmlinuz-`uname -r`* # Kernel que usará la VM.
- *initrd* = */boot/initrd.img-`uname -r`* # Imagen de inicio con la que arranca la nueva VM.
- *arch* = *amd64* # Arquitectura de la VM.
- *serial_device* = *hvc0* # modo de conexión desde la consola del sistema base hacia la VM.
- *output* = */etc/xen/auto* # Directorio donde se creará el fichero de inicio de la VM.
- *extension* = *.cfg* # Extensión del fichero de inicio.

Una vez definidos estos parámetros se guarda los cambios y se sale del fichero.

Para crear las máquinas virtuales para el servidor RADIUS y LDAP se ejecutaron los comandos:

- *xen-create-image --hostname=radius01 --dist=lenny -ip=10.10.20.12 –role=udev*
- *xen-create-image --hostname=ldap01 --dist=lenny -ip=10.10.20.11 –role=udev*

Para arrancar las VMs creadas se ejecutan los comandos:

- *xm create -c /etc/xen/auto/radius01.cfg*
- *xm create -c /etc/xen/auto/ldap01.cfg*

Las configuraciones de las maquinas virtuales creadas se presentan en el ANEXO 4.

4.2 CONFIGURACIÓN DEL SERVIDOR AAA *[27][28]*

El esquema de la infraestructura implementada se muestra en la siguiente Figura:

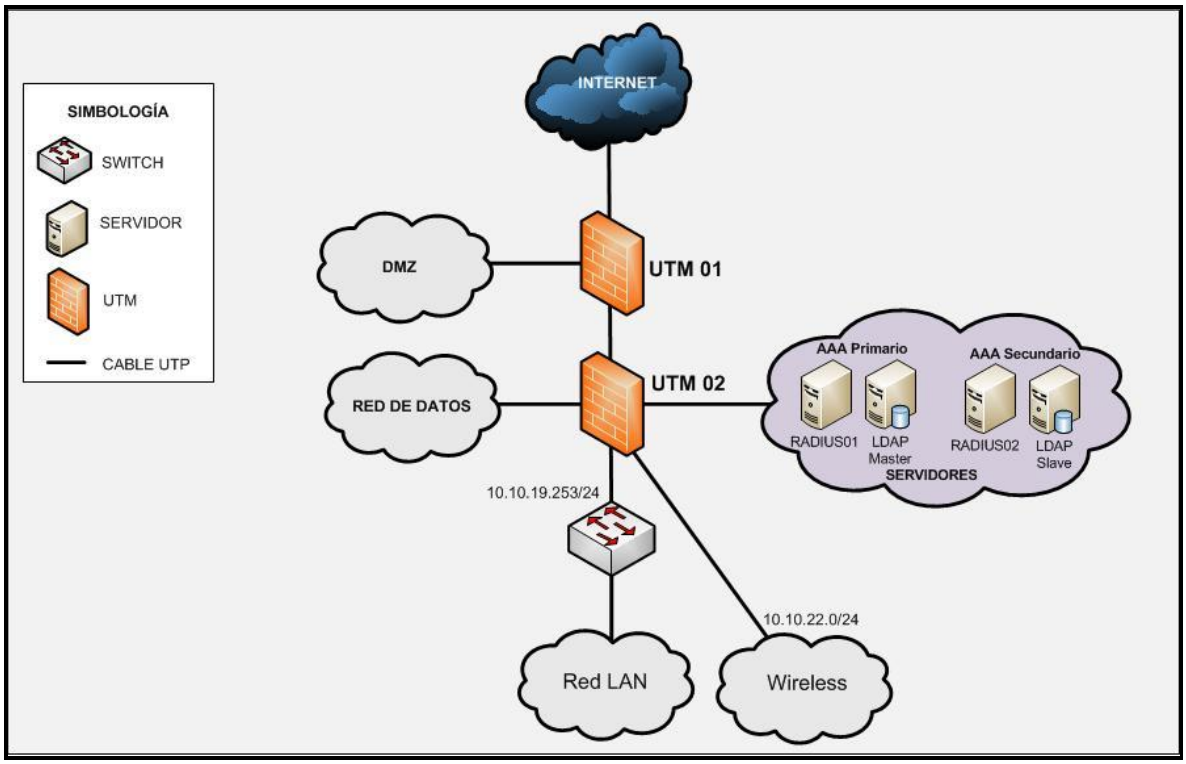


Figura 26. Infraestructura de servicios implementada
Fuente: Carlos Plasencia

Como se observa en el esquema el servicio AAA consta de dos servidores RADIUS, un primario y otro secundario. Las configuraciones de los servidores son idénticas por lo cual se explicará el procedimiento realizado en el servidor primario.

La instalación del servidor AAA está realizada sobre la plataforma LINUX con el sistema operativo Debian Lenny 5.0 con el software FREERADIUS 2.0.4, el mismo que utilizará la base de datos LDAP Master existente.

4.2.1 INSTALACIÓN DE FREERADIUS

La versión de freeradius que incluye los repositorios del sistema operativo no soporta el protocolo EAP-PEAP, por lo cual la versión instalada de freeradius es compilada, ya que a ésta se habilita el soporte de los protocolos de encripción EAP-PEAP, EAP-TLS y EAP-TTLS, además incluye, el módulo OPENSSL, los

cuales son necesarios para aplicar un método de encriptación seguro para el intercambio de información entre el servidor AAA y el usuario.

4.2.1.1 Descarga de paquetes a instalarse

Para compilar la versión de freeradius con soporte de los protocolos EAP, primero se descargan los paquetes fuentes y luego se procede a configurar de modo que soporte los módulos EAP.

Instalación de los elementos necesarios para la compilación y actualización de los repositorios de Debian.

- *aptitude install build-essential #Instalación de herramientas necesarias para la compilación de paquetes.*
- *aptitude install apt-src # Instalación de commando para descarga de paquetes desde los sources.*
- *apt-src update #Actualizar os repositorios para descargar los sources.*

Crear un directorio para descargar las fuentes de FREERADIUS

- *mkdir /usr/build_freeradius*

Ingresar al directorio creado

- *cd /usr/build_freeradius*

Descargar los paquetes FREERADIUS

- *apt-src install freeradius*

Revisar los paquetes descargados

- *ls -l*

4.2.1.2 Configuración de la compilación

La configuración de las fuentes descargadas anteriormente es la siguiente. Ingreso a los archivos de compilación:

- *cd /usr/build_freeradius/freeradius-2.0.4+dfsg/debian*

Modificar el archivo rules para habilitar el soporte de ssl:

- *nano rules*

El fichero de configuración se presenta en el ANEXO 5:

- **with-rlm_eap_tls.-** Habilita el soporte de tls
- **with-rlm_eap_ttls.-** Habilita el soporte de ttls
- **with-rlm_eap_peap.-** Habilita el soporte de peap
- **with-openssl.-** Habilita el soporte de openssl

Modificar el archivo control

- *nano control*

Añadir la dependencia para openssl la librería libssl-dev en la línea:

- *Source: freeradiusBuild-Depends: autotools-dev, debhelper (>= 6.0.7), libgdbm-dev, libiodbc2-dev,libkrb5-dev, libldap2-dev, libltdl3-dev, libmysqlclient15-dev | libmysqlclient-dev, libpam0g-dev, libpcap-dev, libperl-dev, libpq-dev, libsasl2-dev, libsnmp-dev, libtool, python-dev,* ***libssl-dev***

Asegurarse que la librería libssl está instalada

- *aptitude install libssl-dev*

4.2.1.3 Instalación del paquete compilado

Una vez configuradas las fuentes con soporte de los módulos EAP y SSL se procede a la instalación de los paquetes de la siguiente manera.

Construcción de los binarios

- *cd /usr/build_freeradius*
- *apt-src build freeradius*

Una vez completada la compilación, normalmente sin errores, se obtiene la siguiente lista de paquetes:

- *ls -l *.deb*

-rw-r--r-- 1 root root 531478 2010-03-22 09:42 freeradius_2.0.4+dfsg-6_amd64.deb
-rw-r--r-- 1 root root 203504 2010-03-22 09:42 freeradius-common_2.0.4+dfsg-6_all.deb
-rw-r--r-- 1 root root 991796 2010-03-22 09:42 freeradius-dbg_2.0.4+dfsg-6_amd64.deb
-rw-r--r-- 1 root root 132038 2010-03-22 09:42 freeradius-dialupadmin_2.0.4+dfsg-6_all.deb
-rw-r--r-- 1 root root 17548 2010-03-22 09:42 freeradius-iodbc_2.0.4+dfsg-6_amd64.deb
-rw-r--r-- 1 root root 18238 2010-03-22 09:42 freeradius-krb5_2.0.4+dfsg-6_amd64.deb
-rw-r--r-- 1 root root 36052 2010-03-22 09:42 freeradius-ldap_2.0.4+dfsg-6_amd64.deb
-rw-r--r-- 1 root root 24992 2010-03-22 09:42 freeradius-mysql_2.0.4+dfsg-6_amd64.deb
-rw-r--r-- 1 root root 36916 2010-03-22 09:42 freeradius-postgresql_2.0.4+dfsg-6_amd64.deb
-rw-r--r-- 1 root root 75772 2010-03-22 09:42 freeradius-utils_2.0.4+dfsg-6_amd64.deb
-rw-r--r-- 1 root root 91036 2010-03-22 09:42 libfreeradius2_2.0.4+dfsg-6_amd64.deb
-rw-r--r-- 1 root root 115488 2010-03-22 09:42 libfreeradius-dev_2.0.4+dfsg-6_amd64.deb

De la lista anterior se instala sólo lo necesario. En este caso se ha instalado lo siguiente:

- *dpkg -i freeradius_2.0.4+dfsg-6_amd64.deb freeradius-common_2.0.4+dfsg-6_all.deb freeradius-ldap_2.0.4+dfsg-6_amd64.deb freeradius-utils_2.0.4+dfsg-6_amd64.deb freeradius-mysql_2.0.4+dfsg-6_amd64.deb libfreeradius2_2.0.4+dfsg-6_amd64.deb*

- *freeradius_2.0.4+dfsg-6_amd64.deb, freeradius-common_2.0.4+dfsg-6_all.deb y libfreeradius2_2.0.4+dfsg-6_amd64.deb.-* El motor de funcionamiento de freeradius y las librerías necesarias para su ejecución.
- *freeradius-ldap_2.0.4+dfsg-6_amd64.deb.-* Módulo para soporte de la base de datos LDAP.
- *freeradius-mysql_2.0.4+dfsg-6_amd64.deb.-* Módulo para soporte de la base de datos MYSQL.

Una vez concluida la instalación se tendrá errores que freeradius no puede ejecutarse, esto es normal, ya que se encuentra instalado con soporte de los módulos de encriptación EAP y OPENSSL, entonces, para que freeradius se ejecute correctamente se debe crear los certificados con OPENSSL y configurar el archivo *eap.conf* de freeradius.

4.2.1.4 Protección de la versión instalada

Cada vez que se realiza una actualización del sistema operativo se instala las nuevas versiones de los paquetes y en ciertos casos traen nuevos cambios que pueden afectar el funcionamiento normal del servicio. Para evitar que esto suceda se utiliza la protección de la versión instalada.

Cuando se utiliza el comando apt-get dist-upgrade se actualizan todos los paquetes del sistema operativo. Al proteger la versión de un paquete no se tendrá modificaciones cada vez que se actualice la versión del sistema operativo, y de esta manera se evitará que se modifique la configuración de freeradius.

Para proteger la instalación de freeradius se realiza lo siguiente:

Utilizar la herramienta *dpkg* para administrar la selección de los paquetes instalados.

- *dpkg --get-selections > packages*

Con el fin de obtener los paquetes de archivos que se van a editar, buscar los paquetes relacionados con freeradius que se han instalado:

- *aptitude search freeradius* | *grep ^i*

i freeradius - a high-performance and highly configurable
i freeradius-common - FreeRadius common files
i freeradius-ldap - LDAP module for FreeRADIUS server
i freeradius-mysql - MySQL module for FreeRADIUS server
i freeradius-utils - FreeRadius client utilities
i libfreeradius-dev - FreeRADIUS shared library development file
i libfreeradius2 - FreeRADIUS shared library

Buscar los paquetes de archivos que se han instalado con el comando:

- *cat packages* | *grep radius*

freeradius install
freeradius-common install
freeradius-ldap install
freeradius-mysql install
freeradius-utils install
libfreeradius2 install

Editar el fichero packages y modificar install por hold:

- *nano packages*

freeradius hold
freeradius-common hold
freeradius-ldap hold
freeradius-mysql hold
freeradius-utils hold
libfreeradius2 hold

El fichero con la protección de los paquetes se muestra en el ANEXO 5.

Para verificar los cambios ejecutar el comando:

- *cat packages | grep radius*

freeradius hold
freeradius-common hold
freeradius-ldap hold
freeradius-mysql hold
freeradius-utils hold
libfreeradius2 hold

Guadar los cambios en la base de datos

- *dpkg --set-selections < packages*

Para verificar que todo está correcto ejecutar:

- *aptitude search freeradius | grep ^i*

ih freeradius - a high-performance and highly configurable
ih freeradius-common - FreeRadius common files
ih freeradius-ldap - LDAP module for FreeRADIUS server
ih freeradius-mysql - MySQL module for FreeRADIUS server
ih freeradius-utils - FreeRadius client utilities
ih libfreeradius-dev - FreeRADIUS shared library development file
ih libfreeradius2 - FreeRADIUS shared library

Luego de este procedimiento se procede a instalar los certificados requeridos por la configuración de FREERADIUS para eliminar los errores existentes al ejecutar FREERADIUS en modo debug (freeradius -XX).

4.2.1.5 Instalación de certificados para el servidor

El método de autenticación de freeradius utilizado es PEAP el cual se basa en los certificados digitales del servidor, por lo tanto se procede a generarlos de la siguiente manera:

Editar el fichero *openssl.cnf* ejecutando el comando

- *nano /etc/ssl/openssl.cnf*

[CA_default]

dir = ./PKI #Directorio donde se crearán los certificados

Editar el fichero /usr/lib/ssl/misc/CA.sh

CATOP=./PKI

Ingresar al directorio de openSSL

- *cd /etc/ssl*

Ejecutar el comando

- */usr/lib/ssl/misc/CA.sh –newca #Crear certificado raíz de la CA*[25]

En cada parámetro que va apareciendo se ingresa la información requerida.

Si se tiene usuarios Windows XP y se desea crear certificados para la autenticación se crea el fichero xpextensions ejecutando el siguiente comando

- *nano /etc/ssl/PKI/xpextensions*

El contenido del fichero es el siguiente:

[xpclient_ext]

extendedKeyUsage=1.3.6.1.5.5.7.3.2

[xpserver_ext]

extendedKeyUsage=1.3.6.1.5.5.7.3.1

Ingresar al directorio de openSSL

- *cd /etc/ssl*

Ejecutar el comando para la solicitud del certificado del servidor

- *openssl req -new -nodes -keyout PKI/server_key.pem -out PKI/server_req.pem -days 730 -config openssl.cnf*

Establecer la contraseña de intercambio (password challenge)

[25] CA.- Certificate Authority (Autoridad de certificación).

Registrar las peticiones de certificados de usuarios al servidor (usuarios winxp):

- *cd /etc/ssl*
- *openssl ca -config openssl.cnf -policy policy_anything -out PKI/server_cert.pem -extensions xpserver_ext -extfile PKI/xpextensions -infiles PKI/server_req.pem*

Sacar respaldo del certificado del servidor:

- *cd /etc/ssl/PKI/*
- *cp server_cert.pem server_cert.pem-backup*

Concatenar el certificado y contraseña del servidor:

- *cat server_key.pem server_cert.pem > server_keycert.pem*

Crear el certificado para los usuarios:

- *cd /etc/ssl*
- *openssl req -new -keyout PKI/client_key.pem -out PKI/client_req.pem -days 7300 -config openssl.cnf*

Registrar el certificado de los usuarios:

- *cd /etc/ssl*
- *openssl ca -config openssl.cnf -policy policy_anything -out PKI/client_cert.pem -extensions xpclient_ext -extfile PKI/xpextensions -infiles PKI/client_req.pem*

Exportar los certificados con extensión P12. Este paso se usa cuando se utiliza el método de autenticación EAP-TLS basado en la validación de certificados de los usuarios.

- *cd /etc/ssl/PKI:*
- *openssl pkcs12 -export -in client_cert.pem -inkey client_key.pem -out client_cert.p12 -clcerts*

4.2.1.6 Configuración de los certificados en freeradius

Una vez que los certificados del servidor freeradius se crearon con ssl, se los exporta al directorio certs, para que el servidor utilice en el proceso de autenticación.

Copiar los certificados creados en ssl al directorio de freeradius:

- *cp /etc/ssl/PKI/cacert.pem /etc/freeradius/certs/cacert.pem*
- *cp /etc/ssl/PKI/server_keycert.pem /etc/freeradius/certs/server_keycert.pem*

Comprobar que están copiados los ficheros y cambiarlos de propietario.

- *cd /etc/freeradius/certs*
- *openssl dhparam -check -text -5 512 -out dh*
- *dd if=/dev/urandom of=random count=2*
- *chown freerad dh*
- *chmod o-w dh*

4.2.2 CONFIGURACIÓN DE FREERADIUS

El método de encriptación que utilizará FREERADIUS es EAP-PEAP y utilizará el módulo LDAP para autenticar los usuarios tal como se muestra en la *Figura 12*.

Los ficheros que se deben modificar para el funcionamiento de FREERADIUS son los siguientes:

- *eap.conf*.- Define el método de encriptación para el envío de datos.
- *radiusd.conf.*- El fichero principal de freeradius.
- *defaulf*.- Definir la utilización del módulo LDAP.
- *inner-tunnel*.- Sincronización del túnel para comunicación del servidor freeradius.
- *clients.conf.*- Define las entidades que tendrán la función de autenticador.
- *ldap.conf.*- Conexión con la base de datos de los usuarios LDAP.
- *ldap.attrmaps.*- Definir atributos para asignación dinámica de VLAN.
- *samba.schema*.- Esquema samba para control de dominios.

Las modificaciones que se deben realizar en cada fichero para el correcto funcionamiento de FREERADIUS con soporte de LDAP es el siguiente:

4.2.2.1 Configuración del fichero eap.conf

Especifica los módulos de autenticación que se empleará entre el cliente y el servidor, además define la ubicación dónde se encuentran ubicados los ficheros que contienen las claves y los certificados involucrados.

- *nano /etc/freeradius/eap.conf*

```
eap {
        default_eap_type = peap   #metodo de encripción
        timer_expire     = 60
        ignore_unknown_eap_types = no
        cisco_accounting_username_bug = no

      tls {
        certdir = ${confdir}/certs
        cadir = ${confdir}/certs
        private_key_password = moLEro365Ca #Clave privada del certificado
        private_key_file = ${certdir}/server_keycert.pem #certificado creado con ssl
        certificate_file = ${certdir}/server_keycert.pem
        CA_file = ${cadir}/cacert.pem # Clave pública de la CA
        dh_file = ${certdir}/dh
        random_file = ${certdir}/random
        fragment_size = 1024
        include_length = yes
        check_cert_cn = %{User-Name}
        cipher_list = "DEFAULT"
      }

 peap {
        default_eap_type = mschapv2
        copy_request_to_tunnel = yes
        use_tunneled_reply = yes
```

```
        virtual_server = "inner-tunnel"
        }
}
```

4.2.2.2 Configuración del fichero radiusd.conf

Este fichero es el principal de freeradius, en éste se define todos los parámetros y módulos necesarios para su funcionamiento.

- *nano /etc/freeradius/radiusd.conf*

```
auth_badpass = yes  #Registrar en el log cuando la autenticación es incorrecta
auth_goodpass = yes  #Registrar en el log cuando la autenticación es exitosa

# PROXY CONFIGURATION
proxy_requests  = no        #No usará Proxy
#$INCLUDE proxy.conf

mschap {
                use_mppe = yes # cifrado de negociación
                require_encryption = yes
                require_strong = yes
                with_ntdomain_hack = yes
          }
# Include another file that has the LDAP-related configuration.#
$INCLUDE ldap.conf # Conexión con LDAP
```

4.2.2.3 Configuración del fichero default

En este fichero se configura para que freeradius soporte la base de datos ldap

- *nano /etc/freeradius/sites-avaible/default*

```
authorize {
                preprocess
```

```
        chap
        mschap
        suffix
        eap {
        ok = return
        }
        unix
        ldap    #Verificación del usuario en la base de datos LDAP
        expiration
        logintime
        pap
    }
post-auth {
        ldap   #Verificación del usuario en la base de datos LDAP
        exec
        Post-Auth-Type REJECT {
        attr_filter.access_reject
        }
    }
```

4.2.2.4 Configuración del fichero inner-tunnel

Se declara la base de datos que se utiliza para autenticar los usuarios.

- *nano /etc/freeradius/sites-avaible/inner-tunnel*

```
authorize {
        chap
        mschap
        unix
        suffix
        eap {
        ok = return
        }
```

```
        files
        ldap    # Validación contra LDAP
        expiration
        logintime
        pap
    {

authenticate {
        Auth-Type PAP {
        pap
        }
        Auth-Type CHAP {
        chap
        }
        Auth-Type MS-CHAP {
        mschap
        }
        Auth-Type LDAP {
        ldap     #Autenticación de tipo LDAP
        }
        eap
    }
```

4.2.2.5 Configuración del fichero clients.conf

En este módulo se especifica la dirección IP de los dispositivos clientes o de acceso, también se define la contraseña para autenticación y el tipo de soporte de red.

- *nano /etc/freeradius/clients.conf*

```
client 10.10.19.1/24 {
        Ipaddr          = 10.10.19.1 # Tabla descrita en el ANEXO 2
        Secret          = PR01MblTCom # Clave que será comprobada para el
                          autenticador.
```

Nastype = other # Tipo de dispositivo de Acceso a red

}

4.2.2.6 Configuración del fichero ldap.conf

Este módulo hace la conexión con la base de datos LDAP para realizar la autenticación de los usuarios de la red.

- *nano /etc/freeradius/ldap.conf*

El contenido del fichero es el siguiente:

############Configuracion del servidor LDAP############################
ldap {
server = ldap01.ente.gob.ec #IP del servidor LDAP
identity = cn=admin,dc=ente,dc=gob,dc=ec #Usuario de conexión con la base
password = prt01MbWs # Contraseña de conexión
basedn = ou=people,dc=ente,dc=gob,dc=ec # Base de búsqueda
filter = (uid=%{mschap:User-Name:{User-Name}}) #Filtro del usuario
start_tls = no
tls_mode = no
dictionary_mapping = ${raddbdir}/ldap.attrmap
ldap_cache_timeout = 120
ldap_cache_size = 0
ldap_connections_number = 10
password_header = {clear}
password_attribute = userPassword
groupname_attribute = uid
groupmembership_filter = (&(uid=%{Stripped-User-Name:%{User-Name}})(objectclass=radiusprofile))
groupmembership_attribute = radiusGroupName
timeout = 3
timelimit = 5
net_timeout = 1
compare_check_items = no
}

4.2.2.7 Configuración del fichero ldap.attrmaps

Este archivo es un “mapa” de las correspondencias entre los atributos del diccionario *RADIUS* y los atributos del directorio *LDAP,* permitiendo de esta forma “redefinir” el significado de algunos atributos del directorio *LDAP.*

- *nano /etc/freeradius/ldap.attrmaps*

En caso de necesitar atributos RADIUS para la asignación dinámica de VLAN se debe agregar las siguientes líneas:

replyItem Tunnel-Type radiusTunnelType
replyItem Tunnel-Medium-Type radiusTunnelMediumType
replyItem Tunnel-Private-Group-Id radiusTunnelPrivateGroupId

4.2.2.8 Configuración del archivo samba.schema

Dado a que existe un esquema samba en el directorio LDAP, es necesario añadir los atributos del servidor RADIUS.
Los atributos RADIUS son los siguientes:

```
attributetype
  ( 1.3.6.1.4.1.7165.2.1.70 NAME 'radiusFramedProtocol'
    DESC ''
    EQUALITY caseIgnoreIA5Match
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
    SINGLE-VALUE
  )
attributetype
  ( 1.3.6.1.4.1.7165.2.1.71 NAME 'radiusServiceType'
    DESC ''
    EQUALITY caseIgnoreIA5Match
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
    SINGLE-VALUE
  )
Attributetype ( 1.3.6.1.4.1.7165.2.1.72 NAME 'radiusFramedCompression'
    DESC ''
    EQUALITY caseIgnoreIA5Match
```

SYNTAX 1.3.6.1.4.1.1466.115.121.1.26

SINGLE-VALUE

)

Attributetype (1.3.6.1.4.1.7165.2.1.73 NAME 'radiusTunnelMediumType'

DESC ''

EQUALITY caseIgnoreIA5Match

SYNTAX 1.3.6.1.4.1.1466.115.121.1.26

)

Attributetype (1.3.6.1.4.1.7165.2.1.74 NAME 'radiusTunnelType'

DESC ''

EQUALITY caseIgnoreIA5Match

SYNTAX 1.3.6.1.4.1.1466.115.121.1.26

)

Attributetype (1.3.6.1.4.1.7165.2.1.75

NAME 'radiusTunnelPrivateGroupId'

DESC ''

EQUALITY caseIgnoreIA5Match

SYNTAX 1.3.6.1.4.1.1466.115.121.1.26

)

objectclass (1.3.6.1.4.1.7165.2.2.6 NAME 'sambaSamAccount' SUP top AUXILIARY DESC 'Samba 3.0 Auxilary SAM Account' MUST (uid $ sambaSID) MAY (cn $ sambaLMPassword $ sambaNTPassword $ sambaPwdLastSet $ sambaLogonTime $ sambaLogoffTime $ sambaKickoffTime $ sambaPwdCanChange $ sambaPwdMustChange $ sambaAcctFlags $ displayName $ sambaHomePath $ sambaHomeDrive $ sambaLogonScript $ sambaProfilePath $ description $ sambaUserWorkstations $ sambaPrimaryGroupSID $ sambaDomainName $ sambaMungedDial $ sambaBadPasswordCount $ sambaBadPasswordTime $ sambaPasswordHistory $ sambaLogonHours $ radiusFramedProtocol $ radiusServiceType $ radiusFramedCompression $ radiusTunnelMediumType $ radiusTunnelType $ radiusTunnelPrivateGroupId))

4.3 CONFIGURACIÓN DEL AUTENTICADOR

Los equipos que van a cumplir está función son los 7 switches de la marca 3Com de la serie 5500G-EI y el switch 3Com 5500-SI, en los mismos que se realizan las configuraciones para que soporten el método de encriptación EAP.

