UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE UN SISTEMA DE AUTENTICACIÓN DE USUARIOS 802.1X CON ASIGNACIÓN DE VLAN DINÁMICA

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

EDGAR JULIÁN HUAMANÑAHUI ÑACCHA

PROMOCIÓN
2004-I

LIMA-PERÚ
2010

DISEÑO DE UN SISTEMA DE AUTENTICACIÓN DE USUARIOS 802.1X CON ASIGNACIÓN DE VLAN DINÁMICA

A mi hermana Rosa Elena por su valentía

A mi madre Anselma por su amor y apoyo

A Marisol por el amor y la compañía que siempre me da

A Pablo L. por la educación y el invalorable apoyo que me ha brindado

SUMARIO

El presente informe de suficiencia describe un sistema de autenticación de usuarios 802.1x con asignación de VLAN dinámica.

El trabajo presentado contempla altos mecanismos de seguridad para el control de acceso a las redes internas de las empresas con la finalidad de impedir que sujetos ajenos a la empresa y/o empleados malintencionados puedan acceder a la red, leer, escribir y hasta destruir los datos.

La contribución de este trabajo es que servirá para una mejor comprensión de la seguridad en las redes virtuales de área local (VLAN) y para que las empresas y/o ingenieros manejen el sistema presentado para proteger el activo más importante de las empresas que es la información

La solución se puede describir de la siguiente manera: 1) El terminal (cliente) contiene una aplicación denominada "suplicante", el terminal se conecta a un punto de acceso a la red, 2) El punto de acceso (autenticador) puede ser un switch o un access point (wireless) que se encarga de identificar al cliente y comunicarse con un servidor de control de acceso, 3) El servidor de control de acceso (ACS) contiene el perfil del usuario, éste consulta a un servidor de contraseñas, (token) 4) El RADIUS verifica la contraseña y la comunicación se invierte permitiendo o no el acceso al usuario

Los estándares utilizados son el 802.1x, ISO 27001, PCI DSS.

ÍNDICE

INTRODUCCIÓN

El trabajo surge por la necesidad de las empresas de contar con un sistema de autenticación de usuarios (empleados o visitantes) para que hagan uso de los recursos de la red (intranet e Internet) de acuerdo a los perfiles de cada usuario o cliente. Así mismo, de permitir a estos usuarios a desplazarse por la empresa con sus terminales sin la necesidad de recurrir a un administrador de red.

La solución presentada está basada en el estándar IEEE 802.1X, el cual es una norma del Instituto de Ingenieros Electricistas y Electrónicos, diseñada para el control de acceso a red y basada en puertos. Este es parte de los protocolos IEEE 802. Dentro del estándar 802.1x existe el protocolo EAP (Extensible Authentication Protocol) que permite la autenticación de dispositivos conectados a un puerto LAN. Para el fortalecimiento de la autenticación se utiliza un tipo de EAP llamado GTC (Generic Token-Card).

El trabajo orienta su interés también hacia la movilidad de los usuarios, ya sea esté utilizando puntos de acceso inalámbricos o fijos. Las redes virtuales de área local (VLAN) son tradicionalmente configuradas de manera estática pero esto dificulta la movilidad de los usuarios. Esto debido a que se recurre a un administrador de red para que reconfigure el puerto que utilizará para conectarse a la red. Por ello se opta por la utilización de redes virtuales de área local pero dinámica que permitirá una flexibilidad en el desplazamiento de los usuarios por la empresa.

La solución para lograr una autenticación de los usuarios que utilizarán la red (intranet o Internet) involucra a cuatro protagonistas:

1) El terminal o cliente (host), sobre el cual se ejecuta una aplicación denominada "suplicante", la cual solicita permiso para acceder a la red al conectarse a ella en cualquier punto de acceso.

2) El punto de acceso o autenticador es cualquier dispositivo de red o NAD (Network Access Device). Este puede ser un switch o un access point (wireless) el cual es el encargado de identificar al cliente y comunicarse con un servidor de control de acceso.

3) El servidor de control de acceso o ACS (Access Control Server) contiene el perfil del usuario, este a su vez consulta a un servidor de contraseñas (token)

4) Un servidor de contraseñas denominado RADIUS (Remote Autentication Dial-In User Server) el cual verifica la contraseña.

Al llegar al RADIUS la comunicación se invierte de vuelta al cliente. Según el

resultado de la evaluación de su solicitud en ambos servidores se le permitirá o no el acceso a los recursos de la red, y de acuerdo a su perfil predeterminado.

El trabajo es presentado para su utilización de manera general, sin embargo se especificarán los aspectos técnicos de los servidores (hardware y software) utilizados y un caso de ejemplo.

Para la redacción de este informe se han recurrido a diversas fuentes bibliográficas, principalmente al estándar IEEE 802.1x, y a los documentos técnicos de los equipos y aplicaciones utilizadas en el sistema mostrado. En este informe trato de reflejar los conocimientos y experiencia adquiridos a lo largo de cinco años de egresado en varias empresas de telemática.

El trabajo ha sido dividido en cuatro capítulos principales: 1) Marco teórico, en donde se precisa el problema de ingeniería y el objetivo, así como la evaluación del problema, el alcance del trabajo y una sinopsis de la solución , 2) Problemática de la seguridad de redes de telecomunicaciones, en el cual se establece los conceptos básicos del control de acceso a red, el estándar 802.1x, las redes virtuales dinámicas y el RADIUS, 3) La Ingeniería del Proyecto, en donde se detalla los requerimientos y opciones tecnológicas disponibles y los criterios de selección de los elementos utilizados en la solución final, también se detalla el modo de funcionamiento de la solución y los aspectos técnicos de los servidores utilizados, 4) Costos del Proyecto, en donde se mostrarán los costos aproximados de la implementación de la solución, así como las tareas realizadas y los tiempos empleados.

El Informe finaliza con la presentación de conclusiones y es acompañada de los anexos necesarios para una mejor explicación del informe

Agradezco a la empresa Telefónica del Perú SAC por haberme brindado las facilidades para la presentación de este informe de suficiencia bajo el estricto cumplimiento de los normas de confidencialidad. También se agradece a las empresas proveedoras.

CAPÍTULO I
MARCO TEÓRICO

En este capítulo se plantea la ingeniería del problema. Se expondrá el problema en sí y el objetivo del trabajo. Posteriormente se evalúa el problema y se especifica el alcance del informe, haciendo finalmente una síntesis del sistema presentado.

1.1 Descripción del Problema

Se pueden resumir en a) Riesgo de acceso no autorizado a los recursos de la red por falta de un sistema de autenticación fiable, b) Lentitud en la red y c) Dificultad en el desplazamiento de los usuarios por la empresa que deben recurrir a un administrador de red para la configuración de sus puntos de acceso.

1.2 Objetivos

El objetivo es el desarrollo de un sistema de autenticación de usuarios (empleados o visitantes) para que hagan uso de los recursos de la red (intranet e Internet) de acuerdo a los perfiles de cada usuario o cliente, eliminar los síntomas de lentitud y una respuesta tardía ante los requerimientos de sus usuarios y permitir a los terminales de los usuarios su desplazamiento por la empresa sin la necesidad de recurrir a un administrador de red,

La solución se hace efectiva mediante la utilización de servidores ACS y RADIUS, uno conteniendo el perfil y permitiendo las VLAN dinámica, y el otro efectuando la verificación de las contraseñas de los terminales que solicitan el acceso a la red.

El informe tiene los siguientes objetivos:

1. Describir los conceptos básicos relacionados con la Seguridad Informática y el Control de Acceso.
2. Entender cómo funcionan las tecnologías cableadas existentes, así como los mecanismos de seguridad que se pueden enfocar a éstas. Describir conceptos relacionados con la autenticación y los protocolos y estándares RADIUS/EAP/802.1X, así como las especificaciones que faciliten su uso.
3. Proponer políticas para el control de acceso a una red, mediante la instalación y configuración de los servidores RADIUS , el Cisco Secure ACS que maneja los perfiles de los usuario y Vacman Middleware que maneja las claves dinámicas con los tokens.

1.3 Evaluación del problema

El problema es evaluado en sus dos principales componentes: 1) Riesgo de acceso no

autorizado, 2) Lentitud en la red y 3) Dificultad en el desplazamiento de los empleados dentro de la empresa.

1.3.1 Riesgo de acceso no autorizado

La falta de políticas de seguridad para el control de acceso a la red permite la intrusión física, donde se encuentren puertos de red disponibles para la conectividad a la LAN, ocasionando exposición de los recursos de la empresa a extraños malintencionados que generaban los siguientes problemas:

a) Estaciones de trabajo infectadas por malwares.
b) Espionaje industrial.
c) Robo de información confidencial y/o privada.
d) Intrusión en servidores y estaciones de trabajo.
e) Acceso y conocimiento de la topología de la red local.
f) Fraudes
g) Distintas técnicas de ataque local: Captura de contraseñas y sesiones de red, robo de credenciales de acceso a los recursos informáticos, ataques de negación de servicio.

Estos riesgos se podían controlar desactivando los puntos de red expuestos a extraños, y eran activados sólo cuando los empleados lo solicitaban por razones de reuniones o visitas de los "Partners".

Sin embargo al terminar dichas reuniones, el empleado se olvidaba de reportar al administrador de red para la desactivación de dichos puertos, quedando activa para cualquier uso, ya sea para bien o para mal, y este último es el que nos preocupa por los problemas ya expuestos.

1.3.2 Lentitud en la red

Se experimentan síntomas de lentitud y una respuesta tardía ante los requerimientos de sus usuarios, incluso para simples usos como descargar correos o navegar por la Internet.

La solución es aplicar metodologías de VLAN (Redes LAN Virtuales) para poder segmentar la red de la manera más óptima y segura a la vez.

1.3.3 Dificultad en el desplazamiento de los empleados dentro de la empresa

Con la llegada de las computadoras portátiles, las reuniones de trabajo pasaron a ser dinámicas, lo que significa que el usuario se moviliza dentro de las diferentes áreas, en su mayoría a las salas de reuniones. En muchas ocasiones se justifica que el usuario se provea de un punto de red que le permita conectarse a los recursos que suele usar.

Para ello, el empleado tiene que coordinar con los administradores de red para que ejecuten las configuraciones necesarias; sin embargo en algunas circunstancias el administrador de red no se encuentra disponible o se encuentra realizando otras labores,

lo que genera para el empleado un retraso en sus propias obligaciones.

El caso sería grave si se tratara de una presentación de un proyecto a los gerentes de un cliente que están listos para la firmar el contrato, pero el empleado no puede conectarse al servidor y realizar la demo con el cliente.

Debido a las dimensiones que toman las redes locales (LAN) y dada su capilaridad, es necesaria una buena administración del acceso a las mismas. Para lograrlo se debe aplicar una eficiente política de seguridad que permita autenticar y autorizar a cualquier individuo o dispositivo que requiera acceder a la red local.

La solución es asignar dinámicamente políticas de acceso de los dispositivos o usuarios al autenticarse; el estándar 802.1X junto con el servidor Cisco Secure ACS es que permiten el control de acceso de los usuarios y los recursos informáticos a la red local de la empresa basándose de los puertos de accesos provistos por los switches/Acces Point.

Utilizando dicha solución los dispositivos y/o usuarios podrán acceder a la red local únicamente cuando realicen la autenticación necesaria. En caso que la autenticación sea fallida se les deniega el acceso a la red

1.4 Alcance del trabajo

Esta sección expone:

1) los mecanismos de seguridad que debe proveer la solución, y

2) Los aspectos que no están incluidos.

1.4.1 Mecanismos de seguridad

Son expuestos a continuación:

a. La red LAN se debe segmentar por medio de VLAN de acuerdo a las áreas de trabajo.

b. A cada usuario se le debe asignar una IP estática, la cual la conocen muy bien. No se debe utilizar ningún servidor DHCP.

c. La empresa debe contar con una infraestructura LAN switching basada en equipos de la marca CISCO, que son los que están considerados dentro de la presente solución, con lo que se tiene un escenario adecuado para la implementación de la autenticación con 802.1X.

d. Se debe restringir el acceso total a personal no autorizado.

e. El usuario debe poder autenticarse en cualquier punto de red, dentro de las áreas de trabajo, sin solicitar al administrador de red la configuración previa.

f. Se debe contar con una zona para invitados autorizados con acceso sólo a Internet.

g. A cada usuario se le debe asignar un token digipass GO3 con su respectivo PIN para que pueda acceder a la red LAN.

h. En el firewall de la empresa se deberá crear políticas de acceso de acuerdo al perfil

de cada usuario.

i. Para la implementación de la solución se deberá hacer uso de la infraestructura de la empresa. Esta cuenta con firewall redundante, servidor RADIUS Cisco Secure ACS y switches de la marca CISCO con soporte 802.1X.

j. Las reglas de acceso no deben comportarse dinámicamente. Estas deberán ser solicitadas mediante una solicitud hacia el oficial de seguridad, quien será a su vez el único quien solicitará la configuración al área de Conectividad y Seguridad para su configuración.

Se considera además lo siguiente:

a. Comprar de un segundo servidor RADIUS Vacman Middleware con 100 tokens que permitan el uso de claves dinámicas.

b. Comprar el software suplicante SSC que se debe instalar en cada PC de los usuarios.

c. Autenticar las impresoras de red mediante su dirección MAC e imponer reglas específicas para el servicio que brinda.

1.4.2 Aspectos no incluidos

Los siguientes son los aspectos no incluidos en la solución:

a. No se incluirá el inventario de las aplicaciones que estén instalados o se estén ejecutando en las PCs de los usuarios.

b. No se realizará postvalidación del estado de las PC luego de autenticarse e ingresar a la red, ni durante el tiempo que permanece conectado.

c. Los servidores de la intranet de la empresa no formarán parte de esta solución, esto se encuentran protegidos por otra política de seguridad que está fuera del alcance de esta solución.

d. La solución no contará con mecanismos de detección y contención frente ataques de red que proviene de una PC correctamente autenticada. Para ello se cuenta con otra política de seguridad que está fuera del alcance de este trabajo.

e. Sólo se considerarán usuarios de datos, los usuarios/dispositivos de voz (voip=Telefonos, softphones).

f. No se considera el cableado estructurado, los accesorios para montaje en rack, los patch panels, los ordenadores de cable, etc., así como el energizado y/o cableado de energía.

g. Tampoco formarán parte de la solución los servidores de la intranet de la empresa. Estos se encuentran protegidos por otras políticas de seguridad que está fuera del alcance del trabajo.

h. La solución no incluye la configuración de antivirus y tampoco el IPS/firewall personal en cada computadora personal (PC) de le empresa.

1.5 Síntesis del trabajo

Debido a los riesgos que presenta una empresa que no cuenta con una política de control acceso, se plantea la implementación de una solución de acceso cableado y/o inalámbrico autenticado mediante el estándar 802.1x y el Protocolo de Autenticación Extensible (EAP)

También se aplican metodologías de VLAN (Redes LAN Virtuales) para poder segmentar la red de la manera más óptima y segura a la vez.

Para hacer la autenticación aun más robusta, se añade un servidor adicional, Vacman Middleware, que administra los tokens Vasco Middlware, que son los que generan password dinámicos de un sólo uso cada 32 segundos. La Figura 1.1 muestra el diseño de la solución con sus respectivos elementos que lo conforman.

Estos elementos son:

1. **El terminal o cliente (host)**.- Es donde se ejecuta una aplicación denominada "suplicante" o SSC (Cisco Secure Service Client) la cual solicita permiso para acceder a la red al conectarse a ella en cualquier punto de acceso. El usuario se autentica con su user-id y su contraseña. La contraseña que se ingresará es ahora el número que se muestra en el Digipass Go 3 más su PIN.
2. **El punto de acceso o autenticador**.- Es cualquier dispositivo de red o NAD (Network Access Device). Este puede ser un switch o un access point (wireless) el cual es el encargado de detectar al cliente y comunicarse con un servidor de control de acceso o servidor de autenticación (ACS),
3. **El servidor de control de acceso o ACS (Access Control Server)**.- Contiene el perfil del usuario, éste a su vez consulta al servidor de token para su aprobación.
4. **El servidor de Token (Vacman Middleware)**.- Ejecuta la verificación y responde al servidor ACS con un mensaje de acceso-aceptado o acceso-rechazado.

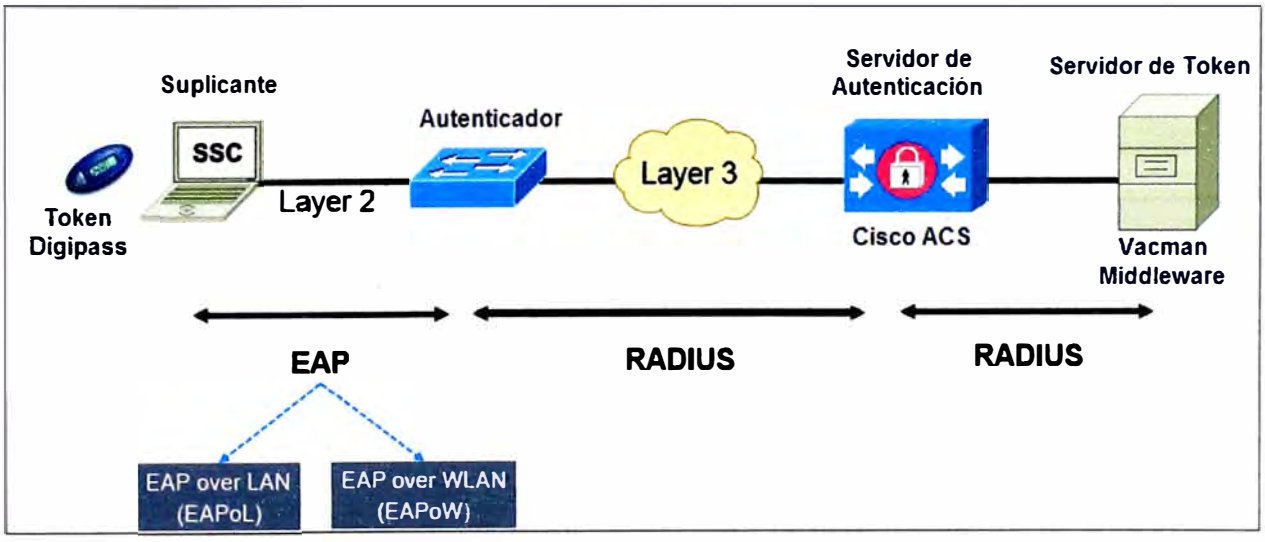

Figura 1.1 Diagrama de solución de autenticación 802.1X

Se explica los pasos del proceso de autenticación.

1. Si el servidor ACS recibe el mensaje de acceso-aceptado, éste le envía al auntenticador (Switch) el mensaje de acceso-aceptado más número de VLAN que el usuario pertenece.
2. El autenticador autoconfigura el puerto donde está conectado el usuario con la VLAN que éste debe pertenecer. A esto se le denomina asignación de VLAN dinámica.
3. Finalmente, el usuario recibe el mensaje de acceso-aceptado, y recién tiene acceso a la red para acceder a los diferentes recursos de la empresa.
4. Claro que una vez autenticado, el usuario tiene acceso sólo a los recursos que fueron configurados previamente en el firewall de la empresa. Esta es la razón por la que los usuarios usan IP estáticas. Cada usuario conoce cual es su IP.

CAPÍTULO II
PROBLEMÁTICA DE LA SEGURIDAD DE REDES DE TELECOMUNICACIONES

En este capítulo se exponen las bases teóricas conceptuales más importantes para la comprensión del sistema descrito en el presente informe.

Los temas a tratar son 1) Seguridad en redes de datos 2) Redes virtuales de área local, 3) El servidor RADIUS, 4) El estándar IEEE 802.1x.

2.1 Seguridad en redes de datos

Se tocarán los siguientes aspectos 1) Redes de Datos, 2) Seguridad, 3) Control de acceso a la red (NAC), 4) Arquitectura AAA

2.1.1 Redes de datos

Una red de datos es un sistema de comunicación entre computadoras que permite la transmisión de datos de una máquina a otra, con lo que se lleva a cabo un intercambio de todo tipo de información y de recursos.

a. Componentes

Una red está integrada por los siguientes componentes:

- Clientes. Usuarios de la red, como PC´s, impresoras, teléfonos, etc.
- Servidores de aplicaciones y bases de datos.
- El hardware de red, que comprende la infraestructura física de la red, a la cual se conectan los clientes y servidores. Como ejemplos se tienen a los switches y hubs, routers, gateways, access points y tarjetas de red.
- El medio en una red interconecta todos los componentes de la red. La conexión se puede llevar a cabo utilizando cables, fibra óptica e incluso el aire.
- Por último se encuentran los protocolos de red, los cuales sirven como estándar de comunicación entre los componentes de la red.

b. Clasificación

De acuerdo a su cobertura se clasifican en redes LAN, WAN y MAN:

b.1 Redes de Área Local, LAN (Local Area Networks). Es un grupo de equipos que pertenecen a la misma organización y están conectados dentro de un área geográfica pequeña a través de una red, generalmente con la misma tecnología.

Una LAN también puede definirse como la interconexión de varios equipos y dispositivos. Su extensión está limitada físicamente a un edificio o a un entorno no muy distante

y su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones.

b.2 Redes de Área Metropolitana, MAN (Metropolitan Area Network). La MAN es una red que abarca un área metropolitana generalmente consta de una o más redes de tipo LAN dentro de un área geográfica común..

b.3 Redes de Área Amplia, WAN (Wide Area Network). Es un tipo de red de computadoras que puede cubrir distancias desde 100 hasta 1000 km, dando el servicio a un país o a un continente.

2.1.2 Seguridad

La seguridad informática es una disciplina que se relaciona con diversas técnicas, aplicaciones y dispositivos, cuyo objetivo principal es asegurar la integridad, confidencialidad y disponibilidad de la información de un sistema informático y sus usuarios.

El establecimiento de políticas de seguridad ayuda a que en una organización se reduzcan los ataques que un sistema informático pueda sufrir. Es necesario administrar cuidadosamente las políticas de seguridad para mantener el equilibrio entre el acceso y uso transparentes y la seguridad de la red; en la figura 2.1 se muestra un diagrama del equilibrio entre las necesidades de la organización y la seguridad informática.

Figura 2.1 Equilibrio entre las necesidades empresariales y la seguridad informática

Algunas amenazas a la seguridad de un sistema informático o computadora son las siguientes: Programas malignos (Virus, espías, troyanos, gusanos, phishing, spamming), Siniestros (Robos, incendios, humedad), Intrusos (Piratas informáticos que pueden acceder remota o físicamente a un sistema para provocar daños), Operadores (Los propios operadores de un sistema pueden debilitar y ser una amenaza a la seguridad de un sistema ya sea por boicot, o por falta de capacitación o de interés).

Ante tales amenazas, uno de los puntos a cubrir son las claves de acceso, no se deben usar claves que en su constitución son muy comunes y no se deben compartir. En

cada nodo y servidor se deben usar antivirus, actualizar o configurar para que automáticamente se integren las nuevas actualizaciones del propio software y de las definiciones o bases de datos de virus registrados. También se deben utilizar programas que detecten y remuevan spywares (programas o aplicaciones que recopilan información sobre una persona u organización sin su conocimiento).

Existen dos tipos de seguridad con respecto a la naturaleza de la amenaza:

Seguridad lógica. Es un conjunto de políticas y mecanismos que permiten garantizar la confidencialidad, la integridad y la disponibilidad de los recursos en un sistema, según los requerimientos de la organización. Debido a la existencia de amenazas, se hace imprescindible la implantación de barreras de seguridad como: cortafuegos, antivirus, antiespías, encriptación de la información y uso de contraseñas, capacitación a los usuarios de los sistemas y capacitación a la población sobre las nuevas tecnologías.

Seguridad física. Es el tipo de seguridad que se utiliza cuando las amenazas son físicas, tales como humedad, incendios u otro medio que ponga en riesgo la seguridad. Los administradores deben tener en cuenta los siguientes aspectos básicos para con la seguridad de la red, los mismos que se extienden a los usuarios.

a. Manejo de Riesgos

Para brindar seguridad a la información es imprescindible realizar una evaluación metódica de los riesgos existentes. Los riesgos pueden ser: acceso o copia de manera indebida a la información, las descargas de programas con virus, hackers, daños por fuego, agua, etc.; estos riesgos pueden llegar a afectar datos, programas, equipos e incluso redes.

El primer paso es conocer los riesgos, una vez identificados los riegos se debe realizar una evaluación de los mismos, la cual debe identificar, cuantificar y priorizar riesgos contra los objetivos relevantes de la organización. La evaluación de los riesgos debe realizarse de manera periódica, y los resultados deben guiar y determinar la apropiada acción de gestión y las prioridades para manejar la información de los riesgos de seguridad y para implementar controles seleccionados para proteger estos riesgos.

b. Políticas de Seguridad Informática

Las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento.

Las políticas de seguridad proporcionan las reglas que gobiernan el cómo

deben ser configurados los sistemas y cómo deben de actuar los empleados de una organización en circunstancias normales y el cómo deben reaccionar si se presentan circunstancias inusuales. Una política de seguridad debe asegurar cuatro aspectos fundamentales en una solución de seguridad: a) Autenticación, b) Control de acceso., c) Integridad, d) Confidencialidad.

2.1.3 Control de acceso a la red (NAC)

Un control de acceso a la red (NAC Network Access Control), se refiere a la habilidad de permitir o denegar el uso de un recurso particular a una entidad en particular. Los mecanismos para el control de acceso pueden ser usados para cuidar recursos físicos, recursos lógicos ó recursos digitales.

Una solución NAC efectiva reduce el riesgo y los costos de la seguridad, identificando e impidiendo las amenazas y vulnerabilidades. Por medio de una evaluación constante de todos los equipos con respecto a las políticas definidas, el control de acceso a la red puede verificar, por ejemplo, que los parches de seguridad están instalados y que no se utilizan aplicaciones no permitidas.

a. Objetivos

Los objetivos generales que persigue un NAC son:

Reducción del riesgo de ataques desconocidos. El punto clave de las soluciones del NAC es la habilidad de prevenir el acceso a la red de equipos terminales que no posean software antivirus, parches de seguridad, o software de prevención de intrusión al equipo, evitando así poner en riesgo los demás equipos de la red contra contaminación de gusanos, virus o código malicioso.

Ejecución de políticas de seguridad. Las soluciones del NAC permiten a los administradores de red definir políticas, tales como cuáles tipos de computadoras, ó cuáles perfiles de usuarios deben tener acceso a determinadas áreas de la red, y forzar su ejecución a través de switches o routers.

Manejo de identidad y acceso. Mientras las redes IP convencionales ejecutan sus políticas de seguridad y acceso en base a direcciones IP, un NAC lo hace basándose en identidades autenticadas, al menos para equipos terminales de usuarios, tales como laptops y desktops.

Para llevar a cabo un adecuado control de acceso se debe realizar una autenticación, es decir, identificar a los usuarios válidos que puedan acceder a los sistemas informáticos. Además, se debe realizar una correcta asignación de privilegios a dichos usuarios. Y por último, un registro de las operaciones ejecutadas en el sistema.

b. Tipos de Control de Acceso a la Red

Existen diferentes tipos de control de acceso a una red, los cuales se explican a

continuación:

Basado en hardware.- Tanto si es "in-line" o "out-of-band", esta opción necesita habitualmente de un equipo (appliance) que tendrá que estar instalado en casi cualquier ubicación donde sea preciso contar con un NAC.