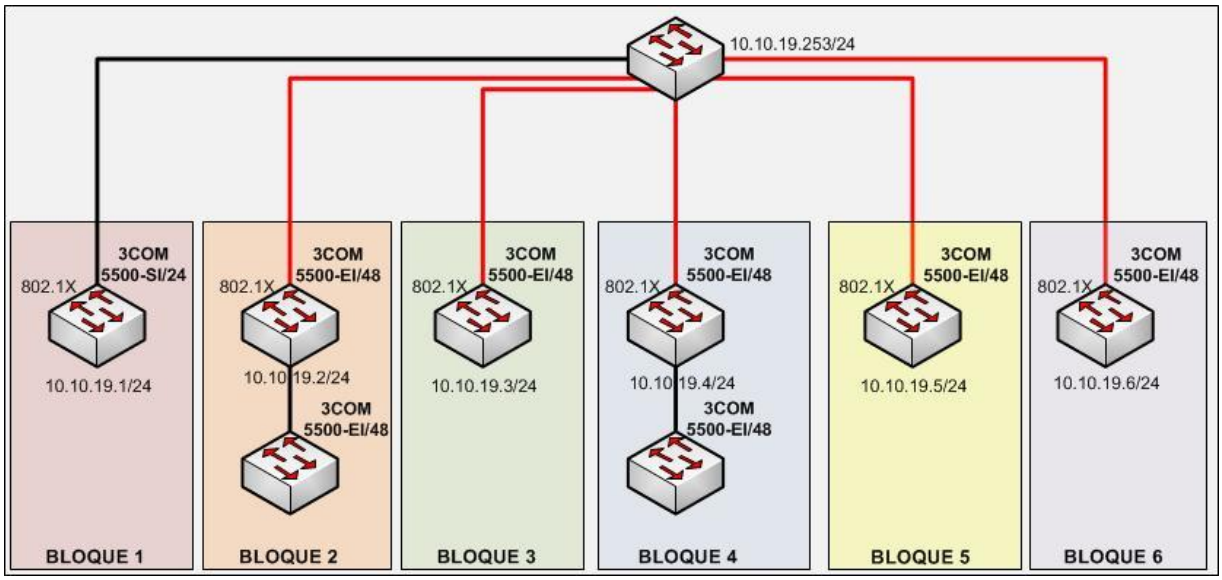


Figura 27. Switches de acceso
Fuente: Carlos Plasencia

4.3.1 CONFIGURACIÓN DE SWITCH 3Com 5500

La configuración es similar para todos los switches de acceso:

- Se habilita el esquema test de radius por defecto:

[swb1]*domain default enable test*

- Se habilita IEEE-802.1X de manera global

<swb1>
<swb1>*sysconfig*
[swb1]*dot1x*

- Método de autenticación

[swb1]*dot1x authentication-method eap*

- Definición del esquema radius con los atributos de los servidores de autenticación

[swb1]*radius scheme system*

[swb1]*radius scheme test*

[swb1-radius-test]*server-type standard*

[swb1-radius-test]*primary authentication 10.10.20.12* #Servidor Radius primario

[swb1-radius-test]*primary accounting 10.10.20.12* #Servidor Radius primario

[swb1-radius-test]*secondary authentication 10.10.20.13* # Servidor Radius secundario

[swb1-radius-test]*secondary accounting 10.10.20.13* # Servidor Radius secundario

[swb1-radius-test]*key authentication PR01MblTCom* # Secreto configurado en el servidor en el fichero clients.conf

[swb1-radius-test]*key accounting PR01MblTCom* # Secreto configurado en el servidor en el fichero clients.conf

[swb1-radius-test]*user-name-format without-domain* #Filtrar el nombre del usuario sin domonio

- Habilitar la autenticación 802.1x en los puertos de acceso:

[swb1]*interface GigabitEthernet 1/0/3*

[swb1-GigabitEthernet1/0/3]*dot1x port-method portbased*

[swb1-GigabitEthernet1/0/3]*dot1x*

4.3.2 CONFIGURACIÓN DEL WIRELESS LAN CONTROLLER

Para la gestión del Access Point 3Com 2750 se cuenta con un switch 3Com WX1200 el cual gestiona los AP de manera centralizada, la configuración para soporte de 802.1X es la siguiente:

- Entrar a modo de configuración

WX12000> enable

- Asistente de configuración del switch 3Com WX1200

WX1200# quickstart

- Borrar la configuración existente y empezar una nueva

This will erase any existing config. Continue? [n]: y

Answer the following questions. Enter '?' for help. ^C to break out

- Esprcificar el nombre del switch

System Name [WX1200]: WX1200

Country Code [US]: EC

- Configuración de la dirección IP del switch

System IP address []: 10.10.21.2

System IP address netmask []: 255.255.255.0

Default route []: 10.10.21.254

- Se va configurar VLAN?. En este caso no.

Do you need to use 802.1Q tagged default VLAN [Y/N]? Y: N

- Datos del administrador del switch

Admin username [admin]: wxadmin

Admin password [optional]: Crb01UtrsA9

Enable password [optional]: enable

- Configuración de la fecha y hora

Do you wish to set the time? [y]: y

Enter the date (dd/mm/yy) []: 15/01/10

Enter the time (hh:mm:ss) []: 09:36:20

- Parámetros de la conexión Wireless

Do you wish to configure wireless? [y]: y

Enter a clear SSID to use: PRINXENTE

Do you want Web Portal authentication? [y]: y

Enter a username with which to do Web Portal, <cr> to exit: admin

Enter a password for admin: fRex56@2owE

- Parámetros para autenticación con 802.1X

Do you want to do 802.1x and PEAP-MSCHAPv2? [y]: y

Enter a crypto SSID to use: EXTINTORSW

Enter a username with which to do PEAP-MSCHAPv2, <cr> to exit: adminpeap

Enter a password for bob: PcfEWpO98C

- Información de los Access Point a administrarse

Do you wish to configure access points? [y]: y

Enter a port number [1-2] on which an AP resides, <cr> to exit: 2

Enter AP model on port 2: ap2750

Do you wish to configure distributed access points? [y]: y

Enter a DAP serial number, <cr> to exit: 0422700351

Enter model of DAP with S/N 0422700351: ap2750

success: created keypair for ssh

success: Type "save config" to save the configuration

- Guardar la configuración

WX1200# save config

- Definición de servidores RADIUS

set radius server radius-server1 address 10.10.20.12 key prW01MblWir

set radius server radius-server2 address 10.10.20.13 key uRewSvTU6Z

- Grupo de servidores radius

set server group group-radius-1 members radius-server1 radius-server2

- Crear perfil del SSID

set service-profile entidad ssid-name EXTINTORSW

- Establecer la asociación cifrada

set service-profile entidad ssid-type crypto

- Crear perfil wpa

set service-profile entidad wpa-ie enable

- Habilitar tkip

set service-profile entidad cipher-tkip enable

- Habilitar autenticacion 802.1x

set service-profile entidad auth-dot1x enable

4.4 CONFIGURACIÓN DEL EQUIPO DEL USUARIO

Para que el usuario pueda acceder a la red y a sus recursos, la tarjeta de red se configura para que soporte la autenticación 802.1X, caso contrario el puerto en el que se encuentra conectado el equipo, por ningún motivo puede acceder a la red.

La configuración en la máquina del usuario es la siguiente:

- Clic en inicio.
- Seleccionar panel de control.
- Ingresar a conexiones de red.
- Clic derecho sobre conexión de área local.
- Seleccionar la pestaña de autenticación.

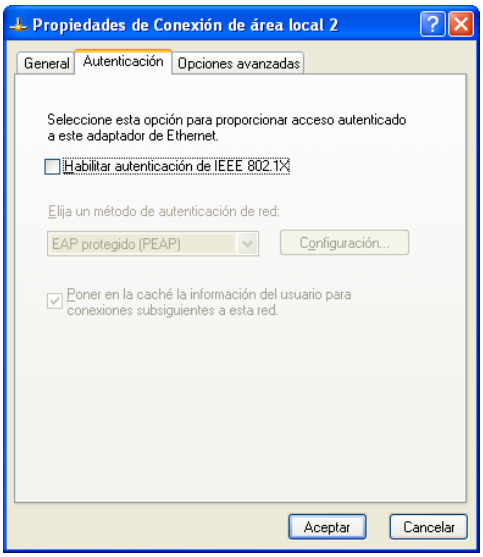
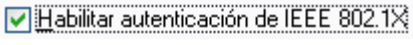
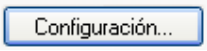


Figura 28.-Pestaña de autenticación en la interfaz de red
Fuente: Capturas del equipo de usuario

- Marcar la pestaña 

.
- En la pestaña de selección del método de autenticación seleccionar la opción EAP protegido (PEAP).
- Seleccionar la opción 

.
- En la siguiente venta escoger la opción EAP-MSCHAP v2.

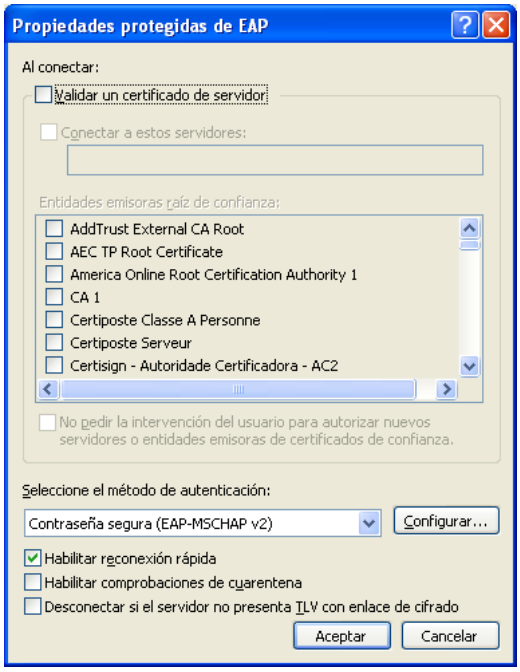


Figura 29.Pestaña para selección del método de autenticación
Fuente: Capturas del equipo de usuario

- Clic sobre la opción 

.
- Deshabilitar la pestaña para autenticar al inicio de sesión.

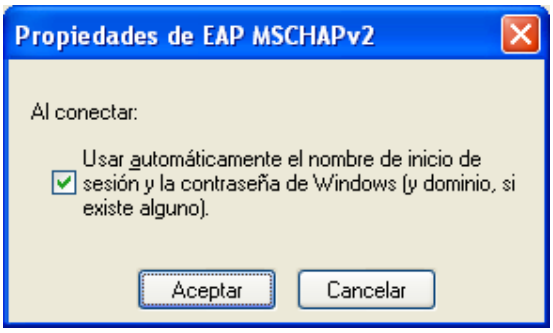


Figura 30.Deshabilitar la autenticación con credenciales de inicio de sesión
Fuente: Capturas del equipo de usuario

- Aceptar 3 veces y cerrar.

Para configurar las interfaces de red inalámbricas de los usuarios con soporte de 802.1X se realiza lo siguiente:

- Clic en inicio.
- Seleccionar panel de control.
- Ingresar a conexiones de red.
- Clic derecho sobre conexión de redes inalámbricas y seleccionar propiedades.

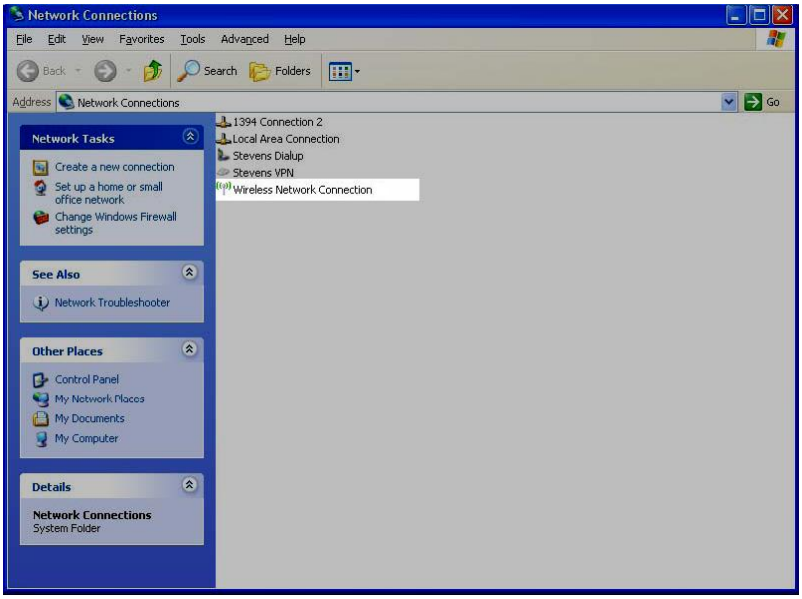


Figura 31. Configuración de conexiones wireless
Fuente: Capturas del equipo de usuario

- Agregar una nueva conexión wireless

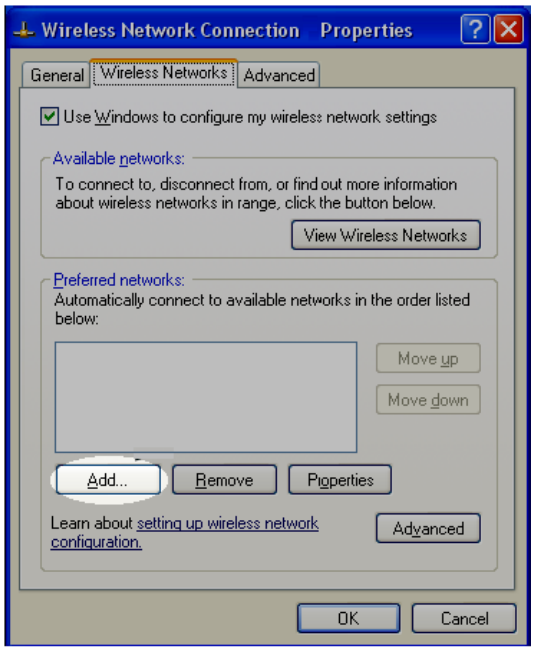


Figura 32. Agregar conexión wireless
Fuente: Capturas del equipo de usuario

- Ingresar el SSID de conexión y el método de cifrado

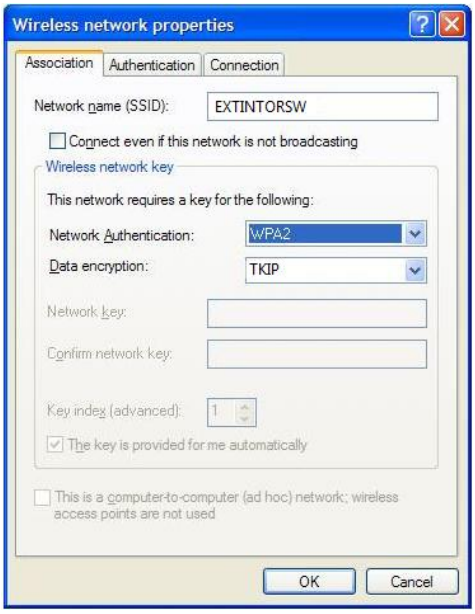


Figura 33. Propiedades de la conexión wireless
Fuente: Capturas del equipo de usuario

- Configurar los parámetros de PEAP

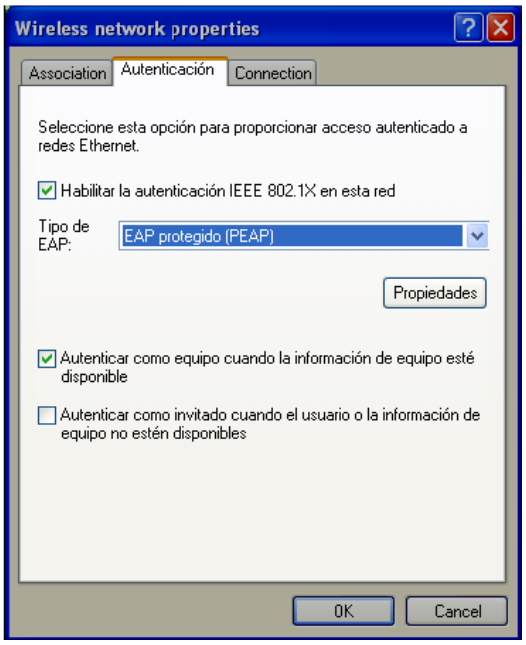


Figura 34. Configuración de PEAP para la conexión wireless
Fuente: Capturas del equipo de usuario

Las configuraciones del método de autenticación PEAP es similar al que se econfiguró anteriormente para la red cableada.

4.5 IMPLEMENTACIÓN DE UTM INTERNO Y EXTERNO

Una vez que el usuario es autenticado y autorizado para hacer uso de los recursos de red, mediante la implementación del UTM se le limitará el acceso únicamente a los servicios necesarios. La instalación y configuración de los UTM interno y externo se explica a continuación.

Los servidores UTM se implementan de acuerdo al esquema que se presenta en la *Figura 26*.

4.5.1 UTM INTERNO

EL UTM interno está instalado sobre un servidor Intel XEON de 4 GB de memoria RAM, 80GB de disco duro y 6 interfaces de red.

El servidor encargado del control del tráfico hacia la red interna de la institución tiene instalado el siguiente software:

- Sistema Operativo: Debian Lenny 5.0
- Firewall: Shorewall
- IDS: Snort
- IPS: PSAD[26]
- Monitoreo de tráfico: NTOP[27]
- Monitoreo Ancho de banda MRTG[28]

4.5.2 UTM EXTERNO

EL UTM externo está instalado sobre un servidor HP DL-380 con 8 GB de memoria RAM, 70 GB de disco duro y 6 interfaces de red.

El servidor encargado del control del tráfico desde la red interna hacia internet y viceversa tiene instalado el siguiente software:

- Sistema Operativo: Debian Lenny 5.0
- Firewall: Shorewall
- IDS: Snort
- IPS: PSAD
- Monitoreo de tráfico: NTOP
- Monitoreo Ancho de banda MRTG
- Proxy: Squid-Squidguard-Sarg

4.5.3 DESCRIPCIÓN Y CONFIGURACIÓN DE LAS HERRAMIENTAS A IMPLEMENTARSE EN LA INFRAESTRUCTURA UTM

En esta sección se realiza una descripción de cada herramienta que se instala y configura en la infraestructura UTM para conocer lo que hace cada una y el modo de utilización.

4.5.3.1 Instalación de paquetes

Para la instalación de paquetes se ejecuta los comandos:

Actualización de repositorios

- *apt-get update*

[26] PSAD.- (Port Scan Attack Detector) Detector de Ataque por Escaneo de Puertos.
[27] NTOP.- Network Top
[28] MRTG.- (Multi Router Traffic Grapher) Generador De Gráficos De Trafico Para Multi Enrutador

Instalación de paquetes

- *apt-get install shorewall squid squidguard sarg snort-mysql ntop mrtg psad mysql-server apache2 php5 php5-gd php5-cli php-pear php5-mysql*

Instalación de la interfaz de administración webmin:

Instalar librerías necesarias

- *apt-get install perl libnet-ssleay-perl openssl libauthen-pam-perl libpam-runtime libio-pty-perl apt-show-versions python*

Descargar la última version de webmin

- *wget http://sourceforge.net/projects/webadmin/files/webmin/1.520/webmin_1.520_all.deb*

Instalar el paquete con el comando

- *dpkg –i webmin_1.520_all.deb*

Para ingresar a la interfaz web, abrir un navegar e ingresar la dirección:

- *https://utm.ente.gob.ec:10000/*

Los ficheros de configuración de los UTM interno y externo se detallan en el ANEXO 6.

4.5.3.2 Firewall - Shorewall *[29]*

Shorewall (Shoreline Firewall) es una robusta y extensible herramienta de alto nivel para la configuración de muros cortafuego. Shorewall necesita que se le proporcionen algunos datos en algunos ficheros de texto simple y automáticamente creará las reglas de cortafuegos correspondientes a través de iptables. Shorewall puede permitir utilizar un sistema como muro cortafuego dedicado, sistema de múltiples funciones como puerta de enlace, dispositivo de encaminamiento y servidor.

El firewall es el encargado de permitir o denegar el acceso a servicios, cada servicio está asociado a un protocolo y puerto, entonces, es el responsable de autorizar o denegar las peticiones de acceso de los usuarios autenticados mediante el servidor AAA en la red de datos de la institución.

El firewall interno controla el tráfico entre las cinco zonas internas definidas en la *Figura 25*, los principales ficheros de configuración son los siguientes:

Ficheros de configuración de shorewall

Las configuraciones realizadas para levantar el servicio de firewall se detalla a continuación:

1. */etc/shorewall/shorewall.conf*

   En éste se definen los parámetros principales de shorewall, en este caso solo se activa las opciones *STARTUP_ENABLED=Yes* para activar el firewall y la opción *IP_FORWARDING=Yes* para habilitar el forwarding.

2. /etc/shorewall/zones

   Este fichero se utiliza para definir las zonas que se administrarán con Shorewall y el tipo de zona (firewall, ipv4 o ipsec). La zona *fw* está presente en éste fichero como configuración predefinida. A continuación se muestra las zonas creadas: hacia UTM externo (net), red hacia entes externos (rdd), red servidores (srv), hacia la red LAN (loc) y hacia la red wireless (wir).

3. /etc/shorewall/interfaces

   En éste fichero se establecen cuales serán las interfaces para las diferentes zonas. Se asocian las interfaces que corresponden a la zona net, srv, rdd, loc y wir. De acuerdo al diseño, la configuración es la siguiente: eth0-zona loc, eth1-zona net, eth2-zona rdd, eth3-zona srv, eth4-zona wir y en todas se solicita se calcule automáticamente la dirección de transmisión (Broadcast).

4. /etc/shorewall/policy

   En este fichero se establece como se accederá desde una zona hacia otra. Por seguridad todo el tráfico de zona a zona está cerrado y en el fichero rules está definido sólo el tráfico que se permite entre zonas.

5. /etc/shorewall/rules

   Todos los puertos están cerrados de modo predefinido, y en este fichero es donde se habilitan los puertos necesarios. Por ejemplo la regla principal para permitir el acceso para el servidor de autenticación AAA es la siguiente:

   ACCEPT loc srv:10.10.20.12,10.10.20.13 udp 1812,1813

   Interpretación

   Aceptar las peticiones desde la zona loc (red LAN) hacia la zona srv (servidores) a las IPs 10.10.20.12 (RADIUS primario) y 10.10.20.13 (RADIUS secundario) por el protocolo UDP a los puertos 1812 y 1813.

6. /etc/default/shorewall

   En este fichero se habilita la opción startup=1 para que empiece a funcionar el firewall.

Una vez configurados los ficheros antes indicados se procede a iniciar el servicio, ejecutando los comandos:

- *shorewall check # Verifica si existe errores en alguna configuración*
- *shorewall start # Inicia el servicio firewall*

4.5.3.3 IDS - Snort *[30][31]*

Un IDS o Sistema de Detección de Intrusiones es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático o red informática en busca de intentos de comprometer la seguridad de dicho sistema.

Snort es un sniffer de paquetes y un detector de intrusos basado en red (se monitoriza todo un dominio de colisión). Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como lo es MySQL. Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y

responder ante cualquier anomalía previamente definida. Así mismo existen herramientas de terceros para mostrar informes en tiempo real (snortreport, ACID[29]) o para convertirlo en un Sistema Detector y Preventor de Intrusos.
La instalación por defecto provee de cientos de filtros o reglas para backdoor, DDoS[30], finger, FTP, ataques web, CGI[31], Nmap.
Puede funcionar como sniffer para poder ver en consola y en tiempo real qué ocurre en la red, además, permite guardar en un archivo los logs para su posterior análisis. Cuando un paquete coincide con algún patrón establecido en las reglas de configuración, produce una alerta. Así se sabe cuándo, de dónde y cómo se produjo el ataque.

El IDS refuerza la seguridad contra ataques que se generen desde las redes externas hacia la institución; ya se ha asegurado el ingreso a la red mediante el servidor AAA, se ha limitado el acceso a servicios mediante el firewall, lo siguiente es detectar y bloquear intentos de ataques que se lleven a cabo desde el exterior de la red para evitar interrupciones en la disponibilidad de aplicaciones.

Configuración de snort

Para que el IDS pueda guardar todas las alertas en MYSQL se crea la base de datos para snort con el respectivo usuario de conexión, a continuación se detalla el procedimiento para crear la base:

- *mysql –u root –p # Ingreso a mysql*
- *mysql> CREATE USER 'snort'@'localhost' IDENTIFIED BY 'snort'; # Crear el usuario para la conexión de snort con mysql*
- *mysql> GRANT ALL PRIVILEGES ON * . * TO 'snort'@'localhost' IDENTIFIED BY 'snort'; # Habilita todos los privilegios al usuario.*
- *mysql> CREATE DATABASE IF NOT EXISTS `snort`; # Crea la base de datos para snort.*

[29] ACID.- (Atomicity, Consistency, Isolation and Durability) Atomicidad, Consistencia, Aislamiento y Durabilidad.
[30] DDoS.- (Distributed Denial of Service) Ataque Distribuído de Denegación de Servicio.
[31] CGI.- (Common Gateway Interface) Interfaz de Entrada Común.

- *mysql> GRANT ALL PRIVILEGES ON snort . * TO 'snort@localhost'; # Habilita los privilegios del usuario snort sobre la base de datos snort.*

Crear las tablas dentro de la bases de datos:

- *cd /usr/share/doc/snort-mysql/*
- *zcat create_mysql.gz | mysql -u snort -h localhost -p snort*

Borrar el error de instalación

- *rm /etc/snort/db-pending-config*

Para terminar de instalar snort ejecutar

- *apt-get upgrade*

Reconfigurar el paquete de snort con el comando

- *dpkg-reconfigure -plow snort-mysql*
  1. *Método de arranque: arranque*
  2. *Indicar la interfaz: eth2*
  3. *Indicar la red local: 10.10.0.0/16*
  4. *Desactivar el modo promiscuo de la interfaz: NO*
  5. *Cambiarse el orden de las pruebas: NO*
  6. *Opciones adicionales: no poner nada, Aceptar*
  7. *Recibir mails con resumenes?: No*
  8. *Ocurrencias antes de incluir una alerta: 5*
  9. *Quiere configurar una base de datos: SI*
  10. *Servidor de base de datos: localhost*
  11. *Base de datos: snort*
  12. *Usuario base de datos: snort*
  13. *Contraseña del usuario: srW21cG7*

Verificar que los ficheros de configuración están correctos

- *snort -devyq -c /etc/snort/snort.conf -l /var/log/snort/ -D*
- *snort -c /etc/snort/snort.conf*

Iniciar el servicio del IDS

- */etc/init.d/snort start*

4.5.3.4 IPS – PSAD *[32]*

PSAD es una herramienta que sirve para detectar las exploraciones de puertos y cualquier otro tráfico sospechoso. Ofrece un sistema de umbrales altamente configurables sobre los niveles de peligrosidad, de mensajes alertas, sobre email, DShield, y de bloqueo automático de direcciones IP.
Psad incorpora muchas firmas del paquete incluidas en Snort para detectar varias clases de exploraciones sospechosas.

El IPS es responsable de procesar los paquetes que han sido bloqueados por el firewall y las alertas generadas por el IDS usando la lógica de análisis de la firma del paquete con el fin de determinar el tipo de exploración que se aplica contra la red. Además, tiene la capacidad de autogenerar iptables para rechazar algún tipo de tráfico malicioso.

Configuración de PSAD

El fichero que únicamente se configura es /etc/psad/psad.conf, lo atributos que se editan son los siguientes:

- *nano /etc/psad/psad.conf*
    - *EMAIL_ADDRESSES admin@dominio.com; # Dirección de correo al que se envía notificaciones de alertas.*
    - *HOSTNAME utm02; # Nombre del servidor*
    - *HOME_NET 10.10.0.0/16; # Redes locales*
    - *FW_MSG_SEARCH DROP; # Tipos de acciones sobre las que actuará el IPS.*
    - *IPT_SYSLOG_FILE /var/log/messages; # Fichero del cual lee los mensajes de bloqueo.*
    - *AUTO_IDS_DANGER_LEVEL 3; # Nivel de peligrosidad que se bloquea.*

Realizadas las configuraciones en las opciones antes indicadas se reinicia el servicio para que tenga efecto los cambios.

- */etc/init.d/psad restart*

4.5.3.5 Monitoreo de tráfico de la red - NTOP *[33]*

NTOP es una herramienta que permite monitorizar en tiempo real una red. Es útil para controlar los usuarios y aplicaciones que están consumiendo recursos de red en un instante determinado y para detectar en algunos casos errores en configuraciones de algún equipo, (aparece un banderín verde, amarillo o rojo, dependiendo si es un error leve o grave), o a nivel de servicio.

Posee interfaz web desde el que cualquier usuario con acceso puede ver las estadísticas del monitoreo.

Cuando una máquina se encuentra con algún tipo de virus que genera tormentas de broadcast, se puede detectar usando ésta herramienta. El ataque empezará a propagarse después que el usuario se autentica con servidor freeradius y se encuentra autorizado a utilizar los recursos de red. Mediante el monitoreo de los recursos de red se detectará el origen del problema.

Configuración de NTOP

Por defecto ntop tiene configurada la eth0 para monitorear la red, en el caso que se desee monitorear el tráfico de otras interfaces se ejecuta el comando:

- *dpkg-reconfigure ntop*

En el cuadro de diálogo que muestra se puede poner una o varias interfaces de red separadas por comas para su monitoreo.

Luego se establece la contraseña para el usuario administrador ejecutando:

- *ntop –set-admin-password*

Para iniciar el servicio ejecutar:

- */etc/init.d/ntop start*

Para hacer un seguimiento de la información que obtiene NTOP abrir un navegador web y escribir:

- *http://utm.ente.gob.ec:3000*

4.5.3.6 Configuración de MRTG *[34]*

MRTG es una herramienta que se utiliza para supervisar la carga de tráfico de interfaces de red. MRTG genera un informe en formato HTML con gráficas que proveen una representación visual de la evolución del tráfico a lo largo del tiempo.
Para recolectar la información del tráfico del dispositivo la herramienta utiliza el protocolo SNMP. Este protocolo recolecta la información de la cantidad de bytes que han pasado por ellos distinguiendo entre entrada y salida. Esta cantidad deberá ser tratada adecuadamente para la generación de informes.
Esta aplicación proporciona como salida dos valores numéricos que se corresponden a la entrada y salida. Habitualmente suelen utilizarse scripts que monitorizan la máquina local.

Asimismo, proporciona una aplicación cfgmaker que genera la configuración para un equipo de red de forma automática utilizando la meta información que proporciona SNMP.

Con MRTG se puede llevar estadísticas de la cantidad de tráfico que ingresa y sale por una determinada interfaz de red, sea ésta de un switch, router o servidor, ayudando a detectar en cierto momento saturación de tráfico.

Configuración de MRTG

Habilitar el protocolo SNMP en el equipo a monitorearse.

Crear el directorio donde se guardarán los archivos principales de la información obtenida vía SNMP de cada equipo.

- *mkdir /etc/mrtg*

Crear el directorio donde se publicarán los gráficos del equipo a monitorearse:

- *mkdir /var/www/mrtg* # Dentro de este directorio se crea una carpeta por cada equipo a ser monitoreado.

Generar la información del equipo:

- *cfgmaker --ifref=name comunidad@utm.ente.gob.ec > /etc/mrtg/utm.cfg*

Editar el fichero generado con extensión .cfg y modificar la ruta de graficación de la siguiente manera:

- *nano /etc/mrtg/utm.cfg*
    - Modificar la línea: WorkDir: /var/www/mrtg/utm

Lo siguiente es crear la página html del equipo ejecutando:

- *indexmaker /etc/mrtg/utm.cfg > /var/www/mrtg/utm/index.html*

Finalmente se agrega en el cron del sistema una entrada para que se actualicen las estadísticas de tráfico para el dispositivo cada cinco minutos, de la siguiente manera:

- *Crontab –e*
    - *0-55/5 * * * * env LANG=C /usr/bin/mrtg /etc/mrtg/utm.cfg*

4.5.3.7 Proxy – Squid, SquidGuard, Sarg *[35]*

Un proxy es un programa o dispositivo que realiza una tarea de acceso a internet en lugar de otro ordenador, es un equipo intermediario situado entre el sistema del usuario e internet. Mediante la implementación de esta herramienta se puede tener un registro completo de los usuarios que acceden a internet además de los sitios a los que acceden. Una de las funciones más esenciales es actuar como filtro a ciertos sitios que los usuarios no estén autorizados según el criterio del administrador de la herramienta.

Luego de la autenticación y autorización del usuario a la red, éste puede acceder a cualquier sitio de internet que se encuentre disponible, pero para optimizar el recurso es importante establecer filtros de acceso a dominios públicos autorizados.

El proxy mejora el rendimiento del acceso WEB ya que posee un espacio de almacenamiento llamado caché en el cual se guardan los sitios web visitados con mayor frecuencia, haciendo que el acceso sea más rápido por cuanto ya lo tiene guardado y no necesita ir a internet para presentar dicha página al usuario.

El proxy que se instala en la infraestructura UTM está compuesto por tres elementos:

1. Squid.- Motor proxy
2. SquidGuard.- Módulo de squid para restringir páginas basado en redireccionamiento.
3. Sarg.- Generador de reportes de squid.

Configuración de squid

El fichero principal de configuración de squid es /etc/squid/squid.conf, se especifica las siguientes opciones:

#Definir la red que estará autorizada a navegar por el proxy
acl localnet src 10.10.16.0/21 #Subredes de las VLAN de los usuarios y Servidores.

#Permitir la navegación libre sin restricciones
http_access allow localnet
http_access allow localhost

#Bloquear todo excepto lo anterior
http_access deny all

#Definición del puerto en el que se levantará servicio de proxy
http_port 8081
#Definición del tamaño del cache del proxy
cache_dir ufs /var/spool/squid 35000 16 256

#Definición del tamaño máximo de los objetos que se almacenarán en la cache
maximum_object_size 40960 KB

#Cantidad de peticiones que serán atendidas a la vez
url_rewrite_children 10

#Redirección de solicitud de páginas web a squidguard
redirect_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf

Al finalizar la configuración se verifica si existe errores en ejecutando el siguiente comando:

- *squid -NCd1*

Configuración de SquidGuard

Descargar las listas negras para SquidGuard.

- *cd /tmp*
- *wget http://squidguard.shalla.de/Downloads/shallalist.tar.gz*

Descomprimir el archivo descargado anteriormente.

- *tar –xzvf shallalist.tar.gz*

Mover el directorio BL hacia el directorio /etc/squid/ renombrándolo como acls.

- *mv BL /etc/squid/acls*

Modificar el fichero /etc/squid/squidGuard.conf especificando la siguiente información:

#Directorio donde se encuentran las listas negras
dbhome /etc/squid/acls
#Directorio donde se almacenarán los archivos de log
logdir /var/log/squid

#Definición de horarios de restricción de la navegación.
time workhours {
    weekly mtwhf 08:00 - 16:30
}

#Grupos de usuarios a los que se les permitirá o negará la navegación a Internet. ANEXO 1.

```
source Alto {
        ip          10.10.17.0/27
        ip          10.10.17.32/27
        ip          10.10.17.64/27
        ip          10.10.17.96/27
        ip          10.10.17.128/27
}

source Medio {
        ip          10.10.17.160/28
        ip          10.10.17.176/28
        ip          10.10.17.192/28
        ip          10.10.17.208/28
        ip          10.10.17.224/28
}

source Servidores {
        ip          10.10.20.9
        ip          10.10.20.10
        ip          10.10.20.11
        ip          10.10.20.12
        ip          10.10.20.13
        ip          10.10.20.14
        ip          10.10.20.15
        ip          10.10.20.16
        ip          10.10.20.17
        ip          10.10.20.18
        ip          10.10.20.19
        ip          10.10.20.20
}
```

```
#Definición de clases de listas negras.
destination movies {
        domainlist      movies/domains
        urllist         movies/urls
        redirect        http://utm.ente.gob.ec/error.html
}

destination adv {
        domainlist      adv/domains
        urllist         adv/urls
        redirect        http://utm.ente.gob.ec/error.html
}

destination aggressive {
        domainlist      aggressive/domains
        urllist         aggressive/urls
        redirect        http://utm.ente.gob.ec/error.html
}

destination alcohol {
        domainlist      alcohol/domains
        urllist         alcohol/urls
        redirect        http://utm.ente.gob.ec/error.html
}

destination automobile {
        domainlist      automobile/bikes/domains
        urllist         automobile/bikes/domains
        domainlist      automobile/boats/domains
        urllist         automobile/boats/domains
        domainlist      automobile/cars/domains
        urllist         automobile/cars/domains
        domainlist      automobile/planes/domains
```

```
        urllist         automobile/planes/domains
        redirect        http://utm.ente.gob.ec/error.html
}
destination chat {
        domainlist      chat/domains
        urllist         chat/urls
        redirect        http://utm.ente.gob.ec/error.html
}

#Acls para restricción de listas negras
acl  {
        Super-Rest {
 pass !adv !aggressive !chat !drugs any
        }

default {
                pass    none
                redirect    http://utm.ente.gob.ec/error.html
        }
}
```

Al finalizar la configuración se verifica si existen errores digitando el siguiente comando:

- *squidGuard –d*

Si la configuración está correcta se generan las bases de datos para todas las listas negras descargadas con el comando.

- *squidGuard –C all*

Cambiar el propietario y el grupo del directorio */etc/squid/acls.*

- *chown –R proxy.proxy /etc/squid/acls*

Si la configuración de squid y squidguard están correctas se reinicia el servicio para que los cambios realizados tengan efecto.

- */etc/init.d/squid restart*

Configuración de Sarg

Este componente de squid genera informes en html, con campos como: usuarios, Direcciones IP, bytes transmitidos, sitios web visitados y tiempos.
Los reportes que se generan son guardados en un directorio que se le especifica, y de esta manera se realiza análisis estadísticos sobre el uso de internet.

La configuración es la siguiente:

Crear el directorio /var/www/squid-reports ejecutando:

- *mkdir /var/www/squid-reports*

Se modifica el fichero /etc/sarg/sarg.conf especificando:

#Fichero del log de squid de donde se recopila los datos para generar el reporte.
access_log /var/log/squid/access.log

#Directorio de salida en donde se generan los reportes
output_dir /var/www/squid-reports

Se Modifica el fichero /etc/sarg/sarg-reports.conf especificando la salida de las páginas html con el reporte de navegación:
HTMLOUT=/var/www/squid-reports

Generar un reporte ejecutando el siguiente comando:

- *sarg-reports today*

Para visualizar el reporte generado se abre en un browser la siguiente dirección:

- *http://utm.ente.gob.ec/squid-reports/*

4.6 ESCENARIO DEMOSTRATIVO

Debido a razones de confidencialidad de la información del ente del ministerio de defensa nacional se presenta un escenario demostrativo que cumple con las funcionalidades implementadas en la institución. La topología de red es la siguiente:

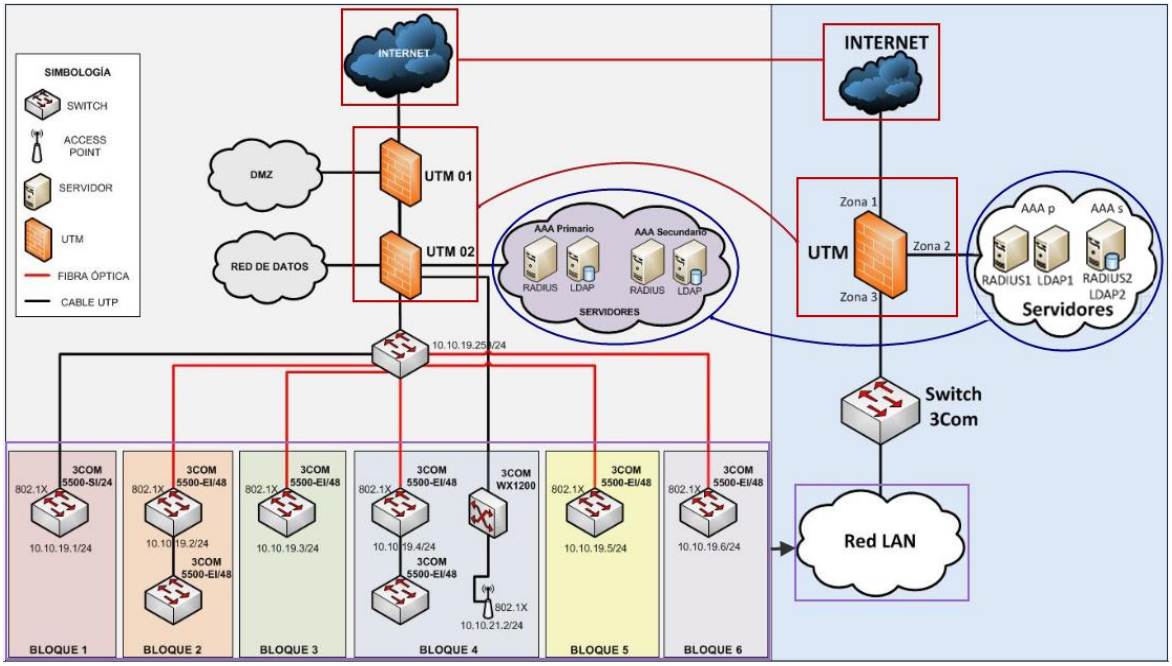


Figura 35. Escenario demostrativo
Fuente: Carlos Plasencia

En la topología mostrada se presenta los componentes de la solución descritos en el presente proyecto:

- Servicio AAA.- Se encuentra en la subred de servidores, conformado por el servidor RADIUS1 (servidor primario), y RADIUS2 (servidor secundario).
- Servicio LDAP.- La base de datos de autenticación se encuentra sobre el servidor LDAP1 y su réplica sobre el servidor RADIUS2. La base de datos constará con 60 usuarios, los mismos que pertenecen a las 5 primeras VLAN descritas en el ANEXO 1.
- Equipos de acceso.- Para la simulación de los equipos de acceso se utiliza un switch cisco catalyst 2950 y un switch 3Com 3226, los mismos que simulan la funcionalidad de los 8 switch 3COM 5500 de la capa de acceso.
- Red LAN.- Simula el acceso de los usuarios hacia la infraestructura de networking.
- UTM.- El servidor simula las funcionalidades de los dos UTM implementados (interno y externo) para control de tráfico entrante y saliente entre las zonas.
- Internet.- Acceso al servicio de navegación.

- Para la simulación del acceso de usuarios a la red wireless se utiliza un Access Point D-Link DWL-2100AP, en el cual se habilita la autenticación mediante 802.1X de la siguiente manera:
    - En la ventana principal de configuración del AP seleccionar la opción Wireless.

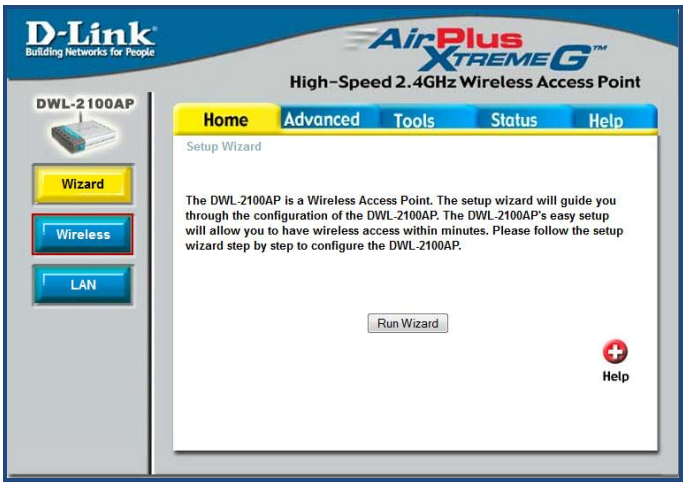


Figura 36.- Ventana principal de configuración del AP D-Link
Fuente: Capturas de la configuración

    - En la ventana que aparece se configura las opciones wireless:
        - Mode.- *Access Point* #Modo de funcionamiento del AP.
        - SSID.- *EXTINTORSW* # SSID
        - Channel.- 6 2.437 GHz #Canal libre
        - Authentication.- WPA2-EAP #Tipo de autenticación

    - En la sección RADIUS Server Settings ingresar los datos del servdor de autenticación.
        - Cipher Type.- AUTO #Tipo de cifrado
        - RADIUS Server.- 10.10.20.12 #IP del servidor AAA
        - RADIUS Port.- 1812 #Puerto de autenticación
        - RADIUS Secret.- prW01MblWir # Secreto compartido

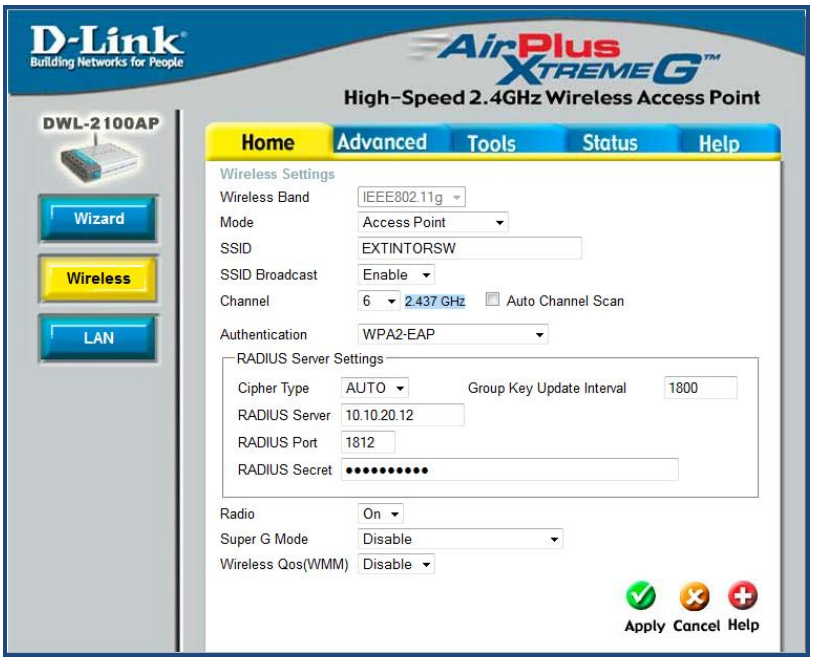


Figura 37. Configuración del Wireless del AP D-Link
Fuente: Capturas de la configuración

Una vez terminado de ingresar todos los parámetros de configuración se guarda los cambios seleccionando la opción Apply.

4.6.1 FUNCIONALIDADES

Servicio AAA.- El servicio se ofrece mediante un servidor primario y otro secundario, los mismos que autentican a los usuarios contra las bases de datos LDAP master y LDAP slave respectivamente. Se encuentran configurados en esquema de alta disponibilidad para evitar de mejor manera la interrupción de servicio en caso de fallas de hardware, mantenimiento u otros eventos no programados.

Equipos de acceso cableado.- Los switches cisco catalyst 2950 y 3Com 3226 representan a los equipos de acceso, los mismos que se configuran como clientes del servidor AAA para realizar la tarea de autenticadores de usuarios, éstos serán los encargados de permitir o denegar el acceso hacia los recursos de red.

Equipo de acceso inalámbrico.- El Access point D-Link representa el acceso de usuarios a la red inalámbrica, el cual está configurado para autenticar a los usuarios usando el servidor AAA.

UTM.- Sobre el servidor se encuentran funcionando los servicios firewall, proxy, DNS interno, MRTG, IDS/IPS y NTOP.

Para el servicio firewall se han configurado tres zonas:

- *Zona 1*.- En el servicio firewall se identifica como zona ***net.*** Se controla el tráfico entrante y saliente hacia internet.
- *Zona 2*.- En el servicio firewall se identifica como zona ***srv.*** Se controla el tráfico entrante y saliente a la subred de servidores. Será responsable de permitir o denegar la autenticación de los usuarios contra el servicio AAA.
- *Zona 3*.- Esta zona se identifica como zona ***loc.*** Se controla el acceso de los usuarios hacia los servicios proxy, correo, AAA, DNS, entre otros.

En el servicio proxy para control de contenidos se han definido tres perfiles de navegación:

- *Alto.-* Este perfil se encuentra restringido la mayoría de las categorías de listas negras.
- *Medio.-* En este perfil se encuentra bloqueado las categorías básicas.
- *Bajo.-* En este perfil se tiene navegación libre excepto a las categorías de pornografía, violencia y citas.
- *Informática*.- Posee un perfil similar al *Medio* pero se permite el acceso para realizar descargas, debido a la necesidad de la adquisición de software para el desarrollo de aplicaciones.

El **DNS** interno es un servicio utilizado para mapear los nombres de los servidores a sus direcciones IP. Este servicio se utiliza únicamente para realizar pruebas de consulta al servicio.

MRTG será el encargado de monitorear la cantidad de tráfico que ingresa y sale por las tres interfaces de red del UTM.

IDS/IPS estarán pendientes de escaneos de puertos y de ataques de firmas sospechosas desde el internet. Generan alertas cuando existen intentos de ataques.

NTOP se activa cuando el administrador de red desea detectar problemas en la red, por ejemplo tormentas de broadcast.

Internet.- Responsable de brindar conectividad hacia dominios públicos que se encuentran en la nube Internet.

4.7 RESULTADOS OBTENIDOS

Para la verificación de funcionalidades del servicio de autenticación AAA se utilizará herramientas que permitan validar el intercambio de información utilizando los parámetros establecidos en el desarrollo del presente trabajo.
Las configuraciones de los equipos del escenario de pruebas se presentan en el ANEXO 7.