Basado en agentes software.- El siguiente paso es el basado en pequeños programas residentes en los ordenadores y dispositivos, instalándose estos agentes en cada uno de los sistemas que deban ser controlados por el NAC. Los agentes escanean y monitorizan el dispositivo, generalmente enviando los resultados a un servidor central. Los sistemas que no cumplen con los requisitos no tendrán autorización de acceso a la red, y a menudo se les envía algún tipo de medida correctora para que cumplan las directivas de seguridad.

Sin agentes software.- El NAC sin agentes es otra de las variantes, y consiste en partes software que se ejecutan puntualmente. Con esta configuración, la idea es que un agente temporal (generalmente algún tipo de control ActiveX) escanee el cliente periódicamente en búsqueda de vulnerabilidades o incumplimientos en la política de seguridad. Los resultados del escaneo son enviados al servidor central de políticas, y se ejecuta una acción si es necesario en caso de que el sistema no cumpla con los requerimientos. Cuando el proceso se completa, el agente se descarga.

NAC dinámico.- El NAC dinámico, que utiliza agentes sólo en un porcentaje determinado de equipos. También se conoce como NAS peer-to-peer, siendo una opción que no requiere cambios a nivel de red o software que deba ser instalado en cada equipo. Los agentes, que en ocasiones pueden llegar a ser obligatorios, son instalados en sistemas seguros.

c. Operación de un Control de Acceso a la Red

A continuación se explica brevemente la operación de un NAC:

Detección e Identificación de nuevos dispositivos conectados a la red. Esto se lleva a cabo por la identificación de peticiones de autenticación, lo anterior se realiza a través de los switches.

Autenticación de usuarios y dispositivos. La Autenticación hablando de sistemas informáticos es un procedimiento que consiste en comprobar la identidad de una entidad (persona o equipo), con vistas a la autorización del acceso de dicha entidad a ciertos recursos (sistemas, redes o aplicaciones). La autenticación se realiza utilizando el estándar 802.1x y un servidor RADIUS, mismos que se describen más adelante.

Evaluación o revisión de sistemas finales. En cuanto a su cumplimiento y/o

vulnerabilidades. En esta parte se hace una revisión de las condiciones en las que se encuentra el equipo, que busca conectarse a la red en cuanto a su cumplimento, con políticas previamente establecidas, como son sistema operativo, programas y aplicaciones instalados, actualizaciones de antivirus así como nivel de parcheo. Esto se realiza con el objetivo de que si un equipo de usuario deja de cumplir con las políticas establecidas, éste será redireccionado a la zona de remediación.

Autorización para usar la red. Basado en los resultados de la autenticación y evaluación. Como ya se mencionó, esta fase depende de los resultados obtenidos previamente, entonces se determina el rol o función que desempeña la estación o equipo final de usuario, y de acuerdo con esto, se autoriza el uso de recursos de red.

Remediación para equipos .Aquellos con problemas de cumplimiento de políticas de seguridad. Aquí se resuelven problemas de cuarentena de sistema finales, y/o usuarios para evitar impacto negativamente en la red.

d. Elementos de un Control de Acceso a la Red

Los elementos que integran un control NAC se listan a continuación:

Equipo cliente. En una red, los equipos clientes son empleados por los usuarios de una red, tales como PC's, impresoras, servidores, entre otros.

Autenticador. Entidad en un extremo de un segmento punto a punto de una LAN que facilita la autenticación de la entidad conectada al otro extremo del enlace.

NAC Gateway. Es un dispositivo que se encuentra entre el servidor de autenticación y el equipo de usuario final. Este dispositivo permite controlar las acciones de autenticación y autorización, mediante la manipulación de los atributos que entrega el servidor de autenticación, a fin de indicar al autenticador la acción a seguir.

Servidor de autenticación. Entidad que facilita servicio de autenticación al autenticador.

e. Tipos de amenazas

Actualmente en el mercado existe unas cuantas soluciones de NAC. Independientemente de sus diferencias, todas fueron diseñadas para proteger contra diversas amenazas a la LAN corporativa. Estas amenazas pueden ser colocados en dos grandes categorías: amenazas no intencionales y amenazas intencionales

e.1 Amenazas no intencionales

El usuario que utiliza el dispositivo actúa con la conciencia tranquila y no hace nada malo a sabiendo que va afectar adversamente a los sistemas y datos en la LAN. Esta es la preocupación del mayor número de empresas, por lo que no desea que una portátil infectada de un proveedor externo, contratista, etc., infecte a sus LAN.

Los empleados pueden causar infecciones no intencionales. Los dos tipos de

dispositivos que se debe considerar en lo que respecta a las amenazas no intencionales son: los dispositivos de propiedad de las empresas que están autorizados a conectarse a la LAN, y los dispositivos de invitados (o desconocidos) que pueden o no estar autorizados a conectarse a la LAN. Para evitar que las amenazas no intencionales (virus, gusanos) sucedan, NAC podría haber hecho lo siguiente:

- Chequeando para ver si el portátil del contratista tenía software de antivirus y se encuentre actualizado hasta la fecha, y puesto en cuarentena o restringido su acceso si no lo estaba.
- Dando cuenta de que su dispositivo fue un invitado y debió ponerlo en un segmento de red o VLAN que no tenían acceso a los sistemas de la empresa.
- Evitando toda la conectividad de red, ya que el sistema estaba decidido a no ser un activo corporativo.

e.2 Amenazas intencionales

Las amenazas intencionales basadas en LAN implican acciones maliciosas a sabiendas y conscientemente que tienen lugar en la LAN. El método de ataque se basa en el establecimiento de la conectividad a la LAN para establecer el ataque. Esta conectividad puede ser establecida por un gran número de diferentes maneras:

- A un contratista, socio de negocios, etc. se le da la autorización y las instrucciones para conectarse a la LAN, aunque él usa el acceso para realizar actos no autorizados y maliciosos.
- A un extraño se le permite el acceso físico dentro de la oficina, aunque no están autorizados a conectarse a la LAN (por ejemplo, un vendedor - Seguridad física importante), caminando dentro de la empresa encuentra una PC desbloqueada de un empleado.
- Un extraño se aprovecha de la no-conectividad Ethernet para obtener acceso (Wi-Fi, acceso telefónico a distancia - war dial).

Todos estos medios para establecer la conectividad son importantes debido a que comparten un rasgo común. Todos ellos fueron capaces de omitir o saltearse al Firewall y a otras tecnologías que se ponen para proteger a la red local de los extraños de Internet. La Figura 2.2 muestra una representación gráfica de esta amenaza.

Una vez conectado a la LAN desde el interior, pueden realizar una gran cantidad de ataques maliciosos. Estos ataques no serán detectados por las líneas tradicionales de defensa e incluyen actos tales como los siguientes:

- Sniffing de datos de la aplicación y archivos que se transfieren a través de la LAN.
- Sniffing de nombres de usuario y contraseñas en la red LAN.
- Atacar a los servidores y estaciones de trabajo para afectar la confidencialidad y la

integridad de los datos.

- Atacar la infraestructura y afectando a la disponibilidad de los sistemas.

Es necesario aclarar que Sniffer o husmeo, es el acto de capturar los datos que está fluyendo a través de una red. Los datos se envían en paquetes, y con frecuencia, estos datos son enviados en texto plano. Mediante el análisis de los paquetes, los datos pueden ser consultados.

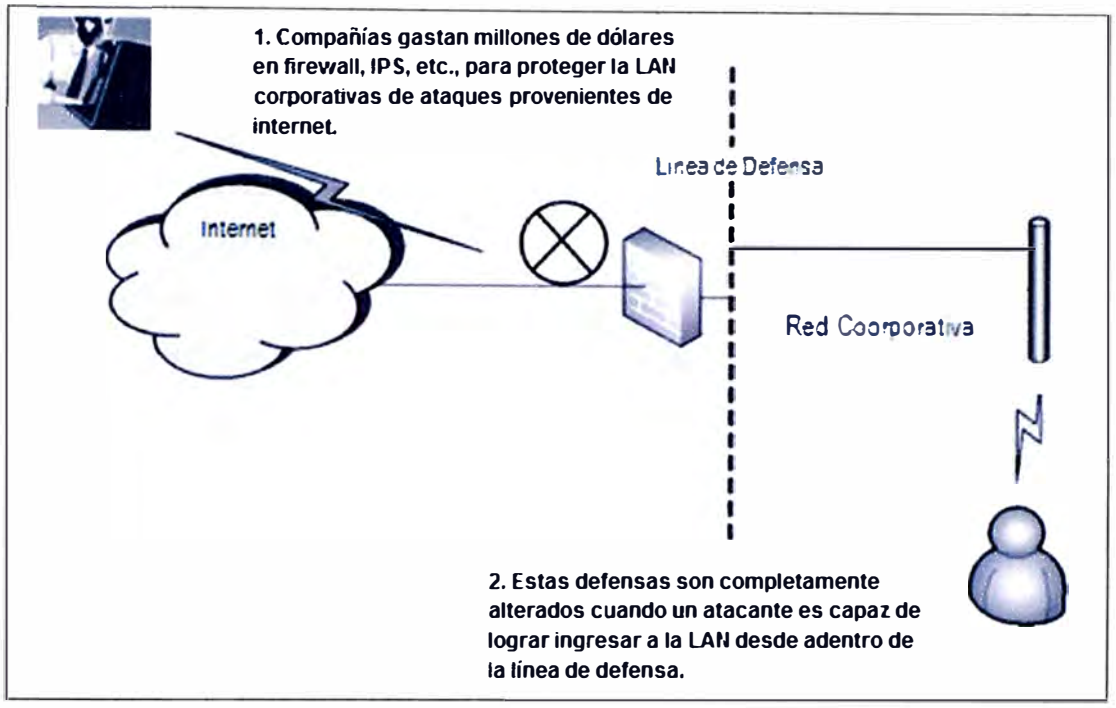

Figura 2.2 Amenaza intencional

f. Tipos de explotación de las LAN

Para saber cómo protegerse de los escenarios explicados anteriormente, es fundamental entender como las LAN pueden ser explotadas.

f.1 Explotación por acceso no autorizado y uso malicioso

En este escenario se utiliza el caso de un contratista malicioso que ha sido contratado por una compañía para entrar y realizar algunas tareas de programación. A éste se le ha dado autorización para conectarse a la LAN para acceder a Internet, además es informado sobre las políticas de seguridad y sobre las acciones que puede y no puede realizar mientras trabaja en la empresa.

Dado que el contratista malicioso no quiere que ninguno de sus acciones deje rastro, él va a realizar un ataque pasivo. Él va a realizar un husmeo (sniffing) a la red para registrar usuarios y contraseñas. La probabilidad de ser capturado es muy baja, salvo que alguien registre en su pantalla.

El acto de husmear se realiza se hace de forma pasiva. Esto significa que los datos no son modificado en tránsito, simplemente se observa lo a que pasa. Husmear la red se realiza con aplicaciones especiales fáciles de adquirir. Estas aplicaciones estarán al

servicio para muchos propósitos, muchos de ellos muy legítimos. Se puede analizar el comportamiento de la red, aplicaciones, etc, por lo que es una herramienta muy valiosa.

El contratista llega a usar una herramienta Wireshark para capturar información sensible de le empresa. Así que fácilmente puede ver un mensaje de correo electrónico que se envió a la red. Por supuesto, él no se limita a sólo a los mensajes de correo electrónico. Se puede ver aplicaciones de mensajería instantánea, archivos que se transfieren, y así sucesivamente. Hay una serie de herramientas disponibles que hacen sniffer a la red para tipos específicos de información. Algunos de estas aplicaciones incluyen las siguientes:

DSniff – captura de contraseñas.

AIM-Sniff- captura el tráfico de mensajería instantánea

MailSnarf- captura el tráfico por e-mail

SMBSpy- captura el tráfico Server Message Block (SMB)

Driftnet: muestra todas las imágenes gráficas que se envían a través de la LAN

URLSnarf: muestra los sitios de Internet que se accede

Otra gran herramienta a tener en cuenta se llama Caín. Caín es una herramienta extraordinariamente útil que puede ser considerado como un cuchillo Swiss Army. Realiza una variedad de funciones en una pequeña herramienta práctica. Se puede hacer sniffer a un montón de diferentes tipos de credenciales, incluyendo las siguientes: HTTP, POP3, VNC, Telnet, SMTP, MS Kerberos, RADIUS keys, RADIUS users.

El MS Kerberos es usado para capturas las credenciales de los dominios de Windows, esta sería la herramienta que el contratista más usaría. Todas ellas son posibles debido a que el contratista tiene acceso físico en la red corporativa.

f.2 Explotación de acceso fisico autorizado y el acceso no autorizado a la LAN

Como huésped de la empresa, el contratista antes mencionado fue autorizado a físicamente entrar en el espacio de la oficina y conectarse a la LAN.

El hecho de que no deben conectarse a la LAN, no significa necesariamente que no podrán. En todas las oficinas que he ingresado, la conectividad LAN directa es sólo un cable Ethernet. Lo único que impide este la conectividad es un empleado que de aviso de una persona no autorizada. En algunas empresas, esa persona no autorizada pueda ser atrapada con bastante rapidez. En otros, la persona podría mostrarse todos los días en el trabajo y nadie le haría cualquier pregunta.

f.3. La explotación no autorizada con acceso fisico y el acceso no autorizado LAN

Estos tipos de explotación son los más difíciles pero no imposibles de realizar, la técnica más usada es la ingeniería social. Para demostrar esto se cita un caso real de una prueba de penetración en una empresa que gastó miles de dólares en compra de

Firewall, IPS, software antispam, antivirus, etc. Para ello se esparció en el área dispositivos de almacenamiento USB infectados (supuestamente perdidos). Se recurría a la curiosidad de los que lo encontraran de saber que contenían. Dado ello, la PC del empleado se infectó severamente, comprometiendo a la red corporativa, con malware y ejecutando programas maliciosos automáticamente por el "Autorun.inf", cuyo contenido puede ser OPEN=keylogger.exe:

En esencia, mediante la inserción de esa unidad USB, El ejecutor de las pruebas de penetración o un hacker podría capturar el nombre de usuario de red y la contraseña que ha sido ingresado por el usuario corporativo quién insertó la unidad USB. También podrían controlar de forma remota el dispositivo y utilizarlo como una plataforma para atacar a los otros sistemas de la red corporativa.

f.4 La explotación no autorizada de accesos inalámbricos y remotos a la red LAN

En los ejemplos anteriores, se mostró al atacante ingresar físicamente a la oficina para ejecutar sus ataques. Para la mayoría de las empresas, ello no es tan necesario. Los atacantes pueden intentar explotar la LAN de las siguientes maneras: 1) A través de portátiles de la compañía, 2) Al romper la red inalámbrica desde las inmediaciones, 3) Al ganar acceso a la red a través de soluciones VPN remotas, 4) Mediante el uso de la dial-war para encontrar el acceso de una línea telefónica a la red LAN

Evitar esto podría hacerse de la siguiente forma:

- Las soluciones NAC que requieren autenticación impediría los accesos no autorizados a la LAN desde sistemas no-corporativos. Esto de reforzaría al usar claves dinámicas.
- Limitación de los contratistas y otras personas ajenas a sus propios segmentos de LAN ayudaría a proteger los sistemas internos.
- Asegurarse de que los activos comunes estén siempre actualizados y parchados o desconectarlos de la LAN cuando se esté corriendo una prueba de penetración o el hacker haya deshabilitado el software de antivirus, algunas soluciones NAC podrían desconectar los sistemas no conformes de la LAN
- Para el contratista que ejecuta el sniffer, posterior a la admisión, NAC podría revisar de manera rutinaria para ver si se están ejecutando aplicaciones (conocidas como sniffer) no permitidas, si fuera el caso, lo detendría y reportaría.

g. Opción de seguridad NAC

A la hora de escoger un producto NAC se debe considerar restringir el acceso a la red a los usuarios no autorizados. Éste parece ser el requisito prioritario en la mayoría de las organizaciones: "si un usuario no autorizado accede físicamente a una conexión de red, debe ser bloqueado de inmediato". NAC se caracteriza, entre otras cosas, por ser: un control automático que se comunica fácilmente con los auditores; muy parecida (si no

idéntica - 802.1X) a los controles implementados en la seguridad de redes inalámbricas en muchas organizaciones. El requisito también supone varias presunciones de lo contrario y que se muestran a continuación:

- Permitir el acceso a los usuarios invitados autorizados con sistemas gestionados en buen estado.- Un contratista o invitado que intenta acceder a la red desde un activo gestionado y en buen estado debe poder acceder a la red. De todas formas, habría que añadir al invitado al dominio para que se conectara al sistema gestionado, de modo que se trataría del mismo caso que un usuario habitual de un sistema gestionado. Sin embargo, es necesario tener en cuenta la directiva de seguridad específica que se aplica a dicho usuario.

- Permitir el acceso a los usuarios invitados y autorizados con sistemas no gestionados en buen estado.- Un contratista o invitado que intente acceder a la red desde un sistema no gestionado debe contar tanto con un mecanismo de autenticación (usualmente algún tipo de formulario Web) como con un método para evaluar su estado.

Si bien muchos invitados tienen de hecho todos los derechos de acceso a sus sistemas para instalar temporalmente un agente o desactivar su firewall o HIPS (sistema de prevención de intrusiones en el host), otros muchos no lo tienen.

- Permitir el acceso de usuarios autorizados con sistemas no gestionados.- En la mayoría de los casos se espera que exista algún método para que los usuarios habituales se conecten a la red con activos empresariales que están fuera de los mecanismos estándar de autenticación, o con sus propios sistemas, tanto conectados físicamente de forma interna o mediante el escenario más común de utilizar una VPN de su casa.

2.1.4 Arquitectura AAA

AAA (Authentication, Authorization, and Accounting) es un estándar para el diseño de sistemas basados en la autenticación, no es un sistema en sí, sino una colección y definición de normas (un marco) para la creación de sistemas. AAA se traduce en Autenticación, Autorización y Arqueo (contabilidad).

La fusión de estos tres conceptos permite crear un sistema de gestión completa de usuarios que controle todos los aspectos relativos a su identificación (autenticación), gestión de recurso o servicios permitidos para su uso (autorización) y gestión de reportes y estadísticas para el control de su utilización (arqueo). Posee una grandísima potencia para gestionar cualquier tipo de servicio, desde los más simples hasta lo más complejos y seguros.

Todo el modelo AAA queda perfectamente explicado en los siguientes documentos de la IETF: 1) RFC2903: Arquitectura genérica AAA, 2) RFC 2905: Marco de autorización AAA, 3) RFC 2905: Ejemplos de aplicación de autorización AAA, 4) RFC 2906:

Requerimientos para la autorización AAA.

Estos documentos son la mejor base para explicar en su totalidad la infraestructura de los sistemas AAA. Específicamente el documento RFC 2905 explica en profundidad el marco de desarrollo del estándar y las relaciones de confianza entre los diferentes componentes de la infraestructura.

La arquitectura AAA es un esquema clásico cliente-servidor. El cliente es el equipo o usuario que solicitaría la autenticación o la entrada al sistema y el servidor es el recurso que provee de servicios. En el caso de AAA, no se debe utilizar esta definición de cliente y servidor, ya que estos podrían llevar a equívocos, puesto que estos conceptos "cliente/servidor" son más ambiguos. En esta cadena de participantes existen diferentes componentes que la hace un poco más compleja:

a. El equipo o usuario que solicita autenticación o entrada se llama suplicante, y no es obligatoriamente quien inicia la secuencia de autenticación.

b. El equipo de red que hace de puerta de entrada física a la red llamado NAS (Network Access Server) o servidor de acceso a la red, es el que permite la entrada física a la red y tramita nuestra autenticación. Puede ser una pila de MODEMS, un Switch de red, un punto de acceso (AP), un router, etc. Este equipo suele ser quien inicia la secuencia de autenticación al detectar una conexión activa en una de sus puertas, por ello se le denomina autenticador. Su labor es la de hacer de intermediario entre el suplicante y el servidor de autenticación. En AAA también se le denomina "Equipo de Servicio" o Service Equipment. El NAS es en la realidad el centro de todo este sistema AAA, ya que es el responsable de abrir o limitar las características reales de funcionamiento de la infraestructura.

c. El Servidor de Autenticación que puede ser RADIUS, TACACS u otros y es el que dirige todo el proceso de autenticación, autorización u arqueo de los servicios y usuarios que solicitan acceso. Por supuesto en AAA se le conoce como "Servidor AAA"

d. El Servidor de Autenticación o Servidor AAA puede hacer el papel de **n** elevando las consultas a otros servidores AAA. De esta manera, un Servidor AAA que hace de Proxy se convierte en cliente de otro servidor.

e. El servidor de directorio o servidor de base de datos de usuarios y credenciales, al cual el servidor de autenticación va a solicitar los datos de autenticación de los solicitantes de acceso. Éste pudiera ser la misma máquina que el servidor de autenticación, aunque en instalaciones reales no suela serlo. Puede ser un servidor de AD (Active Directory) de LDAP (Lightweight Directory Access Protocol), una base de datos SQL (MySQL, Microsoft SQL Server, Oracle, etc.), o un servidor Unix con credenciales de usuarios.

f. El servidor de recursos y servicios que necesita el usuario para realizar su cometido en la red. Puede ser un servidor de almacenamiento de datos, un servidor web, etc.

g. El proveedor de servicios (Service Provider) en el modelo AAA es el propietario de la infraestructura de acceso a la que se conecta el usuario y por lo tanto, es el propietario del servidor AAA y del equipo de servicio o NAS. Puede haber varios proveedores de servicio que colaboren entre sí. Si esto ocurre, y existen varios proveedores en colaboración para prestar un servicio, el servidor contractural del usuario se denomina UHO (User Home Organization).

Es por esta secuencia que se hace difícil definir de forma general en el estándar AAA, quién es el cliente y quién es el servidor. En la terminología que utiliza AAA, el cliente es aquel que envía paquetes con estructura AAA a un servidor AAA. Pero esto lo puede hacer el suplicante, así como el equipo NAS o el propio servidor. Para evitar confusiones se hablará de: suplicante, NAS o auntenticador y Servidor de Autenticación. En líneas generales, en el proceso de configuración de RADIUS, se habla de clientes para definir a los NAS.

a. Autenticación

¿Quién es el solicitante? Hace referencia al proceso por el cual se determina si un usuario tiene permiso para acceder a un determinado servicio de red del que quiere hacer uso. El proceso de autenticación se realiza mediante la presentación de una identidad y unos credenciales por parte del usuario que demanda acceso. Durante el proceso de autenticación de un usuario para acceder a una red, no es el suplicante quien habla el lenguaje AAA con el servidor de Autenticación, sino que el suplicante habla NAS o Autenticador, y es este quien traduce y encamina los paquetes hacia el servidor de autenticación. De esta manera, no existe un camino abierto entre el suplicante y el servidor de autenticación, con lo que se garantiza bastante la seguridad del servidor de autenticación contra ataques directos, ya que un atacante tendría que estar en el interior de su infraestructura.

En la fase se autenticación se produce un mensaje inicial de solicitud de acceso desde el equipo NAS al servidor de autenticación en forma de: Acces Request (Solicitud de acceso). El suplicante envía el nombre de usuario y la contraseña cifrada, si procede hacia el NAS. Este envía entonces al servidor de autenticación el mensaje de Access Request solicitando además el puerto de acceso para el suplicante.

b. Autorización.

¿A qué servicio le voy a permitir acceder? Se refiere a conceder servicios específicos (entre los que se incluye la "negación de servicio") a un determinado usuario, basándose para ello en su propia autenticación, los servicios que está solicitando, y el estado actual

del sistema. Es posible configurar restricciones a la autorización de determinados servicios en función de aspectos como la hora del día, la localización del usuario, o incluso la posibilidad o imposibilidad de realizar múltiples "logins" de un mismo usuario.

El proceso de autorización determina la naturaleza del servicio que se concede al usuario, como son: la dirección IP que se le asigna, el tipo de calidad de servicio (QoS) que va a recibir, el uso de encriptación, o la utilización obligatoria de túneles para determinadas conexiones.

Existen multitud de reglas o campos configurables en los sistemas AAA. Estos campos o parámetros se conocen como atributos o AVP (Attribute Value Pairs) en AAA. El sistema de diseño de este estándar es totalmente modular, ya que todo el intercambio de información y usuarios se basa en estos atributos, unos atributos están definidos en los RFCs comunes y otros son específicos de cada fabricantes de equipos. Todos estos atributos en los que se conoce como diccionarios de atributos (dictionary), si son atributos estándares se almacenan en el diccionario estándar y si son atributos de fabricante en los diccionarios de fabricantes.

En esta fase el servidor de autenticación, tras conocer todos los atributos necesarios para el solicitante, responderá a su solicitud de autenticación mediante un mensaje estándar enviado al equipo NAS para permitir, denegar o volver a preguntar sobre su acceso:

Access – Accept (Aceptación del Acceso). El fin mismo de la solicitud de autenticación es la aceptación del acceso si el mecanismo de acceso ha sido correcto, se le envía este mensaje al NAS con los atributos para regular el acceso del suplicante de forma personalizada.

Access - Reject (Denegación del Acceso). Debido a las circunstancias que puedan no permitir el acceso de un usuario, como por ejemplo: Usuario inexistente, contraseña incorrecta, derechos revocados, etc., se le deniega de forma incondicional el acceso a este solicitante. Se puede incluir en este mensaje el motivo de la denegación del servicio. El NAS que recibe este mensaje no permite el acceso al suplicante enviando un mensaje (si se incluye) al solicitante o suplicante.

Access – Challenge (Solicitud de información adicional para el acceso). Se le solicita al solicitante o suplicante información adicional, como contraclave, tarjeta de acceso, PIN de acceso, o cualquier método alternativo o adicional de acceso. El NAS trasmite la solicitud al suplicante. Este mensaje puede ser intercambiado en múltiples ocasiones, dependiendo del tipo de autenticación y de la información que se precisa.

Tras este intercambio de mensajes, el suplicante estará autorizado o no a utilizar los recursos de la red a la cual desea acceder. Si lo estuviera, estaría regulado por los

derechos u obligaciones asignados durante este proceso, como duración máxima de la conexión, máximo flujo de datos, VLANs de acceso, etc.

c. Arqueo

¿Qué hace el cliente con los servicios que prestó? Una vez realizado el proceso de autorización, se produce la fase de arqueo "Accounting". Esta es iniciada por el autenticador o NAS, tras autorizar el acceso al suplicante. El arqueo es la fase estadística y recolección de datos sobre la conexión. Se produce en forma de contadores o logs de conexión y suelen almacenar en base de datos SQL relacionadas con el usuario o en ficheros tipos log.

Estos datos correctamente manejados y gestionados permiten tomar decisiones en cuanto al uso de los recursos por parte de los usuarios, con el fin de denegar conexiones, cambiar los anchos de bandas mediante QoS (Calidad de Servicio), impedir descargar, etc.

La fase de arqueo está limitada por la capacidad del equipo NAS de registrar información de sesiones. Algunos equipos ni siquiera son capaces de realizar este recuento y de suministrar información alguna de arqueo.

La contabilidad de la conexión permite a los buenos administradores mediante estadísticas gestionar la futura demanda de crecimiento de sus sistemas para, planificar sus ampliaciones. También como debe suceder en los sistemas de seguridad o IDS, se debería generar avisos por intentos reiterados o denegados de conexiones infructuosas para tomar decisiones basadas en la seguridad, si bien la mayor parte de los equipos y servidores no proveen este tipo de información. Durante la fase de arqueo se produce los siguientes mensajes:

Accounting – Request [Start] (Solicitud de inicio de arqueo). Es una solicitud de inicio enviada desde el equipo NAS al servidor, para indicar que ha comenzado la fase de arqueo y se comienzan a registrar los datos de la session del usuario.