Para la captura de las transacciones entre el usuario y el equipo de acceso se utiliza wireshark, las capturas obtenidas son las siguientes:

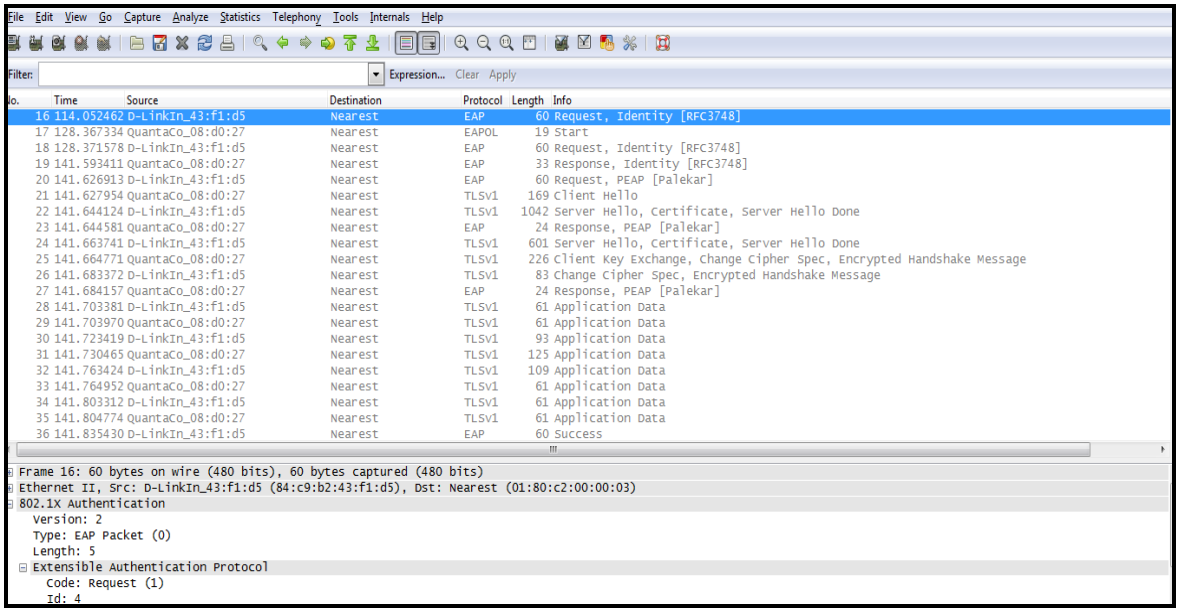
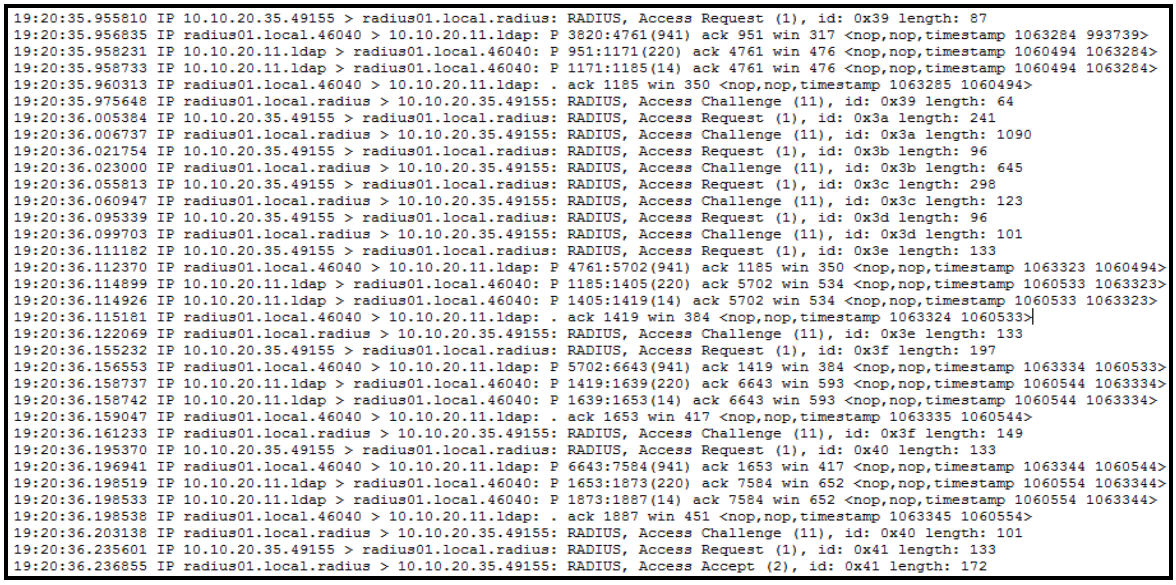


Figura 38. Intercambio de paquetes EAP entre el usuario y el autenticador
Fuente: Capturas con Wireshark

Para verificar las transacciones que se realizan entre el autenticador y el servidor AAA se utiliza el comando TCPDUMP, el cual es un sniffer en los sistemas Linux. De la misma forma en la herramienta se puede observar las

transacciones que se intercambia con el servidor LDAP para la validación de usuario y contraseña.



```
19:20:35.955810 IP 10.10.20.35.49155 > radius01.local.radius: RADIUS, Access Request (1), id: 0x39 length: 87
19:20:35.956835 IP radius01.local.46040 > 10.10.20.11.ldap: P 3820:4761(941) ack 951 win 317 <nop,nop,timestamp 1063284 993739>
19:20:35.958231 IP 10.10.20.11.ldap > radius01.local.46040: P 951:1171(220) ack 4761 win 476 <nop,nop,timestamp 1060494 1063284>
19:20:35.958733 IP 10.10.20.11.ldap > radius01.local.46040: P 1171:1185(14) ack 4761 win 476 <nop,nop,timestamp 1060494 1063284>
19:20:35.960313 IP radius01.local.46040 > 10.10.20.11.ldap: . ack 1185 win 350 <nop,nop,timestamp 1063285 1060494>
19:20:35.975648 IP radius01.local.radius > 10.10.20.35.49155: RADIUS, Access Challenge (11), id: 0x39 length: 64
19:20:36.005384 IP 10.10.20.35.49155 > radius01.local.radius: RADIUS, Access Request (1), id: 0x3a length: 241
19:20:36.006737 IP radius01.local.radius > 10.10.20.35.49155: RADIUS, Access Challenge (11), id: 0x3a length: 1090
19:20:36.021754 IP 10.10.20.35.49155 > radius01.local.radius: RADIUS, Access Request (1), id: 0x3b length: 96
19:20:36.023000 IP radius01.local.radius > 10.10.20.35.49155: RADIUS, Access Challenge (11), id: 0x3b length: 645
19:20:36.055813 IP 10.10.20.35.49155 > radius01.local.radius: RADIUS, Access Request (1), id: 0x3c length: 298
19:20:36.060947 IP radius01.local.radius > 10.10.20.35.49155: RADIUS, Access Challenge (11), id: 0x3c length: 123
19:20:36.095339 IP 10.10.20.35.49155 > radius01.local.radius: RADIUS, Access Request (1), id: 0x3d length: 96
19:20:36.099703 IP radius01.local.radius > 10.10.20.35.49155: RADIUS, Access Challenge (11), id: 0x3d length: 101
19:20:36.111182 IP 10.10.20.35.49155 > radius01.local.radius: RADIUS, Access Request (1), id: 0x3e length: 133
19:20:36.112370 IP radius01.local.46040 > 10.10.20.11.ldap: P 4761:5702(941) ack 1185 win 350 <nop,nop,timestamp 1063323 1060494>
19:20:36.114899 IP 10.10.20.11.ldap > radius01.local.46040: P 1185:1405(220) ack 5702 win 534 <nop,nop,timestamp 1060533 1063323>
19:20:36.114926 IP 10.10.20.11.ldap > radius01.local.46040: P 1405:1419(14) ack 5702 win 534 <nop,nop,timestamp 1060533 1063323>
19:20:36.115181 IP radius01.local.46040 > 10.10.20.11.ldap: . ack 1419 win 384 <nop,nop,timestamp 1063324 1060533>
19:20:36.122069 IP radius01.local.radius > 10.10.20.35.49155: RADIUS, Access Challenge (11), id: 0x3e length: 133
19:20:36.155232 IP 10.10.20.35.49155 > radius01.local.radius: RADIUS, Access Request (1), id: 0x3f length: 197
19:20:36.156553 IP radius01.local.46040 > 10.10.20.11.ldap: P 5702:6643(941) ack 1419 win 384 <nop,nop,timestamp 1063334 1060533>
19:20:36.158737 IP 10.10.20.11.ldap > radius01.local.46040: P 1419:1639(220) ack 6643 win 593 <nop,nop,timestamp 1060544 1063334>
19:20:36.158742 IP 10.10.20.11.ldap > radius01.local.46040: P 1639:1653(14) ack 6643 win 593 <nop,nop,timestamp 1060544 1063334>
19:20:36.159047 IP radius01.local.46040 > 10.10.20.11.ldap: . ack 1653 win 417 <nop,nop,timestamp 1063335 1060544>
19:20:36.161233 IP radius01.local.radius > 10.10.20.35.49155: RADIUS, Access Challenge (11), id: 0x3f length: 149
19:20:36.195370 IP 10.10.20.35.49155 > radius01.local.radius: RADIUS, Access Request (1), id: 0x40 length: 133
19:20:36.196941 IP radius01.local.46040 > 10.10.20.11.ldap: P 6643:7584(941) ack 1653 win 417 <nop,nop,timestamp 1063344 1060544>
19:20:36.198519 IP 10.10.20.11.ldap > radius01.local.46040: P 1653:1873(220) ack 7584 win 652 <nop,nop,timestamp 1060554 1063344>
19:20:36.198533 IP 10.10.20.11.ldap > radius01.local.46040: P 1873:1887(14) ack 7584 win 652 <nop,nop,timestamp 1060554 1063344>
19:20:36.198538 IP radius01.local.46040 > 10.10.20.11.ldap: . ack 1887 win 451 <nop,nop,timestamp 1063345 1060554>
19:20:36.203138 IP radius01.local.radius > 10.10.20.35.49155: RADIUS, Access Challenge (11), id: 0x40 length: 101
19:20:36.235601 IP 10.10.20.35.49155 > radius01.local.radius: RADIUS, Access Request (1), id: 0x41 length: 133
19:20:36.236855 IP radius01.local.radius > 10.10.20.35.49155: RADIUS, Access Accept (2), id: 0x41 length: 172
```

Figura 39. Intercambio de paquetes EAP entre el servidor AAA y el autenticador
Fuente: Capturas con tcpdump

4.7.1 DESCRIPCIÓN DE PAQUETES CAPTURADOS

Cuando inicia el proceso de autenticación en la comunicación AAA, el equipo del usuario envía una petición de inicio EAP.

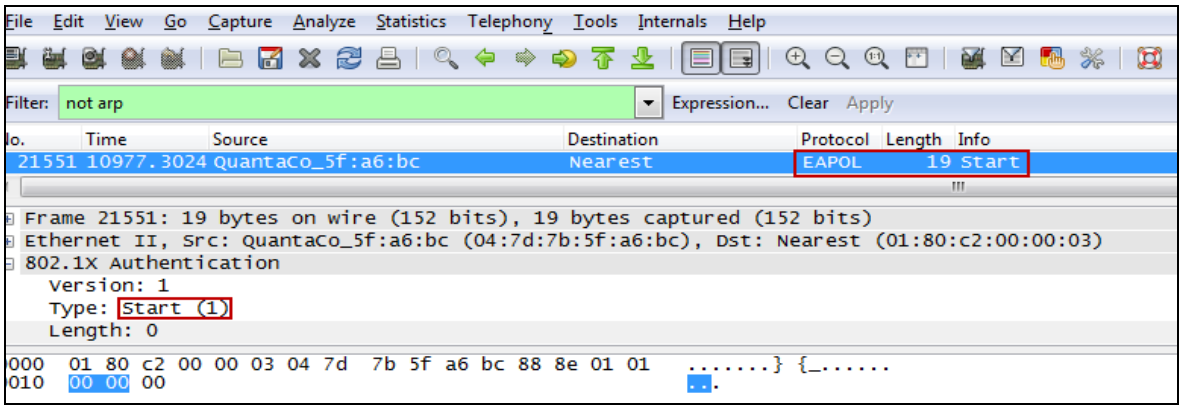


Figura 40. Inicio de autenticación EAP
Fuente: Capturas con wireshark

El autenticador envía al usuario una solicitud de identidad:

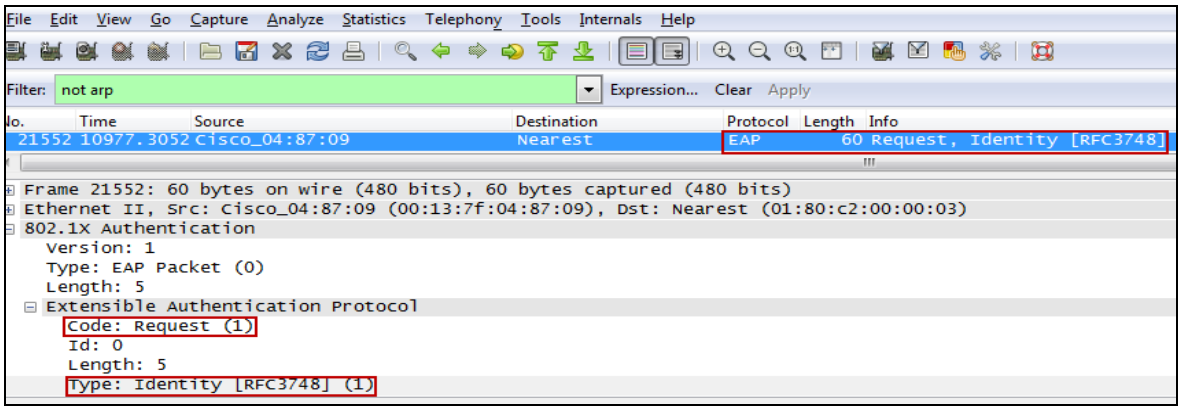


Figura 41. Solicitud de identidad EAP
Fuente: Capturas con wireshark

El usuario envía sus credenciales de conexión al autenticador.

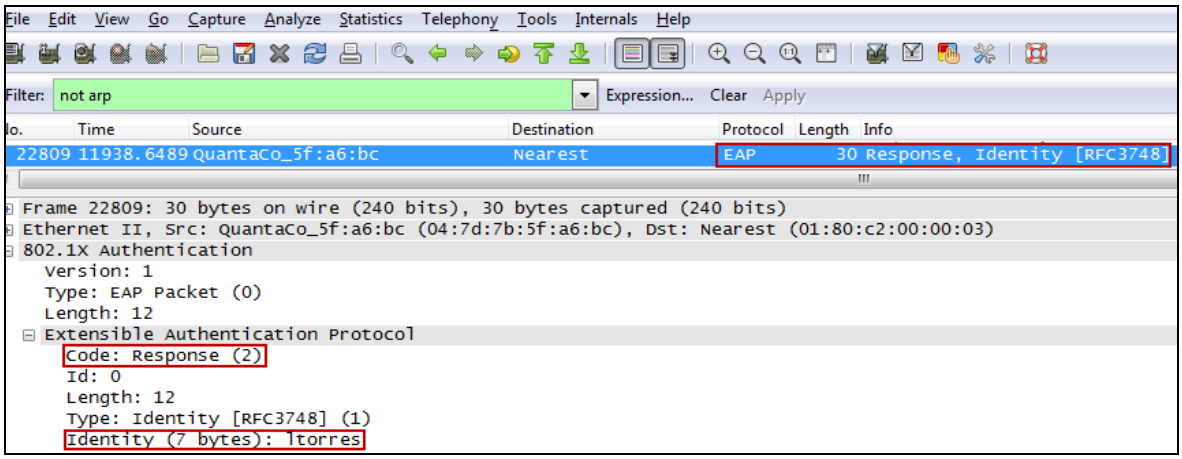


Figura 42. EAP de respuesta
Fuente: Capturas con wireshark

Luego el autenticador encapsula la respuesta EAP en un mensaje RADIUS y la envía al servidor de autenticación AAA para que realice la respectiva validación usando la base de usuarios LDAP.

```
19:20:35.955810 IP 10.10.20.35.49155 > radius01.local.radius: RADIUS, Access Request (1), id: 0x39 length: 87
19:20:35.956835 IP radius01.local.46040 > 10.10.20.11.ldap: P 3820:4761(941) ack 951 win 317 <nop,nop,timestamp 1063284 993739>
19:20:35.958231 IP 10.10.20.11.ldap > radius01.local.46040: P 951:1171(220) ack 4761 win 476 <nop,nop,timestamp 1060494 1063284>
19:20:35.958733 IP radius01.local.46040 > 10.10.20.11.ldap: P 1171:1185(14) ack 4761 win 476 <nop,nop,timestamp 1060494 1063284>
19:20:35.960313 IP radius01.local.46040 > 10.10.20.11.ldap: . ack 1185 win 350 <nop,nop,timestamp 1063285 1060494>
```

Figura 43. Intercambio de paquetes EAP entre el servidor AAA y el autenticador
Fuente: Capturas con tcpdump

El servodor AAA valida el nombre del usuario en la base de datos LDAP y luego envía un RADIUS de negociación al autenticador con el tipo de autenticación EAP que se establece entre el usuario y el servidor, en este caso PEAP.

```
IP radius01.local.radius > 10.10.20.35.49155: RADIUS, Access Challenge (11), id: 0x39 length: 64
```

Figura 44. RADIUS de negociación PEAP
Fuente: Capturas con tcpdump

El autenticador enviará al usuario la petición de establecimiento de una comunicación PEAP.

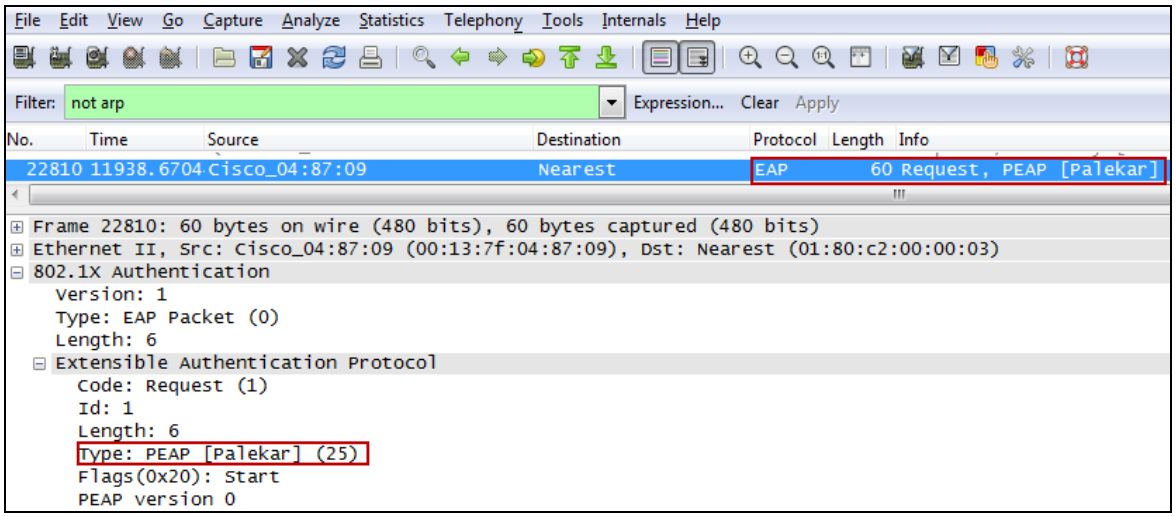


Figura 45. Solicitud de comunicación PEAP
Fuente: Capturas con wireshark

El usuario negocia el método de la conexión y envía al autenticador un EAP de respuesta con el saludo para establecimiento del canal TLS (client hello).

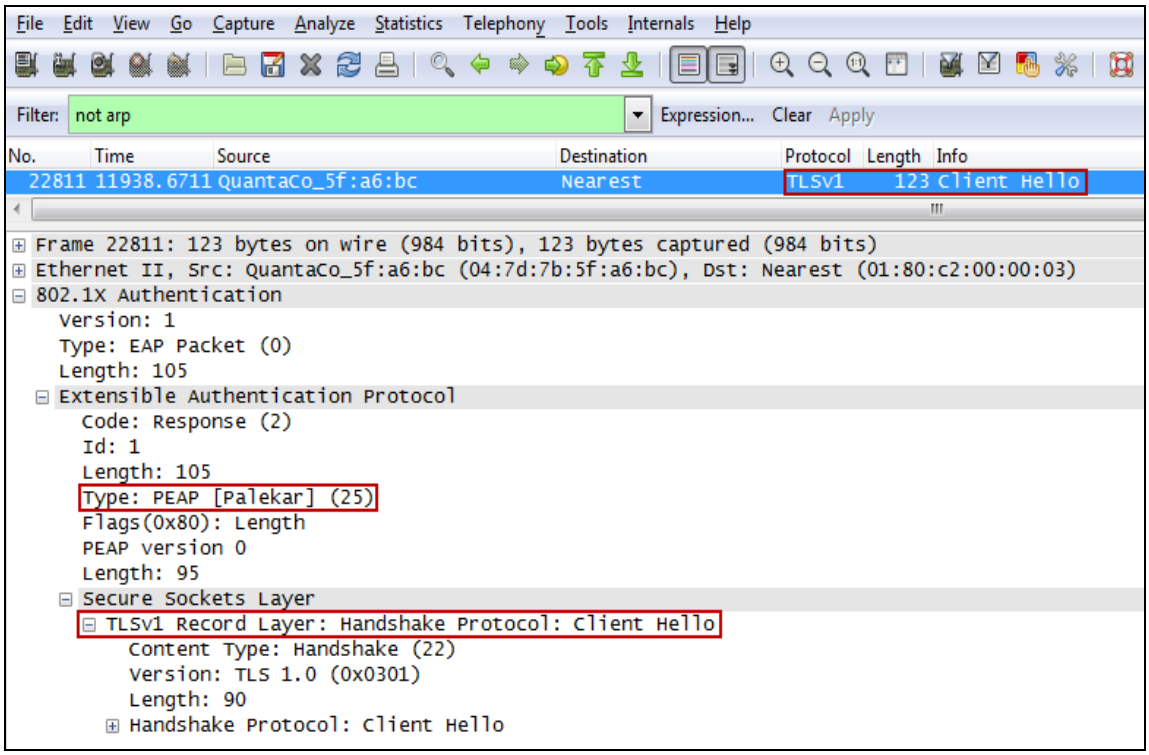


Figura 46. Negociación del canal TLS
Fuente: Capturas con wireshark

EL autenticador encapsula la trama EAP-Response en un mensaje RADIUS-request y lo envía al servidor.

```
IP 10.10.20.35.49155 > radius01.local.radius: RADIUS, Access Request (1), id: 0x3a length: 241
```

Figura 47. Inicio de establecimiento del canal TLS
Fuente: Capturas con tcpdump

EL servidor verifica el mensaje enviado por el usuario y le responde con su certificado en un mensaje RADIUS-Challenge.

```
IP radius01.local.radius > 10.10.20.35.49155: RADIUS, Access Challenge (11), id: 0x3a length: 1090
```

Figura 48. Respuesta TLS del servidor
Fuente: Capturas con tcpdump

El autenticador recibe el mensaje RADIUS y envía el certificado del servidor al usuario en un EAP-request TLS de credencial del usuario.

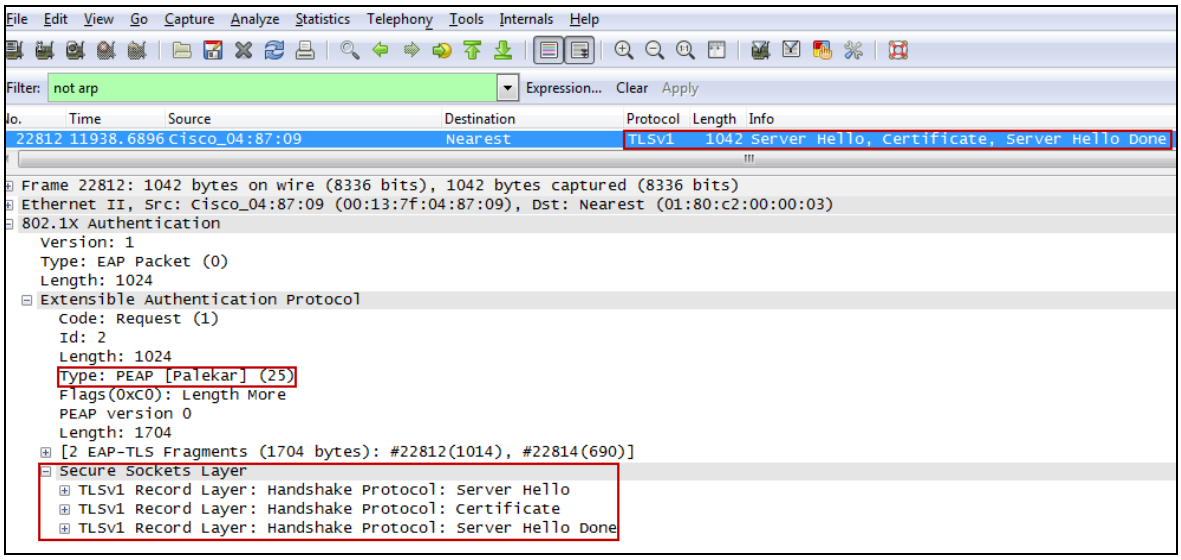


Figura 49. EAP request TLS
Fuente: Capturas con wireshark

El usuario responde una trama EAP confirmando el establecimiento de la autenticación PEAP.

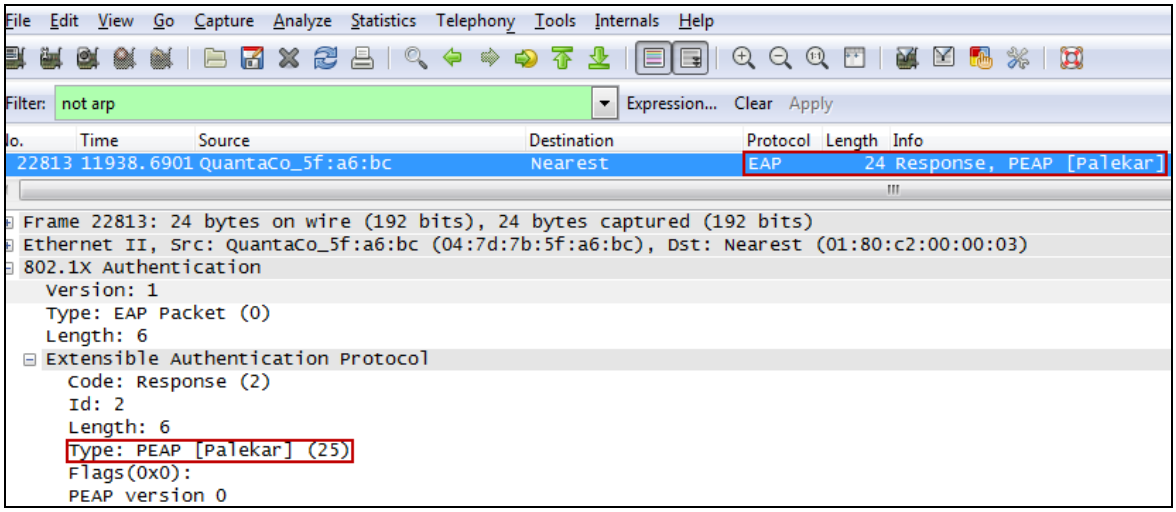


Figura 50. Establecimiento de autenticación PEAP
Fuente: Capturas con wireshark

El autenticador encapsula la trama EAP en un mensaje RADIUS y la envía al servidor AAA.

```
IP 10.10.20.35.49155 > radius01.local.radius: RADIUS, Access Request (1), id: 0x3b length: 96
```

Figura 51. Confirmación de establecimiento del canal PEAP
Fuente: Capturas con tcpdump

Nuevamente el servidor envía su certificado en un mensaje RADIUS al autenticador para cifrar el canal antes negociado (PEAP).

```
IP radius01.local.radius > 10.10.20.35.49155: RADIUS, Access Challenge (11), id: 0x3b length: 645
```

Figura 52. Envío del certificado del servidor
Fuente: Capturas con tcpdump

El autenticador recibe el mensaje RADIUS y envía el certificado del servidor al usuario en un EAP-request TLS de contraseña de cifrado.

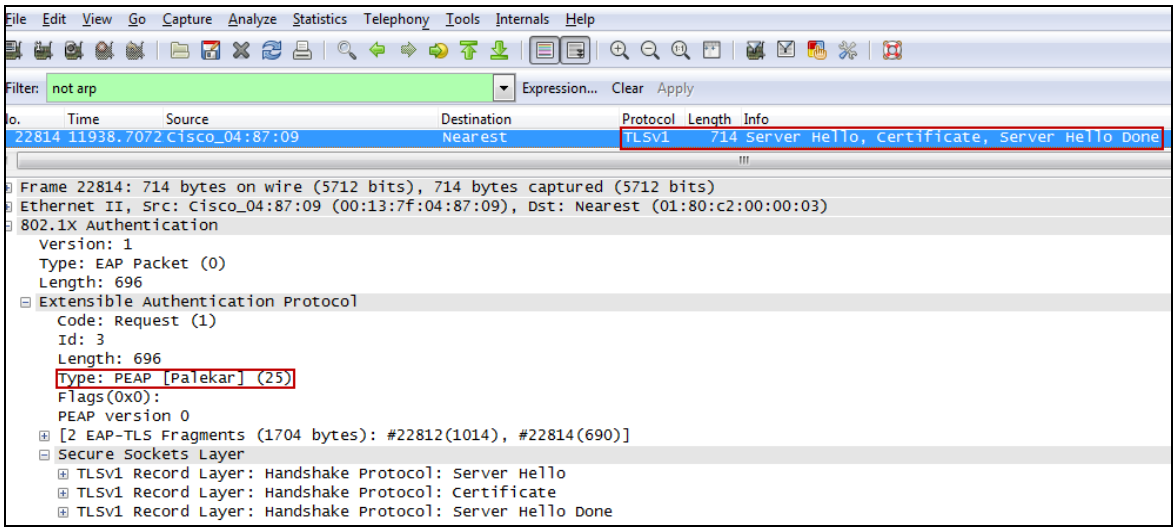


Figura 53. EAP request TLS
Fuente: Capturas con wireshark

El usuario responde un mensaje EAP intercambiando la contraseña para cifrar el canal.

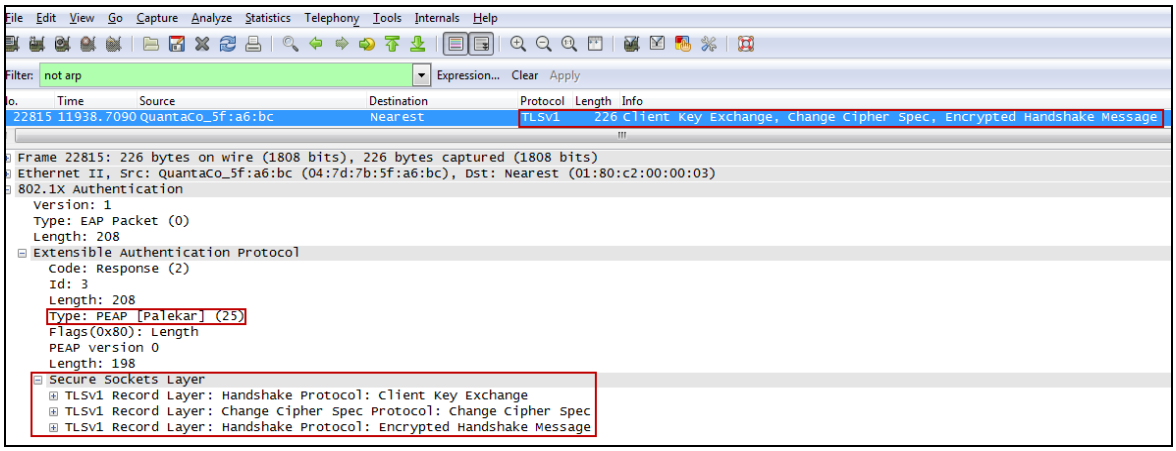


Figura 54. Envío de contraseña para cifrar el canal
Fuente: Capturas con wireshark

El autenticador encapsula la trama EAP en un mensaje RADIUS y la envía al servidor AAA.

```
IP 10.10.20.35.49155 > radius01.local.radius: RADIUS, Access Request (1), id: 0x3d length: 96
```

Figura 55. Solicitud de validación de contraseña para cifrado del canal
Fuente: Capturas con tcpdump

Confirmación del canal PEAP cifrado en un mensaje RADIUS al autenticador.

```
IP radius01.local.radius > 10.10.20.35.49155: RADIUS, Access Challenge (11), id: 0x3d length: 101
```

Figura 56. RADIUS con Confirmación de canal cifrado
Fuente: Capturas con tcpdump

El autenticador envía al usuario la confirmación del canal cifrado

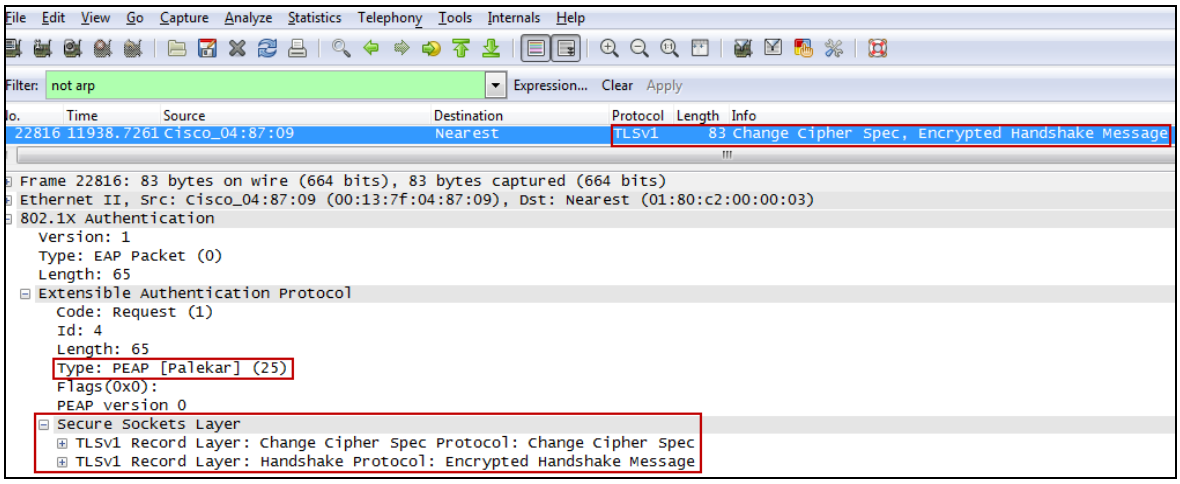


Figura 57. EAP confirmación de PEAP cifrado
Fuente: Capturas con wireshark

El usuario confirma el establecimiento del canal cifrado y se encuentra listo para negociar los atributos ofrecidos por el servidor AAA al usuario.

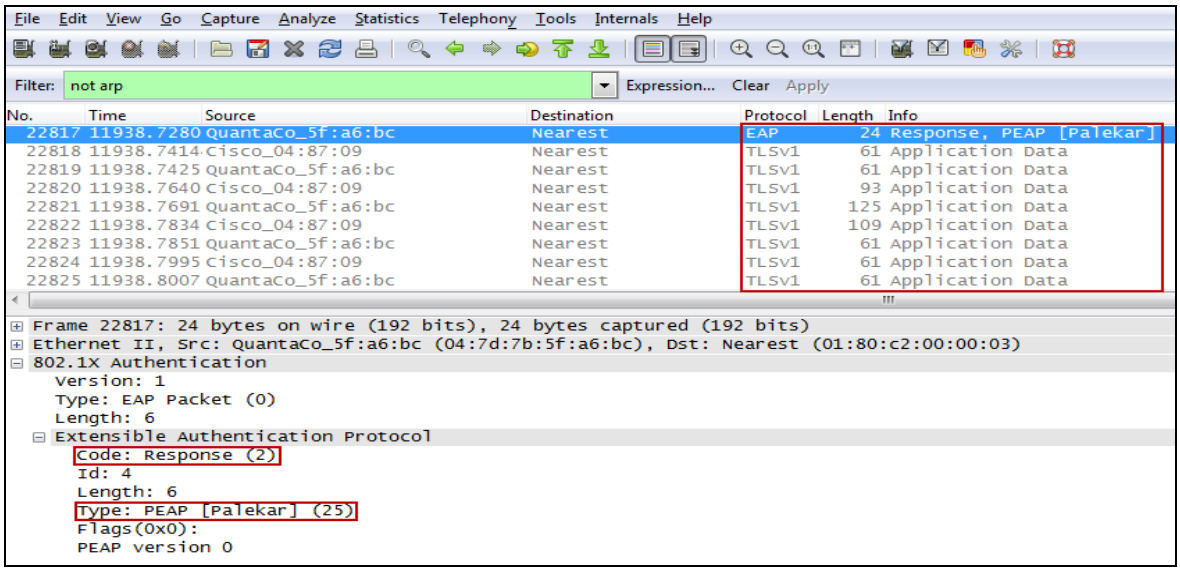


Figura 58. Negociación de atributos RADIUS
Fuente: Capturas con wireshark

De la misma manera el servidor AAA negocia los atributos establecidos para el usuario en la base de datos LDAP.

```
IP 10.10.20.35.49155 > radius01.local.radius: RADIUS, Access Request (1), id: 0x3e length: 133
IP radius01.local.46040 > 10.10.20.11.ldap: P 4761:5702(941) ack 1185 win 350 <nop,nop,timestamp 1063323 1060494>
IP 10.10.20.11.ldap > radius01.local.46040: P 1185:1405(220) ack 5702 win 534 <nop,nop,timestamp 1060533 1063323>
IP 10.10.20.11.ldap > radius01.local.46040: P 1405:1419(14) ack 5702 win 534 <nop,nop,timestamp 1060533 1063323>
IP radius01.local.46040 > 10.10.20.11.ldap: . ack 1419 win 384 <nop,nop,timestamp 1063324 1060533>
IP radius01.local.radius > 10.10.20.35.49155: RADIUS, Access Challenge (11), id: 0x3e length: 133
IP 10.10.20.35.49155 > radius01.local.radius: RADIUS, Access Request (1), id: 0x3f length: 197
IP radius01.local.46040 > 10.10.20.11.ldap: P 5702:6643(941) ack 1419 win 384 <nop,nop,timestamp 1063334 1060533>
IP 10.10.20.11.ldap > radius01.local.46040: P 1419:1639(220) ack 6643 win 593 <nop,nop,timestamp 1060544 1063334>
IP 10.10.20.11.ldap > radius01.local.46040: P 1639:1653(14) ack 6643 win 593 <nop,nop,timestamp 1060544 1063334>
IP radius01.local.46040 > 10.10.20.11.ldap: . ack 1653 win 417 <nop,nop,timestamp 1063335 1060544>
IP radius01.local.radius > 10.10.20.35.49155: RADIUS, Access Challenge (11), id: 0x3f length: 149
IP 10.10.20.35.49155 > radius01.local.radius: RADIUS, Access Request (1), id: 0x40 length: 133
IP radius01.local.46040 > 10.10.20.11.ldap: P 6643:7584(941) ack 1653 win 417 <nop,nop,timestamp 1063344 1060544>
IP 10.10.20.11.ldap > radius01.local.46040: P 1653:1873(220) ack 7584 win 652 <nop,nop,timestamp 1060554 1063344>
IP 10.10.20.11.ldap > radius01.local.46040: P 1873:1887(14) ack 7584 win 652 <nop,nop,timestamp 1060554 1063344>
IP radius01.local.46040 > 10.10.20.11.ldap: . ack 1887 win 451 <nop,nop,timestamp 1063345 1060554>
IP radius01.local.radius > 10.10.20.35.49155: RADIUS, Access Challenge (11), id: 0x40 length: 101
IP 10.10.20.35.49155 > radius01.local.radius: RADIUS, Access Request (1), id: 0x41 length: 133
```

Figura 59. Negociación de atributos RADIUS para el usuario
Fuente: Capturas con tcpdump

Si todo el proceso anterior ha sido satisfactorio se envía un mensaje RADIUS Accept para autorizar al usuario hacer uso de los recursos de la red, caso contrario, si el proceso falla el servidor AAA envía un mensaje RADIUS Reject y el usuario no tiene acceso a la infraestructura de networking.

```
IP radius01.local.radius > 10.10.20.35.49155: RADIUS, Access Accept (2), id: 0x41 length: 172
```

Figura 60. Mensaje RADIUS de autenticación satisfactoria
Fuente: Capturas con tcpdump

El mensaje RADIUS de éxito es enviado hacia el autenticador, y este lo envía al usuario un EAP de éxito y le autoriza a utilizar los recursos de la red.

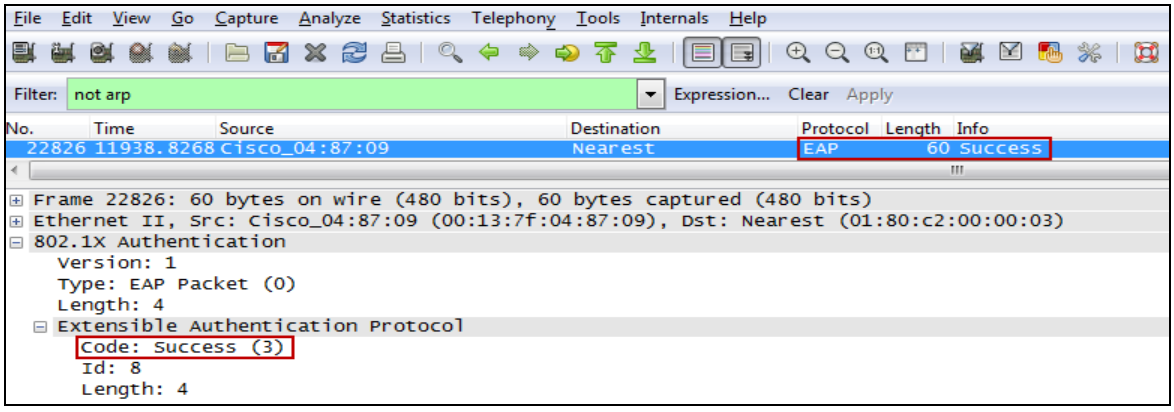


Figura 61. Validación Exitosa
Fuente: Capturas con wireshark

En caso que la autenticación falle la trama que se envía al usuario es un EAP de falla.

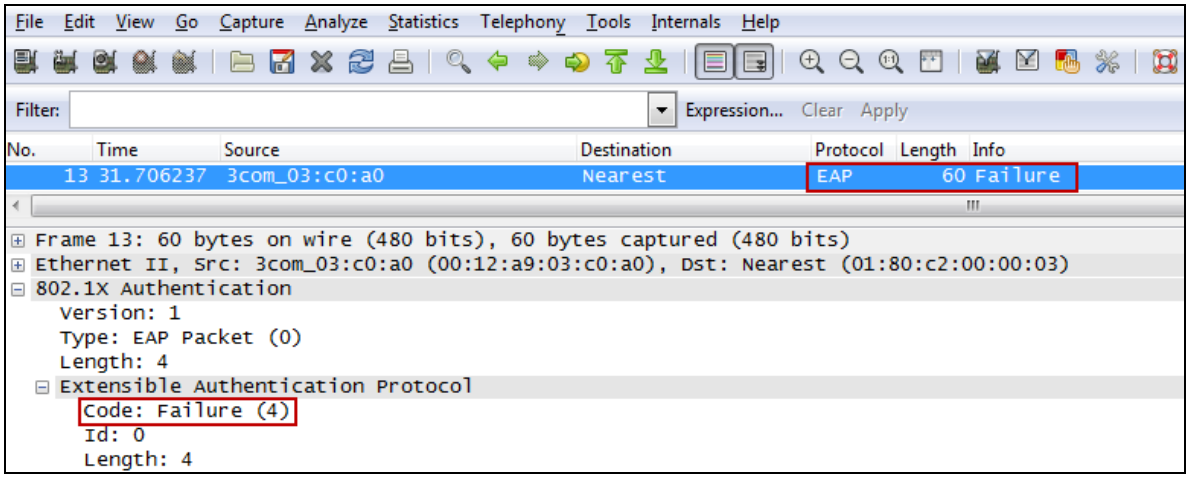


Figura 62. EAP de acceso no autorizado
Fuente: Capturas con wireshark

Es importante señalar que todo el proceso antes descrito es similar tanto para la autenticación de la red cableada como en la red inalámbrica, además es totalmente transparente para el usuario.

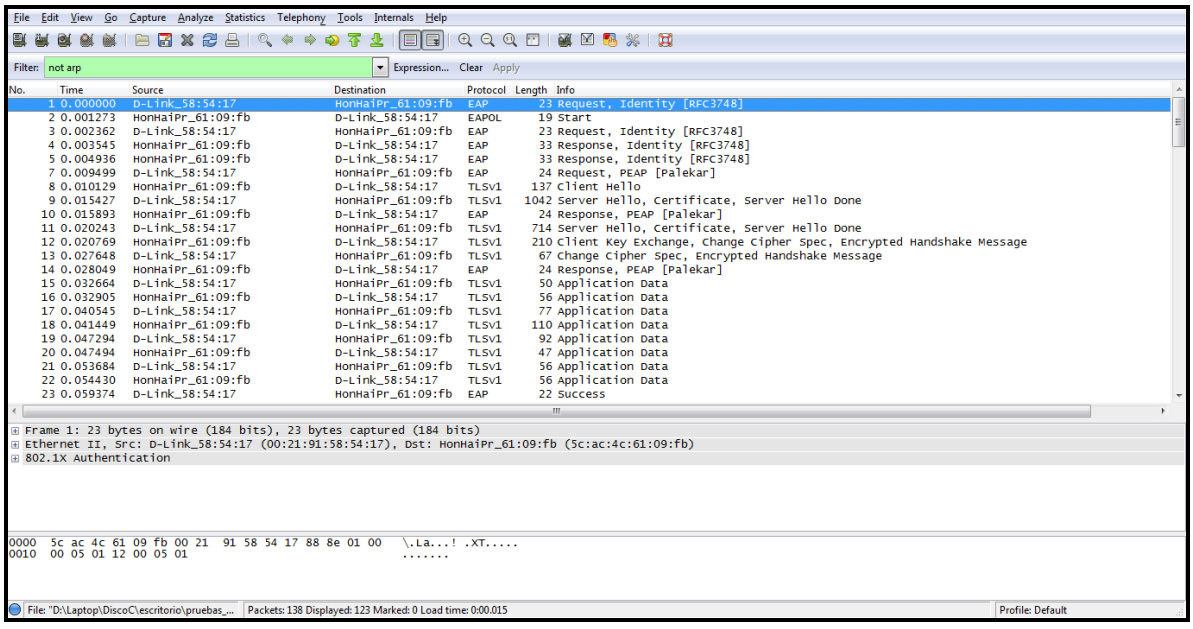


Figura 63. Tramas intercambiadas con el AP D-Link
Fuente: Capturas con wireshark

4.7.2 ACCESO A LA BASE DE DATOS LDAP

Para la administración y gestión de la base de datos de usuarios se utiliza la herramienta phpldapadmin, la misma que permite agregar, eliminar, modificar usuarios y atributos de manera sencilla. La interfaz de administración es la siguiente:

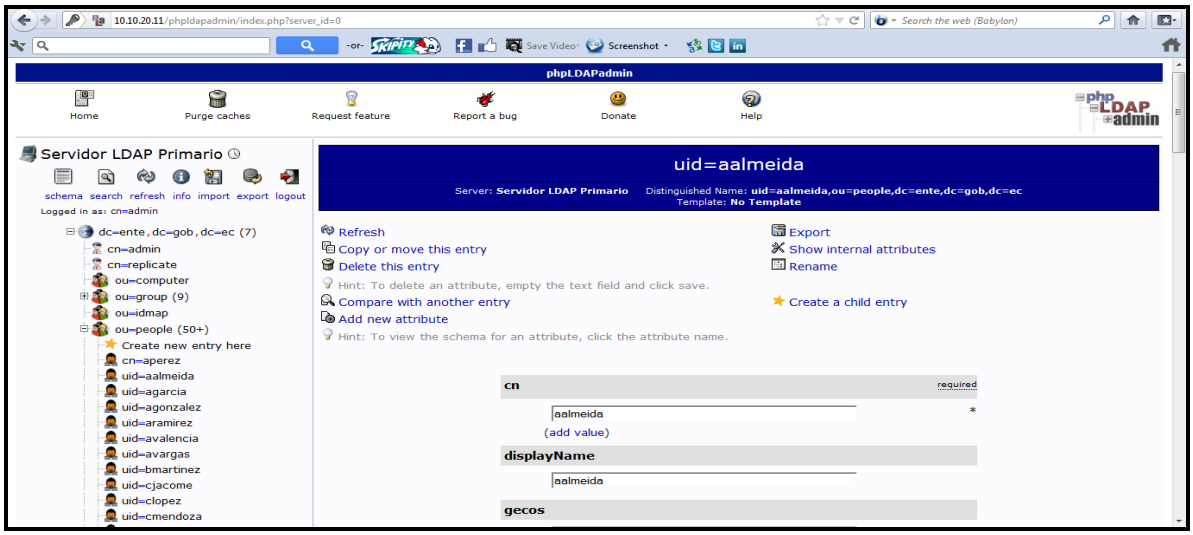


Figura 64. Administración de LDAP usando phpldapadmin
Fuente: Capturas de la interfaz WEB

La base de autenticación de donde busca el servidor AAA a los usuarios para la autenticación es *"ou=peole,dc=ente,dc=gob,dc=ec".* Dentro de la unidad organizativa llamada "*people*" se encuentran todos los usuarios creados con el comando:

- *smbldap-useradd –a –P nombre_usuario*
    - *El parámetro –a sirve para indicar que es un usuario Windows,*
    - *El parámetro –P sirve para ingresar la contraseña del usuario*

Para cambiar la contraseña de un usuario se usa el comando:

- *smbldap-passwd nombre_usuario*

Para eliminar la cuenta de un usuario se usa el comando:

- *smbldap-userdel nombre_usuario*, o directamente desde phpldapadmin.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- El servidor AAA valida a los usuarios que intentan acceder a la infraestructura de networking de la institución, consultando la base de datos de usuarios LDAP, si el usuario no es encontrado o la contraseña es incorrecta, el servidor rechaza la petición de acceso del usuario, y no le permite hacer uso de los recursos ofrecidos en la institución.

- El método de autenticación PEAP es uno de los más utilizados dentro de implementaciones AAA debido a la facilidad de integración y por su elevado nivel de seguridad. Cuando el usuario se autentica contra el servidor usando su nombre y contraseña el canal se cifra usando TLS basado en la confianza del certificado digital del servidor.

- Poseer esquemas de seguridad es imprescindible para proteger la información que circula por la red. Como se apreció en el presente trabajo con la implementación del estándar 802.1X se controla a los usuarios que acceden a la red interna de la institución otorgando acceso únicamente al usuario permitido.

- El sistema de autentificación esta implementado en todos los dispositivos que soportan el estándar 802.1X. En la actualidad la mayoría de equipos de acceso de distintas marcas están diseñados con soporte del estándar facilitando la integración de seguridad en redes que no poseen control de acceso de sus usuarios.

- El estándar 802.1X es un componente primordial de las mejores recomendaciones de seguridad actual y futura, por lo cual su adopción es una práctica que no solo eleva el nivel de seguridad de las infraestructuras

de acceso cableado e inalámbrico, sino que prepara a las organizaciones para llegar a cumplir con los futuros estándares de seguridad.

- El usar bases de datos para realizar la autenticación de usuarios centraliza y facilita la administración de usuarios, ya que si se desea cambiar de contraseña, sólo se cambia una sola vez.

- La implementación de infraestructura de seguridad trabaja adecuadamente cuando se encuentra apoyada por normas y políticas sobre el uso de recursos informáticos como son: usuarios, contraseñas, internet, portales web, etc.

- El sistema operativo Linux seleccionado para la instalación del servidor AAA fue Debian para mantener un estándar a nivel de las aplicaciones y servicios en la institución, además por las ventajas que posee en cuanto a la virtualización, ya que la limitación que se presenta es por la capacidad de hardware más no por la cantidad de máquinas virtuales que pueden crearse sin costo alguno.

- Llegar a tener seguridad total en una red es inalcanzable pero con la mejora continua y la adopción de métodos y estándares de seguridad de la información se mantiene un nivel de seguridad aceptable que reduce los riesgos de la red.

- A pesar de las existencias de nuevas técnicas y dispositivos innovadores con respecto a la administración de seguridad, se puedan usar viejas técnicas o soluciones para adaptarse a cada situación. Por ejemplo el uso de shorewall para control de tráfico entre zonas no es una herramienta nueva, sino es una aplicación con bastante trayectoria pero que posee gran versatilidad en el bloqueo de tráfico no permitido.

- El uso de soluciones Open Source en las instituciones públicas del país se ha convertido en un punto fundamental en la implementación de

soluciones tecnológicas. El trabajo y tiempo dedicado a estas tecnologías brinda cierto nivel de confianza y reduce en gran medida el costo de desarrollo.

- El usuario es el elemento principal que interviene en el funcionamiento de las tecnologías de la información; las mismas que se encuentran implementados para asegurar y facilitar el desarrollo de las actividades laborales.

- El emplear el servicio ssh para la administración remota por línea de comandos de los servidores evita que ataques como “hombre en el medio” puedan llevarse a cabo, ya que al interceptar el tráfico, éste se encuentra encriptado.

- El software de código abierto tiene una gran aceptación y cada vez va ganando más espacio por la robustez y bajos costes que demanda la puesta en producción.

- La paravirtualizacion en el entorno Debian es una arquitectura que optimiza los recursos de un servidor físico, permitiendo la ejecución de las instrucciones de las máquinas virtuales directamente en el Kernel pero manejándose cada una como un servicio totalmente independiente. Si una máquina virtual falla los demás servicios no se afectan.

- Las herramientas de monitoreo como MRTG y NTOP ayudan al administrador de la red a tener referencias sonbre el consumo de recursos de la red, facilitándoles la detección de problemas como: saturación de servicios, tormentas de broadcast, entre otros.

- La utilización de un IDS/IPS previene a la red interna de ataques que pueden producirse desde el exterior, detectando escaneos de puertos o intentos de inserción de código malicioso en el tráfico que ingresa a la red.

5.2 RECOMENDACIONES

- Se debe implementar bitácoras en las que se registre cambios en los sistemas implementados y se debe actualizar cada vez que se modifique una configuración o se implementen nuevos esquemas.

- Cada vez que un usuario deje de utilizar el sistema de autenticación y servicios asociados debe ser eliminado de la base de datos LDAP, para facilitar la administración de la misma y mantenerla organizada.

- Se debe realizar evaluaciones periódicas del funcionamiento tanto de la infraestructura de control de usuarios como las normas y políticas que se están aplicando en la institución con el fin de verificar si se están mitigando los riesgos de seguridad de la información, y en el caso de que no se estén cumpliendo les permita tomar medidas.

- El canal dedicado de CNT se lo debe contratar como servicio alterno de internet y de esta manera balancear la navegación en el UTM externo, con la finalidad de obtener mayor disponibilidad del servicio.