Accounting – Response [Start] (Respuesta de asentimiento al inicio de arqueo). El servidor de autenticación responde a la solicitud inicial, registrando la información de inicio y enviando este paquete al NAS para mostrar su conformidad.

Accounting – Request [Stop] (Solicitud de final de arqueo). El NAS comprueba la desconexión del usuario y envía al servidor un mensaje de final de la fase del arqueo con los siguientes datos de la sesión del usuario.

a. Delay Time: tiempo de intento de envío de este mensaje.
b. Input Octets:Número de byte recibidos por el usuario
c. Output Octets: Número de byte enviados por el usuario
d. Session time: Duración en segundo de la session del usuario.

e. Input packet: Número de paquetes recibidos por el usuario.
f. Output packet: Número de paquetes enviados por el usuario.
g. Reason: Motivo de la desconexión de la session del usuario.

Accounting – Response [Stop] (Respuesta de asentimiento al dinal de arqueo). El servidor tras almacenar la información anterior, envía al NAS su conformidad al final de la fase de arqueo, admitiendo haber recibido correctamente toda la información de la sesión.

Es importante observar el porqué la arquitectura del AAA es en promedio una mejor estrategia que otras. Antes de que el AAA fuera introducido, un solo equipo individual tenía que ser utilizado para autenticar a usuarios. Sin un estándar formal, cada máquina tenía probablemente un método diferente de autenticación – algunos probablemente utilizaron perfiles, mientras que otras pudieron haber utilizado el protocolo de Challenge/Handshake (CHAP), y algunas otras pudieron haber usado una base de datos interna pequeña de consultas con SQL.

2.2 Redes virtuales de área local

Una red de área local (LAN) está definida como una red de computadoras dentro de un área geográficamente acotada como puede ser una empresa o una corporación. Uno de los problemas que nos encontramos es el de no poder tener una confidencialidad entre usuarios de la LAN como pueden ser los directivos de la misma, también estando todas las estaciones de trabajo en un mismo dominio de colisión el ancho de banda de la misma no era aprovechado correctamente.

La solución a este problema era la división de la LAN en segmentos físicos los cuales fueran independientes entre si, dando como desventaja la imposibilidad de comunicación entre las LANs para algunos de los usuarios de la misma. La necesidad de confidencialidad, como así el mejor aprovechamiento del ancho de banda disponible dentro de la corporación ha llevado a la creación y crecimiento de las VLANs.

Una VLAN se encuentra conformada por un conjunto de dispositivos de red interconectados (hubs, bridges, switches o estaciones de trabajo) la definimos como una subred definida por software y es considerada como un dominio de Broadcast que pueden estar en el mismo medio físico o bien puede estar sus integrantes ubicados en distintos sectores de la corporación (Figura 2.3).

La tecnología de las VLANs se basa en el empleo de Switches, en lugar de hubs, de tal manera que esto permite un control más inteligente del tráfico de la red, ya que este dispositivo trabaja a nivel de la capa 2 del modelo OSI y es capaz de aislar el tráfico, para que de esta manera, la eficiencia de la red entera se incremente. Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, se

logra el incremento del ancho de banda en dicho grupo de usuarios. Una VLAN tiene dos funciones principales: 1) Contiene broadcasts, 2) Agrupa dispositivos. Los dispositivos ubicados en una VLAN no son visibles para los dispositivos ubicados en otra VLAN.

Es necesario que el tráfico cuente con un dispositivo de Capa 3 para poder transmitirlo entre VLAN.

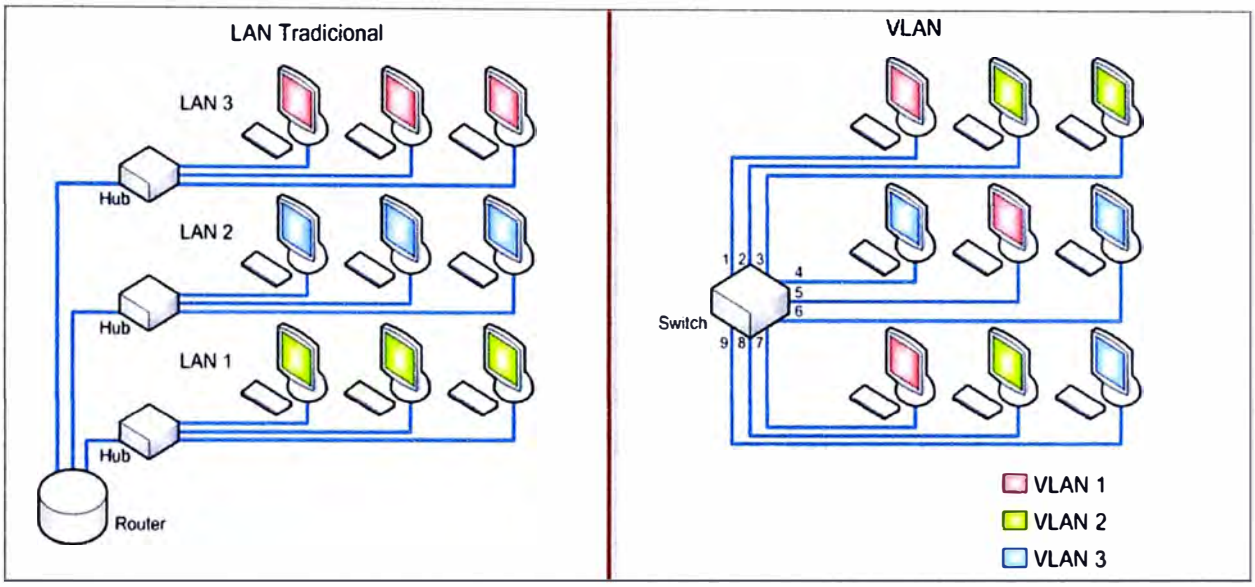

Figura 2.3 LAN vs. VLAN

2.2.1 Membresía estática y dinámica

En una red conmutada, un dispositivo puede asignarse a una VLAN según su ubicación, su dirección MAC, su dirección IP o las aplicaciones que utiliza con más frecuencia. Los administradores pueden asignar la membresía a una VLAN de forma estática o dinámica.

Este tipo de membresía a una VLAN es el más fácil de configurar y también es el más difundido; sin embargo, requiere un mayor grado de apoyo administrativo en caso de adiciones, traslados y cambios. Por ejemplo, el traslado de un host de la VLAN a otra requiere reconfigurar manualmente el puerto del switch para asignarlo a la nueva VLAN o conectar el cable de la estación de trabajo a otro puerto del switch de la nueva VLAN.

La membresía dinámica a VLAN requiere un servidor de política de administración de VLAN (VMPS). El VMPS contiene una base de datos que asigna direcciones MAC a la VLAN. Cuando se conecta un dispositivo a un puerto del switch, el VMPS busca en la base de datos una coincidencia con la dirección MAC, y asigna ese puerto de forma temporal a la VLAN correspondiente.

La membresía dinámica a VLAN requiere más organización y configuración, pero crea una estructura con mucha más flexibilidad que la membresía estática a una VLAN. En una VLAN dinámica, los traslados, las adiciones y los cambios están automatizados, y no requieren intervenciones por parte del administrador.

2.2.2 Identificación de VLAN

Cuando se crea una VLAN, se le asigna un número y un nombre. El número de la VLAN puede ser cualquier número del rango disponible en el switch, con la excepción de VLAN1. Algunos switches admiten aproximadamente 1000 VLAN, mientras que otros admiten más de 4000. Se considera que la asignación de nombres a las VLAN es una de las mejores prácticas de administración de redes.

Los dispositivos conectados a una VLAN sólo se comunican con otros dispositivos de la misma VLAN, independientemente de que estén en el mismo switch o en switches diferentes.

Un switch asocia cada puerto con un número de VLAN específico. Cuando una trama ingresa a ese puerto, el switch agrega el ID de la VLAN (VID) en la trama Ethernet. La adición del número de ID de la VLAN a la trama Ethernet se denomina etiquetado de tramas. El estándar de etiquetado de tramas más frecuente es IEEE 802.1q.

El estándar 802.1Q, a veces abreviado a dot1q ("punto1q"), agrega un campo de etiquetado de 4 bytes a la trama Ethernet. Esta etiqueta se incluye entre la dirección de origen y el campo de tipo/longitud.

Las tramas Ethernet tienen un tamaño mínimo de 64 bytes y uno máximo de 1518 bytes. Sin embargo, una trama Ethernet etiquetada puede tener un tamaño de hasta 1522 bytes. Las tramas contienen campos como: 1) Las direcciones MAC de origen y destino, 2) La longitud de la trama, 3) Los datos de carga, 4) La secuencia de verificación de trama (FCS)

2.2.3 Puertos

Una VLAN tiene tres funciones principales:

- Limita el tamaño de dominios de broadcast
- Mejora el rendimiento de la red
- Proporciona un nivel de seguridad

A fin de aprovechar todos los beneficios de las VLAN, éstas se extienden por diversos switches. Los puertos de switch pueden configurarse para dos funciones diferentes. Un puerto se clasifica como puerto de acceso o puerto de enlace troncal. Ver Figura 2.4

a. Puerto de acceso

Un puerto de acceso pertenece sólo a una VLAN. Por lo general, los dispositivos individuales como las PC o los servidores se conectan a este tipo de puerto. Si un hub conecta varias PC a un único puerto de acceso, todos los dispositivos conectados al hub son miembros de la misma VLAN.

b. Puerto de enlace troncal

Un puerto de enlace troncal es un enlace punto a punto entre el switch y otro

dispositivo de red. Los enlaces troncales transmiten el tráfico de diversas VLAN mediante un único enlace, y permiten que las VLAN se extiendan por toda la red. Los puertos de enlace troncal son necesarios para transmitir el tráfico de diversas VLAN entre dispositivos al conectar dos switches entre sí, un switch a un router o un host NIC compatible con los enlaces troncales definidos en 802.1Q.

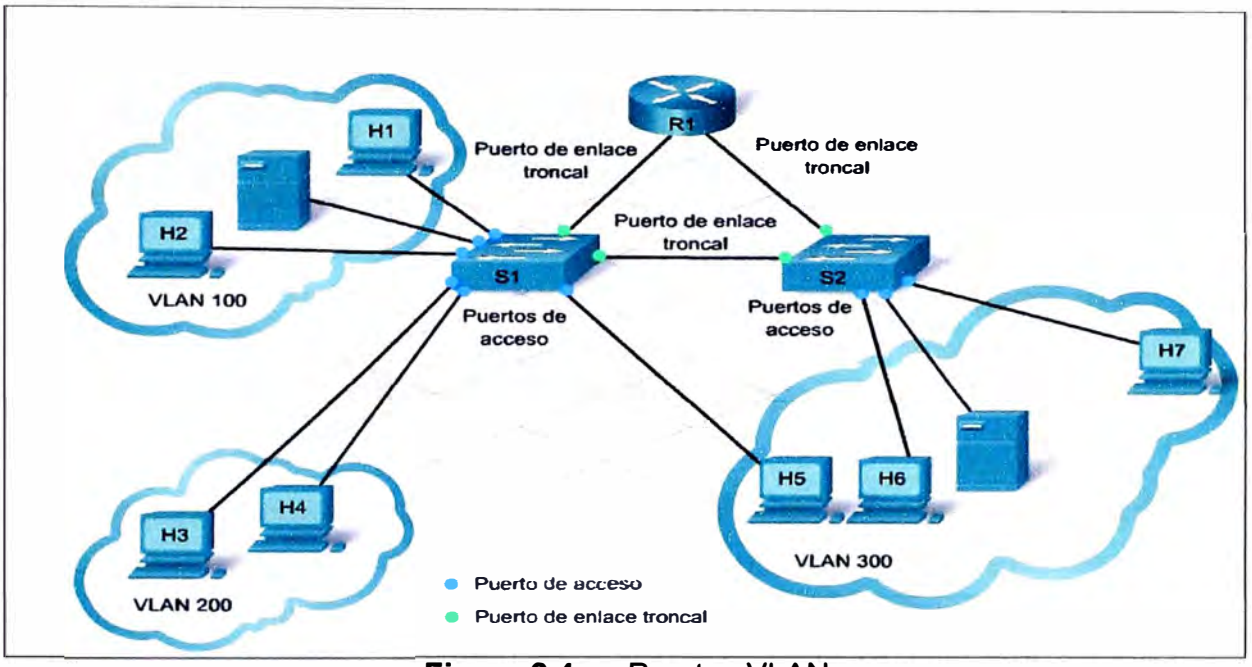

Figura 2.4 Puertos VLAN

Sin los puertos de enlace troncal, cada VLAN requiere una conexión separada entre switches. Por ejemplo, una empresa con 100 VLAN requiere 100 enlaces de conexión. Este tipo de disposición no es fácil de escalar y resulta muy costosa. Los enlaces troncales ofrecen una solución a este problema al transportar tráfico de diversas VLAN a través del mismo enlace.

Cuando se transmiten diversas VLAN por el mismo enlace, éstas deben contar con identificación. Un puerto de enlace troncal es compatible con el etiquetado de tramas. El etiquetado de tramas agrega información sobre las VLAN a la trama.

IEEE 802.1Q es el método estandarizado y aprobado para llevar a cabo el etiquetado de tramas. Cisco ha desarrollado un protocolo de etiquetado de tramas patentado denominado enlace Inter-Switch (ISL, Inter-Switch Link). Los switches de mayor nivel, como la serie Catalyst 6500, aún son compatibles con ambos protocolos de etiquetado. Sin embargo, la mayor parte de los switches LAN -como el 2960- son compatibles con 802.1Q únicamente.

2.2.4 Extensión de VLAN en switches

Los enlaces troncales permiten a las VLAN enviar tráfico entre switches mediante un único puerto. Un enlace troncal configurado con 802.1Q en ambos extremos permite transmitir tráfico con un campo de etiquetado de 4 bytes agregado a la trama. Esta

etiqueta de la trama contiene el ID de la VLAN.

Cuando un switch recibe una trama etiquetada en un puerto de enlace troncal, elimina la etiqueta antes de enviarla a un puerto de acceso. El switch envía la trama sólo si el puerto de acceso es miembro de la misma VLAN que la trama etiquetada.

Sin embargo, es necesario que cierto tráfico se transmita a través del enlace configurado según 802.1Q sin un ID de VLAN. El tráfico sin ID de VLAN se denomina sin etiquetar. Entre los ejemplos de tráfico sin etiquetar se cuentan el protocolo de descubrimiento de Cisco (CDP), VTP y ciertos tipos de tráfico de voz. El tráfico sin etiquetar minimiza los retrasos asociados con la inspección de la etiqueta de ID de la VLAN.

Para procesar el tráfico sin etiquetar, existe una VLAN especial llamada VLAN nativa. Las tramas sin etiquetar recibidas en el puerto de enlace troncal con 802.1Q son miembros de la VLAN nativa. En los switches Catalyst de Cisco, la VLAN 1 es la VLAN nativa predeterminada.

Puede configurarse cualquier VLAN como VLAN nativa. Asegúrese de que la VLAN nativa para un enlace troncal con 802.1Q sea la misma en ambos extremos de la línea de enlace troncal. Si son diferentes, pueden ocasionarse bucles en Spanning Tree.

2.2.5 Enrutamiento entre VLANs

Aunque las VLAN se extienden para abarcar diversos switches, sólo los miembros de la misma VLAN pueden comunicarse. Un dispositivo de Capa 3 proporciona conectividad entre diferentes VLAN. Esta configuración permite que el administrador de red controle estrictamente el tipo de tráfico que se transmite de una VLAN a otra.

Un método para realizar el enrutamiento entre VLAN requiere una conexión de interfaz aparte al dispositivo de Capa 3 para cada VLAN. Otro método para proporcionar conectividad entre distintas VLAN requiere una función llamada subinterfaces. Las subinterfaces dividen lógicamente una interfaz física en diversas rutas lógicas. Es posible configurar una ruta o una subinterfaz para cada VLAN.

La compatibilidad con la comunicación inter-VLAN mediante subinterfaces requiere configuración tanto en el switch como en el router.

El host de la VLAN de origen envía el tráfico al router mediante el gateway predeterminado. La subinterfaz de la VLAN especifica el gateway predeterminado para todos los hosts de esa VLAN. El router ubica la dirección IP de destino y lleva a cabo una búsqueda en la tabla de enrutamiento.

Si la VLAN de destino se encuentra en el mismo switch que la VLAN de origen, el router vuelve a enviar el tráfico al origen mediante los parámetros de subinterfaz del ID de la VLAN de origen. Este tipo de configuración a menudo se denomina router-on-a-stick

("router en un palo"). Si la interfaz de salida del router es compatible con 802.1Q, la trama conserva su etiqueta de VLAN de 4 bytes. Si la interfaz de salida no es compatible con 802.1Q, el router elimina la etiqueta de la trama y le devuelve su formato de Ethernet original.

2.3 RADIUS

RADIUS (Remote Authentication Dial-Up Server), significa servidor de autenticación remota para sistemas de marcado de telefónico a redes. El protocolo fue desarrollado originalmente como un protocolo de control de acceso que verifica y autentifica a usuarios basados en el método comúnmente usado de desafío/respuesta (CHAP). El protocolo RADIUS tiene un lugar prominente entre los servicios de proveedores de Internet, pertenece a cualquier ambiente en donde sea necesaria o deseada la autenticación central, la autorización regulada, y el manejo de cuentas de usuario. RADIUS es un protocolo que cumple todas las normas de estándar AAA,

2.3.1 Características del protocolo

Las especificaciones mínimas que debe ofrecer un servidor RADIUS propicio para la aplicación a la que va a ir destinado son las siguientes:

Debe Cumplir la función para la cual se va adquirir, incluir todas las tecnologías necesarias para que pueda cubrir las necesidades del usuario final de autenticación, a través de cualquier sistema operativo y/o plataforma de seguridad, soportar el sistema de base de datos o servicio de directorio que hayamos elegido para la gestión de usuarios y de arqueo de cuentas, disponer de la arquitectura adecuada para la instalación en la plataforma servidora elegida, soportar o ser soportado por todas las plataformas de hardware que utilicemos en la infraestructura interna de red, como equipos de electrónica de Red, NAS, Plataforma PPP, ADSL, GSM, Wi-Fi, Wi-Max, enrutadores, etc.,

Debe ser fácilmente configurable y administrable, cumplir unos niveles adecuados de seguridad en su parte de cliente y de proveedor de seguridad, fiel a los estándares y RFC, que los regulan, ser transportable y migrables a otros entornos, ser abierto con otros sistemas, a la hora de intercambio de información,

Si fuera necesario, disponer de un sistema de gestión centralizado de servidores, si precisamos de ello, disponer de la redundancia y escalabilidad necesarias para una gran instalación, disponer de control de carga y de calidad de servicio, proveer de sistemas de control de sesiones de usuarios activas o cambios dinámicos en la autorización, ser preciso y concienzudo en el registro de información sobre sesiones para ofrecer estadísticas y registros adecuados. Es necesario en algunos casos que sea capaz de manejar SNMP o información de syslog,

Debe incluir técnicas de troubleshooting y depuración para localizar fácilmente la

causa de los problemas que se detecten, debe poseer posibilidad de enlazar el accounting contra sistemas de tarificación si se precisa de ellos, ser un producto actualizable y adaptable a los cambios que se produzcan, tanto en el cliente como en el mercado, ofrecer garantías de servicio y soporte técnico adecuado a las necesidades.

Todas estas características, dependiendo del tipo de implementación que se necesita, son las que definen a RADIUS o cualquier servidor AAA.

2.3.2 Descripción del protocolo

RADIUS es un protocolo que se ejecuta en una de las múltiples plataformas que permite (Unix, GNU/Linux, Windows y Solaris, entre otras) y que permanece de forma pasiva a la escucha de solicitudes de autenticación. Para lograrlo utiliza el Protocolo de Datagrama de Usuario, UDP (User Datagram Protocol) y permanece a la escucha en los puertos 1812 para la autenticación y 1813 para el arqueo.

RADIUS es el servidor de autenticación, que junto con el solicitante y el autenticador, son los componentes principales del estándar AAA. RADIUS está basado en un modelo cliente-servidor, ya que escucha y espera en forma pasiva las solicitudes de sus clientes o Servidores NAS.

En este modelo el NAS es el responsable del envío y de la correcta recepción de las solicitudes de acceso, y es el servidor RADIUS el responsable de verificar las credenciales del usuario y de ser correctas, de enviar al NAS los parámetros de conexión necesarios para prestar el servicio a los solicitantes.

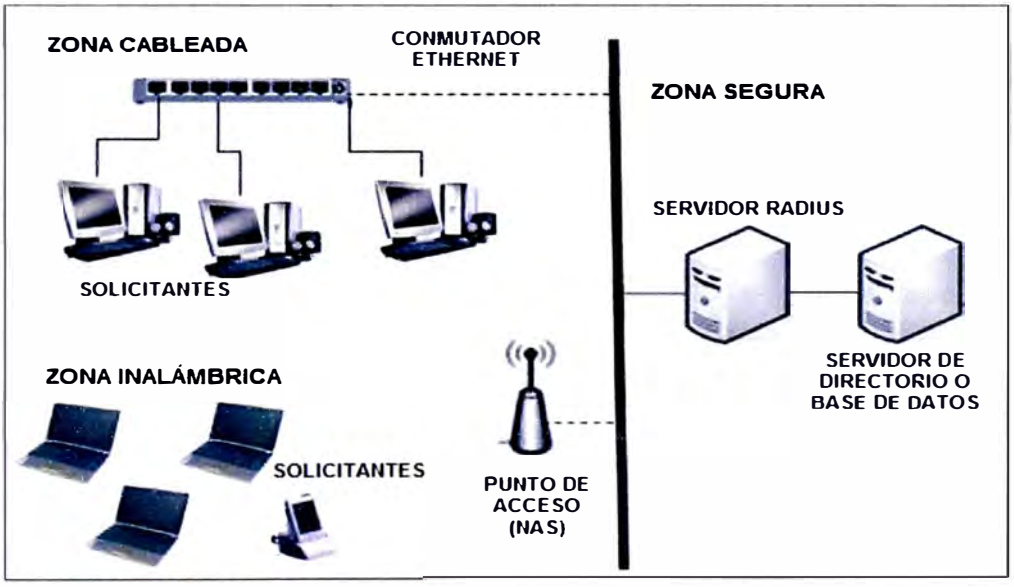

Figura 2.5 Infraestructura simple RADIUS

En la figura 2.5 se puede observar el modelo típico de implantación de un servidor RADIUS, en dicha figura se tiene una zona segura donde se encuentran el servidor RADIUS y el servidor de directorio y base de datos (BD), esta zona está protegida para los usuarios externos, los cuales primeramente deben autenticarse

mediante el NAS para poder llegar a ella. El solicitante deberá realizar una petición al NAS o al Conmutador Ethernet, mismos que gestionarán su solicitud al servidor RADIUS. Este a su vez, consultará el servidor de directorio o BD de credenciales y permitirá o no el acceso al solicitante.

2.3.3 Métodos de autenticación

Los métodos de autenticación son paquetes de software o módulos de software sobre los que basa el proceso de autenticación de usuario una plataforma de RADIUS. Estos módulos son realmente complejas cajas matemáticas encargadas de realizar el cifrado, descifrado y empaquetado de todos los procesos complejos de autenticación. Desde el método nativo de RADIUS que es PAP hasta los más actuales como algunos tipos nuevos de EAP, la evolución en cuanto a seguridad ha sido notable.

Cuando RADIUS recibe una solicitud de acceso, va pasándola por cada uno de los módulos de autenticación que tenga activándose en su configuración, hasta que algunos de esos módulos reconozcan sus algoritmos o las credenciales del usuario y se encargue de validar la autenticación.

PAP (Password Authentication Protocol o protocolo de autenticación mediante contraseña). El "atributo de contraseña" del usuario en un paquete solicitado señala al servidor RADIUS que el protocolo PAP va a ser usado para la transacción.

CHAP (Challenge Handshake Authentication Protocol o protocolo de desafío mutuo). Es un método del tipo de secreto compartido, ya que ambos sistemas comparten el conocimiento de una contraseña o hash. El suplicante o usuario conoce su contraseña en texto plano y el servidor tiene también que conocer la contraseña. En el momento de la autenticación, el servidor envía una frase aleatoria (desafío) para que el suplicante la pase junto con su contraseña por una función MD5 y se la reenvíe. Al recibirla el servidor, que ya conoce su valor calculado, la compara con su resultado recibido y, si es correcto, permite la entrada del suplicante a la red. Ese desafío se puede repetir en varias ocasiones durante la sesión del usuario, pero con frases de desafío diferentes.

MS-CHAPv1. La mejora de MS-CHAP sobre CHAP es que el servidor ni el cliente deben almacenar la contraseña de usuario en texto plano, ya que tanto al procesar el desafío por parte del cliente como por parte del servidor, ambos utilizan el valor hash de la contraseña y no la contraseña en sí.

MS-CHAPv2. Es la versión actual de CHAP de Microsoft, que tiene soporte en todos su SO desde Windows 200 y que es incompatible con la v1. Permite soporte para cambios de contraseña y mensaje de respuesta con estados.

Unix. Se pueden utilizar simplemente los nombres de usuarios y contraseñas existentes en un sistema Unix/Linux que se encuentran almacenados en el directorio etc de Unix en

el fichero passwd o mediante la función shadow.

HTTP Digest. Es también un protocolo de autenticación por desafío para clientes de servidores web con autenticación RADIUS; para evitar los ataques de repetición usa también frases precomputadas únicas. También utiliza MD5 como algoritmo, aunque maneja otros como SHA-1.

Otros métodos de autentificación soportados por RADIUS, contempla los métodos EAP: EAP-MD5, EAP-TLS, EAP-PEAP (MSCHAPV2, TLS, GTC), EAP-TTLS (PAP, CHAP, MSCHAP, MSCHAPV2, MD5), EAP-GTC, EAP-SIM, EAP-AKA, EAP-MSCHAPV2, LEAP.

a. Tipos de Autenticación

La manera de almacenar los nombres de usuarios y contraseñas de los solicitantes, puede realizarse de diferentes maneras:

Autenticación contra archivo de usuarios. Esta es la forma más básica utilizada por los servidores de autenticación. Utiliza un fichero de texto en el cual se almacenan las credenciales de los usuarios y los parámetros asociados a éstos. Se recomienda sólo para redes con un número reducido de usuarios.

Autenticación contra el sistema operativo. Aquí basta dar los privilegios suficientes para que un módulo del servidor de autenticación pueda leer los usuarios y sus contraseñas almacenadas en las formas nativas que utilizan los sistemas operativos.

Autenticación contra bases de datos. En este tipo de autenticación contra una base de datos, generalmente del tipo SQL, como Oracle, Microsoft SQL Server, MySQL y PostGreSQL, los datos de credenciales de usuarios, sus atributos de autorización y la información de arqueo de cuentas se almacenan en bases de datos pudiéndolo hacer de manera cifrada utilizando funciones como MD5 o SHA1, por ejemplo.

Autenticación contra servicios de Directorio. Este tipo de autenticación es apropiado para empresas medianas a grandes que quieran autenticar a sus empleados contra sus sistemas internos de gestión de usuarios.

b. Reautenticación

La reautenticación del solicitante se lleva a cabo si se pierde la conexión y necesita volver a autenticarse en el servidor RADIUS. También se puede forzar esta reautenticación en intervalos de tiempo para incrementar la seguridad; sin embargo, se debe tener cuidado para programar este tiempo a fin de evitar saturar al servidor.

2.3.4 Estructura de las comunicaciones

RADIUS requiere que las consultas fallidas hacia un servidor sean redirigidas a un

segundo servidor, y para hacer esto, una copia del pedido original debe existir sobre la capa de transporte del modelo de red (modelo OSI). Esto, en efecto obliga a usar tiempo de retransmisión.