- El administrador de la infraestructura de seguridad debe realizar revisiones periódicas para verificar las actualizaciones de reglas del IDS/IPS y listas negras del proxy, debido a que éstas cambian diariamente por la cantidad de ataques que pueden llevarse a cabo desde internet.

- Para el buen funcionamiento de las herramientas de seguridad es necesario educar a los usuarios para el manejo adecuado de las mismas, ya que de nada sirve implementar las mejores herramientas si los usuarios no respetan las políticas y normas descritas en el SGSI y documentos de seguridad de la institución.

- Al emplear mecanismos de autenticación basados en nombre de usuario y contraseña, es necesario difundir a los usuarios las normas y políticas y la importancia del cumplimiento de las mismas.

- Realizar mantenimientos periódicos por lo menos cada 6 meses de las infraestructuras tecnológicas para garantizar el buen funcionamiento de las mismas (revisión de logs, almacenamiento, actualizaciones, entre otras).
- Generar planes de concientización de los usuarios con la finalidad de mejorar el uso de las tecnologías de la información y evitar que por razones de desconocimiento no se aproveche al máximo los recursos disponibles en la institución.

- Se debe establecer políticas de respaldo de información de los servicios críticos de la institución, en este caso es importante realizar backups de la base de datos de usuarios LDAP, configuraciones del servidor AAA y switches de acceso.

- Revisar constantemente el uso de recursos de los servidores usando únicamente un software de monitoreo, debido a que la utilización de varios sistemas de monitoreo producen mayor consumo de recursos del servicio monitoreado.

- En los sistemas Linux basados en la distribución Debian que utilizan los gestores de paquetes *apt* y *aptitude* se recomienda utilizar la desinstalación de paquetes con el comando *aptitude remove* para evitar que se queden instaladas librerías huérfanas de una aplicación.

- Se recomienta la implementación de servicios AAA en las redes que se quiera tener control de los usarios que acceden a los recursos de la red evitanto el acceso no autorizado de personas ajenas a la institución.

- Es recomendable implementar la arquitectura de paravirtualizacion en entornos que se posea infraestructuras de servidores robustas para aprovechar al máximo sus recursos.

- Se recomienta la implementación del método de autenticación PEAP cuando se desee autenticar usuarios basados en el nombre de la cuenta y contraseña, facilitando la adopción de métodos de seguridad de la información sin procedimientos complejos para el usuario.

REFERENCIAS BIBLIOGRÁFICAS

[1] 3Com Switch 5500 Family. (s.f.) *Configuration Guide. Internet 6 de Junio del 2010* Recuperado de: http://support.3com.com/infodeli/tools/switches/5500/DUA1715-0BAA01.pdf

[33] Administrador, (2012) TUTORIAL NTOP: MANUAL PRACTICO DE NTOP. En *Armgasa*. Recuperado de: http://www.armgasa.com/index.php?option=com_content&view=article&id=70:ntop&catid=53:ntop&Itemid=71

[20] Ags, Dans. (2011, Septiembre 2) *Breve semblanza de Red Hat* [Red Hat-RPM y su importancia para Linux] Recuperado de: http://www.clubso.com.ar/forum/topic_1538/last

[8] Baonza, Clara. *(n.d.)* En *Cypsela.* Recuperado de: http://www.cypsela.es/especiales/pdf206/confidencialidad.pdf

[17] Borges Esteban. (2010) SCP corriendo en background. En *Encuentroalternativo*. Recuperado de: http://www.encuentroalternativo.com/scp-corriendo-en-background/

[24] Buyya, Rajkumar. HIGH PERFORMANCE CLUSTER COMPUTING: ARCHITECTURES AND SYSTEMS Vol. 1, Prentice All, Australia, 1999.

[28] CANAIMA. (n.d.) Freeradius con Soporte EAP-TLS e Integrado LDAP. En *freeradius*. Recuperado de: http://wiki.canaima.softwarelibre.gob.ve/mediawiki/index.php?title=Especial:PdfPrint&page=Freeradius

[34] Caterpillar. (2009) SNMP and MRTG on Debian. *En Jitamitra.* Recuperado de: http://jitamitra.blogspot.com/2009/02/snmp-and-mrtg-on-debian.html

[13] Cepeda, César & Proaño Pablo. (2007). DISEÑO E IMPLEMENTACIÓN DE UN CLIENTE RADIUS EN LINUX.Recuperada de: http://dspace.epn.edu.ec/bitstream/15000/8963/5/T10761CAP1.pdf

[6] Chamorro Juan M. (2005). En *Consideraciones para la implementación de 802.1x en WLAN's.* Recuperado de: http://www.sans.org/reading_room/whitepapers/wireless/consideraciones-para-la-implementacion-de-8021x-en-wlan-039-s_1607

[14] Cisco Systems, FUNDAMENTOS DE SEGURIDAD DE REDES, Pearson Educación, Madrid, 2005.

[31] Corletti Estrada, Alejandro. (2011) SEGURIDAD POR NIVELES. Recuperado de: http://www.jampudia.com/wp-content/uploads/2011/09/ Seguridad_por_Niveles_v001.pdf

[7] Debby Russell & G.T. Gangemi (1991). *COMPUTER SECURITY BASICS*, Estados Unidos, O'reilly.

[10] Dhanjani Nitersh, *CLAVES HACKERS EN LINUX Y UNIX*, Mc Graw-hill, Madrid, 2004.

[29] Eastep Thomas. (2010) Shorewall. En *Shorewall*. Recuperado de: http://shorewall.net/

[5] El rincón de Zerial. (2009). En *La importancia de la seguridad de la información.* Recuperado de: http://blog.zerial.org/seguridad/la-importancia-de-la- seguridad-en-la-informacion/

[19] Equipo del instalador de Debian. (2004-2010) GUÍA DE INSTALACIÓN DE DEBIAN GNU/LINUX. Recuperado de: http://www.debian.org/releases/stable/i386/

[9] Ercole, Santiago & Usseglio Maximiliano. (2009). En *Slideshare*. Recuperado de: http://www.slideshare.net/lamugre/ataques-y-vulnerabilidades

[30] Esler Joel. (2010) Snort. En *Snort*. Recuperado de: http://www.snort.org/

[11] FERNÁNDEZ, Yago; RAMOS, Antonio & GARCÍA MORAN, Jean (2009), *AAA RADIUS 802.1x - Sistemas Basados en la autenticación En Windows Y Linux/GNU Seguridad Máxima* (1ra Edición), España-Alfaomega.

[22] GARFINKEL Simson, *SEGURIDAD PRÁCTICA EN UNIX E INTERNET*, Mc Graw- hill, México, 1999.

[12] GÓMEZ VIEITES Alvaro*, ENCICLOPEDIA DE LA SEGURIDAD INFORMÁTICA,* Alfaomega, México, 2007.

[15] Jassell Jonathan (2002), *RADIUS*, Estados Unidos, O'reilly.

[21] Monge Enrique & Murcia Camilo (n.d.) *Conoce a Debian GNU/Linux* [Más que una distribución GNU/Linux, su movimiento, filosofía y comunidad] Recuperado de: http://teotihua.org/articles/articulo_debian.pdf

[25] PEAP (s.n.). En *Microsoft*. Recuperado de: http://technet.microsoft.com/es-es/library/cc757996%28v=ws.10%29.aspx

[16] Prácticas Tecnol. Red Avanzadas. (n. d.) *Instalación Y Configuración De Un Servidor Radius.* Recuperado de: http://www.grc.upv.es/docencia/tra/PDF/Radius.pdf

[4] ¿Qué es un SGSI? (n.d.) Recuperado de: http://www.iso27000.es/sgsi.html#section2a

[32] Rash Michael. (2010) psad: Intrusion Detection and Log Analysis with iptables. En *Cipherdyne*. Recuperado de: http://cipherdyne.org/psad/

[18] RedHat. (s.f) RED HAT ENTERPRISE VIRTUALIZATION. Recuperado de: http://ar.redhat.com/rhecm/rest-rhecm/jcr/repository/collaboration/jcr:system/jcr:versionStorage/bb4efb500a05260150d9554f7c1dd58a/3/jcr:frozenNode/rh:resourceFile

[27] Rice Tobias. (2009) Setting Up 802.1X Authentication with Debian Linux y Freeradius Part 1. En *fatofthelan*. Recuperado de: http://www.fatofthelan.com/technical/setting-up-802-1x-authentication-with-debian-linux-and-freeradius-part-1

[35] Servidor Proxy. (2011) En *Linux para todos*. Recuperado de: http://www.linuxparatodos.net/portal/staticpages/index.php?page=19-0-como-squid-general

[3] SGSI, (2009) Sistema de Gestión de Seguridad de la Información interno del Ente del Ministerio de Defensa Nacional.

[26] Timme Falko. (2009) Virtualization With Xen On Debian Lenny (AMD64). En *HowtoForge*. Recuperado de: *http://www.howtoforge.com/virtualization-with-xen-on-debian-lenny-amd64*

[23] Velásquez Eugenio (2009), ¿QUÉ ES LA VIRTUALIZACIÓN?. En *Tecnologiapyme*. Recuperado de: http://www.tecnologiapyme.com/software/que-es-la-virtualizacion

[2] Vidal, Jack. (2009). En *Sistemas de Cableado Estructurado*. Recuperado de: http://www.slideshare.net/lpajaro/ansi-tiaeia-568-b

GLOSARIO DE TÉRMINOS

Agujero de Seguridad.- Es un fallo en un programa que permite mediante su explotación violar la seguridad de un sistema informático.

Bombas lógicas.- Es una parte de código insertada intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones preprogramadas, en ese momento se ejecuta una acción maliciosa.

Bugs.- Es el resultado de un fallo o deficiencia durante el proceso de creación de programas de ordenador o computadora (software). Dicho fallo puede presentarse en cualquiera de las etapas del ciclo de vida del software aunque los más evidentes se dan en la etapa de desarrollo y programación.

CA: es una entidad de confianza, responsable de certificar y revocar los certificados digitales utilizados en la firma electrónica o identificación electrónica.

Downtime.- Es un termino usado para referirse a los periodos de tiempo cuando un servicio no está disponible.

FDDI.- Es un conjunto de estándares ISO y ANSI para la transmisión de datos en redes de computadoras de área extendida o local (LAN) mediante cable de fibra óptica. Se basa en la arquitectura token ring y permite una comunicación tipo Full Duplex. Dado que puede abastecer a miles de usuarios, una LAN FDDI suele ser empleada como backbone para una red de área amplia (WAN).

FSF.- Es una organización creada por Richard Stallman y otros entusiastas del software libre. La fundación se dedica a eliminar las restricciones sobre la copia, redistribución, entendimiento, y modificación de programas de computadoras. Con este objeto, promociona el desarrollo y uso del software libre en todas las áreas de la computación, pero muy particularmente, ayudando a desarrollar el sistema operativo GNU.

GNU.- El sistema GNU fue diseñado para ser compatible con UNIX, un sistema operativo que no es libre. GNU es un sistema operativo completamente libre.

GPL.- Es una licencia que está orientada principalmente a proteger la libre distribución, modificación y uso de software. Su propósito es declarar que el software cubierto por esta licencia es software libre y protegerlo de intentos de apropiación que restrinjan esas libertades a los usuarios.

Help-desk.- La Mesa de Ayuda funciona como un único punto de contacto para atender cualquier requerimiento de soporte tecnológico de los usuarios finales. Es un recurso de información y asistencia para resolver problemas informáticos.

Hypervisor.- Es una plataforma que permite aplicar diversas técnicas de control de virtualización para utilizar, al mismo tiempo, diferentes sistemas operativos sobre un mismo equipo computacional.

Kernel.- Es el principal responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema. Es el encargado de que el software y el hardware del ordenador puedan trabajar juntos.

MAC.- es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo.

Malware.- Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.

Middleware: es un software de conectividad que ofrece un conjunto de servicios que hacen posible el funcionamiento de aplicaciones distribuidas sobre plataformas heterogéneas. Funciona como una capa de abstracción de software distribuida, que se sitúa entre las capas de aplicaciones y las capas inferiores (sistema operativo y red).

OSI.- Es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

PKI.- Una infraestructura de clave pública es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

Puerta trasera: son programas que permiten acceso ilimitado a un equipo de forma remota. El problema, para quien quiere usar este ataque, es que debe convencer al usuario de que instale el servidor en el equipo.

Rlogin.- Es una aplicación TCP/IP que comienza una sesión de terminal remoto sobre el anfitrión especificado como host.

Sniffer: es un software destinado para detectar tramas en la red. Tiene diversos usos como monitorear redes para detectar y analizar fallos o ingeniería inversa de protocolos de red. También es habitual su uso para fines maliciosos, como robar contraseñas, interceptar mensajes de correo electrónico, espiar conversaciones de chat, etc.

Telnet.- Es un protocolo de Internet estándar que permite conectar terminales y aplicaciones usando el puerto 23.

TKIP.- Es un protocolo de seguridad usado en WPA para mejorar el cifrado de datos en redes inalámbricas. Este protocolo cambia las claves temporales cada 10.000 paquetes. Esto proporciona un método de distribución dinámico, lo que mejora significativamente la seguridad de la red.

Token ring.- Es una arquitectura de red desarrollada por IBM en los años 1970 con topología física en anillo y técnica de acceso de paso de testigo, usando un frame de 3 bytes llamado token que viaja alrededor del anillo. Token Ring se recoge en el estándar IEEE 802.5. En desuso por la popularización de Ethernet; actualmente no es empleada en diseños de redes.

WEP.- Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits.

WPA.- Es la abreviatura de Wifi Protect Access, y consiste en un mecanismo de control de acceso a una red inalámbrica, pensado con la idea de eliminar las debilidades de WEP.

WPA-PSK.- Corresponde con las iniciales de PreShared Key y viene a significar clave compartida previamente, es decir, a efectos del cliente basa su seguridad en una contraseña compartida. La gestión dinámica de claves aumenta notoriamente el nivel de seguridad.

ANEXOS

ANEXO 1

USUARIOS Y DIRECCIONAMIENTO IP ASIGNADO

En el presente anexo se muestra el listado de usuarios del ente del ministerio de defensa nacional con el direccionamiento IP asignado.

Tabla 5. Direccionamiento IP de usuarios
Fuente: Cralos Plasencia

VLAN 5: Recursos_Humanos		**Mascara: 255.255.255.224**		**Gateway:10.10.17.30**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.17.1	Luis Torres	Ltorres	12hyt8dfa	D2-01	B2-01
10.10.17.2	Alfredo Ramirez	Aramirez	sdr36opA2	D2-02	B2-02
10.10.17.3	Sonia Benitez	Sbenitez	DOp98som	D2-03	B2-03
10.10.17.4	Juan Moreno	Jmoreno	Jmon67dQ	D2-04	B2-04
10.10.17.5	Manuel Hurtado	Mhurtado	bTy74RT1	D2-05	B2-05
10.10.17.6	Andres Garcia	Agarcia	34GarT68	D2-06	B2-06
10.10.17.7	Soledad Jimenez	Sjimenez	Utvb12OO	D2-07	B2-07
10.10.17.8	Maria Pantoja	Mpantoja	YNy67uni	D2-08	B2-08
10.10.17.9	Rosario Salcedo	Rsalcedo	84btRSok	D2-09	B2-09
10.10.17.10	Mario Carrillo	Mcarrillo	56cvTRwm	D2-10	B2-10
10.10.17.11	Sebastian Cuero	Scuero	piUx75nm	D2-11	B2-11
10.10.17.12	Bryan Martinez	Bmartinez	Hdb82xu@	D2-12	B2-12
10.10.17.13	Juan Hidalgo	Jhidalgo	bSwuY4rG	D2-13	B2-13
10.10.17.14	Pedro Silva	Psilva	yTGH1uOP	D2-14	B2-14
10.10.17.15	Wilson Hernandez	Whernandez	mHa789k6	D2-15	B2-15

VLAN 6:Administrativo_1		Mascara: 255.255.255.240		Gateway: 10.10.17.238	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.17.225	Elena Mejia	Emejia	Gru51TyQ	D2-16	B2-16
10.10.17.226	Gustavo Armendariz	Garmendariz	27T@o43h	D2-17	B2-17
10.10.17.227	Patricio Santillan	Psantillan	Bftr67Wc	D2-18	B2-18
10.10.17.228	Gerardo Aguas	Gaguas	Ytxa40!g	D2-19	B2-19
10.10.17.229	Cecilia Tobar	Ctobar	Juw71Sdo	D2-20	B2-20
10.10.17.230	Celia Rosero	Crosero	37@12Fec	D2-21	B2-21
10.10.17.231	Ines Tenelema	Itenelema	Trsc7Hu1	D2-22	B2-22
10.10.17.232	Rene Alvarez	Ralvarez	Uvds9c3F	D2-23	B2-23
10.10.17.233	Silvia Arteaga	Sarteaga	uBfrEw3L	D2-24	B2-24
10.10.17.234	Julio Crespo	Jcrespo	uTrfLb52	D2-25	B2-25
VLAN 7: Administrativo_2		**Mascara: 255.255.255.240**		**Gateway: 10.10.18.78**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.18.65	Patricio Moncayo	Pmoncayo	Pla65qGo	D1-01	B1-01
10.10.18.66	Elizabeth Carranco	Ecarranco	94GdFc0D	D1-02	B1-02
10.10.18.67	Alexandra Almeida	Aalmeida	GrT28Sub	D1-03	B1-03
10.10.18.68	Carmen Perugachi	Cperugachi	sKyT18rV	D1-04	B1-04
10.10.18.69	Pilar Cisneros	Pcisneros	KabT451x	D1-05	B1-05
10.10.18.70	Wilson Crespo	Wcrespo	RreJsc8@	D1-06	B1-06
10.10.18.71	Oswaldo Enriquez	Oenriquez	Mzut63dM	D1-07	B1-07
10.10.18.72	Pablo Pantoja	Ppantoja	36BhToYP	D1-08	B1-08
VLAN 8: Administrativo_3		**Mascara: 255.255.255.248**		**Gateway: 10.10.18.246**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.18.241	Catalina Yandun	Cyandun	0TVsiMAw	D3-01	B3-01
10.10.18.242	Gustavo Dominguez	Gdominguez	Jst73NB2	D3-02	B3-02
10.10.18.243	Norma Cadena	Ncadena	u8Ft57eL	D3-03	B3-03
10.10.18.244	Felix Lara	Flara	ortIU912	D3-04	B3-04

VLAN 9: Administrativo_4		Mascara: 255.255.255.248		Gateway: 10.10.18.230	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.18.225	Fernando Arteaga	Farteaga	YTRb89sC	D4-01	B4-01
10.10.18.226	Ignacio Lopez	Ilopez	451emTyP	D4-02	B4-02
10.10.18.227	Juan Almeida	Jalmeida	7ftR62wz	D4-03	B4-03
10.10.18.228	Katiuska Cortéz	Kcortez	nVcTRM45	D4-04	B4-04
10.10.18.229	Susana Suarez	Ssuarez	GFdtr73Ka	D4-05	B4-05
VLAN 10: Administrativo_5		**Mascara: 255.255.255.224**		**Gateway: 10.10.17.94**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.17.65	Angelina Valencia	Avalencia	jsY8cY4W	D4-06	B4-06
10.10.17.66	Roberto Cárdenas	Rcardenas	0GVf28xQ	D4-07	B4-07
10.10.17.67	Francisco Paredes	Fparedes	dMgUp5Wj	D4-08	B4-08
10.10.17.68	Cecilia Mendoza	Cmendoza	39gHtPDa	D4-09	B4-09
10.10.17.69	Jesus Portilla	Jportilla	t34ZuFkc	D4-10	B4-10
10.10.17.70	Gonzalo Briones	Gbriones	4Bct65TT	D4-11	B4-11
10.10.17.71	Andres Vargas	Avargas	8Vfd0hds	D4-12	B4-12
10.10.17.72	Elena Montero	Emontero	Em206UgL	D4-13	B4-13
10.10.17.73	Alejandro Villacis	Avillacis	sTuioUT8	D4-14	B4-14
10.10.17.74	Miguel Armas	Marmas	rtJvE65L	D4-15	B4-15
10.10.17.75	Maria Rosales	Mrosales	7UtrDwM1	D4-16	B4-16
10.10.17.76	Paulina Morales	Pmorales	542FguOb	D4-17	B4-17
10.10.17.77	Lucia Paredes	Lparedes	hYuCv6n9	D4-18	B4-18
10.10.17.78	Antonio Galeano	Agaleano	gHuW23c5	D4-19	B4-19
10.10.17.79	Lenin Jurado	Ljurado	9Tr3Vhb4	D4-20	B4-20
10.10.17.80	Alexander Baez	Abaez	JhtxQ87U	D4-21	B4-21
10.10.17.81	Nelson Cotacachi	Ncotacachi	6TcE3XpO	D4-22	B4-22
10.10.17.82	Luis Jijón	Ljijon	dFr5bTcA	D4-23	B4-23
10.10.17.83	Dario Mina	Dmina	64Df32FR	D4-24	B4-24

VLAN 11: Administrativo_6		Mascara: 255.255.255.240		Gateway: 10.10.17.254	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.17.241	Humberto Yanez	Hyanez	8d6RhPsL	D4-25	B4-25
10.10.17.242	Carmen López	Clopez	AhTuzRmf	D4-26	B4-26
10.10.17.243	Cristina Jácome	Cjacome	Htsd52bX	D4-27	B4-27
10.10.17.244	Patricio Rivera	Privera	BmE481La	D4-28	B4-28
10.10.17.245	Armando Gonzalez	Agonzalez	YvtR2B8d	D4-29	B4-29
10.10.17.246	Ramiro Godoy	Rgodoy	OtcGkA5Y	D4-30	B4-30
10.10.17.247	Felix Patiño	Fpatino	K63rCs8f	D4-31	B4-31
10.10.17.248	Miguel Tuqueres	Mtuqueres	nJuyR45A	D4-32	B4-32
10.10.17.249	Diego Pazmiño	Dpazmino	eRtNvc4p	D4-33	B4-33
10.10.17.250	Grace Andrade	Gandrade	56CfAQun	D4-34	B4-34
VLAN 12: Coordinacion_Laboral_1		**Mascara: 255.255.255.240**		**Gateway: 10.10.18.94**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.18.81	Ricardo Montalvo	Rmontalvo	J26gUb7e	D1-09	B1-09
10.10.18.82	Obdulia Jaramillo	Ojaramillo	bYm1A5hC	D1-10	B1-10
10.10.18.83	Karina Ortega	Kortega	9XiTdSrm	D1-11	B1-11
10.10.18.84	Catalina Nuñez	Cnunez	cT7n5Gfa	D1-12	B1-12
10.10.18.85	Hugo Pineda	Hpineda	258321dG	D1-13	B1-13
10.10.18.86	Damián Olivo	Dolivo	ceS32649	D1-14	B1-14
10.10.18.87	Samuel Bustamante	Sbustamante	6RchEaQ2	D1-15	B1-15
10.10.18.88	Carlos Viera	Cviera	uTh5KmA3	D1-16	B1-16
VLAN 13: Coordinacion_Laboral_2		**Mascara: 255.255.255.240**		**Gateway: 10.10.18.62**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.18.49	Segundo Santos	Ssantos	OuTeBgTs	D2-26	B2-26
10.10.18.50	Magali Pinto	Mpinto	cFrWq1uY	D2-27	B2-27
10.10.18.51	Paola Romero	Promero	56CrWn8F	D2-28	B2-28
10.10.18.52	Ricardo Londoño	Rlondono	mU6D2vfr	D2-29	B2-29

10.10.18.53	Victor Salazar	Vsalazar	783Fz67Q	D2-30	B2-30
10.10.18.54	Magdalena Mera	Mmera	rCfy51K9	D2-31	B2-31
10.10.18.55	Fabian Alvear	Falvear	rTcdE38B	D2-32	B2-32
10.10.18.56	Vinicio Navarro	Vnavarro	45Cde29V	D2-33	B2-33
10.10.18.57	Xavier Naranjo	Xnaranjo	HsWm8D1c	D2-34	B2-34
VLAN 14: Coordinacion_Laboral_3		**Mascara: 255.255.255.224**		**Gateway: 10.10.17.62**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.17.33	Edmundo Delgado	Edelgado	vfDr54Gh	D3-05	B3-05
10.10.17.34	Narcisa Yepez	Nyepez	BcRj76Wa	D3-06	B3-06
10.10.17.35	Alvaro Díaz	Adiaz	uBr32562	D3-07	B3-07
10.10.17.36	Tomas Pasquel	Tpasquel	76VCXw2N	D3-08	B3-08
10.10.17.37	Fidel Quilca	Fquilca	CfsWdO3M	D3-09	B3-09
10.10.17.38	Natalia Cifuentes	Ncifuentes	45CfRyBm	D3-10	B3-10
10.10.17.39	Klever Ordoñez	Kordonez	FvEw28nU	D3-11	B3-11
10.10.17.40	Martín Zambrano	Mzambrano	3V5C4BoW	D3-12	B3-12
10.10.17.41	Sonia Criollo	Scriollo	gt56X21O	D3-13	B3-13
10.10.17.42	Cristian Mejía	Cmejia	rVtCvbn7	D3-14	B3-14
10.10.17.43	Hector Vizcaino	Hvizcaino	6cp3Nh49	D3-15	B3-15
10.10.17.44	Renata Arcos	Rarcos	yVfXeWqi	D3-16	B3-16
10.10.17.45	Miguel Proaño	Mproano	fVgtReM8	D3-17	B3-17
10.10.17.46	Ramiro Ramos	Rramos	5Vfg6gJw	D3-18	B3-18
10.10.17.47	Rafael Machado	Rmachado	pTcFeQ12	D3-19	B3-19
10.10.17.48	Josefina Erazo	Jerazo	rFcu7BdM	D3-20	B3-20
10.10.17.49	Angel Morales	Amorales	56cR2B8f	D3-21	B3-21
10.10.17.50	Jonás Arias	Jarias	TvgTbT4Q	D3-22	B3-22
10.10.17.51	Gilberto Moya	Gmoya	unRx59wq	D3-23	B3-23
10.10.17.52	Robalino Oña	Rona	yCaq2M5G	D3-24	B3-24
10.10.17.53	Armando Padilla	Apadilla	tCew23Vb	D3-25	B3-25