RADIUS no es afectado por los estados del equipo como pérdida de poder, reinicio, tráfico, pesado, y decomisión del sistema. UDP previene todas estas dificultades ya que permite que una sesión se abra y se mantenga abierta durante toda la transacción.

UDP permite que RADIUS despache múltiples pedidos al mismo tiempo, además en cada sesión posee habilidades de comunicación sin restricciones entre el equipo de red y los clientes. La desventaja de utilizar UDP es que los desarrolladores por sí mismos deben crear y administrar tiempos de retransmisión, pero esta desventaja no se compara con la conveniencia y simplicidad de usar estos segmentos de transporte en red .

a. Estructura de un mensaje RADIUS

Los paquetes RADIUS consisten de los campos: 1) código, 2) identificador, 3) tamaño, 4) autenticador y 5) atributos (Figura 2.5).

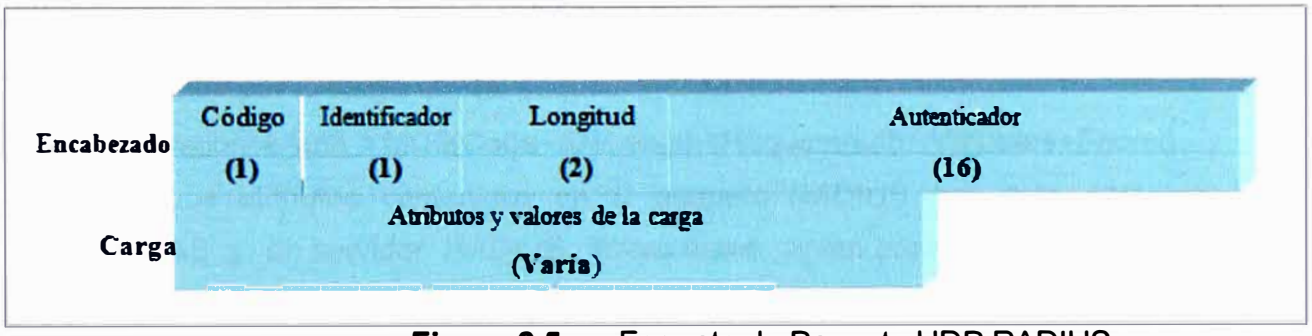

Figura 2.5 Formato de Paquete UDP RADIUS .

Este paquete RADIUS viene encapsulado dentro de un paquete UDP estándar. A continuación se describe cada campo:

Código.- La región de código tiene una longitud de un byte y sirve para distinguir que tipo de mensaje RADIUS ha sido enviado en el paquete. Los paquetes con campos inválidos son desechados sin notificación. Los códigos validos son:

Tabla 2.1 Valores campo código

Código	Tipo de paquete
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
6	Accounting-Status
7	Password-request
9	Password-reject
11	Access-Challenge

Identificador.- El identificador tiene una longitud de un byte y es usado para hacer threading (secuencias), o enlace automático de los pedidos iniciales y contestaciones

subsecuentes. El servidor RADIUS generalmente puede interceptar mensajes duplicados con examinar factores como el origen de la dirección IP, el origen del puerto UDP, la duración entre los mensajes sospechosos, y el campo de identificación.

Longitud.- La región de longitud es de dos bytes y se usa para especificar el tamaño del mensaje RADIUS. El valor en este campo se calcula al analizar los campos de: código, identificador, longitud, autenticador, y haciendo la suma de sus atributos.

Autenticador.- La región de autentificación tiene una longitud por lo regular de 16 bytes, este es el campo en que la integridad de la carga útil del mensaje se inspecciona y verifica. Hay dos tipos específicos de valores de autenticación: los valores de pedido y respuesta. Los de pedido son usados con los paquetes de Authentification-Request y Accounting-Request. El valor de pedido es de 16 bytes y es generado aleatoriamente para prevenir cualquier ataque.

El autenticador de respuesta es usado en los paquetes Acces-Accept, Acces-Reject, y Acces-Challenge. El valor es calculado con una función hash generada por los valores en las regiones del paquete: código, identificador, longitud, y la región de autenticador de pedido, seguido por la carga útil del paquete y el secreto compartido

Ejemplo: ResponseAuth = MD5(Code+ID+Length+RequestAuth+Attributes+Secret)

Atributos. Los atributos contenidos en el paquete RADIUS son datos comunicados entre el NAS y el servidor RADIUS. Estos datos sirven para el funcionamiento de todo el proceso AAA. Existen atributos de todo tipo, como los atributos User-Name y User-Password, que se utilizan en las solicitudes de autenticación y que definen al usuario y a su contraseña. Todos los procesos que realiza RADIUS se realizan mediante atributos, existiendo atributos para la fase de Autenticación, para la de Autorización y para la de Arqueo. Algunos de estos atributos se muestran en la Tabla 2.2, y se incluye el campo código, el cual debe ir en el paquete

Tabla 2.2 Atributos RADIUS

Código	Atributo
1	User-name
2	User-password
3	CHAP-password
4	NAS-IP-address
5	NAS-Port
46	Acct- session-time
64	Password-reject

b. Tipos de paquetes

Existen cuatro tipos de paquetes que son relevantes para las fases de autentificación y la autorización en la transacción AAA.

Access-Request (Petición de acceso) El paquete de petición de acceso se utiliza por el consumidor de servicios cuando esta solicitando un servicio particular de la red. Lo que caracteriza a un paquete de petición es que el valor del campo de código en el encabezado es igual a uno. (Figura 2.6)

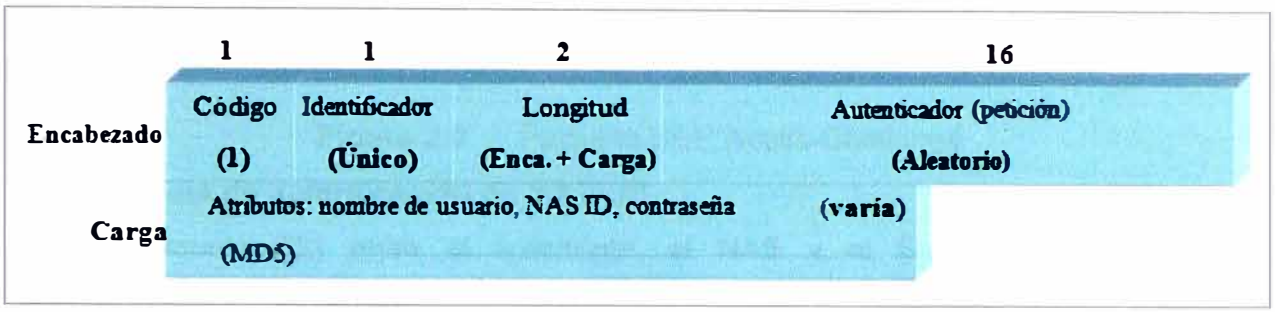

Figura 2.6 Paquete UDP *Acces-Request*.

Acces-Accept (Acceso aceptado) Los paquetes de acceso aceptado son enviados por el servidor RADIUS al cliente para reconocer que se conoce la petición del cliente. Si todas las peticiones en la carga útil que forman la petición de acceso son aceptadas, entonces el servidor RADIUS debe fijar el campo de código a dos. (Figura 2.7)

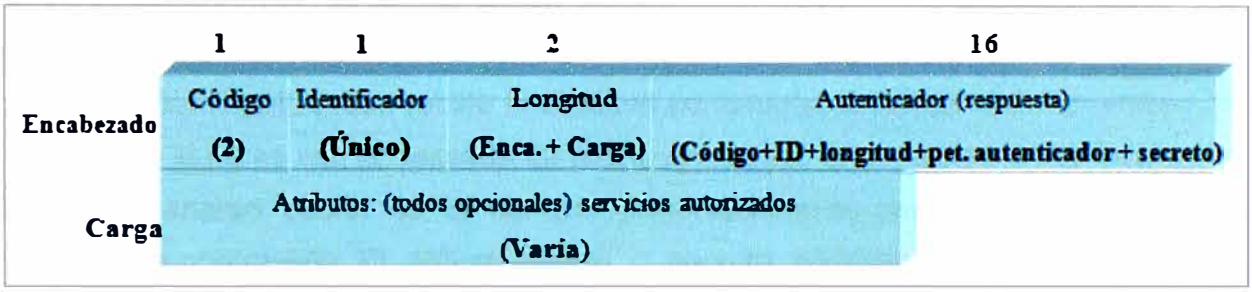

Figura 2.7 Paquete UDP *Acces-Accept*.

Access-Reject (Acceso rechazado) El servidor RADIUS es requerido para mandar un paquete de acceso denegado de regreso al cliente, si es denegado cualquiera de los servicios pedidos en el paquete de petición de acceso. La negación puede estar basada en políticas de sistemas, privilegios insuficientes, o cualquier otro criterio. (Figura 2.8)

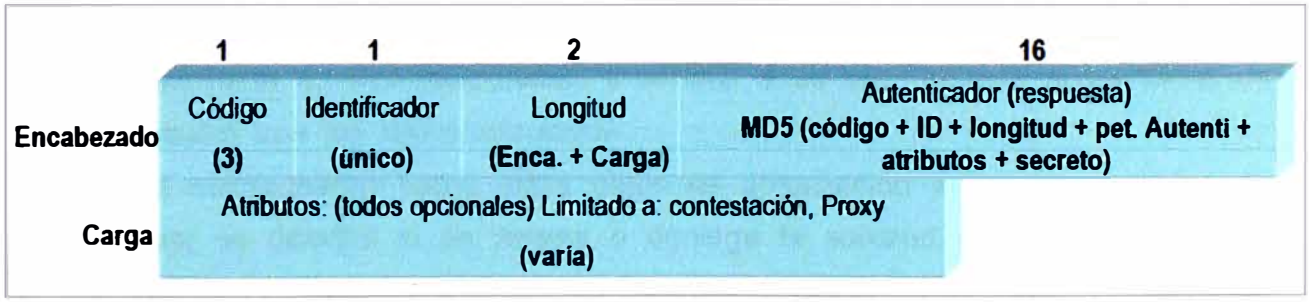

Figura 2.8 Paquete UDP Acces-Reject.

Acces-Challenge (Desafío de Acceso). Si el servidor recibe información conflictiva de un usuario, requiere más información, o simplemente desea disminuir el riesgo de una autenticación fraudulenta, puede publicar un paquete de desafió de acceso al cliente. Ver en la Figura 2.9 la estructura del paquete UDP Acces-Challenge

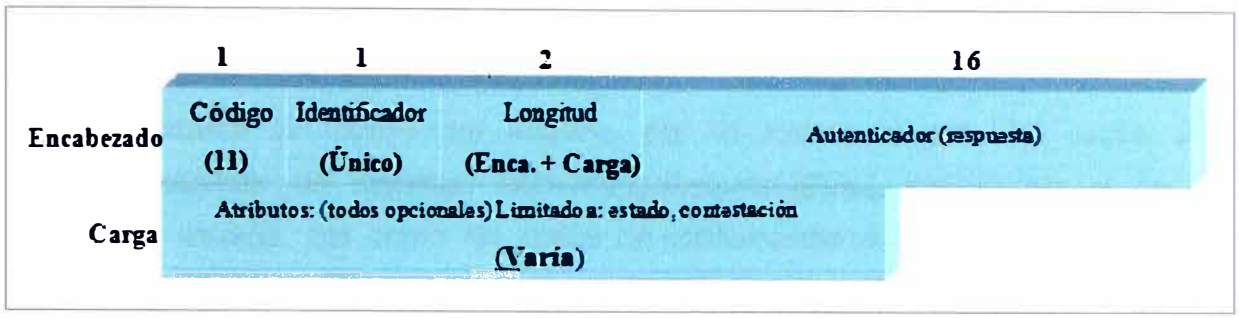

Figura 2.9 Paquete UDP Acces-Challenge

b. Secuencia de autenticación de RADIUS

La comunicación entre el solicitante, el NAS y el Servidor de autenticación tiene la siguiente secuencia.

1. La secuencia comienza por un Access-Request, esta solicitud de acceso es un mensaje que contiene atributos como el nombre de usuario, la contraseña, el número de puerto NAS y el ID de cliente. El NAS envía esta solicitud al servidor RADIUS que tenga preestablecido en su lista de servidores, si es que tuviera más de uno. Si no recibiera respuesta en un tiempo determinado, reintentará el envío cierto número de veces.

2. El servidor RADIUS que recibe la solicitud comprueba si proviene de un equipo NAS autorizado, si no es así, la descarta de forma silenciosa. Si el cliente NAS está en su lista y el shared secret es el correcto comprueba en su base de datos el nombre de usuario y la contraseña. El shared secret o secreto compartido de RADIUS es una contraseña con formato alfanumérico de hasta 128 bytes que se define en los dos extremos de un canal RADIUS, esos extremos son el servidor RADIUS y su cliente, el cliente puede ser un equipo NAS, un servidor Web o un Proxy RADIUS. Este secreto se utiliza para encapsular las comunicaciones entre el cliente y el servidor RADIUS.

3. Si el tipo de autenticación está basada en el desafío, se envía al solicitante un mensaje de Access-Challenge con una frase aleatoria que debe calcular. Después de esto, el solicitante enviará este cálculo y el NAS a su vez, enviará nuevamente un Access-Request con los datos calculados.

4. Una vez comprobados todos estos datos de autorización y la base de datos de credenciales, se decidirá si se acepta o deniega la solicitud. Así, se enviará ya sea un mensaje de Access-Accept o uno de Access-Reject al NAS con los atributos necesarios para activar o denegar el servicio.

5. Si el mensaje anterior es un Access-Accept, el NAS abrirá el puerto con los atributos designados y enviará un mensaje de Accounting-Request [Start] al servidor RADIUS, indicándole que ha comenzado el arqueo de la sesión del usuario. El servidor RADIUS confirmará la recepción del inicio de sesión enviando al NAS un mensaje

Accounting-Response [Start] y guardará los datos de inicio de la sesión de usuario que le envío el NAS con el Accounting-Request [Start]

6. Al terminarse la sesión del usuario, por él mismo o por otra razón el NAS envía al servidor un mensaje Accounting-Request [Stop], indicándole el fin de la sesión del usuario, así como los datos de consumo del usuario.

7. Finalmente el servidor confirma la recepción de esos datos mediante un mensaje Accounting-Response [Stop], enviándolo al NAS, terminando así el proceso de autenticación. En la Figura 2.10 se muestra la secuencia RADIUS.

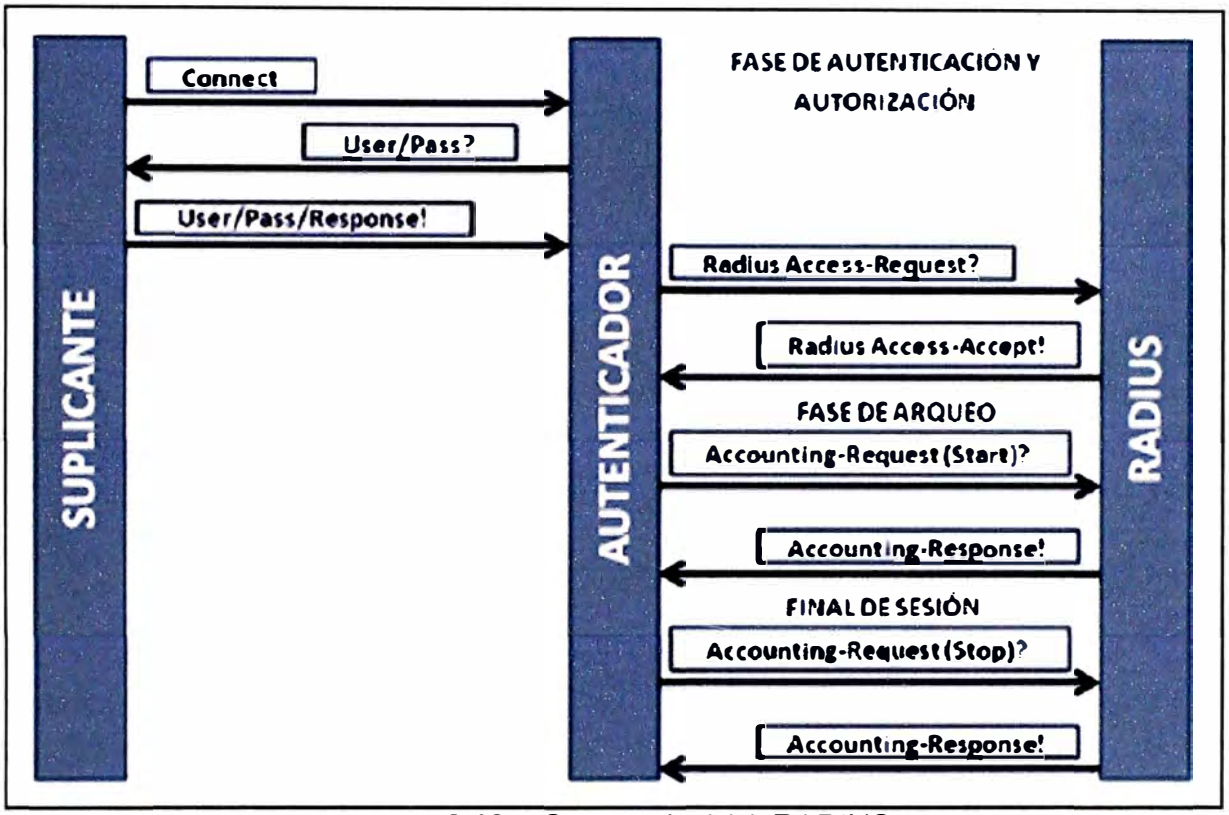

Figura 2.10 Secuencia AAA RADIUS

2.4 El estándar 802.1x

802.1x no es un nuevo protocolo de comunicación sino una extensión del sistema de autenticación RADIUS a las capas más bajas de una red, a ello nos referimos a la capa 2 o capa de enlace, ya que establecer la seguridad de control de acceso en la capa 1 sería como poner un cerrojo en el enchufe de la red de la pared.

El campo de actuación de 802.1x es la capa de enlace en redes cableadas o inalámbricas, para segurizar la conexión de dispositivos a la infraestructura de red de la organización.

Antes de la creación de este estándar, cuando un intruso ganaba acceso a la red cableada o inalámbrica, todas las infraestructuras de red quedaban en situación de riesgo, por lo que el hacker o intruso tenía grandes posibilidades de interceptar todo tipo de información relacionada con la organización. Muchos administradores de red, en la

práctica basan su seguridad en el perímetro de la red, pero una vez dentro la preocupación de blindar cada uno de los equipos interiores no le preocupa tanto.

La seguridad de la redes se basan en los siguientes conceptos.

Control de acceso. La seguridad en el acceso a la red es un punto de gran importancia, debiéndose denegar totalmente el acceso a la red, a cualquiera que no este autorizado a acceder.

Privacidad. La privacidad es otro punto vital para evitar la intercepción de los datos transmitidos por un usuario o equipo, que esté utilizando como medio de transporte una red de datos.

Autenticación y autorización. Esto es el motor que va a permitir llevar a cabo, de forma integra, los puntos anteriores. La autenticación debe asegurar los medios para su propia integridad, impidiendo la intercepción de las credenciales o los intentos de penetración no autorizados. La autorización se ocupará de limitar el uso del canal y de los recursos por parte del equipo del usuario.

La seguridad de una red Ethernet, siempre ha comenzado en las capas superiores, desde la capa 7 y descendiendo. Cuando entramos en el correo electrónico o una página HTTP nos autenticamos en la capa de aplicación, dejando abierto el tráfico de otros protocolos de la capa tres y de los protocolos de autenticación, que actúan sobre la capa dos.

A 802.1x se la llama comúnmente EAPoL (Extensible Authenticacion Protocolo ver Lan) o EAP sobre Ethernet. Si se aplica a tecnologías inalámbricas se le suele llamar EAPoW (EAP over Wireless). EAP es el protocolo de transporte de la autenticación sobre tramas Ethernet, lo que le permite trabajar en la capa dos del modelo OSI. También lo definen un sistema de autenticación basados en puertos puestos que el control de admisión se realiza a través de puertos virtuales LAN.

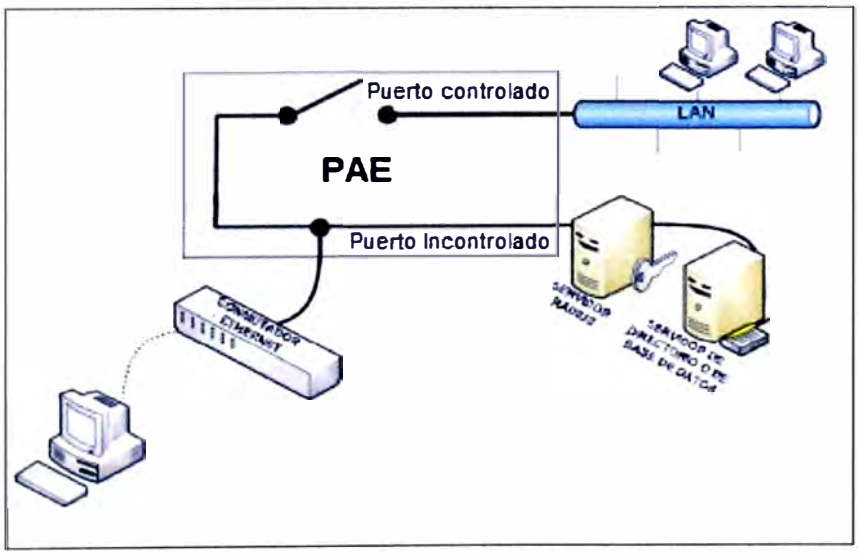

Figura 2.11 Estado del puerto 802.1X

Un equipo NAS que trabaje sobre 802.1x emplea un sistema virtual de dividir cada puerto físico LAN (PAE Port Access Entity) en dos puertos virtuales, un puerto controlado y un puerto incontrolado.

Desde el momento de conexión de un dispositivo al puerto físico LAN hasta el momento en el que se produzca una autenticación exitosa, sólo el puerto virtual incontrolado está abierto. Y este puerto puerto incontrolado solamente permite el paso de paquetes del tipo EAPoL, a fin de permitir el proceso de autenticación del suplicante. Ver Figura 2.11.

Una vez que el suplicante se haya autenticado exitosamente, el puerto pasa a un estado autorizado o "controlado" y se abre para este dispositivo. Cuando está abierto, el equipo autorizado puede simplemente a hacer uso de la red, de forma normal.

A través del proceso de autorización, que gestiona el servidor RADIUS, se le pueden asignar al suplicante características como una dirección IP estática/dinámica de un ámbito definido, o simplemente dejar a ese equipo en una red virtual (VLAN), segmentando la red en diferentes partes para diferentes usos.

El estándar 802.1x se recoge en el RFC 3580 (IEEE 802.1X RADIUS Usage Guidelines) y el estándar IEEE 802.11i ratificado en 2004 está incluido en el RFC 4017. Ver Figura 2.12

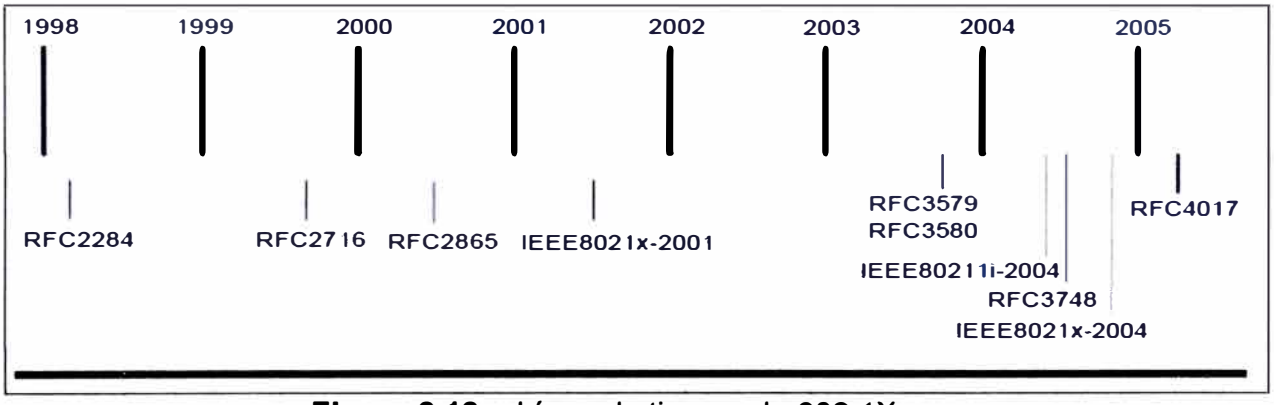

Figura 2.12 Línea de tiempo de 802.1X

2.4.1 El protocolo EAP

EAP es Extensible Authentication Protocol o EAP es la extensión de autenticación que ha permitido que RADIUS resurja de las cenizas y es porque cuando ya los demás métodos de autenticación estaban en seria duda de seguridad, se precisaba de un nuevo método que pudiera extender la autenticación hacia un futuro a medio plazo.

Un error que cometemos habitualmente es considerar a EAP como un protocolo de autenticación, ya que en realidad no lo es. EAP es un protocolo encargado del transporte, encapsulado y seguridad de la autenticación, y en su interior se encuentran los métodos de autenticación que se desea utilizar.

Por ello cuando hablamos de EAP siempre se incluye un sufijo como MD5, MSCHAP,

etc. Existen más de cuarenta métodos de autenticación sobre EAP, lo que lo hace muy versátil para cualquier tipo de implementación a cualquier escala.

La verdadera potencial de EAP es que puede trabajar de forma independiente como protocolo de transporte sobre la capa dos de OSI, prescindiendo de la dependencia hacia otros protocolos como IP o PPP. Al ser EAP un protocolo de transporte como PPP dispone de sus propios sistemas de control de entrega, retransmisión y de integridad de paquete.

La única función del NAS en la conversación es encapsular los paquetes de tipo EAP en paquetes RADIUS. El protocolo RADIUS se encarga de forma transparente del transporte de esos paquetes entre el autenticador y el servidor de autenticación.

En condiciones normales, el servidor de métodos de autenticación de EAP reside en el mismo sistema que el autenticador y suele ser el propio RADIUS. La labor que realiza RADIUS es encapsular los paquetes EAP en sus mensajes estándar de Acces-Request, Acess-Challenge, Acess-Accept y Acess-Reject.

Este encapsulamiento se produce de forma muy sencilla, introduciendo los paquetes EAP en forma de atributos EAP-Message y Message-Authenticator. Esta forma de encapsulamiento funciona de forma muy adecuada, excepto en algunas configuraciones de Proxy RADIUS en las que puede tener algunos inconvenientes. Existen innumerables métodos de autenticación que funcionan sobre EAP, entre los más comunes son:

a. Métodos basados en claves compartidas.- Los métodos basados en claves compartidas han existido siempre y pienso que seguirán existiendo otros muchos años. El problema de ellos consiste en la forma de distribución, transporte o almacenamiento de las credenciales. Dando por hecho que cada usuario debe tener bien guardada su clave en sitio seguro. Algunos métodos basados son PAP, CHAP, EAP-MD5, EAP-MSCHAPv2, EAP-FAST, EAP-SIM, EAP-AKA.

b. Métodos basados en certificados y otros sistemas de claves no compartidas. Estos son los métodos más adecuados para una buena implantación de seguridad, pero también son los más complicados de implantar.

Los sistemas basados en la generación de una clave inmediata, como los token, son más fiables que los anteriores, pero los certificados PKI o las tarjetas criptográficas ofrecen soluciones más complejas de implementar, pero muchos más cómodos y adecuados, una vez funcionales. Algunos de estos métodos son EAP-TLS, EAP-TTLS, EAP-PEAP.

c. Métodos basados en características físicas. En la actualidad están apareciendo nuevas implementaciones de seguridad basadas en EAP que utilizan biometría como medio de identidad. También se pueden clasificar los métodos de autenticación sobre

EAP en otros dos tipos, basándose en su sistema de seguridad:

d. Métodos no tunelados. Los primeros tipos de autenticación sobre EAP como EAP-MD5, EAP-MSCHAPv2, EAP-SIM, etc., no son tunelados.

El tráfico EAP completo no es cifrado por el suplicante, autenticado y servidor de autenticación. Sólo la información de contraseña de usuario y algunos otro paquetes delicados se cifran en el interior de los paquetes que circulan por la red.

Si se interceptan los paquetes que se generan en el proceso de autenticación, se pueden captura los hashes para poder obtener las credenciales de los usuarios. Existen otros tipos de EAP no tunelados, como EAP-OTC y EAP-GTC que utilizan sistemas como Tokens generadores de claves instantáneos de un solo uso. Figura 2.13

Figura 2.13 Token

e. Métodos tunelados. El sistema de tunelamiento de EAP es principalmente EAP-TLS y sus sucesores que utilizan un sistema criptográfico simétrico/asimétrico para la encriptación completa del tráfico durante el proceso de autenticación, autorización y arqueo.

Este cifrado asimétrico se sustenta de certificados X.509 que son intercambiados entre el servidor y el suplicante, y utiliza un tunelamiento similar a SSL.

De esta manera, se incrementa la seguridad del canal de forma bastante robusta contra la interceptación de tráfico o los ataques de MITM (hombre en el medio). Algunos de esos métodos son EAP-PEAP y EAP-TTLS.

Resulta una decisión difícil elegir el tipo de EAP tunelado que podemos implementar en una instalación. La Tabla 2.3 compara los tipos más comunes de EAP para una implementación.

La decisión sobre los tipos de EAP que se debe introducir la van a determinar varios factores como, por ejemplo:

- El Medio de conexión, la complejidad de la implantación, la plataforma de producción que vamos a utilizar, el Intercambio dinámico de claves de sesión.

Tabla 2.3 Comparación de tipos comunes de EAP

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	EAP-PEAP
Certificado de servidor	No	Si[3]	si	Si	Si
Certificado de cliente	No [1]	No [1]	Obligatorio (Posible smartcard)	Opcional[2]	Opcional[2]
Validación de certificados	No	No	OCSP TLS	OCSP TLS	OCSP TLS
Credenciales soportadas	MD5 hash	Hash similar a MS-CHAP	Certificados de cliente	CHAP, PAP, MS-CHAPv1 y v2	EAP-MSCHAPv2 EAP-GTC y otros tipos de EAP
Cambio de contraseña	No	No	No	Si	Si
Autenticación mutua	No [4]	Si[3]	Si	Si	Si
Tunelado	No	No	Si, TSL	Si, TSL	Si, TSL
Claves dinámicas	No	Si	Si	Si	Si
Reconexión rápida	No	No	Si (a partir de RFC5216)	Si	Si
Base de datos de autenticación	SQL, en formato MD5	AD, NTLM	AD, NTLM, Token, LDAP, Novell NDS,OTP	AD, NTLM, Token, LDAP	AD, NTLM, Novell NDS, Token
Suplicante que lo soportan	Microsoft WPA Suplicant MacOs	Propietarios MacOs Linux	Microsoft MacOs Linux	Junip. Oddisey SecureW2 WPA Supplicant MacOs	Microsoft MacOs Linux Cisco
Muestra nombres de usuarios	Si	Si	Si	Anónimo en la fase 1	Anónimo en la fase 1
Vulnerable MiTM	Si	Si	No	No	No
Vulnerable actualmente	Si Diccionario	Si	No	No	No
Usos recomendados	Solo Redes cableadas 802.1X	No recomendado	802.1X Alámbrica e inalámbrica Smartcards	802.1X Alámbrica e inalámbrica	802.1X Alámbrica e inalámbrica

[1] Nombre de usuarios y contraseña mediante challenge

[2] (credenciales de usuario)

[3] Challenge

[4] sólo cliente

2.4.2 Estructura de las comunicaciones EAP

En esta sección se describe la estructura de un paquete de datos EAP (muy similar a la estructura de un paquete de RADIUS) y la forma en la que se establece una comunicación completa sobre este protocolo. Ver arquitectura 802.1x en la Figura 2.14.

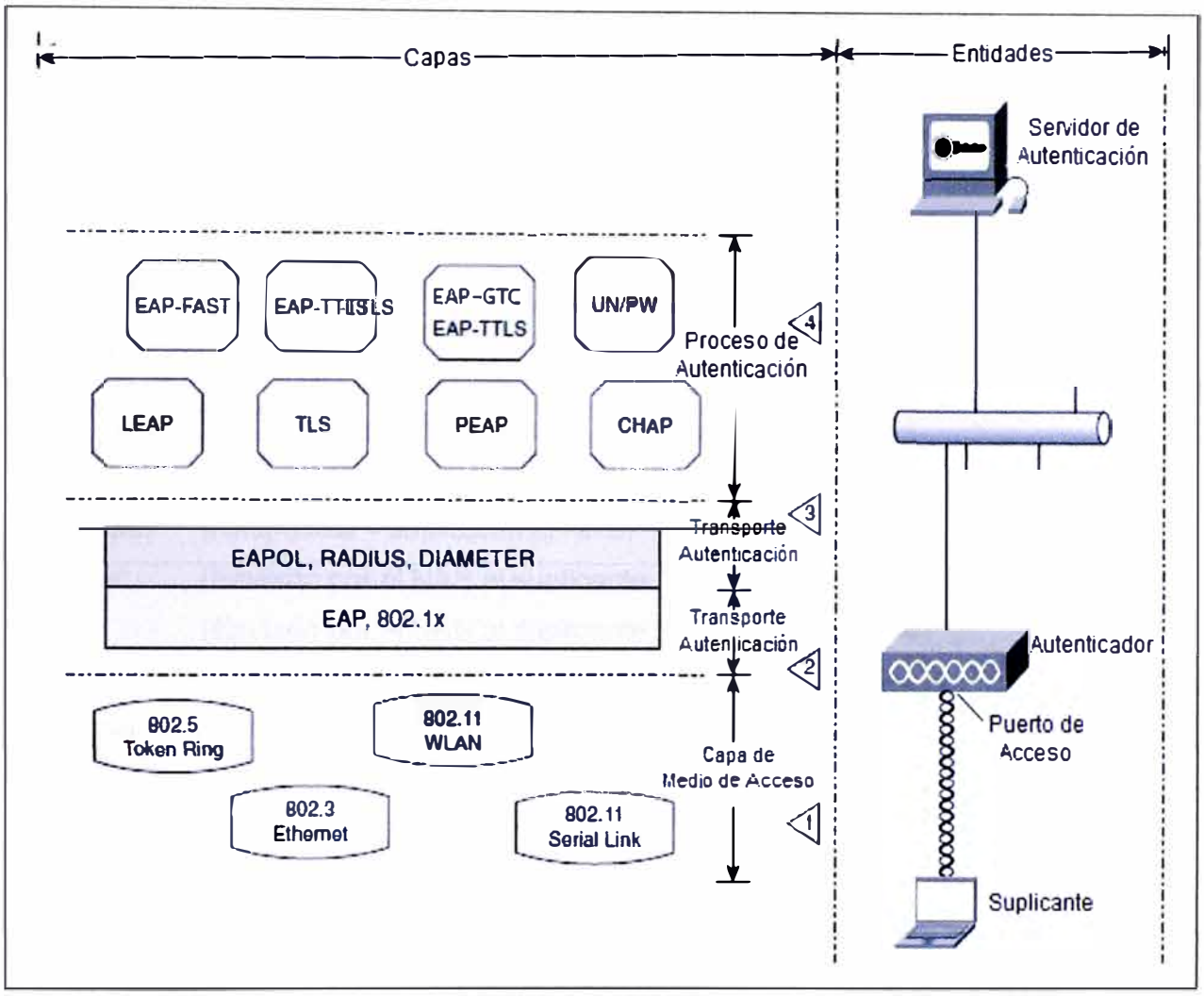

Figura 2.14 Arquitectura 802.1X

a. Formato de mensaje EAP. Paquete de datos

Le estructura genérica corresponde a un paquete EAPOL sobre 802.3/Ethernet.

Tipo Ethernet de PAE (Port Access Entity Ethernet Type)de (2bytes). Es un campo utilizado para describir el tipo de protocolo ethernet que utiliza el puerto del NAS implicado.

Versión de EAP (Protocolo Version) (1byte). Un número positivo en formato binario que representa el método de autenticación EAP que se está utilizando.

Tipo de paquetes EAP (1 byte). Un número positivo en formato binario que representa el tipo de mensaje EAP incluido. Sus valores pueden ser:

–EAP-Packet: Paquete de intercambio de datos del protocolo EAP

– EAPOL-Start: Inicio de las comunicaciones EAP, estímulo, desde el suplicante al NAS

– EAPOL-Logff: Desconexión, el suplicante desde desconectar y envía al NAS este mensaje.

– EAPO-Key: Para intercambio de claves de cifrado en sesiones posteriores de protocolos que requieren cifrado como WPA o tunelamiento VPN.

– EAPOL-Encapsulated-ASF-Alert. Para el intercambio de alertas en protocolo como SNMP

Tamaño del cuerpo (2 bytes). Valor entero sin signo que representa el tamaño en bytes del cuerpo del paquete, donde se incluyen los valores.

Cuerpo del mensaje. En el cuerpo del mensaje se incluyen los valores y atributos de tipo EAP. Este cambio sólo estará presente en los mensajes de EAP tipo: EAP-Packet, EAP-Key y EAP-Encapsulated-ASF-Alert. El formato de los atributos de EAP es muy similar a los de RADIUS.

- Código (1byte).El código o tipo de atributo EAP.

Request. (Request Identity – NAS al suplicante)

Response: (Respuesta – suplicante al NAS)

Success: (Enviado por el NAS al suplicante – Acceso permitido)

Failure: (Enviado por el NAS al suplicante – Acceso denegado)

- Identificador (1byte). Al igual que en un paquete RADIUS, el indetificador se utiliza para relacionar los paquetes y las sesiones entre si.

- Tamaño (2 byte). Señala el tamaño total del paquete EAP, incluyendo todos los campos de cabecera y cuerpo de mensaje.

- Tipo de EAP (1 byte). Indica el tipo de autenticación EAP que se utiliza en la conversación. Muestra unos ejemplos entre otros.

1. Identity (Intercambio de Indentidad)
2. Notification
3. NAK
4. MD5-Challenge
5. One Time Password
6. Generic Token Card

13. TTS

21. TTLS

25. PEAP

29. MSCHAPv2

Datos del paquete (Tamaño – 5 bytes). El valor de datos que se está transmitiendo, que depende del tipo de EAP que se utilice. La figura 2.15 muestra el paquete EAP

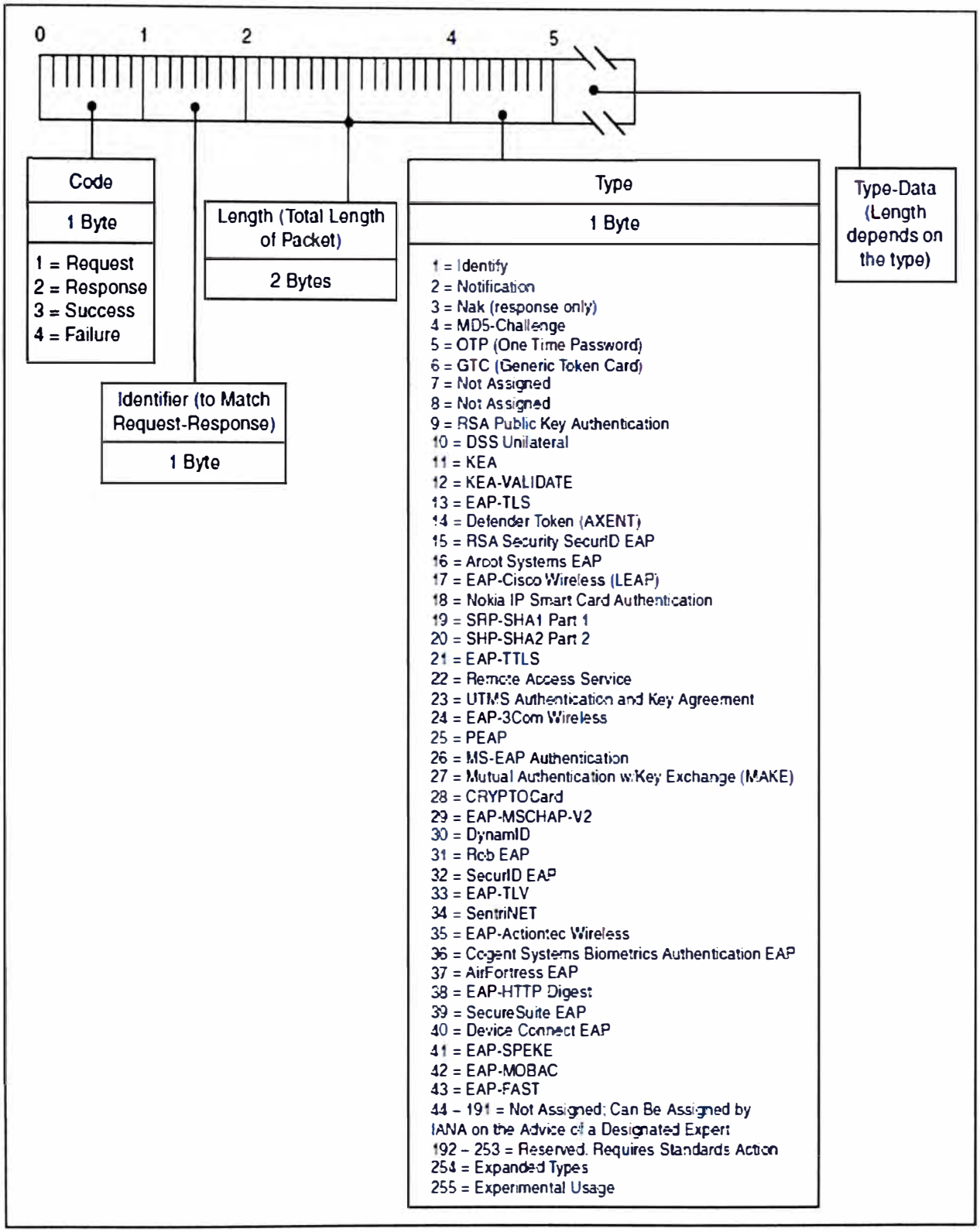

Figura 2.15 Paquete EAP

b. Secuencias de autenticación EAP

Es importante conocer la forma en la que se desarrolla una secuencia completa AAA basada en el protocolo de transporte EAP.

No hay una fórmula universal para realizar esta secuencia, ya que dependerá de ciertos factores variables, como por ejemplo el tipo de EAP utilizado o de la capacidad de

iniciar la conversación o no por parte del equipo NAS. En el caso de un conmutador que haga de autenticador, será éste quien detecte que un equipo se conecta a uno de sus puertos, o que un equipo acaba de activarse o encenderse; pero en el caso de un AP inalámbrico que no tiene puertos físicos, el suplicante debe iniciar la conversación tras asociarse con el punto de acceso mediante un mensaje EAPOL-Start, ya que el AP no es capaz de detectar al nuevo cliente de otra manera.

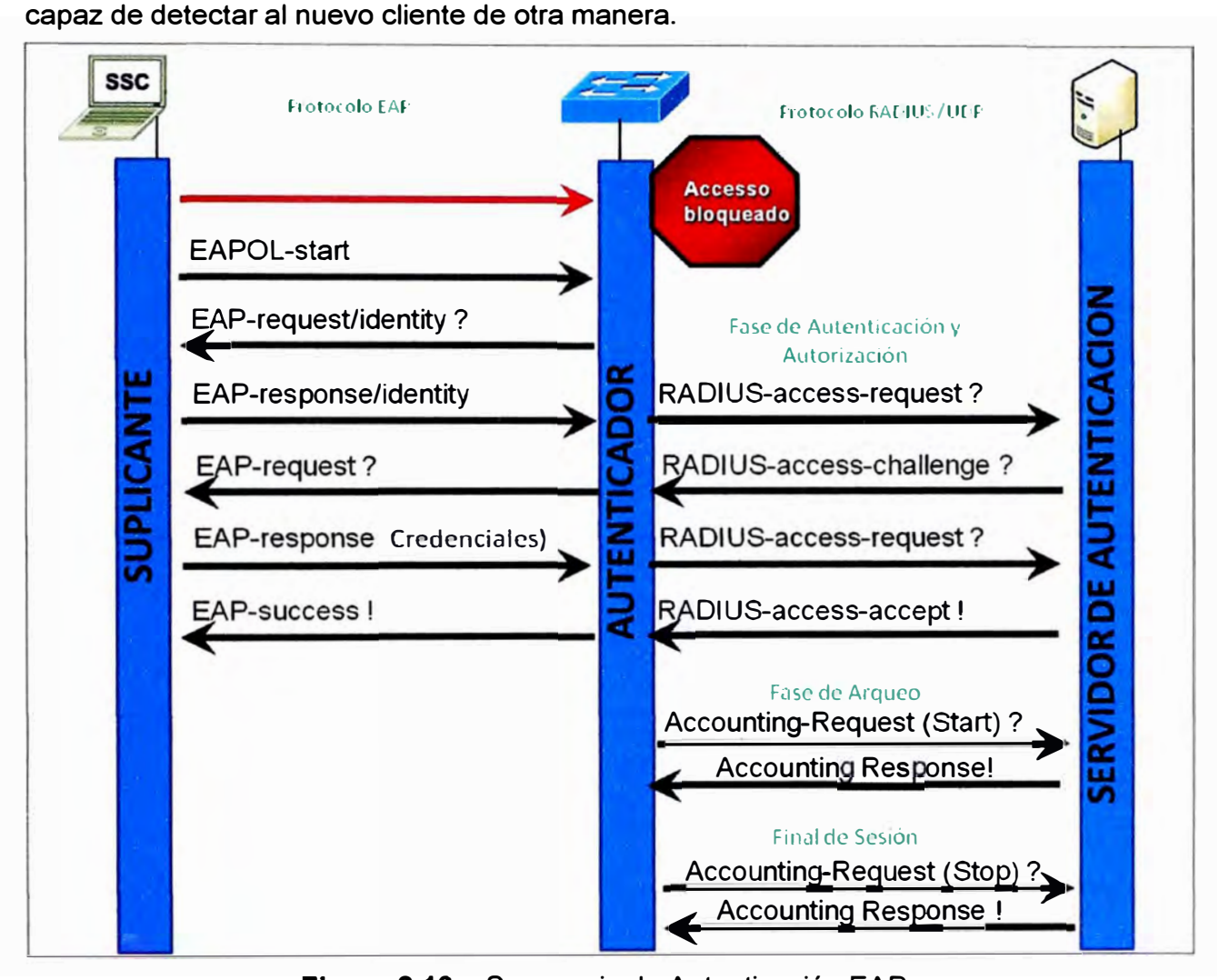

Figura 2.16 Secuencia de Autenticación EAP

En la Figura 2.16 se puede ver una secuencia de autenticación estándar sobre el tipo de autenticación hecho en EAP-PEAP.:

1. Cuando el suplicante o el NAS se han detectado, la secuencia suele comenzar por un paquete EAPOL-Start, para indicar que se desea iniciar una conversación EAP.
2. Cuando el NAS (autenticador) detecta un paquete EAPOL-Start, cuando detecta la actividad del suplicante conectándose a uno de sus puertos, o asociándose a 802.11, envía EAP tipo "EAP-Request/Identity" al suplicante.
3. El suplicante responde mediante un paquete de tipo "EAP-Response/Identity" con su identidad (en PEAP debe ser anónima en esta fase). El NAS envía este paquete EAP encapsulado en forma de atributo EAP-Message dentro de un paquete UDP estándar de

RADIUS.

4. El servidor RADIUS solicita un desafío o challenge al NAS, dependiendo del método de autenticación EAP demandando y disponible. El NAS realiza su misión de desencapsular y encapsular los mensajes tipo RADIUS a EAP y se lo envía al suplicante. Se producen intercambios de paquete Challenge, dependiendo del método EAP y del tipo de autenticación mutua.

5. El suplicante responde a los mensajes Challenge a través del NAS, que siempre encapsula todos los mensajes EAP en formato RADIUS y se los envía al Servidor RADIUS.

6. Tras los procesos necesarios para la creación del túnel e intercambios de identidades y si además cada uno de los procesos de autenticación, dentro y fuera del túnel, se ha superado correctamente, el servidor RADIUS responderá con un mensaje Access-Accept enviado al NAS con todos los parámetros necesarios de autorización para permitir el acceso del puerto del cliente. El NAS responderá al suplicante con mensaje EAP-Success.

7. Se produce (en caso de VPN o red inalámbrica Wi-Fi) el intercambio de las claves de sesión necesarias para que se establezca un correcto cifrado durante la consiguiente sesión segura del usuario a la red.

Estos procesos descritos anteriormente pueden variar ligeramente o drásticamente, dependiendo del tipo de EAP que se decida implantar; pero la teoría es la misma para cualquiera de los intercambios de paquetes entre diferentes componentes.

CAPÍTULO III
INGENIERÍA DEL PROYECTO

En el presente capítulo se describe la ingeniería del proyecto a modo de un resumen ejecutivo que permita la comprensión del mismo, pero apoyado en el marco teórico ya expuesto.

Este capítulo se divide en tres partes: 1) Análisis de la solución, 2) Esquema de la solución, 3) Aspectos técnicos de la solución, 4) Funcionamiento..

3.1 Análisis de la solución

El análisis de la solución es desarrollado en esta sección tomando en consideración los siguientes ítems: 1) El problema a resolver, 2) El Planteamiento de una solución al problema.

El escenario inicial propuesto se trata de una empresa que cuenta con una oficina principal ubicada en la ciudad de Lima, en donde se encuentra ubicado su infraestructura principal (servidores de correo, base de datos, Web, entre otros), así como las oficinas de los principales ejecutivos de la empresa (gerente general y gerentes de áreas), jefes de áreas, ejecutivos de ventas, ingenieros, técnicos, personal de administración y logística, entre otros.

La oficina principal tiene una salida a Internet por medio de un router gateway, el cual le brinda una velocidad a Internet de hasta 10 Mbps, mediante acceso dedicado con un un pool de direcciones IP pública fija (estática). En el anexo A se puede observar un diagrama físico (como se encuentra distribuido el equipamiento de red) y lógico (como se ha realizado el direccionamiento IP) para el estado inicial de esta red.

3.1.1 Problema a resolver

El problema puede ser visto en tres partes:

a. Falta de políticas de seguridad para el control de acceso a la red local

La falta de políticas de seguridad para el control de acceso a la red local debe ser considerada como uno de los factores principales para la protección de la información confidencial. Sin el control de acceso a la red, se permitiría la intrusión física donde se encuentren puertos de red disponibles para la conectividad a la LAN.Toda una serie de amenazas y vulnerabilidades plantean riesgos para la empresa, por ejemplo:

1. **Dispositivos no identificados**. Según un estudio de Enterprise Strategy Group

(ESG), más de las tres cuartas partes de las organizaciones empresariales ofrecen actualmente credenciales de acceso a la red a personas que no son empleados. Confiar en los dispositivos de terceros es un verdadero problema para los administradores de seguridad de la red, ya que un solo dispositivo infectado podría causar graves daños en la red.

2. Puntos finales vulnerables. Para elevar al máximo la protección de la red, las vulnerabilidades de software deben solucionarse de forma puntual y coherente. Este proceso ya es lo suficientemente difícil con los PC de escritorio, ni qué decir tiene como lo será con el cada vez mayor número de móviles y puntos finales de terceros que entran en la red.

3. Ataques de códigos malévolos. Aunque las amenazas de gusanos y virus se han reducido en los últimos años, los investigadores están preocupados por la próxima generación de "supergusanos" que utilizan varios métodos de propagación muy rápidos y que producen efectos muy destructivos. Unas defensas de la seguridad eficaces y basadas en la red deben formar parte de las soluciones de acceso a la misma.

4. Espionaje y piratas de la red. Los usuarios de confianza con dispositivos limpios pueden plantear problemas si fisgonean por la red, examinan recursos de red y sondean puntos débiles. Los usuarios deben estar limitados a los recursos que necesitan para desempeñar su trabajo, reduciendo así el riesgo de que surja cualquier problema interno.

5. La administración de la red se vuelve compleja, al no contar con medios dinámicos que incrementarían la productividad de los empleados a favor de la empresa.

Con respecto al problema se ve necesario aprovechar las recomendaciones que indica los estándares de seguridad de la información como la ISO 27001 y PCI DSS, que indican contar con políticas de control de acceso como normas claramente establecidas y derechos basados en perfiles de usuario; una adecuada combinación lógica (técnicas) y controles de acceso físico, así como también la segregación de las funciones de control de acceso - por ejemplo, solicitar el acceso, la autorización de acceso, administración de acceso; y requisitos para la autorización formal de las solicitudes de acceso y la oportuna eliminación de los derechos de acceso.

b. El estado actual de la red no es el óptimo

Debido a un simple pero inadecuado direccionamiento IP de la red, si como una mala distribución del equipamiento de red, ha ocasionado que se presenten síntomas de lentitud y una respuesta tardía ante los requerimientos de sus usuarios, incluso para simples usos como descargar correos o navegar por la Internet.

Para la cantidad de usuarios que está soportando la red se ve necesario implementar mecanismos de segmentación lógica de la red aplicando metodologías de subnetting

(dividir la red en subredes) para asi poder manejar el tráfico de broadcasts (mensajes enviados por un equipo dirigidos a todos los equipos dentro de su misma subred). Así mismo, seria recomendable aplicar metodologías de VLAN (Redes LAN Virtuales) para poder segmentar la red de la manera más óptima y segura a la vez.

c. Ineficiencia para el desplazamiento de usuarios

Una organización que cuenta con una red LAN en su oficina principal que cuenta con toda su red LAN cableada, siendo esto una gran traba para sus usuarios móviles que cuentan con computadoras portátiles (notebooks) y se encuentran en constante movimiento dentro de dicho local; ya que requieren ubicar un punto de red cercano a donde se encuentren para poder descargar sus correos o buscar alguna información en la Internet, lo que trae consigo incomodidad y una disminución en el desempeño de dicha persona al perder tiempo realizando este proceso; tiempo que se traduce en una disminución de su productividad.

Se ve así la necesidad de asignar dinámicamente políticas de acceso de los dispositivos o usuarios al autenticarse; el estándar 802.1X junto con el servidor Cisco Secure ACS es que permiten el control de acceso de los usuarios y los recursos informáticos a la red local de la empresa basándose de los puertos de accesos provistos por los switches/Acces Point.

3.1.2 Planteamiento de una solución al problema

Es necesario establecer un procedimiento para plantear una adecuada solución al problema. Este procedimiento estará comprendido por cuatro etapas: 1) En la primera etapa se procederá con el levantamiento de información relevante al problema, 2) en la segunda etapa se listarán los requerimientos necesarios para la solución, 3) en la tercera etapa se definirán los alcances y limitaciones propios de la solución planteada, 4) se definirá la arquitectura de la solución.