10.10.17.54	Liliana Carvajal	Lcarvajal	yVcdE34z	D3-26	B3-26
VLAN 15: Medio_Ambiente		**Mascara: 255.255.255.240**		**Gateway: 10.10.17.174**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.17.161	Rosa Aguilar	Raguilar	y6D27vFq	D3-27	B3-27
10.10.17.162	Fabián Urresta	Furresta	mBcFjT5L	D3-28	B3-28
10.10.17.163	Eugenia Dávila	Edavila	nTcW3V51	D3-29	B3-29
10.10.17.164	Carlos Escobar	Cescobar	U6cEKq3z	D3-30	B3-30
10.10.17.165	Irene Noboa	Inoboa	5C3xd2sP	D3-31	B3-31
10.10.17.166	Jorge Peralta	Jperalta	4Vcf5UbJ	D3-32	B3-32
10.10.17.167	Abelardo Cabascango	Acabascango	6Bh7Z20k	D3-33	B3-33
10.10.17.168	Gustavo Ugalde	Gugalde	ue23vf5x	D3-34	B3-34
10.10.17.169	Byron Justicia	Bjusticia	8c4b3f9y	D3-35	B3-35
10.10.17.170	Julio Osorio	Josorio	7gRwMc1L	D3-36	B3-36
10.10.17.171	Milton Perez	Mperez	tcHyA2m7	D3-37	B3-37
10.10.17.172	Celia Arévalo	Carevalo	HBty5CxE	D3-38	B3-38
10.10.17.173	Esmeralda León	Eleon	2nuRcK8o	D3-39	B3-39
VLAN 16: Administracion_Sistemas		**Mascara: 255.255.255.240**		**Gateway: 10.10.18.14**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.18.1	Mónica Ayala	Mayala	vGtX3MkU	D4-35	B4-35
10.10.18.2	Remigio Acosta	Racosta	6c4d3e8u	D4-36	B4-36
10.10.18.3	Omar Palacios	Opalacios	m8RE3LzN	D4-37	B4-37
10.10.18.4	Santiago Calle	Scalle	7d3KLt69	D4-38	B4-38
10.10.18.5	Federico Luna	Fluna	7f4328nV	D4-39	B4-39
10.10.18.6	Alex Morán	Amoran	976c45BF	D4-40	B4-40
10.10.18.7	Lucia Benavides	Lbenavides	p9V54C2T	D4-41	B4-41
10.10.18.8	Ignacio Imbaquingo	Iimbaquingo	LiT5v3S3	D4-42	B4-42
10.10.18.9	Olmedo Padilla	Opadilla	0bf4C65q	D4-43	B4-43
10.10.18.10	Rosario Arce	Rarce	r4C37Gti	D4-44	B4-44

VLAN 17: Telecomunicaciones		Mascara: 255.255.255.224		Gateway: 10.10.17.126	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.17.97	Manuel Cuastumal	Mcuastumal	gFrtVf4M	D4-45	B4-45
10.10.17.98	Fausto Carrión	Fcarrion	nJyfE34V	D4-46	B4-46
10.10.17.99	Gerónimo Velasco	Gvelasco	KurcT52N	D4-01-2	B4-01-2
10.10.17.100	Rubén Santillan	Rsantillan	MhyR50Na	D4-02-2	B4-02-2
10.10.17.101	Martín Caceres	Mcaceres	nHtr2xR4	D4-03-2	B4-03-2
10.10.17.102	Leonardo Puga	Lpuga	loDe3Ch6	D4-04-2	B4-04-2
10.10.17.103	Germán Gualoto	Ggualoto	UngR4X1o	D4-05-2	B4-05-2
10.10.17.104	Patricio Quiña	Pquina	bTscYt41	D4-06-2	B4-06-2
10.10.17.105	Olga Carpio	Ocarpio	MntXde5v	D4-07-2	B4-07-2
10.10.17.106	Daysi Albuja	Dalbuja	TgDw2N79	D4-08-2	B4-08-2
10.10.17.107	Salomón Intriago	Sintriago	86Vfre7C	D4-09-2	B4-09-2
10.10.17.108	Esperanza Esparza	Eesparza	nTecFre3	D4-10-2	B4-10-2
10.10.17.109	Mercedes Reina	Mreina	05Vft6N7	D4-11-2	B4-11-2
10.10.17.110	Sebastián Cornejo	Scornejo	5VgfR4sw	D4-12-2	B4-12-2
10.10.17.111	Eduardo Reyes	Ereyes	btcR43Xs	D4-13-2	B4-13-2
10.10.17.112	Ulpiano Salazar	Usalazar	8Htr4cfE	D4-14-2	B4-14-2
10.10.17.113	Jessica Paredes	Jparedes	nFreVtru	D4-15-2	B4-15-2
10.10.17.114	Ronny Terán	Rteran	YtreCfJ1	D4-16-2	B4-16-2
10.10.17.115	Alonso Chiza	Achiza	OnhRcF6A	D4-17-2	B4-17-2
10.10.17.116	Luis Guaygua	Lguaygua	otvFd3Cd	D4-18-2	B4-18-2
10.10.17.117	Ruth Cisneros	Rcisneros	yVgf5f7E	D4-19-2	B4-19-2
10.10.17.118	Fernando Cuasquer	Fcuasquer	7vRcd3Nh	D4-20-2	B4-20-2
VLAN 18: Desarrollo_1		**Mascara: 255.255.255.240**		**Gateway: 10.10.18.158**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.18.145	Fernanda Landeta	Flandeta	nHtcFedU	D1-17	B1-17
10.10.18.146	Patricio Chacón	Pchacon	8HgfEw2C	D1-18	B1-18

10.10.18.147	Deonicio Rios	Drios	cf9cDecD	D1-19	B1-19
10.10.18.148	Adán Fuertes	Afuertes	654dCf4N	D1-20	B1-20
10.10.18.149	Carlos Espinoza	Cespinoza	8NbfRecd	D1-21	B1-21
10.10.18.150	Amanda Fierro	Afierro	8nFreCf1	D1-22	B1-22
VLAN 19: Desarrollo_2		**Mascara: 255.255.255.240**		**Gateway: 10.10.18.174**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.18.161	Jaime Aguirre	Jaguirre	unHrfd2c	D4-21-2	B4-21-2
10.10.18.162	Cristian Ponce	Cponce	TveWe9H6	D4-22-2	B4-22-2
10.10.18.163	Olivia Alarcón	Oalarcon	nHYT78fD	D4-23-2	B4-23-2
10.10.18.164	Ximena Venegas	Xvenegas	45Vf3DE6	D4-24-2	B4-24-2
10.10.18.165	Alexander Paguay	Apaguay	NhfRED39	D4-25-2	B4-25-2
10.10.18.166	Diego Guanoluisa	Dguanoluisa	MhfRE45X	D4-26-2	B4-26-2
VLAN 20: Informatica		**Mascara: 255.255.255.240**		**Gateway: 10.10.18.30**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.18.17	Daniel Cevallos	Dcevallos	RxzWsaQF	D4-27-2	B4-27-2
10.10.18.18	Guido Velastegui	Gvelastegui	OyhTrdEw	D4-28-2	B4-28-2
10.10.18.19	Angel Bedón	Abedon	h7gR4dE2	D4-29-2	B4-29-2
10.10.18.20	Elvia Tito	Etito	hTrcweRT	D4-30-2	B4-30-2
10.10.18.21	Karina Quinteros	Kquinteros	tVreMzQ3	D4-31-2	B4-31-2
10.10.18.22	Francisco Quito	Fquito	u7Vfr3Cf	D4-32-2	B4-32-2
10.10.18.23	David Escobar	Descobar	ycDew3Vg	D4-33-2	B4-33-2
10.10.18.24	Israel Samaniego	Isamaniego	8Ve3C5f4	D4-34-2	B4-34-2
10.10.18.25	Alvaro Montalvo	Amontalvo	76c356F1	D4-35-2	B4-35-2
10.10.18.26	Raúl Chicaiza	Rchicaiza	unfRe43T	D4-36-2	B4-36-2
VLAN 21: Centro_de_Mando_1		**Mascara: 255.255.255.248**		**Gateway: 10.10.18.254**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.18.249	Patricio Rubio	Prubio	oNgtrCd6	D5-01	B5-01
10.10.18.250	Eduardo Valencia	Evalencia	6VFDEvCq	D5-02	B5-02

10.10.18.251	Reinaldo Solis	Rsolis	ASIYbf49	D5-03	B5-03
10.10.18.252	Rafael Cabascango	Rcabascango	unGrdseQ	D5-04	B5-04
VLAN 22: Centro_de_Mando_2		**Mascara: 255.255.255.240**		**Gateway: 10.10.18.126**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.18.113	Roger Salas	Rsalas	6548vFre	D5-05	B5-05
10.10.18.114	Andrea Coello	Acoello	34VFdr45	D5-06	B5-06
10.10.18.115	Salome Rodriguez	Srodriguez	BvreCswL	D5-07	B5-07
10.10.18.116	Humberto Recalde	Hrecalde	UbRcfG5B	D5-08	B5-08
10.10.18.117	Alex Pozo	Apozo	7249BvfR	D5-09	B5-09
10.10.18.118	Rogelio Maldonado	Rmaldonado	fvR563BA	D5-10	B5-10
10.10.18.119	Claudio Guerrón	Cguerron	OmhTr42X	D5-11	B5-11
VLAN 23: Centro_de_Mando_3		**Mascara: 255.255.255.248**		**Gateway: 10.10.22.6**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.22.1	Ismael Cadena	Icadena	8C4dE3gT	D5-12	B5-12
10.10.22.2	Feliberto Ruales	Fruales	876cF2Na	D5-13	B5-13
10.10.22.3	Jorge Realpe	Jrealpe	6bd4Vgt6	D5-14	B5-14
10.10.22.4	Jesus Delgado	Jdelgado	9mHfrWq5	D5-15	B5-15
VLAN 24: Direccion_General_1		**Mascara: 255.255.255.248**		**Gateway: 10.10.22.14**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.22.9	Cesar Dávila	Cdavila	7unDecFt	D5-16	B5-16
10.10.22.10	Telmo Perez	Tperez	7TvHyt3B	D5-17	B5-17
10.10.22.11	Juan Vaca	Jvaca	hTfDe5Bd	D5-18	B5-18
10.10.22.12	Salomón Quelal	Squelal	mTvfDe4V	D5-19	B5-19
VLAN 25: Direccion_General_2		**Mascara: 255.255.255.240**		**Gateway: 10.10.18.190**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.18.177	Cristian Aza	Caza	yBfrE3bT	D3-40	B3-40
10.10.18.178	Lorena Saa	Lsaa	7692Vfrs	D3-41	B3-41

10.10.18.179	Victoriano Gómez	Vgomez	NhtE428C	D3-42	B3-42
10.10.18.180	Elias Morejon	Emorejon	vFcdErt5	D3-43	B3-43
10.10.18.181	Carlos morejón	Cmorejon	SwcFrgT2	D3-44	B3-44
10.10.18.182	Gustavo Moreta	Gmoreta	QadrcYb5	D3-45	B3-45
VLAN 26: Direccion_General_3		**Mascara: 255.255.255.240**		**Gateway: 10.10.18.206**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.18.193	Domingo Enriquez	Denriquez	9NbfCrep	D2-35	B2-35
10.10.18.194	Karla Ibujéz	Kibujez	FtrVhY5V	D2-36	B2-36
10.10.18.195	Guillermo Michilena	Gmichilena	mkuBfRD2	D2-37	B2-37
10.10.18.196	José Quevedo	Jquevedo	KunFrd23	D2-38	B2-38
10.10.18.197	Byron Silva	Bsilva	8NgrCds2	D2-39	B2-39
10.10.18.198	Damián Carrera	Dcarrera	iFreCf48	D2-40	B2-40
VLAN 27: Coordinacion_Institucinal		**Mascara: 255.255.255.224**		**Gateway: 10.10.17.158**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.17.129	Miguel Orbe	Morbe	6VfrCdER	D5-20	B5-20
10.10.17.130	Oscar Sandoval	Osandoval	8NhyCdrF	D5-21	B5-21
10.10.17.131	Jonatan Campues	Jcampues	hRcfRT53	D5-22	B5-22
10.10.17.132	Mariana Vega	Mvega	uNBTcfE5	D5-23	B5-23
10.10.17.133	Kevin Santacruz	Ksantacruz	byCFDER1	D5-24	B5-24
10.10.17.134	Santiago Cevallos	Scevallos	Zceqas74	D5-25	B5-25
10.10.17.135	Andrés Cajamarca	Acajamarca	ZxCdeVPo	D5-26	B5-26
10.10.17.136	Rocío León	Rleon	98235VF6	D5-27	B5-27
10.10.17.137	Oswaldo Flores	Oflores	65129GtA	D5-28	B5-28
10.10.17.138	Carlos Gudiño	Cgudino	fRE2953B	D5-29	B5-29
10.10.17.139	Estefanía Tobar	Etobar	76CFR43n	D5-30	B5-30
10.10.17.140	Ricardo Reyes	Rreyes	87BGTde4	D5-31	B5-31
10.10.17.141	Ruperto Basantez	Rbasantez	cdxzQWc5	D5-32	B5-32
10.10.17.142	Rubén Ipiales	Ripiales	tGfrDRfV	D5-33	B5-33

10.10.17.143	Braulio Chamarro	Bchamorro	7Gt4Cd3V	D5-34	B5-34
10.10.17.144	Marcos Acosta	Macosta	yFr4CF2i	D5-35	B5-35
10.10.17.145	Ramiro Alfaro	Ralfaro	iuYtBg5Q	D5-36	B5-36
10.10.17.146	Darwin Checa	Dcheca	tVfRe562	D5-37	B5-37
VLAN 28: Operacion_Institucional_1		**Mascara: 255.255.255.248**		**Gateway: 10.10.22.22**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.22.17	Xavier Salgado	Xsalgado	gRfdTfCV	D2-41	B2-41
10.10.22.18	Gabriel Heredia	Gheredia	5Frc328M	D2-42	B2-42
10.10.22.19	Alejandra Pantoja	Apantoja	9165FcB7	D2-43	B2-43
10.10.22.20	Gustavo Pantoja	Gpantoja	fVG56V29	D2-44	B2-44
VLAN 29: Operacion_Institucional_2		**Mascara: 255.255.255.240**		**Gateway: 10.10.18.222**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.18.209	Mariano Rivera	Mrivera	iYtNo7Ge	D6-01	B6-01
10.10.18.210	Vicente Cruz	Vcruz	5VfRT6Vg	D6-02	B6-02
10.10.18.211	Luis Aro	Laro	HnDcf4C1	D6-03	B6-03
10.10.18.212	Mario Toapanta	Mtoapanta	OvfLp0Qc	D6-04	B6-04
10.10.18.213	Eloy Paz	Epaz	fReCvN6A	D6-05	B6-05
10.10.18.214	Demetrio Guevara	Dguevara	7BfRE2XP	D6-06	B6-06
10.10.18.215	Tarquino Román	Troman	PvDxcO7B	D6-07	B6-07
10.10.18.216	Edison Pozo	Epozo	4CfdWbHt	D6-08	B6-08
VLAN 30: Operacion_Institucional_3		**Mascara: 255.255.255.240**		**Gateway: 10.10.17.190**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.17.177	Fidel Balseca	Fbalseca	ugVfrCd2	D6-09	B6-09
10.10.17.178	Blanca Quilca	Bquilca	yVfrCSqZ	D6-10	B6-10
10.10.17.179	Alvaro Montesdeoca	amontesdeoca	8NvfCXs3	D6-11	B6-11
10.10.17.180	Marisol Rivadeneira	Mrivadeneira	tCVFeXs9	D6-12	B6-12
10.10.17.181	Luis Echeverría	Lecheverria	76326DcG	D6-13	B6-13
10.10.17.182	Alfo Bernal	Abernal	ygVfRcdN	D6-14	B6-14

10.10.17.183	Joaquín Ayala	Jayala	yBf5Bg7C	D6-15	B6-15
10.10.17.184	Sebastián Aviléz	Savilez	9N7v5C3X	D6-16	B6-16
10.10.17.185	Agustín Cueva	Acueva	hTfHyt6V	D6-17	B6-17
10.10.17.186	Emilio Vallejo	Evallejo	gHTfJu35	D6-18	B6-18
10.10.17.187	Nolberto Araujo	Naraujo	JuBghY6X	D6-19	B6-19
10.10.17.188	Roberto Aguilar	Raguilar	tR5432Xq	D6-20	B6-20
VLAN 31: Asuntos_Internos_1		**Mascara: 255.255.255.240**		**Gateway: 10.10.17.222**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.17.209	Marcelo Almeida	Malmeida	yHG5FD4z	D6-21	B6-21
10.10.17.210	Josue Navarrete	Jnavarrete	7BgrCdxz	D6-22	B6-22
10.10.17.211	Miriam Navas	Mnavas	iNucFd54	D6-23	B6-23
10.10.17.212	Romulo Medrano	Rmedrano	aSwCf7Bc	D6-24	B6-24
10.10.17.213	Martín Alvarado	Malvarado	bCeXsw8z	D6-25	B6-25
10.10.17.214	Irene Sánchez	Isanchez	65VfrCd3	D6-26	B6-26
10.10.17.215	Pablo Altamirano	Paltamirano	tVfCd4Bt	D6-27	B6-27
10.10.17.216	Benito Aguilar	Baguilar	uNrcW36C	D6-28	B6-28
10.10.17.217	Camilo Caicedo	Ccaicedo	iNvrCdeB	D6-29	B6-29
10.10.17.218	Arturo Bolaños	Abolanos	tVrcExW2	D6-30	B6-30
10.10.17.219	Bayardo Bravo	Bbravo	iBpWcQo5	D6-31	B6-31
10.10.17.220	Federico Cando	Fcando	rCde3XqL	D6-32	B6-32
10.10.17.221	Lorenzo Burbano	Lburbano	r9dwXe4Z	D6-33	B6-33
VLAN 32: Asuntos_Internos_2		**Mascara: 255.255.255.240**		**Gateway: 10.10.18.110**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.18.97	Luis Córdova	Lcordova	ygCfr5cD	D2-01-2	B2-01-2
10.10.18.98	Ignacio Mina	Imina	yVfeXsw5	D2-02-2	B2-02-2
10.10.18.99	Emiliano Ruiz	Eruiz	tCeXwq2p	D2-03-2	B2-03-2
10.10.18.100	Clara Rojas	Crojas	6VfrWxpY	D2-04-2	B2-04-2
10.10.18.101	Jacinto Montes	Jmontes	5CfEw280	D2-05-2	B2-05-2

10.10.18.102	Segundo Palacios	Spalacios	6VrcjUtz	D2-06-2	B2-06-2
10.10.18.103	Felipe Estrada	Festrada	2CtrPleX	D2-07-2	B2-07-2
10.10.18.104	Monica Castillo	Mcastillo	uTvRcEx5	D2-08-2	B2-08-2
10.10.18.105	Walter Vergara	Wvergara	8V5c4xW3	D2-09-2	B2-09-2
VLAN 33: Educativa		**Mascara: 255.255.255.240**		**Gateway: 10.10.18.142**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.18.129	Marco Arcos	Marcos	oNhyTc56	D6-34	B6-34
10.10.18.130	Nicolas Castillo	Ncastillo	hBr4Xs2A	D6-35	B6-35
10.10.18.131	Cristian Bedoya	Cbedoya	pBrcElt2	D6-36	B6-36
10.10.18.132	Fausto Larrea	Flarrea	54209Cdz	D6-37	B6-37
10.10.18.133	Elias Cazar	Ecazar	7BtrCd3Z	D6-38	B6-38
10.10.18.134	Cornelio Castro	Ccastro	qYtvcE31	D6-39	B6-39
10.10.18.135	Mateo Paspuel	Mpaspuel	86Vcx3Xq	D6-40	B6-40
VLAN 34: Servicios_Publicos		**Mascara: 255.255.255.240**		**Gateway: 10.10.18.46**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.18.33	Mauricio Mantilla	Mmantilla	98456vFq	D2-10-2	B2-10-2
10.10.18.34	Aurelio Aragón	Aaragon	4V6fT7Nq	D2-11-2	B2-11-2
10.10.18.35	Cosme Aguilera	Caguilera	9nYv6Cd3	D2-12-2	B2-12-2
10.10.18.36	Ricardo Burgos	Rburgos	kLrCf6Vg	D2-13-2	B2-13-2
10.10.18.37	Vicente Hormaza	Vhormaza	GvL8Cd4a	D2-14-2	B2-14-2
10.10.18.38	Edmundo Morán	Emoran	NhcRdExQ	D2-15-2	B2-15-2
10.10.18.39	Manuel Hinojoza	Mhinojoza	oNtvRx46	D2-16-2	B2-16-2
10.10.18.40	Hernesto Naranjo	Hnaranjo	uBtvRdep	D2-17-2	B2-17-2
10.10.18.41	Soledad Huertas	Shuertas	Tvf562Lk	D2-18-2	B2-18-2
10.10.18.42	Hugo Portilla	Hportilla	6vFrqZs7	D2-19-2	B2-19-2
VLAN 35: Investigacion		**Mascara: 255.255.255.240**		**Gateway: 10.10.17.206**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.17.193	Fabián Saltos	Fsaltos	UnhT56Cd	D2-20-2	B2-20-2

10.10.17.194	Ignacio Armas	Iarmas	5VfeCr34	D2-21-2	B2-21-2
10.10.17.195	Gonzalo Acosta	Gacosta	5CdeWQzX	D2-22-2	B2-22-2
10.10.17.196	Gerardo Aguas	Gaguas	uBtcFrew	D2-23-2	B2-23-2
10.10.17.197	Leonardo Prado	Lprado	7V5de341	D2-24-2	B2-24-2
10.10.17.198	Franklin Medina	Fmedina	bTcRcF42	D2-25-2	B2-25-2
10.10.17.199	Teodoro Congo	Tcongo	7Gt543Cd	D2-26-2	B2-26-2
10.10.17.200	Martín García	Mgarcia	bGtreXdg	D2-27-2	B2-27-2
10.10.17.201	Celio Garzón	Cgarzon	UntvREwP	D2-28-2	B2-28-2
10.10.17.202	Marcelo Endara	Mendara	uTrCvf52	D2-29-2	B2-29-2
10.10.17.203	Eduardo Guerrero	Eguerrero	oRcdEwp9	D2-30-2	B2-30-2
VLAN 35: Movilizacion		**Mascara: 255.255.255.248**		**Gateway: 10.10.18.238**	
Dirección IP	**Nombre de Usuario**	**Cuenta**	**Clave**	**Patch-Pannel**	**Switch**
10.10.18.233	Arturo Ramos	Aramos	8b6Cfr5z	D5-38	B5-38
10.10.18.234	Lucio Solano	Lsolano	93cf54Vz	D5-39	B5-39
10.10.18.235	Dario Zurita	Dzurita	yVfr3XqP	D5-40	B5-40
10.10.18.236	Alexander Carrillo	Acarrillo	uNytCoL8	D5-41	B5-41

ANEXO 2

ESPECIFICACIONES TÉCNICAS DE LAS CUCHILLAS INTEL HS21 Y HS22

Características de la Cuchilla Intel HS-21:

Tabla 6. Características cuchilla HS-21
Fuente: http://www-03.ibm.com/systems/ec/bladecenter/hardware/servers/index.html

Components	**IBM BladeCenter HS21**
Processor	Dual-Core Intel Xeon up to 3.0 GHz and up to 1333 MHz front-side bus or Quad-Core Intel Xeon up to 3.0 GHz and up to 1333 MHz front-side bus
Number of processors (std/max)	1/2 p
Cache (max)	4 MB L2 shared (dual-core) or 2x4 MB L2 (quad-core)
From-side bus	Up to 1333 MHz
Memory	Up to 16 GB Fully Buffered DIMMs (internal)
Internal hard disk drives	Up to two Small Form Factor (2.5") 10,000rpm SAS HDDs installed on each blade (plus support for up to 3 hot-swap SAS drives with optional Storage and I/O blade)
Maximum internal storage	734 GB6 with optional Storage and I/O Expansion Unit
RAID support	Integrated RAID-0 or -1 standard on blade server, integrated RAID-1E or RAID-5 optional with storage and I/O blade
Network	Dual Gigabit Ethernet (TOE-enabled)
I/O upgrade	1 PCI-X expansion card connection (traditional) and 1 PCI-Express (high speed)
Systems management hardware	Integrated systems management processor
Standards	NEBS-3/ETSI characteristics
Limited warranty	3-year customer replaceable unit and onsite limited warranty

Características de la cuchilla Intel HS-22:

IBM BladeCenter HS22 at a glance	
Form factor	Single-wide (30 mm)
Processor (max)	Choice of two Intel Xeon 5600 series processors, up to 3.60 GHz
Number of processors (std/max)	1/2
Memory (max)	Twelve DDR-3 VLP DIMM slots (up to 192 GB of total memory capacity and memory speeds up to 1333 MHz) with memory sparing
Expansion slots	One CIOv slot (standard PCIe daughter card) and one CFFh slot (high-speed PCIe daughter card) for a total of eight ports of I/O to each blade, including 4 ports of high-speed I/O
Disk bays (total/hot-swap)	Two hot-swap bays supporting SAS HDDs or solid-state drives
Maximum internal storage	Up to 1.0 TB total internal storage
Network interface	Virtual Fabric Adapter (10 GbE) ships integrated in some models Broadcom 5709S onboard NIC with dual Gigabit Ethernet ports with TOE
Hot-swap components	Internal storage bays
RAID support	RAID-0, -1 and -1E (optional RAID-5 with battery-backed cache)
Systems management	Unified Extensible Firmware Interface (UEFI), IBM Integrated Management Module (IMM), Predictive Failure Analysis, optional embedded hypervisor for virtualization, IBM Systems Director Active Energy Manager™, light path diagnostics, IBM Systems Director and IBM ServerGuide™
Operating systems supported	Microsoft® Windows®, Red Hat Enterprise Linux®, SUSE Linux Enterprise, VMware, Oracle Solaris
Limited warranty	Three-year customer replaceable unit and onsite and offsite limited warranty

Figura 65. Caracteristicas de la cuchilla HS-22
http://public.dhe.ibm.com/common/ssi/ecm/en/blo03029usen/BLO03029USEN.PD

ANEXO 3

SERVICIOS DE LA INSTITUCIÓN Y ELEMENTOS DE PARTE ACTIVA

En la siguiente tabla se muestra los servicios y el direccionamiento IP asignado

Tabla 7. Lista de servicios de la institución
Fuente: Carlos Plasencia

Servicio	Nombre_Servidor	Dirección IP	Sistema Operativo	Puertos
Monitoreo	mon01	10.10.20.5	Debian 5.0	Tcp 22,80 udp 161
Base Virtual	xen1	10.10.20.10	Debian 5.0	tcp 22
LDAP-Master	ldap1	10.10.20.11	Debian 5.0	tcp 389,22,80
RADIUS Primario	radius01	10.10.20.12	Debian 5.0	udp 22,1812,1813
Base Virtual	xen2	10.10.20.9	Debian 5.0	tcp 22
RADIUS Secundario	radius02	10.10.20.13	Debian 5.0	udp 22,1812,1813
LDAP-Slave	ldap2	10.10.20.14	Debian 5.0	tcp 389,22,80
Samba	Smb	10.10.20.15	Debian 5.0	tcp 22,137,138,139,445
Correo-Electrónico	Mail	10.10.20.16	Debian 5.0	tcp 22,25,80,443
Dns-Interno	Dns	10.10.20.17	Debian 5.0	udp 53 tcp 22,53
Portal WEB	App	10.10.20.18	Debian 5.0	tcp 80,443
Antivirus Kaspersky	Antivirus	10.10.20.19	Windows Server 2003	tcp 13000,14000,15000
Help Desk	Otrs	10.10.20.20	Debian 5.0	tcp 22,80
UTM Interno	utm1	10.10.20.254	Debian 5.0	tcp 22,80,3000,10000
UTM Externo	utm2	10.10.21.253	Debian 5.0	tcp 22,80,3000,8081,10000

En la siguiente tabla se presenta los elementos de parte activa con el respectivo direccionamiento IP.

Tabla 8. Direccionamiento IP de la infraestructura de networking
Fuente: Carlos Plasencia

Modelo	Nombre	Ubicación	Dirección IP/Mascara
3Com 5500-SI	B1	Bloque 1	10.10.19.1/24
3Com 5500-EI	B2	Bloque 2	
3Com 5500-EI			10.10.19.2/24
3Com 5500-EI	B3	Bloque 3	10.10.19.3/24
3Com 5500-EI	B4	Bloque 4	
3Com 5500-EI			10.10.19.4/24
3Com 5500-EI	B5	Bloque 5	10.10.19.5/24
3Com 5500-EI	B6	Bloque 6	10.10.19.6/24
3Com 7750	B1	Bloque 1	10.10.19.253/24
3Com 2780	B4	Bloque 4	10.10.21.0/24

ANEXO 4

CONFIGURACIONES DE VIRTUALIZACIÓN

Fichero de configuración de la máquina virtual del servidor RADIUS primario.

```
#
# Configuration file for the Xen instance radius01, created
# by xen-tools 3.9 on Tue Mar 23 10:42:27 2010.
#

#
#  Kernel + memory size
#
kernel      = '/boot/vmlinuz-2.6.26-2-xen-amd64'
ramdisk     = '/boot/initrd.img-2.6.26-2-xen-amd64'
memory      = '1024'

#
#  Disk device(s).
#
root        = '/dev/xvda2 ro'
disk        = [
                  'file:/home/xen/domains/radius01/swap.img,xvda1,w',
                  'file:/home/xen/domains/radius01/disk.img,xvda2,w',
                ]


#
#  Hostname
#
name        = 'radius01'

#
#  Networking
#
vif         = [ 'ip=10.10.20.12,mac=00:16:3E:61:2D:4F' ]

#
#  Behaviour
#
on_poweroff = 'destroy'
on_reboot   = 'restart'
on_crash    = 'restart'
```

Figura 66. Configuración de la máquina virtual radius01.cfg
Fuente: Capturas mediante putty

Fichero de configuración de la máquina virtual del servidor RADIUS secundario

```
#
# Configuration file for the Xen instance radius02, created
# by xen-tools 3.9 on Wed Mar 24 11:25:02 2010.
#

#
#  Kernel + memory size
#
kernel      = '/boot/vmlinuz-2.6.26-2-xen-amd64'
ramdisk     = '/boot/initrd.img-2.6.26-2-xen-amd64'
memory      = '1024'

#
#  Disk device(s).
#
root        = '/dev/xvda2 ro'
disk        = [
                  'file:/home/xen/domains/radius02/swap.img,xvda1,w',
                  'file:/home/xen/domains/radius02/disk.img,xvda2,w',
                ]


#
#  Hostname
#
name        = 'radius02'

#
#  Networking
#
vif         = [ 'ip=10.10.20.13,mac=00:16:3E:42:B2:3C' ]

#
#  Behaviour
#
on_poweroff = 'destroy'
on_reboot   = 'restart'
on_crash    = 'restart'
```

Figura 67. Configuración de la máquina virtual radius02.cfg
Fuente: Capturas mediante putty

Fichero de configuración de la máquina virtual del servidor LDAP master

```
#
# Configuration file for the Xen instance ldap01, created
# by xen-tools 3.9 on Tue Mar 23 09:13:27 2010.
#


#
#  Kernel + memory size
#
kernel      = '/boot/vmlinuz-2.6.26-2-xen-amd64'
ramdisk     = '/boot/initrd.img-2.6.26-2-xen-amd64'
memory      = '512'

#
#  Disk device(s).
#
root        = '/dev/xvda2 ro'
disk        = [
                  'file:/home/xen/domains/ldap01/swap.img,xvda1,w',
                  'file:/home/xen/domains/ldap01/disk.img,xvda2,w',
                ]


#
#  Hostname
#
name        = 'ldap01'

#
#  Networking
#
vif         = [ 'ip=10.10.20.11,mac=00:16:3E:6D:18:7B' ]

#
#  Behaviour
#
on_poweroff = 'destroy'
on_reboot   = 'restart'
on_crash    = 'restart'
```

Figura 68. Configuración de la máquina virtual ldap01.cfg
Fuente: Capturas mediante putty

Fichero de configuración de la máquina virtual del servidor LDAP slave

```
#
# Configuration file for the Xen instance ldap02, created
# by xen-tools 3.9 on Fri Mar 26 10:26:32 2010.
#

#
#  Kernel + memory size
#
kernel      = '/boot/vmlinuz-2.6.26-2-xen-amd64'
ramdisk     = '/boot/initrd.img-2.6.26-2-xen-amd64'
memory      = '512'

#
#  Disk device(s).
#
root        = '/dev/xvda2 ro'
disk        = [
                  'file:/home/xen/domains/ldap02/swap.img,xvda1,w',
                  'file:/home/xen/domains/ldap02/disk.img,xvda2,w',
              ]


#
#  Hostname
#
name        = 'ldap02'

#
#  Networking
#
vif         = [ 'ip=10.10.20.14,mac=00:16:3E:1F:64:5E' ]

#
#  Behaviour
#
on_poweroff = 'destroy'
on_reboot   = 'restart'
on_crash    = 'restart'
```

Figura 69. Configuración de la máquina virtual ldap02.cfg
Fuente: Capturas mediante putty

Validación de las máquinas encendidas desde la consola del hypervisor xen en la cuchilla HS-21:

```
xen01:~# xm list
Name                                        ID   Mem VCPUs      State   Time(s)
Domain-0                                     0 31079     4     r-----     17.4
ldap01                                       2   512     1     -b----      3.8
radius01                                     1  1024     1     -b----      3.7
```

Figura 70. Validación de Máquinas virtuales encendidas en servidor HS-21
Fuente: Capturas mediante putty

Validación de las máquinas encendidas desde la consola del hypervisor xen en la cuchilla HS-22:

```
xen02:~# xm list
Name                                        ID   Mem VCPUs      State   Time(s)
Domain-0                                     0 31079     4     r-----     25.8
ldap02                                       2   512     1     -b----      5.3
radius02                                     1  1024     1     -b----      4.6
```

Figura 71. Validación de Máquinas virtuales encendidas en servidor HS-22
Fuente: Capturas mediante putty

ANEXO 5

INSTALACIÓN Y CONFIGURACIÓN DE FREERADIUS

Configuración de las fuentes descargadas de freeradius:

- Fichero rules

```
        mv config.sub config.sub.dist
endif
ifeq (config.guess.dist,$(wildcard config.guess.dist))
        rm config.guess
else
        mv config.guess config.guess.dist
endif
        ln -s /usr/share/misc/config.sub config.sub
        ln -s /usr/share/misc/config.guess config.guess


        ./configure $(confflags) \
                --prefix=/usr \
                --exec-prefix=/usr \
                --mandir=$(mandir) \
                --sysconfdir=/etc \
                --libdir=$(libdir) \
                --datadir=/usr/share \
                --localstatedir=/var \
                --with-raddbdir=$(raddbdir) \
                --with-logdir=/var/log/$(package) \
                --enable-ltdl-install=no --enable-strict-dependencies \
                --with-large-files --with-udpfromto --with-edir \
                --enable-developer \
                --config-cache \
                --with-rlm_eap_tls \
                --with-rlm_eap_ttls \
                --with-rlm_eap_peap \
                --without-rlm_eap_tnc \
                --without-rlm_otp \
                --with-rlm_sql_postgresql_lib_dir=`pg_config --libdir` \
                --with-rlm_sql_postgresql_include_dir=`pg_config --includedir` \
                --with-openssl \
                --without-rlm_eap_ikev2 \
                --without-rlm_sql_oracle \
                --without-rlm_sql_unixodbc \
                --with-system-libtool

#Architecture
```

Habilitar soporte de EAP

Habilitar soporte de ssl

Figura 72. Fichero rules de la compilación de freeradius
Fuente: Capturas mediante putty

- Fichero Control

```
Source: freeradius
Build-Depends: autotools-dev, debhelper (>= 6.0.7), libgdbm-dev, libiodbc2-dev, libkrb5-dev, libldap2-dev,libltdl3-dev, libmysqlclient15-dev |
libmysqlclient-dev, libpam0g-dev, libpcap-dev, libperl-dev, libpq-dev, libsasl2-dev, libsnmp-dev, libtool, python-dev, libssl-dev
Section: net
Priority: optional
Maintainer: Stephen Gran <sgran@debian.org>
Uploaders: Mark Hymers <mhy@debian.org>
Standards-Version: 3.7.3
```

Figura 73. Fichero control de la compilación de freeradius
Fuente: Capturas mediante putty

- Fichero packages

```
cpp-4.3                                  install
cron                                     install
debconf                                  install
debconf-i18n                             install
debhelper                                install
debian-archive-keyring                   install
debianutils                              install
dhcp3-client                             install
dhcp3-common                             install
diff                                     install
dmidecode                                install
dpkg                                     install
dpkg-dev                                 install
e2fslibs                                 install
e2fsprogs                                install
ed                                       install
fakeroot                                 install
file                                     install
findutils                                install
freeradius                               hold
freeradius-common                        hold
freeradius-dialupadmin                   hold
freeradius-ldap                          hold
freeradius-mysql                         hold
freeradius-utils                         hold
g++                                      install
g++-4.3                                  install
gcc                                      install
gcc-4.2-base                             install
gcc-4.3                                  install
gcc-4.3-base                             install
gettext                                  install
gettext-base                             install
gnupg                                    install
gpgv                                     install
grep                                     install
groff-base                               install
gzip                                     install
hostname                                 install
```

Figura 74 Fichero packages de la compilación de freeradius
Fuente: Capturas mediante putty

Nota: Debido a la extensión de los ficheros de configuración de freeradius, se adjuntan en formato digital.

ANEXO 6

CONFIGURACIONES DE LOS UTM INTERNO Y EXTERNO

Código fuente de los ficheros de shorewall del UTM interno:

Definición de zonas (fichero zones):

```
###############################################################################
#ZONE    TYPE    OPTIONS                 IN                      OUT
#                                      OPTIONS                 OPTIONS
fw      firewall #Por defecto
loc     ipv4     #Red LAN de la institucion
net     ipv4     #Red de acceso a internet
rdd     ipv4     #Red de datos de todos los Entes
srv     ipv4     #Red de servidores
wir     ipv4     #Red Wireless
#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
```

Figura 75. Fichero de zonas del UTM interno
Fuente: Capturas mediante putty

Asociación de las zonas a las interfaces del UTM (fichero interfaces):

```
###############################################################################
#ZONE INTERFACE   BROADCAST       OPTIONS
 -      eth0        -
net     eth1       detect          tcpflags,routefilter,nosmurfs,logmartians
-       eth2        -
srv     eth3       detect          tcpflags,routefilter,nosmurfs,logmartians,routeback
wir     eth4       detect          tcpflags,routefilter,nosmurfs,logmartians,routeback

#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Figura 76. Fichero de interfaces del UTM interno
Fuente: Capturas mediante putty

Subredes que se comunican a través de la interfaz eth0 y eth2 (fichero hosts)

```
###############################################################################
#ZONE    HOST(S)                                     OPTIONS
loc     eth0:10.10.17.0/24,10.10.18.0/24,10.10.22.0/24                  routeback
rdd     eth2:192.168.0.0/16,172.30.20.0/24,172.30.30.0/24,10.20.0.0/16  routeback
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS LINE -- DO NOT REMOVE
```

Figura 77. Fichero hosts del UTM interno
Fuente: Capturas mediante putty

Políticas globales aplicadas (fichero policy)

```
###############################################################
#SOURCE          DEST            POLICY          LOG LEVEL

$FW             loc     REJECT          info
$FW             net     REJECT          info
$FW             rdd     REJECT          info
$FW             srv     REJECT          info
$FW             wir     REJECT          info

loc             $FW     REJECT          info
loc             net     REJECT          info
loc             rdd     REJECT          info
loc             srv     REJECT          info
loc             wir     REJECT          info

net             loc     REJECT          info
net             $FW     REJECT          info
net             rdd     REJECT          info
net             srv     REJECT          info
net             wir     REJECT          info

rdd             loc     REJECT          info
rdd             net     REJECT          info
rdd             $FW     REJECT          info
rdd             srv     REJECT          info
rdd             wir     REJECT          info

srv             loc     REJECT          info
srv             net     REJECT          info
srv             rdd     REJECT          info
srv             $FW     REJECT          info
srv             wir     REJECT          info

wir             loc     REJECT          info
wir             net     REJECT          info
wir             rdd     REJECT          info
wir             srv     REJECT          info
wir             $FW     REJECT          info

# THE FOLLOWING POLICY MUST BE LAST
all             all     REJECT          info
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS LINE -- DO NOT REMOVE
```

Figura 78. Fichero de políticas del UTM interno
Fuente: Capturas mediante putty

Accesos permitidos de tráfico entre zonas (fichero rules)

```
#######################################################################
#ACTION  SOURCE    DEST     PROTO   DEST    SOURCE    ORIGINAL
#                                                      PORT    PORT(S)         DEST
#Reglas desde la red LAN
ACCEPT  loc     net     tcp     8081,80,25,8443,2082,2096
ACCEPT  loc     srv     tcp     80,8080,8081,8082,2095,135,137,138,139,445,389
ACCEPT  loc     srv     udp     53,1812,1813 # Acceso a servicio DNS y AAA
ACCEPT  loc     rdd     tcp     80,82,8080,8081

#Administracion de servidores
ACCEPT  loc:10.10.10.144/28  srv  tcp   22,22022,23,21,10000,58000,22443,3389 #VLAN Desarrollo
ACCEPT  loc:10.10.18.0/28    $FW        tcp     22,10000 #VLAN Administracion_Sistemas

#Reglas de conectividad
Ping/ACCEPT     loc     $FW
Ping/ACCEPT     loc     net
Ping/ACCEPT     loc     srv
Ping/ACCEPT     loc     rdd

#Reglas desde la red de servidores
ACCEPT  srv     net     tcp     80,8081,443,25,21,22 #Salida a trves del UTM externo
ACCEPT  srv:10.10.20.5          $FW     udp     161,162 # Monitoreo via SNMP
ACCEPT  srv:10.10.20.5          net     udp     53,161,162 #Monitoreo al UTM externo
ACCEPT  srv:10.10.20.5          $FW     tcp     22,10000 #Monitoreo de servicios
ACCEPT  srv:10.10.20.5          net     tcp     22,10000,80 #Monitoreo de servicios

#Reglas de conectividad
Ping/ACCEPT     srv     loc
Ping/ACCEPT     srv     net
Ping/ACCEPT     srv     rdd

#Reglas desde la red de datos
ACCEPT  rdd     net:10.10.22.225        tcp     80,443 #Acceso a Portal publico
ACCEPT  rdd     srv:10.10.20.19 tcp     13000,14000,15000
ACCEPT  rdd     srv:10.10.20.15 tcp     80,82,8082,8080

#Reglas de conectividad
Ping/ACCEPT     rdd     $FW
Ping/ACCEPT     rdd     srv:10.10.20.10,10.10.20.15

#Reglas desde la red wireless
ACCEPT  wir     net     tcp     8081 # Servicio Proxy
ACCEPT  wir     srv     udp     53,1812,1813 #Servicio DNS y AAA

#Reglas de conectividad
Ping/ACCEPT     wir     $FW
Ping/ACCEPT     wir     net

#Reglas desde el firewall
ACCEPT  $FW             net     tcp     8081,80,22 #Acceso a traves del UTM externo
ACCEPT  $FW             net     udp     53 #Servicio DNS

#Conectivida del firewall hacia todas las zonas
Ping/ACCEPT             $FW     all
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Figura 79. Fichero de reglas del UTM interno
Fuente: Capturas mediante putty

Código fuente de los ficheros de shorewall del UTM externo:

Configuración del fichero zones

```
###############################################################################
#ZONE    TYPE    OPTIONS                 IN                      OUT
#                                       OPTIONS                 OPTIONS
fw      firewall        #Servidor UTM
net     ipv4            #Red de acceso a internet
dmz     ipv4            #Red DMZ
lan     ipv4            #Acceso a la RED LAN y UTM interno
#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
```

Figura 80. Fichero de zonas del UTM externo
Fuente: Capturas mediante putty

Configuración del fichero interfaces

```
###############################################################################
#ZONE INTERFACE   BROADCAST       OPTIONS
net     eth0      detect        tcpflags,routefilter,nosmurfs,logmartians
dmz     eth2      detect        tcpflags,routefilter,nosmurfs,logmartians,routeback
-       eth3         -
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Figura 81. Fichero de interfaces del UTM externo
Fuente: Capturas mediante putty

Configuración del fichero hosts

```
###############################################################################
#ZONE    HOST(S)                                 OPTIONS
lan     eth3:10.10.0.0/16                               routeback
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS LINE -- DO NOT REMOVE
```

Figura 82. Fichero hosts del UTM externo
Fuente: Capturas mediante putty

Configuración del fichero de políticas globales policy

```
###############################################################################
#SOURCE          DEST    POLICY          LOG LEVEL       LIMIT:BURST

$FW             net     REJECT          info
$FW             lan     REJECT          info
$FW             dmz     REJECT          info

lan             $FW     REJECT          info
lan             net     REJECT          info
lan             dmz     REJECT          info

net             $FW     DROP            info
net             lan     DROP            info
net             dmz     DROP            info

# THE FOLLOWING POLICY MUST BE LAST
all     all     DROP            info
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS LINE -- DO NOT REMOVE
```

Figura 83. Fichero de políticas del UTM externo
Fuente: Capturas mediante putty

Configración de accesos permitidos por el UTM definidas en el fichero rules

```
#####################################################################
#ACTION  SOURCE    DEST     PROTO   DEST    SOURCE    ORIGINAL
#                                                     PORT    PORT(S)          DEST
#Reglas de acceso desde el firewall hacia internet
ACCEPT  $FW             net             tcp     80,81,82,8080,8081,443,25,110,495,2095,2096,21,7776
ACCEPT  $FW             net             udp     53

#Reglas desde la red LAN
ACCEPT  lan             $FW             tcp     8081,80
ACCEPT  lan             dmz             tcp     80,443
ACCEPT  lan             $FW             tcp     22,10000,3000
ACCEPT  lan             net             udp     53
ACCEPT  lan             $FW             udp     161
ACCEPT  lan             dmz             tcp     22,21,23,3389

#Reglas desde la DMZ
ACCEPT  dmz             net             tcp     80,25,443
ACCEPT  dmz             lan             udp     53
ACCEPT  dmz             $FW             tcp     8081

#Reglas de conectividad
Ping/ACCEPT     lan     $FW
Ping/ACCEPT     dmz     $FW
Ping/ACCEPT     $FW     all
Ping/ACCEPT     dmz     lan
Ping/ACCEPT     dmz     net
Ping/ACCEPT     lan     dmz

#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS LINE -- DO NOT REMOVE
```

Figura 84. Fichero de reglas del UTM externo
Fuente: Capturas mediante putty

Configuración del enmascaramiento de las redes locales en el fichero masq

```
########################################
#INTERFACE                SOURCE
eth0                      eth1
eth0                      eth2
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

Figura 85. Fichero de enmascaramiento del UTM externo
Fuente: Capturas mediante putty

ANEXO 7

CONFIGURACIONES DEL ESCENARIO DEMOSTRATIVO

Virtualización:

Para la validación de funcionalidades de la paravirtualización de utiliza un PC con las siguientes características:

- Procesador: Intel core i5
- Memoria RAM: 8 GB
- Disco Duro: 500 GB

El sistema operativo utilizado es Debian Lenny 5.0 y sobre el equipo se crean tres máquinas virtuales:

1. Servidor RADIUS primario
2. Servidor LDAP master
3. Servidor RADIUS secundario y LDAP slave

Las configuraciones de las máquinas virtuales son las siguientes:

Servidor RADIUS primario

```
#
# Configuration file for the Xen instance radius01, created
# by xen-tools 3.9 on Tue Dec 27 11:07:48 2011.
#


#
#  Kernel + memory size
#
kernel      = '/boot/vmlinuz-2.6.26-2-xen-686'
ramdisk     = '/boot/initrd.img-2.6.26-2-xen-686'
memory      = '300'

#
#  Disk device(s).
#
root        = '/dev/xvda2 ro'
disk        = [
                  'file:/home/xen/domains/radius01/swap.img,xvda1,w',
                  'file:/home/xen/domains/radius01/disk.img,xvda2,w',
                ]


#
#  Hostname
#
name        = 'radius01'

#
#  Networking
#
vif         = [ 'ip=10.10.20.12,mac=00:16:3E:01:B0:6E' ]

#
#  Behaviour
#
on_poweroff = 'destroy'
on_reboot   = 'restart'
on_crash    = 'restart'
```

Figura 86. Configuración de la máquina virtual radius01.cfg del escenario
Fuente: Capturas mediante putty

Servidor LDAP master

```
#
# Configuration file for the Xen instance ldap01, created
# by xen-tools 3.9 on Tue Dec 27 11:00:51 2011.
#

#
#  Kernel + memory size
#
kernel      = '/boot/vmlinuz-2.6.26-2-xen-686'
ramdisk     = '/boot/initrd.img-2.6.26-2-xen-686'
memory      = '300'

#
#  Disk device(s).
#
root        = '/dev/xvda2 ro'
disk        = [
                  'file:/home/xen/domains/ldap01/swap.img,xvda1,w',
                  'file:/home/xen/domains/ldap01/disk.img,xvda2,w',
                ]


#
#  Hostname
#
name        = 'ldap01'

#
#  Networking
#
vif         = [ 'ip=10.10.20.11,mac=00:16:3E:F8:84:4D' ]

#
#  Behaviour
#
on_poweroff = 'destroy'
on_reboot   = 'restart'
on_crash    = 'restart'
```

Figura 87. Configuración de la máquina virtual ldap01.cfg del escenario
Fuente: Capturas mediante putty

Servidor RADIUS secundario y LDAP slave

```
#
# Configuration file for the Xen instance RADIUS_LDAP, created
# by xen-tools 3.9 on Tue Dec 27 11:12:56 2011.
#


#
#  Kernel + memory size
#
kernel      = '/boot/vmlinuz-2.6.26-2-xen-686'
ramdisk     = '/boot/initrd.img-2.6.26-2-xen-686'
memory      = '300'

#
#  Disk device(s).
#
root        = '/dev/xvda2 ro'
disk        = [
                  'file:/home/xen/domains/RADIUS_LDAP/swap.img,xvda1,w',
                  'file:/home/xen/domains/RADIUS_LDAP/disk.img,xvda2,w',
                ]


#
#  Hostname
#
name        = 'RADIUS_LDAP'

#
#  Networking
#
vif         = [ 'ip=10.10.20.13,mac=00:16:3E:38:4A:9D' ]

#
#  Behaviour
#
on_poweroff = 'destroy'
on_reboot   = 'restart'
on_crash    = 'restart'
```

Figura 88. Configuración de la máquina virtual RADIUS-LDAP.cfg del escenario
Fuente: Capturas mediante putty

Servidor AAA

Las configuraciones de los servidores AAA primario y secundario para el escenario demostrativo son extensas por lo cual se adjunta en formato digital, cabe señalar que las configuraciones son similares a las descritas en el desarrollo del proyecto.

Autenticador cisco

En switch cisco catalyst 2950 soporta el estándar 802.1X, siendo útil para demostrar la funcionalidad del control de acceso a la red.

La configuración aplicada es la siguiente:

```
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SW_ISP
!
aaa new-model   #Habilitación global de la autenticacion 802.1X
aaa authentication dot1x default group radius
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
dot1x system-auth-control
!
!
!
!
interface FastEthernet0/1
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 5 #Usuario de la VLAN 5
 switchport mode access
 dot1x port-control auto  #Habilitacion de autenticación en el puerto
 spanning-tree portfast
!
interface FastEthernet0/3
 switchport access vlan 5
```

```
 switchport mode access
 dot1x port-control auto #Habilitacion de autenticación en el puerto
 spanning-tree portfast
!
interface FastEthernet0/4
 switchport access vlan 5
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/5
 switchport access vlan 6
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/6
 switchport access vlan 6
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/7
 switchport access vlan 6
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/8
 switchport access vlan 7
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/9
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/10
 switchport access vlan 7
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/11
 switchport access vlan 8
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
```

```
interface FastEthernet0/12
 switchport access vlan 8
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/13
 switchport access vlan 8
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/14
 switchport access vlan 9
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/15
 switchport access vlan 9
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/16
 switchport access vlan 9
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
 switchport trunk allowed vlan 1,5-9
 switchport mode trunk
!
interface Vlan1
 ip address 10.10.19.2 255.255.255.0
 no ip route-cache
```

```
!
ip default-gateway 10.10.19.254
ip http server
radius-server host 10.10.20.12 auth-port 1812 acct-port 1813 key
prW01Mbl   #Parámetros de autenticación contra el servidor externo
AAA
radius-server retransmit 3
!
line con 0
line vty 5 15
!
!
end
```