Luego de realizado todo este análisis se pasará a ver el diseño propio de la solución y finalmente su implementación y sometimiento a pruebas.

a. Levantamiento de información

Para iniciar el planteamiento de una solución se requiere obtener la mayor cantidad de información relevante al problema en cuestión. Así, si bien ya se ha mencionado algunas características de los tres problemas en mención, se procede a describir todo el estado actual de la red que tenga relación al problema en discusión.

En primer lugar se tiene el direccionamiento IP plano implementado en la red actualmente. Este tipo de direccionamiento IP se caracteriza por ser bastante sencillo y útil en redes pequeñas (no mayores a 16 o 20 usuarios y no cuenten con servicios de red avanzados tales como servidores Web, base de datos, etc.) por su simple, rápida y fácil

implementación. Sin embargo, en un entorno cómo el de una empresa con más de 100 personas que acceden a los servicios de la red y la respuesta de estos servicios repercute en su desempeño dentro de la oficina, con más de un equipo por el cual pueden acceder a la red, puede concluirse que es inapropiado mantener un esquema de direccionamiento IP plano.

Se requiere implementar mecanismos de subnetting para poder dividir a toda la gran red en redes pequeñas pero manejables y que solo se puedan comunicar los usuarios entre estas redes en los momentos necesarios y no todo el tiempo (evitando así el malgasto de los recursos de la red).

Con respecto al equipamiento de red con el que cuenta actualmente la empresa se sabe que cuenta con cinco switches de acceso Fast Ethernet, de los cuales tres son de 24 puertos y dos son de 48 puertos. Todos estos switches son conmutadores Fast Ethernet 10/100 y soportan el estándar 802.1x. Así mismo, se cuenta con un servidor Cisco ACS que es utilizado para la configuración TACACS de los equipos de red, y finalmente se cuenta un Firewall de la Marca Alcatel que es utilizado para la protección perimetral de la empresa.

En la Tabla 3.1 se resume toda la información levantada con respecto a este escenario inicial planteado y a continuación, pasaremos a listar los requerimientos que serían necesarios para poder proponer una solución a estos problemas:

Tabla 3.1 Resumen de levantamiento de la Información

Característica de la red	Descripción
Direccionamiento de IP plano	Todos los equipos se encuentran configurados para operar dentro de la misma red
Switches de capa 2	Switches de marca Cisco Modelos: WS-C2960-24TT y WS-2960G-48TC-L
Servidor Cisco ACS	Plataforma de control de políticas de acceso que tiene una solución única que ofrece la AAA para ambos protocolos TACACS y RADIUS
Firewall Alcatel-Lucent	Aplicaciones de seguridad que integran inspección de la capa de aplicación, función firewall con capacidades de VPN avanzadas para oficinas pequeñas a través de los requisitos de centros de datos

b. Lista de requerimientos para la solución

Luego de tener una visión más detallada del estado actual de la red al levantar la información concerniente, se puede realizar el listado de todos los requerimientos que para la solución propuesta.

1. Switches de Capa 2: Para la solución del primer problema es necesario contar con switches administrables, los equipos que se tiene cumplen este requisito sólo deben contar con una versión de software mínima para el soporte de 802.1X. Esta versión

mínima es Cisco IOS® Software Release 12.2(52)SE para los modelos Cisco Catalyst 2960 .

2. **Servidor de Token**: Para el servicio de autenticación robusta con OTP (One Time Password) para los accesos de usuarios a la red interna, se necesitará adquirir un software RADIUS Vacman Middleware de la marca VASCO.

3. **Tokens**: Se necesitará comprar 100 Digipass G03, los cuales serán repartidos a los usuarios para que puedan usarlo para autenticarse y así poder acceder a la red.

Suplicante: Como parte de la solución, es necesario contar con un software que se intalará en cada PC de los usuarios, para lo cual se adquirida el producto Cisco SSC (Cisco Secure Service Client) con licencia válido para 100 usuarios.

4. **Redireccionamiento IP**: Se requiere cambiar por completo el direccionamiento IP de toda la red; asignando así a cada área de la empresa una subred distinta. Además, la recomendación adicional que sería la de implementar un esquema de VLANs (Virtual Local Area Network) dentro de toda esta red.

5. **Creación de Firewall virtuales**: En el Firewall Alcatel-Lucent actual que cuenta la empresa, se necesitará crear firewall virtuales para cada área de la empresa, esta deberá hacer match con su respectiva VLAN que se le asigne. La subida de dichas VLAN de conectan a una sola interface del Firewall por medio de un troncal.

c. Definición de los alcances y limitaciones de la solución

Después de haber levantado la información y haber listado los requerimientos para plantear una solución, se ve necesario definir cuales serán los alcances y limitaciones de la solución propuesta.

c.1 Alcances

La red LAN se basará en los más óptimos mecanismos de seguridad explicados dentro del marco teórico del presente trabajo; por lo cual no se permitirá que un intruso pueda ser capaz de acceder a la red sin contar con un token previamente asignado y configurado en los servidores Radius Cisco ACS y Vacman Middleware.

La solución contemplará la gestión de los accesos de los usuarios a la red LAN llevando así la contabilidad de dichos accesos como tambien la contabilidad de accesos a los diferentes recursos de la empresa, ya sea la intranet o Internet.

Debido a que el acceso seguro a la red LAN requerirá de una configuración previa en los equipos (notebooks) de dicha red, se realizará la elaboración de una guía de conexión detallada para que el usuario pueda instalar el software de suplicante, Cisco SSC que se encontrará previamente configurada y lista a ser ejecutado por el usuario. Solamente para los casos extremos en los que los usuarios no sean capaces de llevar a cabo dicha guía es que el mismo administrador de la red tendrá que realizar dicha

configuración. Es por esto que la guía ha implementar contemplará ser lo más sencilla y fácil de llevar a cabo posible; como para que un simple usuario de oficina pueda ser capaz de seguir las instrucciones allí descritas y así prescindir del administrador de red para que pueda enfocar su trabajo en otras tareas más importantes dentro de la red de la empresa.

c.2 Limitaciones

La solución planteada no contemplará ningún mecanismo de redundancia en caso de fallas. Cada servidor será implementado en la manera standalone, por lo que no contarán con otro equipo que responda cuando alguno de éstos se encuentre fuera de servicio. La implementación de clusters para estos servidores es una mejora que se tiene considerado para futuros proyectos.

d. Arquitectura a utilizar en la solución

Por último, se establece la arquitectura que se utilizará en la solución planteada, describiendo cada uno de sus elementos así como la operación de todos estos dentro del sistema. La arquitectura de la solución estará basada en cinco elementos principales: 1) el Token Digipass GO3, 2) el suplicante Cisco SSC, 3) el autenticador (switches catalyst), 4) el servidor de autenticación Cisco ACS y 5) el servidor de Tokens Vacman Middleware.

1. Digipass GO3: Es parte de la autenticación de 2 factores: a) Algo que el usuario tiene, y b) Algo que el usuario sabe: un código PIN secreto y único. A todos los usuarios habilitados para acceder a los recursos de la red se le asigna un token, previamente registrado en el servidor de token. El Digipass GO3 cuenta con un display de 6 dígitos que cambia cada 32 segundos. Junto con el PIN conocido sólo por el usuario más los 6 dígitos proporcionado por el digipass se genera un contraseña, la cual tendrá que se corroborada con el servidor de token.

2. Cisco Secure Services Client (SSC): Es un software suplicante que permite la autenticación de dispositivos para acceder a la red cableada/inalámbrica. Tiene soporte en los diferentes métodos de autenticación PEAP, entre ellos EAP-GTC la cual será usado en esta implementación.

3. Switches Cisco Catalyst: Son conmutadores que soportan 802.1x, estos dispositivos reciben los requerimientos de los suplicantes y negocian con el Servidor de Autenticación. A este rol se le conoce como autenticador.

4. Servidor Seguro de Control de Acceso (ACS): Este servidor es normalmente un servidor RADIUS que cumple con las funciones de AAA (Autenticación, Autorización, Arqueo) el cual guarda información particular del usuario que se valida(usuario, VLAN a la que pertenece). Este servidor es quien recibe las solicitudes reenviadas de los puntos de acceso por parte de los usuarios y le solicita al servidor de Token la información

correspondiente para poder validar si es que dicho usuario cuenta con los permisos necesarios para acceder a la red (es decir, que la información de usuario/contraseña (PIN+OTP) que ha enviado sea válida). De encontrar que es correcta, le envía un mensaje al switch de "acceso autorizado" para que éste tome el control del acceso al usuario y continúe con el resto de la comunicación. A este rol se le conoce Servidor de Autenticación.

5. Servidor Vacman Middleware: Este servidor contiene todas semillas de todos tokens que administra, se registrarán a todos los usuarios que cuenten con el permiso de acceder a la red, y es donde se realiza el match usuario – semilla, de modo que puede validar si la contraseña (PIN+OTP) ingresara por el usuario es correcta o no. A este rol de lo conoce como servidor de token.

A continuación se explica la secuencia del procedimiento por el cual un usuario se conecta a la red.

a. Un usuario se conecta a la red, inicia una sesión y envía sus credenciales usuario y contraseña (PIN+OTP).

b. El autenticador o switch recibe las credenciales del usuario y las reenvía al servidor de autenticación Cisco ACS para que le indique el perfil del usuario y brinde acceso a la red LAN. Caso contrario, impide su acceso y le envía un mensaje de falla de autenticación.

c. El servidor de autenticación recibe la solicitud por parte del autenticador, verifica que se encuentre registrado como un dispositivo AAA autorizado para brindar accesos a la red (mediante una llave compartida entre el swtich y el servidor) y de ser estos correctos, inicia una sesión con el servidor de Token para enviarle la validación de las credenciales del usuario.

d. El servidor de Token revisa si es que se encuentra registrado el usuario en su sistema y de ser así, procede a verificar si la contraseña (PIN+OTP) ingresada es correcta. En caso que el usuario no se encuentre registrado, envía un mensaje de Access-Rejected (acceso rechazado). De ser correcto, devuelve un mensaje de Access-Accepted (acceso aceptado) al servidor de autenticación.

e. El servidor de autenticación recibe la autorización por parte del servidor de Token y envía un mensaje al switch con el perfile del usuario para que le brinde acceso a la red al usuario.

f. El switch o autenticador recibe la autorización para el usuario junto con su perfil e inicia una autoconfiguración del puerto con la VLAN que el usuario debe pertenecer.

g. Al momento de recibir la autorización, el autenticador inicia a registrar todas las actividades de tráfico del usuario y las envía al servidor de ACS para registrar el

momento exacto en el que el usuario inicia su acceso a la red y se registrará el tiempo que estuvo conectado, el momento en el que se desconecta, así como otras estadísticas (número de bytes enviados, número de bytes recibidos, entre otros).

h. El usuario al contar con un IP estática y al contar con acceso a la red, puede empezar hacer uso a los diferentes recursos de la red de acuerdo con las políticas que preconfiguradas en el Firewall de la empresa.

Adicionalmente, en el anexo B se podrá encontrar una captura de tramas realizada con el analizador de protocolos Wireshark, en la cual se ha logrado capturar el intercambio de tramas entre el suplicante, el autenticador (switch), el servidor de autenticación y el servidor de Token en el momento en el cual un usuario solicita conectarse a la red LAN.

3.2 Esquema de la solución

Para el esquema de la solución propuesta se ha tenido en cuenta las consideraciones vistas dentro del marco teórico de este trabajo, asegurando así un óptimo grado de seguridad en la comunicación entre el usuario y el punto de acceso; dado que este lugar es el más vulnerable de toda la solución al poder estar siendo vigilado por posibles intrusos al sistema. Así, se brinda un acceso seguro impidiendo que usuarios ajenos acceder a la red y por ello acceder a los recursos privados de ésta.

3.2.1 Segmentación de la Red

La segmentación de la red se realizó por áreas de trabajo asignando una VLAN para cada uno de ellos, considerando que en cada área existen aproximadamente 10 personas laborando, se consideró una subnet con máscara 255.255.255.240, la Tabla 3.2 indica lo realizado. Para el caso de invitados, se añadió un nuevo segmento con su respectiva VLAN. Ver cálculo de la segmentación de la en el Anexo C.

Tabla 3.2 Áreas de trabajo, VLANs y segmentos asignados

Área de trabajo	VLAN	Segmento asignado	IP en el firewall
Administración de servicios	751	192.168.173.16/28	192.168.173.17
Conectividad y seguridad	752	192.168.173.32/28	192.168.173.33
Control de proyecto	753	192.168.173.48/28	192.168.173.49
Planeamiento calidad	754	192.168.173.64/28	192.168.173.65
Gestión de cambio	755	192.168.173.80/28	192.168.173.81
HelDesk	756	192.168.173.96/28	192.168.173.97
Implementación	757	192.168.173.112/28	192.168.173.113
Integración de servicio	758	192.168.173.128/28	192.168.173.129
Planeamiento y calidad	759	192.168.173.144/28	192.168.173.145
Procesos y monitoreo	760	192.168.173.160/28	192.168.173.161
Externos	761	192.168.174.0/27	192.168.174.1

a. En cada switch de la empresa se configura los puertos que se interconectan con los switches de distribución, como troncales permitiendo el pase desde la vlan751 hasta la vlan761.

b. La interface de Firewall que se conecta con los switches de distribución se configura en troncal dejando pasar todas las vlans más la vlan de internet.

c. En el firewall, se configura cada 11 zonas adicionales con su respectivo número de VLAN, y estas zonas tienen un direccionamiento IP que se especifica en la tabla anterior.

d. Debido a la solución planteada, las recomendaciones y al negocio de la empresa, no se cuenta no ningún servidor DHCP, para lo cual a cada usuario se le asignó una IP estática de acuerdo al área de trabajo que pertenece y siguiendo el esquema de la tabla anterior.

La Figura 3.1 explica el trabajo de la segmentación donde cada Switch de acceso se conecta físicamente a los switches DIST-1 y DIST-2. Esto por la redundancia que la empresa cuenta para los equipos de distribución, Core y para los firewall.

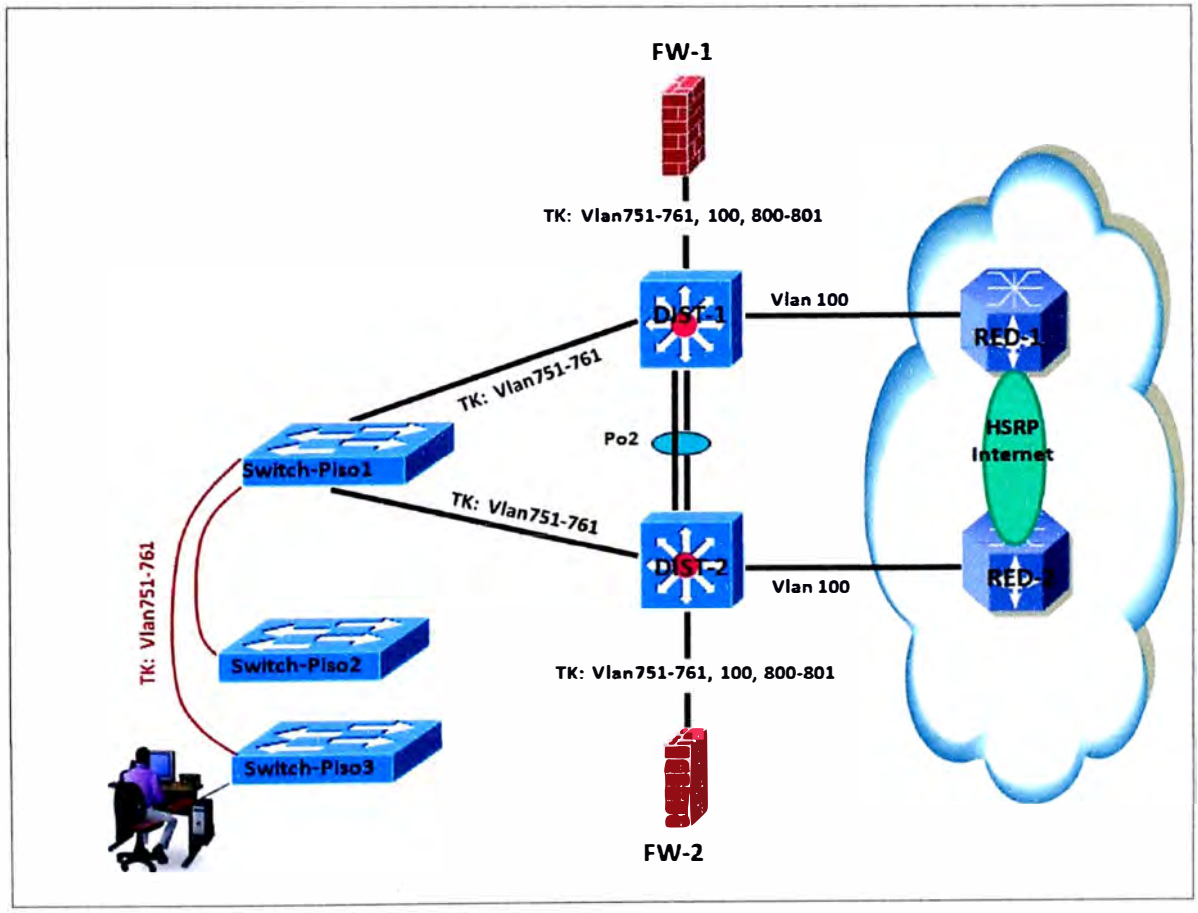

Figura 3.1 Esquema de segmentación

3.2.2 Creación de políticas en el Firewall

Debido a que los usuarios cuentan con direcciones IP estáticas, se configuró reglas de acceso individuales por usuario, de esta manera se puede lograr un mayor control de los accesos a los recursos de la red. La Tabla 3.3 resume las consideraciones para las

configuraciones de políticas de acceso.

Tabla 3.3 Políticas de accesos

	Usuarios externos			Usuarios internos		
	Invitado	Cliente	Consultor	Impresora	Empleado	Ejecutivo
Cuando	L-V 8-5	L-V 8-5	cualquiera	cualquiera	cualquiera	cualquiera
Donde	Sala Conf.	Sala. Conf	Cualquiera		cualquiera	cualquiera
OS	Cualquiera	Cualquiera	Cualquiera	N/A	Win XP	Win XP
Acceso	Internet	Internet, impresora	Internet, impresora y servidores específicos	Solicitudes de impresión	Accesos específicos de impresión	cualquiera

3.2.3 El usuario podrá autenticarse en cualquier punto de red

Los empleados podrán movilizarse dentro de la empresa y conectarse a cualquier punto de acceso, autenticándose correctamente sin necesitar llamar al administrador de red para que configure dicho punto en un VLAN particular. Para el caso de usuarios externos, estos podrán conectarse desde salones específicos con la excepción de los consultores.

3.2.4 Configuración de los switches como autenticadores

Lo siguiente es una guía para configurar la solución planteada en los switches catalyst de Cisco.

Tabla 3.4 Configuración de switches como autenticadotes

AAA Settings	
aaa new-model aaa authentication dot1x default group radius aaa authorization network default group radius aaa accounting dot1x default start-stop group radius	Habilitar AAA Crear el método de autenticación 802.1X basado en puerto. Habilitar el arqueo 802.1X
RADIUS	
radius-server host acs4.2.server.ip* auth-port 1645 acct-port 1646 radius-server key user-defined-shared-key (e.g.,cisco123)**	Especificar la dirección IP del servidor RADIUS. Especificar la Contraseña
802.1X	
dot1x system-auth-control	Habilitar globalmente la autenticación 802.1X basado en puerto.

3.2.5 Configuración del Servidor Cisco ACS

Se procede de la siguiente forma:

1. Registrar el switch en el servidor ACS. Figura 3.2

2. Integración del servidor Cisco ACS con el Servidor de Token, para lo cual se crea el objeto especificando la IP y el password de validación entre ambos. Figura 3.3.

3. Crear la los usuarios con sus respectivo perfil. En la parte de password authentication se especifica al servidor de Token creado en el paso anterior, este proceso se tiene que

realizar para todos los usuarios que ingresarán a la red. Figura 3.4

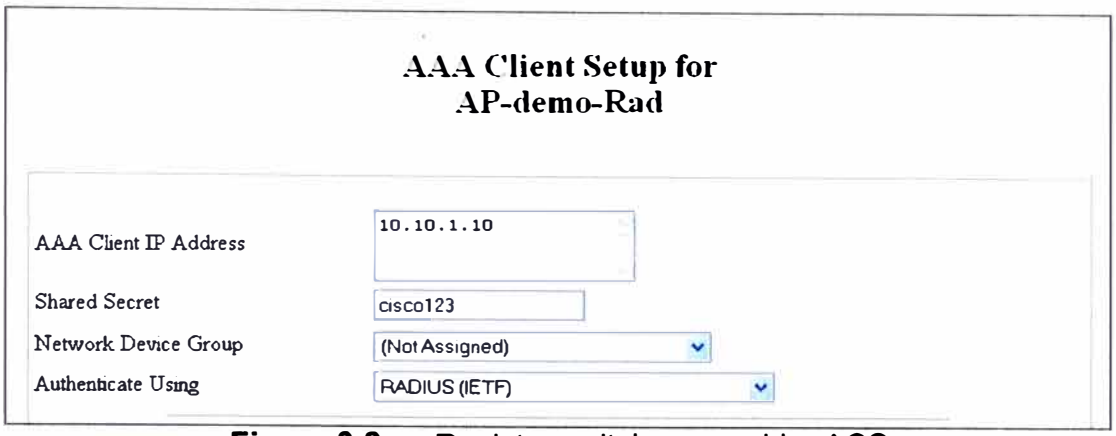

Figura 3.2 Registro switch en servidor ACS

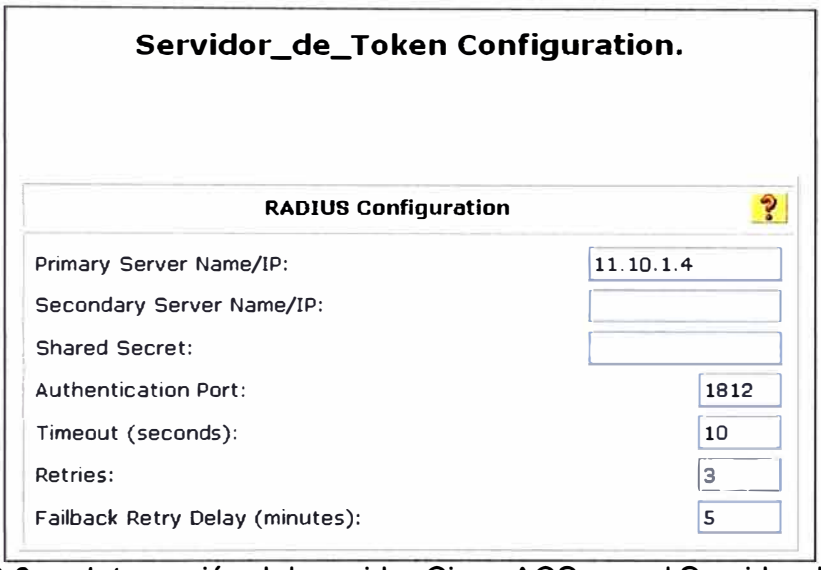

Figura 3.3 Integración del servidor Cisco ACS con el Servidor de Token

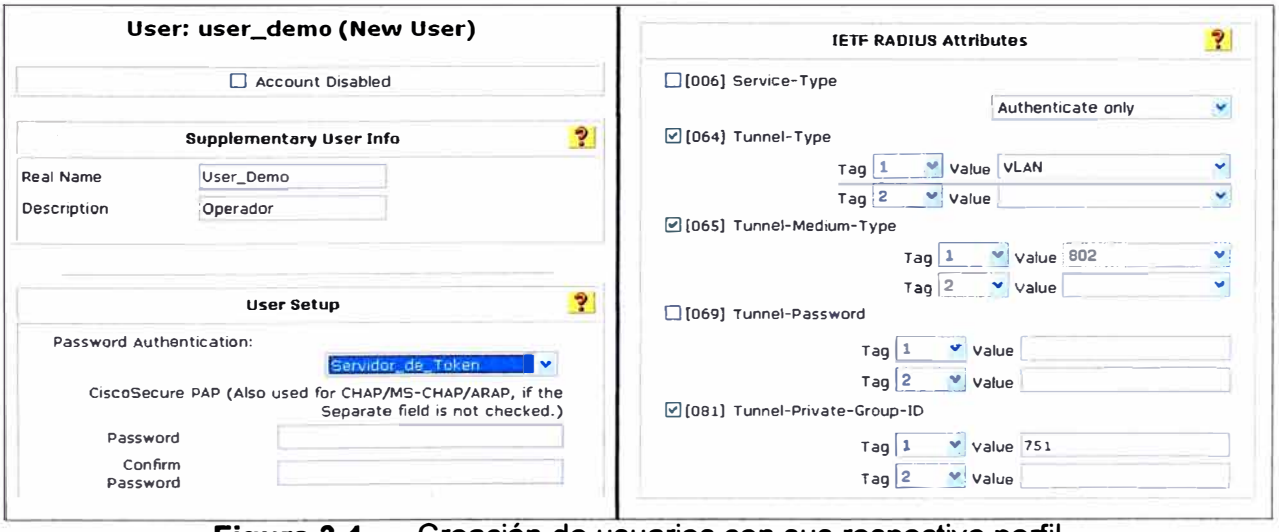

Figura 3.4 Creación de usuarios con sus respectivo perfil

3.2.6 Configuración del Servidor de Token

Se procede de la siguiente manera:

1. Añadir al servidor Cisco ACS como cliente RADIUS. Figura 3.5
2. Crear un usuario que tiene que coincidir con el usuario creado en el servidor Cisco

ACS. Al final, buscar el número de serie del token Digipass GO3 y asignarle al usuario creado. Esto tiene que repetirse para todos los usuarios creados creado en el servidor ACS. Figura 3.6

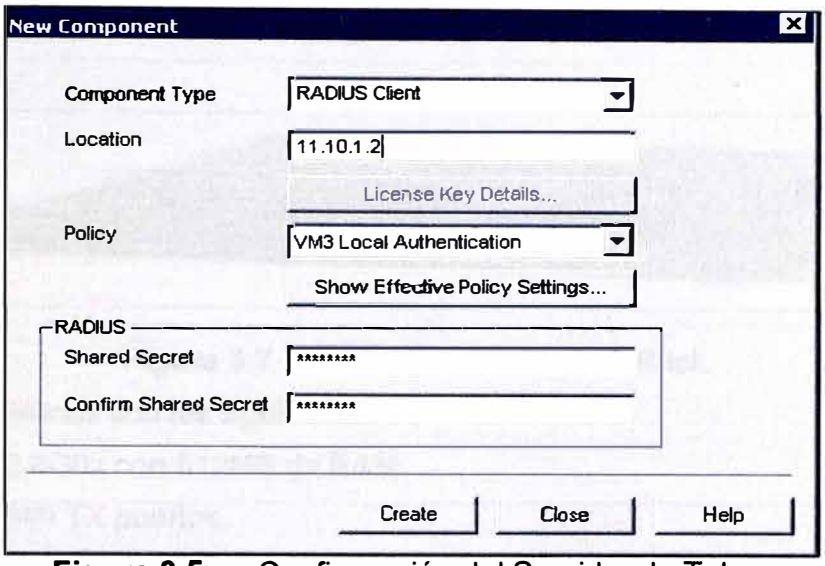

Figura 3.5 Configuración del Servidor de Token

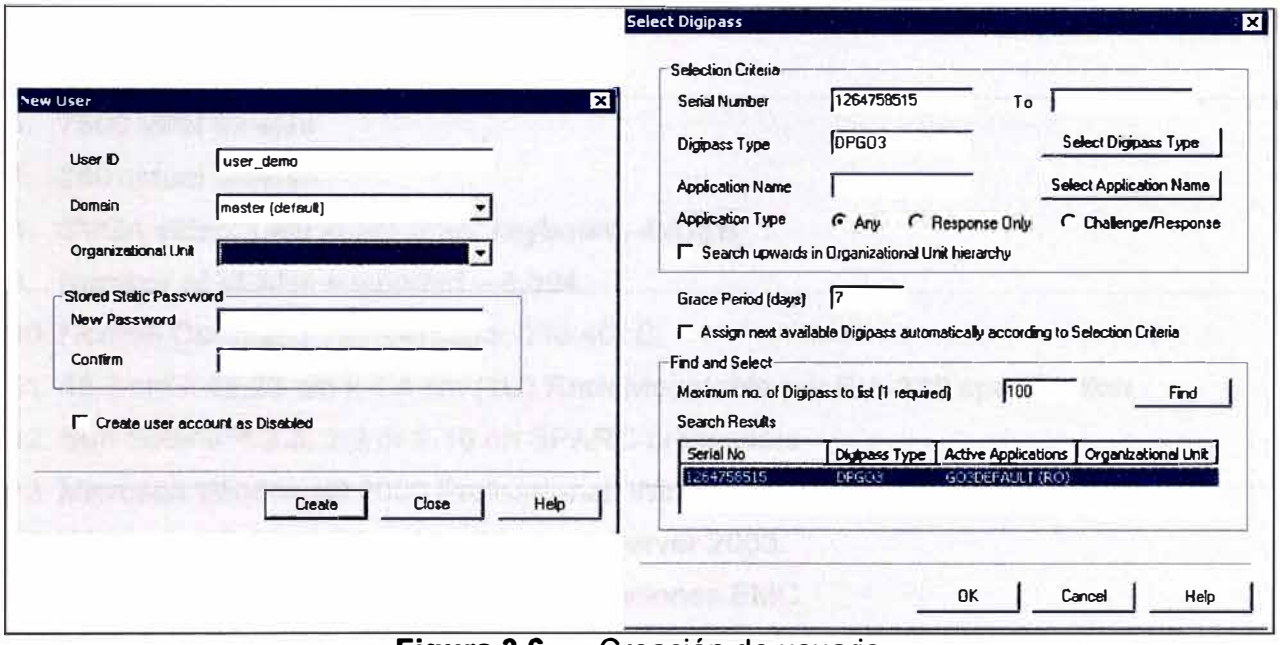

Figura 3.6 Creación de usuario

3.3 Aspectos técnicos de la solución

En esta parte se describen las características técnicas de los elementos involucrados en la solución. Se detallan los siguientes elementos: 1 Equipo VPN Firewall Brick,2) Softwate Cisco Secure ACS, 3) Software Vacman Middleware., 4) Dispositivo Digipass GO 3, 5) Switches Cisco Catalyst, 6) Software Cisco Secure Services Client (SSC).

3.3.1 VPN Firewall Brick

El equipo firewall que soporta aplicaciones de seguridad que integra inspección a la capa de aplicación, provee función de firewall con capacidades de VPN avanzadas para oficinas pequeñas, medianas y grandes a través de los requisitos de centros de datos.

Para la administración de este dispositivo de hardware es necesario contar con un servidor de gestión de seguridad (SMS) Alcatel-Lucent que contiene: el software para firewall, VPN, calidad de servicio y VLAN sólido y perfectamente sincronizado, y gestión de políticas de firewall virtual.

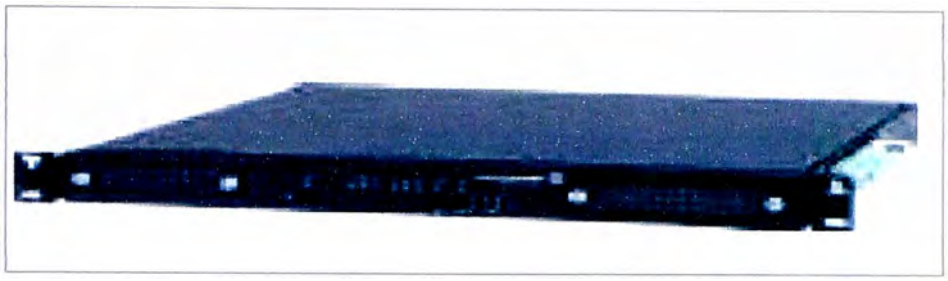

Figura 3.7 Firewall VPN Firewall Brick

Sus características son las siguientes:

1. Procesador 2.8Ghz con 512MB de RAM.
2. (8) 10/100/1000 TX puertos.
3. 1.7 Gbps Firewall.
4. 425Mbps 3DES
5. Un millón de sesiones concurrentes.
6. 7500 VPN túneles.
7. 350 virtual firewall.
8. SVGA video, DB9 serial, PS/2 keyboard, 4xUSB.
9. Number of VLANs supported – 4,094.
10. Normal Operating Temperature: 0 to 40° C.
11. 48.3 cm x 48.23 cm x 4.4 cm (1U) Rack Mountable per EIA-310 specification.
12. Sun Solaris™ 2.8, 2.9 or 2.10 on SPARC processors
13. Microsoft Windows® 2000 Professional, Windows® 2000 Server,
14. Windows XP Professional or Windows Server 2003.
15. USA – FCC Part 15, Class A certificaficaciones EMC
16. Canada – IC-ES003 certificaciones EMC

3.3.2 Cisco Secure ACS

El software Cisco Secure ACS para Windows Server (AS), es una solución única que ofrece la AAA para ambas TACACS + y RADIUS, a diferencia de muchos servidores de autenticación de nivel empresarial.

Cisco Secure ACS es una iniciativa altamente escalable, de alto rendimiento del servidor de control de acceso que pueden ser aprovechados para el control de acceso de administrador y la configuración para todos los dispositivos de red en una red de compatibilidad con RADIUS o TACACS + o ambos. La Figura 3.8 muestra una imagen de la pantalla del aplicativo.

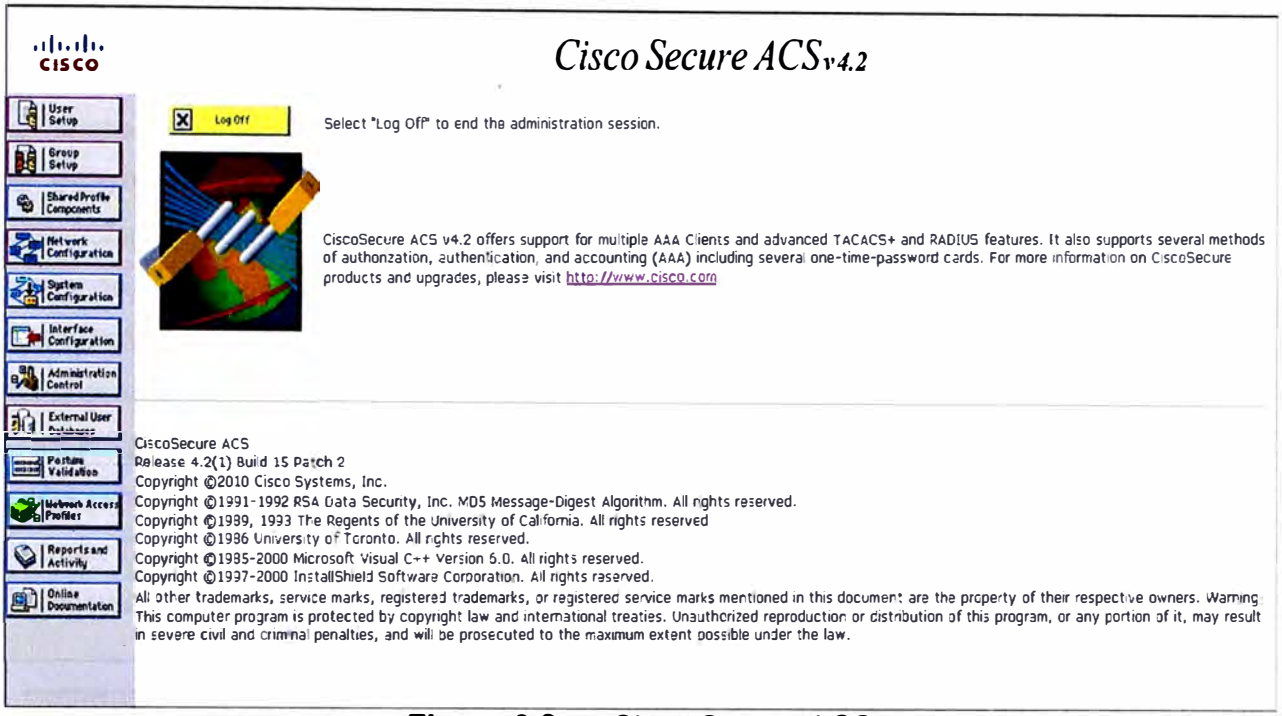

Figura 3.8 Cisco Secure ACS

Cisco Secure ACS ofrece una variedad de características avanzadas:

a. Servicio automático de seguimiento

b. Base de datos de la sincronización y la importación de herramientas para los despliegues a gran escala

c. LDAP autenticación de usuario de apoyo

d. Usuario con acceso administrativo y de información

e. Restricciones de acceso a la red basado en criterios tales como la hora del día y el día de la semana

f. Usuario y grupo de perfiles de dispositivo

La Tabla 3.5 muestra los requerimientos mínimos para instalar el software Cisco Secure ACS versión 4.2.

Tabla 3.5 Requerimientos mínimos

Especificaciones	**Requerimientos Mínimos**
Procesador	Pentium IV processor, 1.8 GHz or faster
Memoria	Mínimo 1 GB RAM
Memoria Virtual	Mínimo 1 GB
Disco Duro	Por lo menos 1 GB de espacio libre.
Sistema Operativo	Windows Server 2008, Enterprise Edition or Standard Edition (Sólo English Version) Windows Server 2003 Service Pack 1, Enterprise Edition o Standard Edition (Sólo English Version) Japanese Windows Server 2003, Service Pack 1 Windows Server 2003, R2, Standard Edition Windows Server 2003, Service Pack 2 Windows Server 2003, R2, Service Pack 2
Resolución	Mínimo de 800 x 600 (256 colores)

3.3.3 Servidor Vacman Middleware

VACMAN Middleware es una suite de software para organizaciones de todos los tamaños que necesitan autenticar a usuarios remotos que acceden a la red y recursos de la empresa. Esta tecnología de VASCO se utiliza para verificar las solicitudes de autenticación y la administración centralizada de las políticas de autenticación de los usuarios. VACMAN Middleware y los Tokens DIGIPASS de VASCO proporcionan autenticación robusta y segura para el acceso a las aplicaciones web, aplicaciones empresariales y redes privadas virtuales.

La Tabla 3.6 indica las especificaciones técnicas y los requerimientos mínimos que debe cumplir al instalar el servidor Vacman Middlerware.

La Figura 3.9 muestra el esquema de implementación del servidor Vacman Middleware con sus respectivos flujos de comunicación.

Tabla 3.6 Especificaciones técnicas y lo requerimientos mínimos

Especificaciones Técnicas	
Radius	RFC 2865 and 2866
Autenticación	DIGIPASS OATH
Requerimientos del Sistema	
Sistemas Operativos	Windows 2000/XP Windows Server 2000/2003 Windows NT Server 4.0 with SP 6 or greater
Procesador	Pentium 500 MHz or mayor
Memoria	Capacidad Mínima de RAM de 512 MB
Espacio de Disco	Capacidad Mínima de espacio libre 100 MB
Winsock	Version 2.0 o mayor

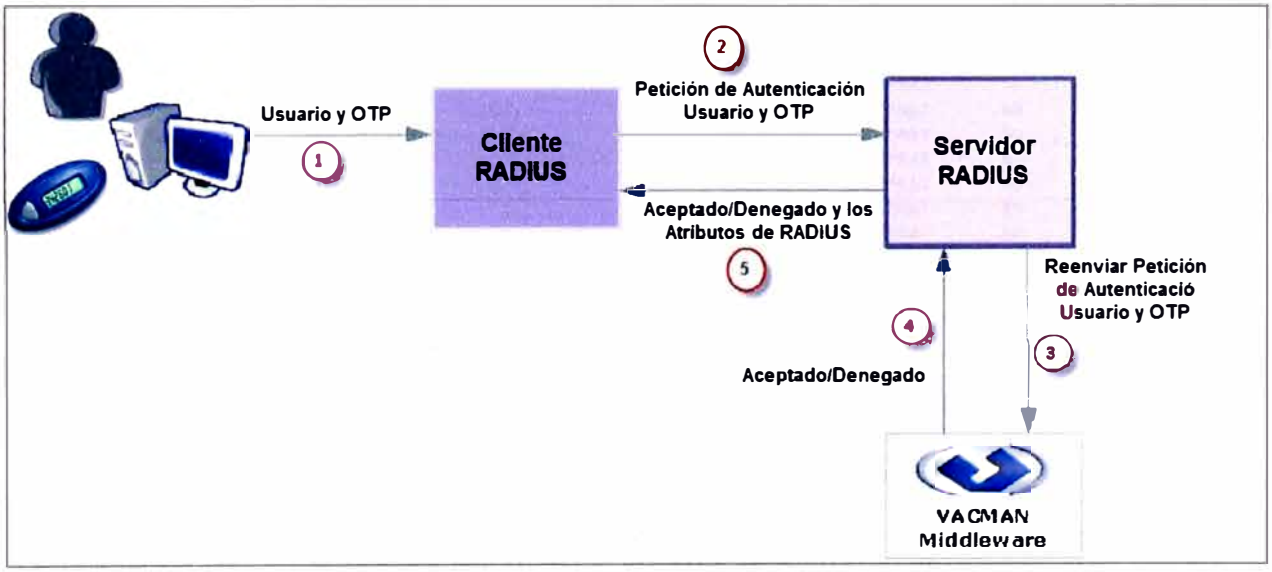

Figura 3.9 Esquema de implementación del servidor Vacman Middleware

3.3.4 Digipass GO 3

Las herramientas de seguridad para la aceptación de los usuarios es un factor crucial para garantizar el éxito de implementaciones de soluciones de seguridad para el acceso remoto seguro a las aplicaciones y redes.

El Digipass GO 3 es muy asequible, ultra-fácil de usar, y rápido y eficiente para el despliegue a los usuarios. Estas ventajas permiten a cerrar todas las brechas de seguridad en la autenticación de usuarios en cuestión de horas.

El Digipass GO 3 es el equilibrio perfecto entre un diseño elegante, y un grado sin precedentes de la portabilidad y la accesibilidad en un fácil utilizar el dispositivo de seguridad. La Figura 3.10 muestra la consola de administración del Digipass y la 3.11 al token.

Sus características técnicas son: 1) Peso de 10 gramos incluido la batería, 2) Tamaño: 12,5 x 30 x 60 mm (H x W x L), 3) Display LCD de 8- Caracteres, 4) Activación con sólo presionar el botón pequeño, 5) DES o 3-DES, 6) Reloj en tiempo real , 7) Tiempo sincrónico, 8) Tiempo y evento sincrónico, 9) Se puede combinar con una entrada de PIN, 10) Tiempo esperado de vida de la batería: mínimo 5 años, 11) Compatible con todos los miembros de la familia DIGIPASS, 12) Puede ser programado con el Programador DIGIPASS y DigiLink o se puede entregar totalmente programado, 13) Compatible con más de 50 principales proveedores de software de aplicación.

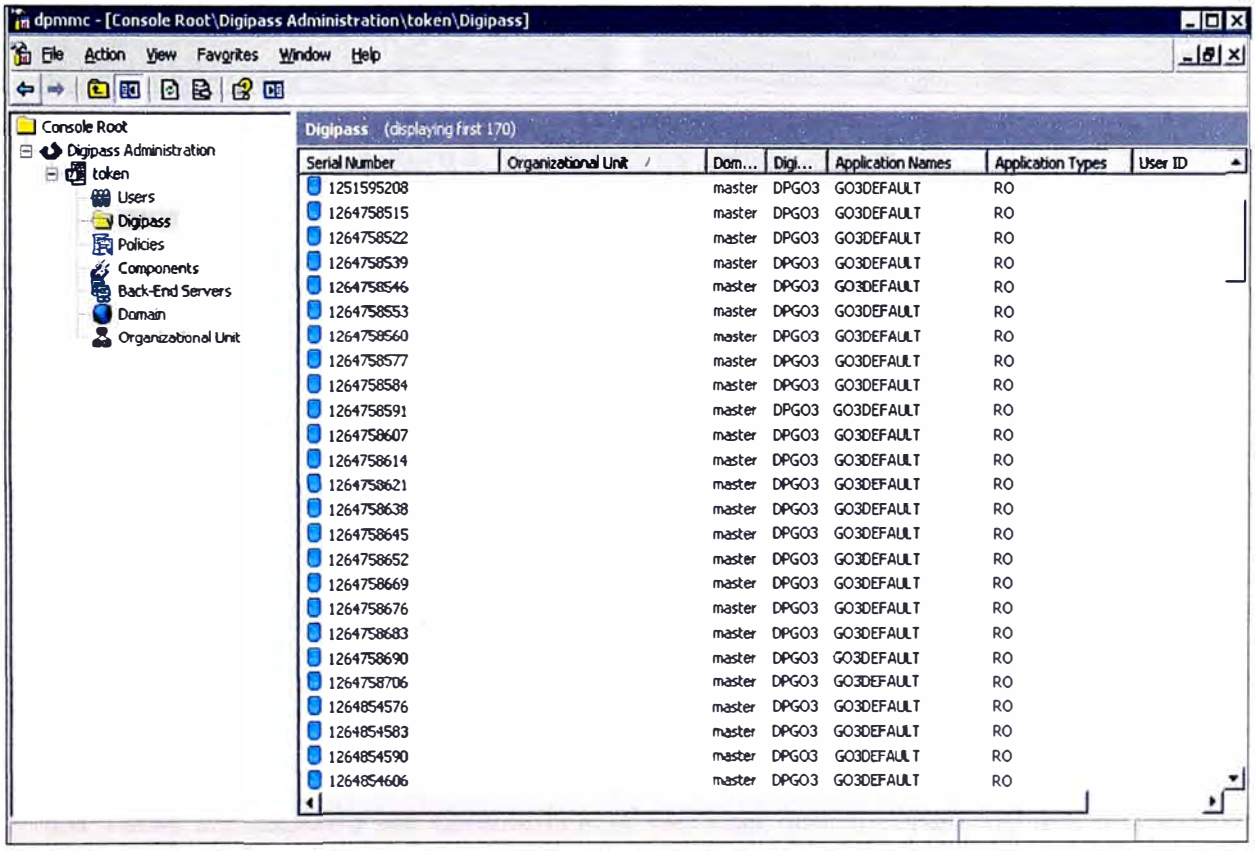

Figura 3.10 Vista de la consola de administración del Digipass

Figura 3.11 Token

3.3.5 Switches Cisco Catalyst

Las distintas familias de switches Cisco Catalyst proporcionan la infraestructura necesaria para desplegar con éxito los servicios sobre los cuales se basan los procesos de negocio en su empresa.

Los switches Cisco Catalyst construyen una red inteligente sobre la cual se brindan funcionalidades cada vez más importantes en el mundo de negocios de hoy:

La Figura 3.12 muestra la diversidad de switches Cisco Catalyst.

Figura 3.12 Switches Cisco Catalyst.

Sus características son las siguientes:

Monitoreo y Análisis de Red

VLANs

QoS (Calidad de Servicio)

Manejo de Ancho de Banda (EtherChannels)

Seguridad

Voice-aware Switches

PoE (Power over Ethernet)

Estandar 802.1x

NAC (Network Admission Control)

Alta Disponibilidad (Spanning Tree)

La Tabla 3.7 muestra las características técnicas que soportan los dos modelos de switches con la que cuenta la empresa.

Tabla 3.7 Características técnicas Switches Catalyst

	WS-C2960G-48TC-L	**WS-C2960-24TT-L**
Switching Fabric (Gbps)	32	16
Miembros máximo en stack	0	0
Clustering	Yes, 16 Switches/Cluster	Yes, 16 Switches/Cluster
Total de ancho de banda por Stack (Gbps)	N/A	N/A
Paquetes por segundo por caja (Mpps)	39	6.5
Cantidad de direcciones MAC	8000	8000
Soporte de ruteo	N/A	N/A
Memor+ia (DRAM MB)	64	64
Densidad de 10 GbE	N/A	N/A
Densidad de Gigabit Ethernet GBIC/SFP	4*	0
Densidad de puerto 10 GbE XENPAK/X2	N/A	N/A
Densidad 10/100/1000	48	2
Densidad 10/100	0	24
Densidad 100BASE-FX	0	0
Máximo consumo de potencia en Watt	140	30
Soporta AC/DC	AC only	AC only
Soporta Fuente Redundante	Yes	Yes
Dimensiones (H x W x D) pulgadas	1.73 x 17.5 x 12.9	1.73 x 17.5 x 9.3
Dimensiones (H x W x D) Centímetro	4.4 x 44.5 x 32.8	4.4 x 44.5 x 23.6
Peso unitario Libras (Kilogramos)	12 (5.4)	8 (3.6)

3.3.6 Cisco Secure Services Client (SSC)

El Cisco ® Secure Services Client es una aplicación de software que permite a las empresas desplegar un marco de autenticación única a través de dispositivos de punto final para el acceso a redes de cable e inalámbricas. El Cisco Secure Services ofrece una solución de cliente de administración simplificada, seguridad robusta, y un menor costo total de propiedad.

A través de un mecanismo de implementación simplificada y escalable, los administradores de TI pueden desplegar y gestionar el Cisco Secure Services cliente en toda la empresa. El cliente de software maneja el usuario y la identidad de dispositivos y los protocolos de acceso de red necesarios para un acceso seguro.

El Cisco Secure Services Client utiliza el estándar de autenticación IEEE 802.1X para proporcionar una sólida línea de defensa contra las intrusiones de red no autorizada.

La Tabla 3.8 muestra las características de los productos SSC.

Tabla 3.8 Características de los productos SSC

Sistemas Operativos	**Windows XP, Windows 2000, Windows Vista**
Protocolos EAP (XP/2000)	EAP-Message Digest 5 (MD5), EAP-Transport Layer Security (TLS), EAP-Tunneled TLS (TTLS), Cisco LEAP, EAP-Flexible Authentication via Secure Tunneling (FAST), Protected Extensible Authentication Protocol (PEAP)
Protocolos EAP (Vista)	Cisco LEAP, EAP-Flexible Authentication via Secure Tunneling (FAST), Protected Extensible Authentication Protocol (PEAP)
EAP-TTLS (XP/2000)	Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Microsoft CHAP (MSCHAP), MSCHAPv2, EAP-MD5
EAP-PEAP (XP/2000)	EAP-MSCHAPv2, EAP-TLS, and EAP-Generic Token Card (GTC)
EAP-PEAP (Vista)	EAP-MSCHAPv2 and EAP-GenericToken Card (GTC)
Cifrado	WEP, WPA, WPA2, WPA-Pre-Shared Key (WPA-PSK), WPA2-PSK, Dynamic WEP (802.1X), AES, TKIP
Medio de acceso	Ethernet cableado 802.3 y Wi-Fi 802.11a, 802.11b, 802.11g, 802.11n
Interoperabilidad con Switches	Cualquier switch o access point que soporte 802.1X
Interoperabilidad con AAA	Soporta RADIUS estándar, como Cisco Secure ACS y Microsoft Internet Authentication Service (IAS)
Despliegue empresarial	Exporta los perfiles y bloquear la interface del usuario.
Integración VPN	La opción automática de conexión VPN necesita el siguiente software pre-instalado. Cisco IPSec VPN version 4.8 or últimas sobre Windows XP Cisco IPSec VPN version 5.0.03.0560 or últimas sobre Windows Vista

Usando el estándar 802.1X, las decisiones de control de acceso se realizan antes de que el dispositivo de punto final se conceda una dirección IP y el acceso a la red.

Esto le da al cliente de Cisco Secure Services la flexibilidad para implementar una seguridad sólida para la gestión de acceso basado en identidades para los usuarios y dispositivos, y para ofrecer una solución de gestión portuaria eficaz. Como resultado, el costo operativo de protección de la red se reduce.

Cisco Secure Services Client versión 5.1 contiene una característica de implementación en la empresa que permite a los administradores configurar e implementar perfiles de cliente para toda la organización. Implementar el cliente desde una ubicación centralizada ahorra mucho tiempo y en última instancia, ayuda a reducir el coste total de propiedad (TCO) de la implementación de un suplicante 802.1X

3.4 Funcionamiento

Para validar el funcionamiento de la solución planteada, el resultado de las pruebas lo vamos a presentar 1) Resultado del funcionamiento de la autenticación 802.1X 2) Resultado del funcionamiento de la asignación de VLAN dinámicas.

3.4.1 Resultado del funcionamiento de la autenticación 802.1X

Para el funcionamiento del Control de Acceso implementado se consideran los siguientes escenarios:

Escenario 1. Usuario que no cumple con Políticas de Seguridad.- Se refiere a un equipo que requiere ingresar a la red de la organización pero no se encuentra definido como un usuario de la red y por esta razón incumplirá en la política de seguridad y se le denegará el acceso.

Para comprobar la funcionalidad de este escenario se realizaron pruebas con tres equipos en los que al tratar de ingresar con un usuario y contraseña que no se encuentran definidos como datos válidos se les denegó el acceso a la red. En la Figura 3.13 se muestra la autenticación de rechazo.

La Figura 3.14 fue obtenida del Servidor ACS, el intento de conexión se muestra como fallida debido a que se trata de un usuario desconocido.

En el caso que el usuario hubiera sido valido, pero su contraseña fue incorrecta, el evento siguiente se obtiene desde el servidor de Token. En la Figura 3.15 se muestra que el usuario user_demo existe en la base de datos de usuarios tanto en el servidor ACS como en el servidor Token; sin embargo el usuario no ha ingresado correctamente su contraseña (PIN+OTP) y de acuerdo con los eventos encontrados en el servidor de token, se evidencia que el usuario no ingreso correctamente su PIN (Static Password).

Escenario 2. Usuario que cumple con las Políticas de Seguridad.- Se refiere a un equipo que requiere ingresar a la red de la organización, el cual cumple con la política de seguridad establecida, por lo que el sistema le permite el acceso a la red.

Para comprobar la funcionalidad de este escenario se realizaron pruebas con 3 equipos en los que al tratar de ingresar con un usuario y contraseña que fueron definidos como usuarios dentro de la configuración de los archivos del servidor RADIUS, al solicitar el ingreso a la red con datos válidos se permite el acceso. La Figura 3.14 muestra el proceso de autenticación.

El registro del acceso exitoso a la red se evidencia en los eventos encontrados en los servidores de token y ACS (Figura 3.17).

3.4.2 Resultado del funcionamiento de asignación de VLAN dinámicas

De acuerdo con las pruebas del escenario 2, el usuario user_demo logró acceder a la red mediante la autenticación 802.1X y el uso de los digipass como contraseña.

Se necesita evidenciar, que el puerto del switch donde se conecta el usuario se ha configurado de acuerdo al perfil preconfigurado en el servidor ACS para el usuario user_demo.

El perfil del usuario (Figura 3.18) user_demo lo configuramos en el capitulo anterior, la siguiente figura muestra que el usuario user_demo pertenece a la VLAN 751, y este valor es el que debe configurarse el puerto del switch donde el usuario se ha conectado.

Luego que el usuario se ha autenticado exitosamente, se evidencia que el puerto del switch efectivamente se ha configurado en la VLAN 751. Esta configuración dinámica (Figura 3.19) libera a los administradores de red de una carga laboral bastante recurrente.

Para el usuario la autenticación exitosa y la configuración dinámica de VLAN se ve por el acceso a la red, la Figura 3.20 muestra los instantes en que el puerto del switch pasa de un estado bloqueado donde no permite por nada ningún tráfico hacia la red, y otro instante cuando el puerto se encuentra desbloqueado, luego de una autenticación exitosa.

Una vez terminadas las etapas de instalación, configuración y pruebas del servidor RADIUS, así como la configuración del autenticadores y de los equipos solicitantes, la organización aprueba la implementación del control de acceso y se comienza con la etapa de capacitación a los usuarios sobre la forma en que se autenticarán para el acceso a la red cableada de la organización.

La implementación del control de acceso permitirá a la organización contar con un sistema de seguridad en el que sólo los usuarios que se autentiquen podrán accesar a la red de la organización, dando solución a la problemática de restricción de acceso a usuarios no autorizados.

En resumen, las páginas que muestran a continuación las siguientes figuras. Estas están numeradas del 3.13 a la 3.20.

En el siguiente capítulo se desarrollará el tema correspondiente a la estructura de costos y al cronograma de trabajos.

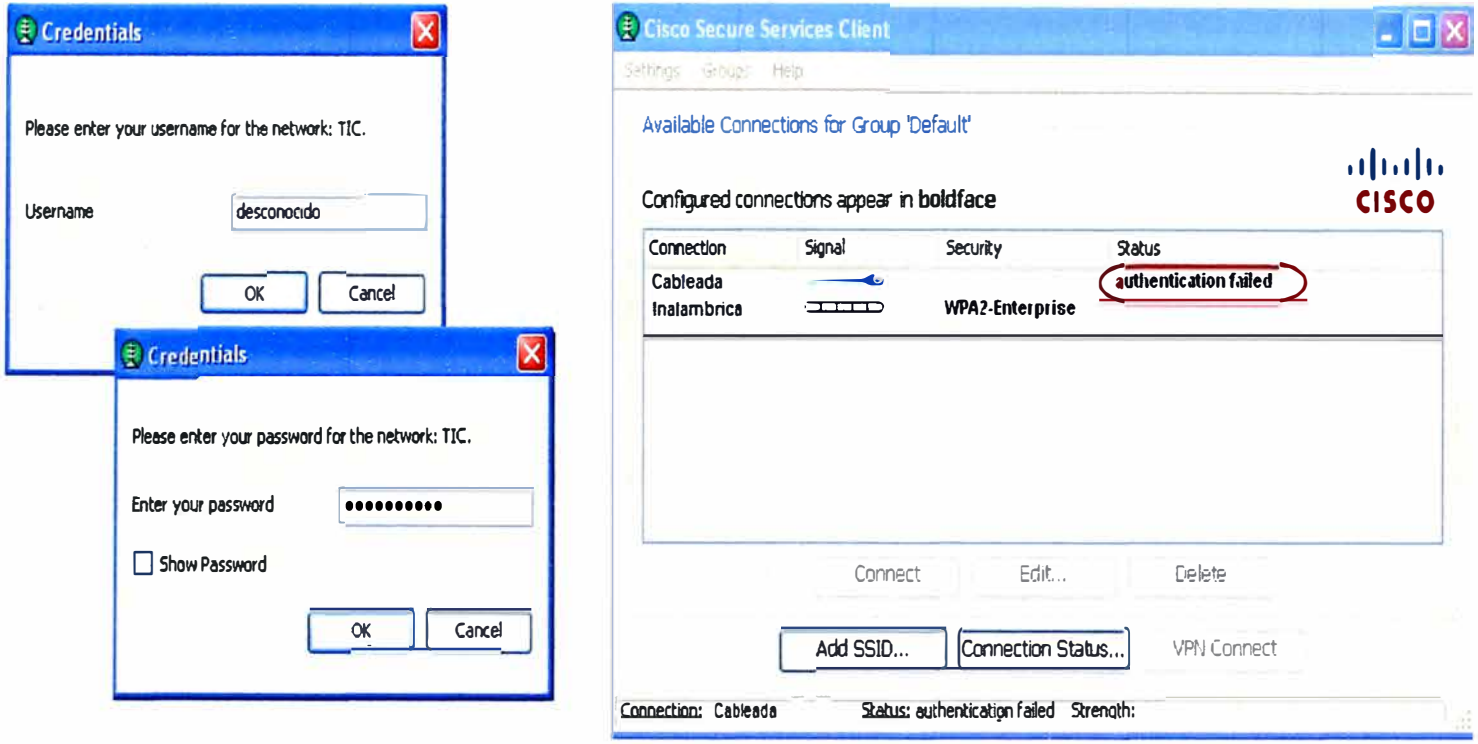

Figura 3.13 Denegación de acceso a usuarios no autorizados

Date	Time	Message-Type	User-Name	Group-Name	Caller-ID	Network Access Profile Name	Authen-Failure-Code	NAS-Port	NAS-IP-Address	EAP Type	EAP Type Name	Reason	Access Device
08/19/2010	14:25:05	Authen failed	anonymous	ADMIN-NOC	00-1E-EC-86-ED-8E	(Default)	ACS user unknown	anonymous	10.10.1.10	25	CISCO-PEAP	..	SWS-Piso3

Figura 3.14 Intento de conexión fallida por usuario desconocido

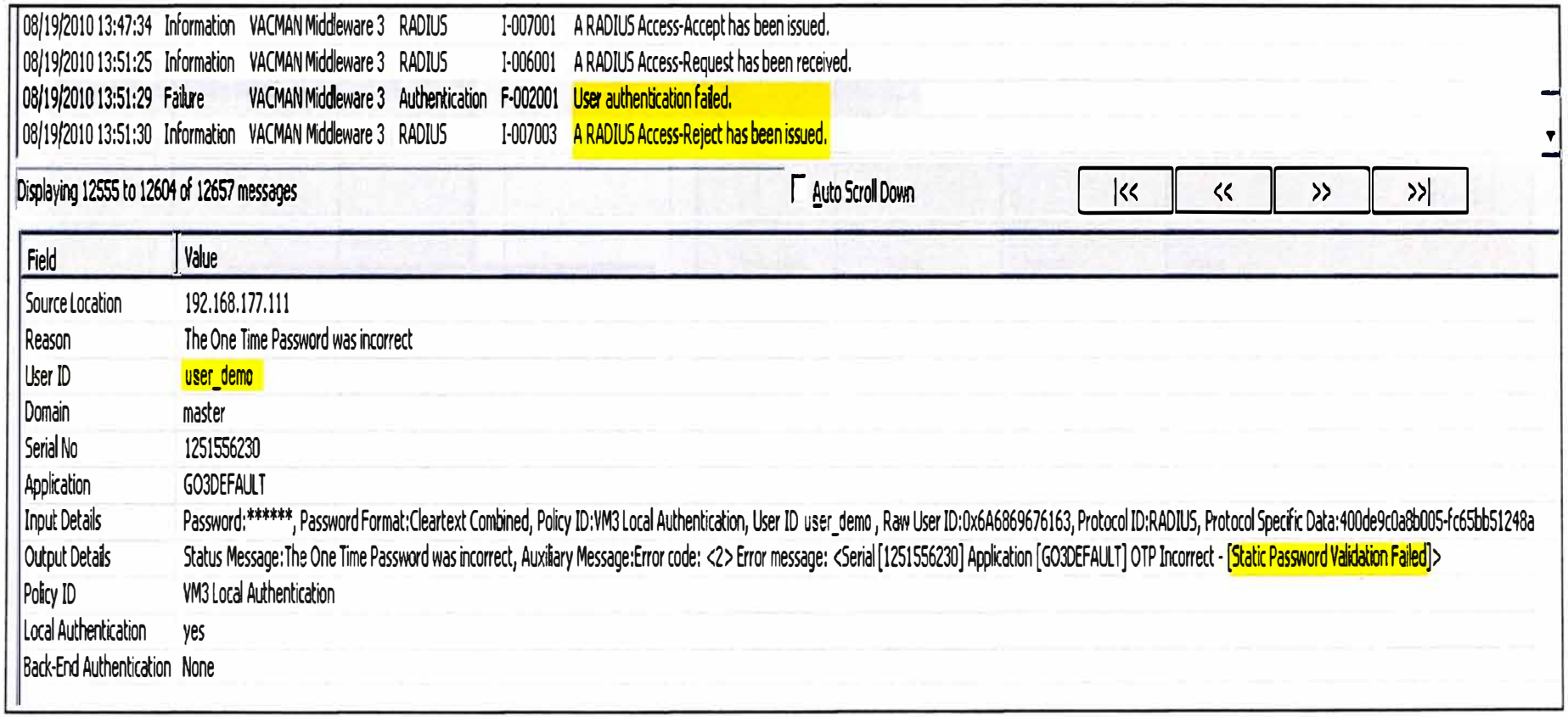

Figura 3.15 Acceso fallido por contraseña (PIN) incorrecta

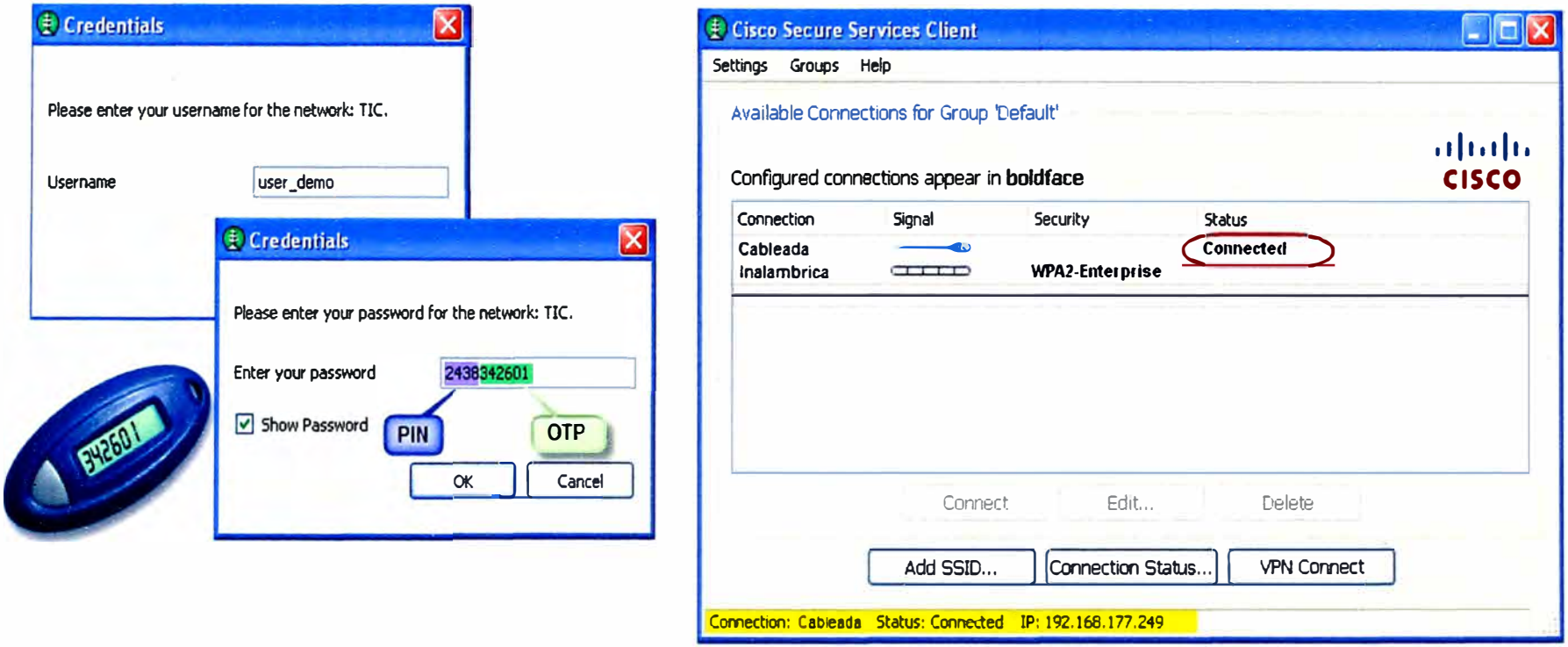

Figura 3.16 Aceptación de acceso a la red

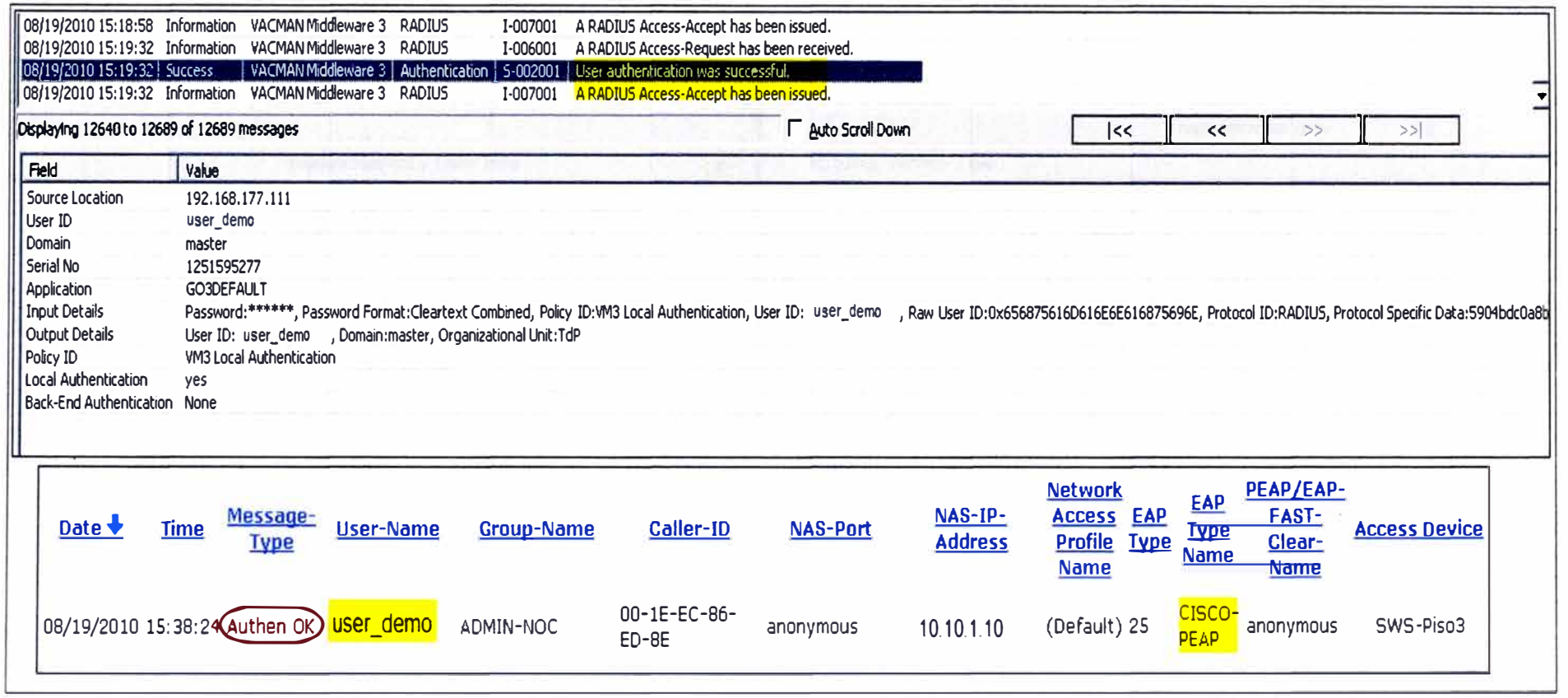

Figura 3.17 Evidencia de la autenticación exitosa

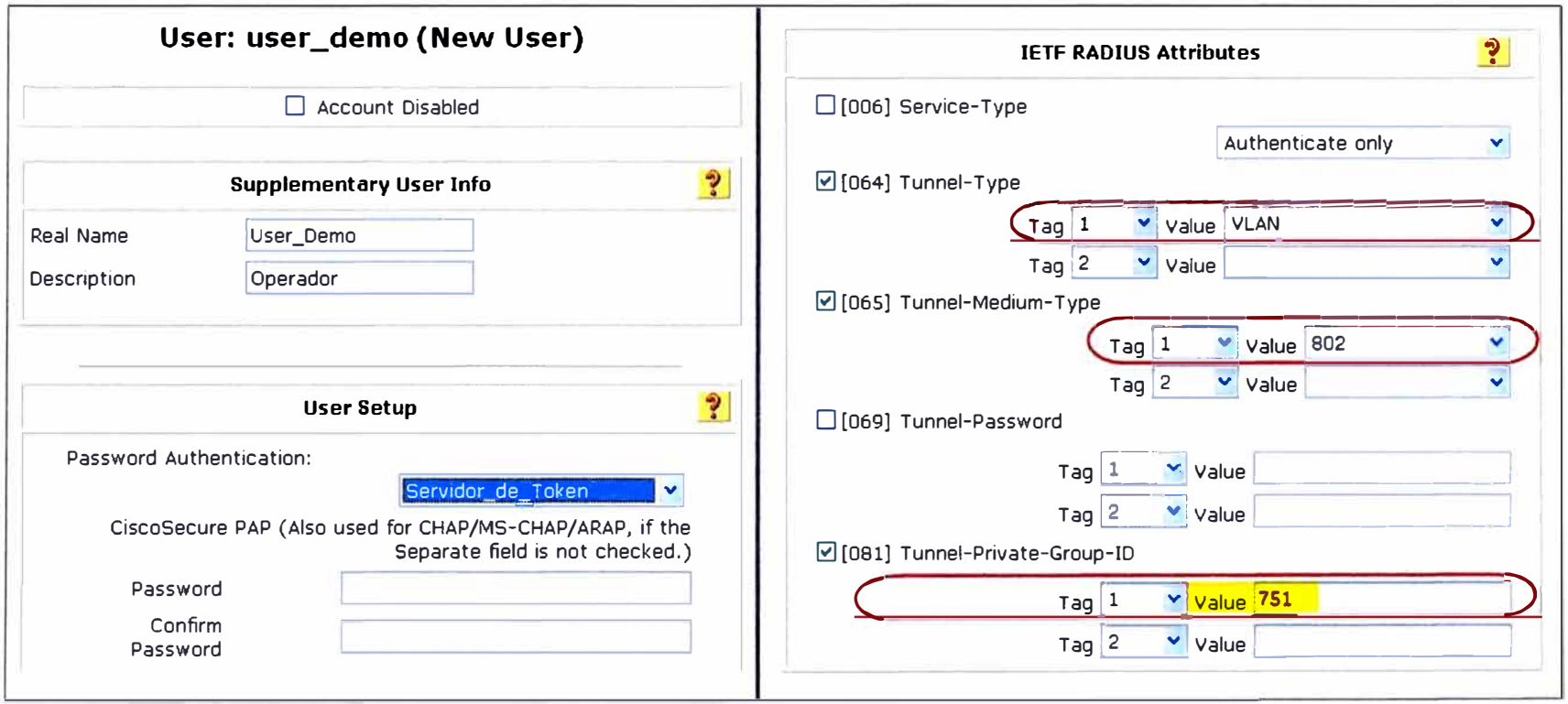

Figura 3.18 Perfil del usuario user_demo en el Servidor ACS

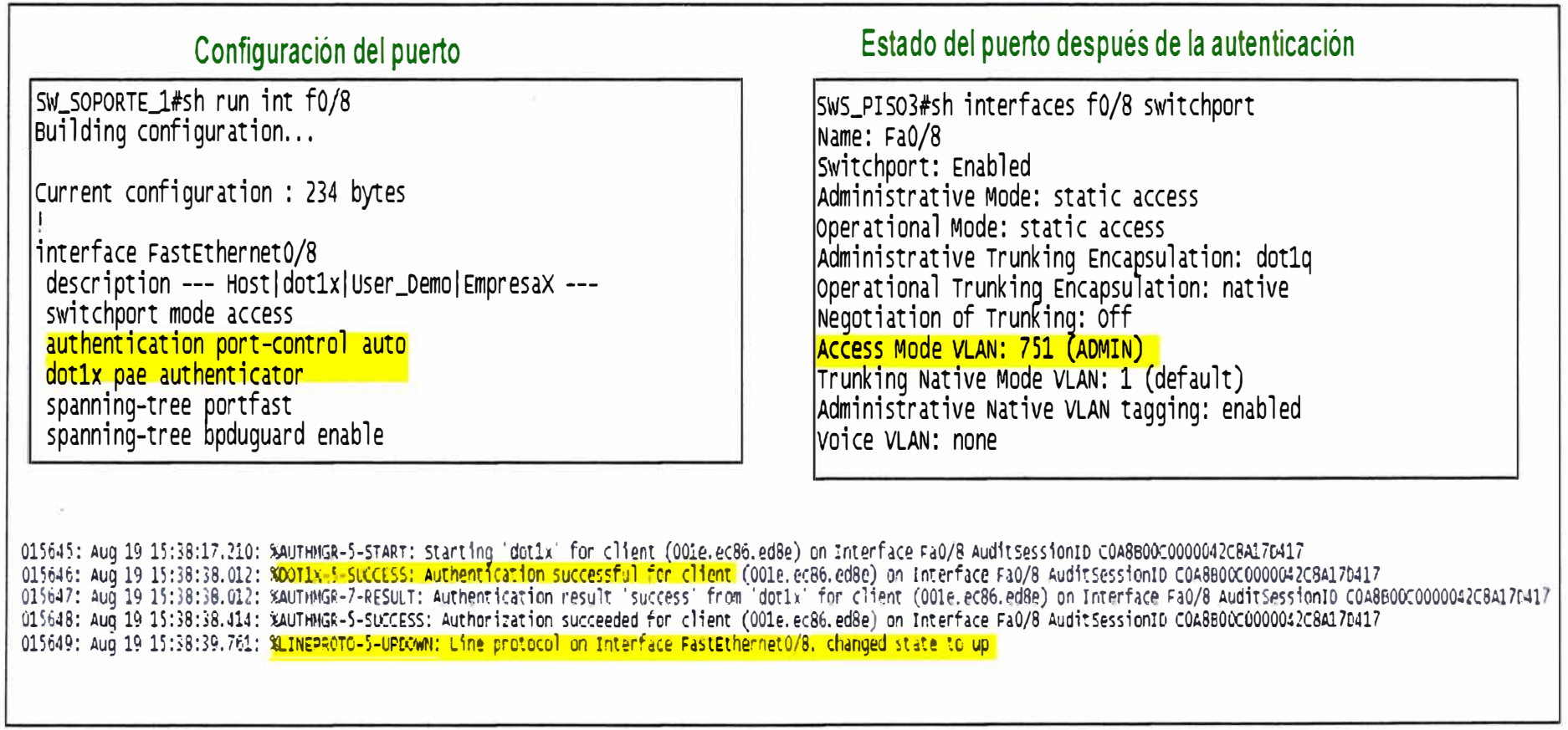

Figura 3.19 Configuración dinámica del puerto del switch

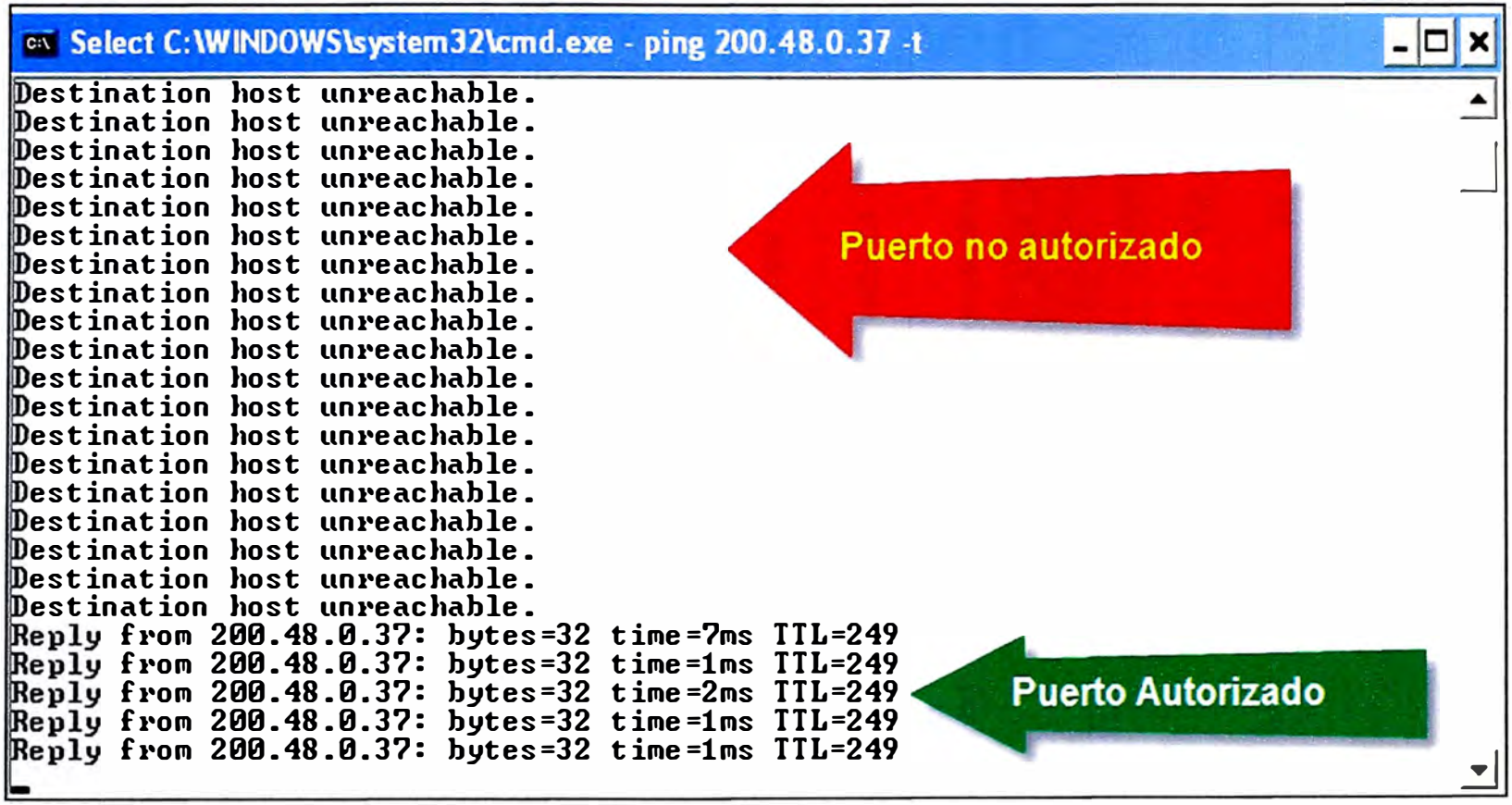

Figura 3.20 Cambio de estado del puerto de acceso.

CAPÍTULO IV
COSTOS DEL PROYECTO

En el presente capítulo se tocan los temas involucrados al funcionamiento, presupuesto y cronograma del proyecto de ingeniería.

4.1 Desarrollo del presupuesto

Debido a las decisiones de compra que son a nivel de la casa matriz y que es un proyecto para la propia empresa utilizando sus propios recursos y equipamiento, no fue posible realizar estimaciones de costos, y tampoco un análisis comparativo con otros productos de otras marcas.

Dado el requerimiento planteado en el capítulo anterior, y debido al planteamiento de la solución se ha visto necesario la adquisición de los siguientes productos de software.

a. Licencia de funcionamiento del Software Vacman Middleware
b. Token Digipass GO3
c. Licencia de funcionamiento de software suplicante Cisco Secure Services Client (SSC)

La Tabla 4.1 muestra los valores en dólares de los productos adquiridos por sistema (Item 1 y 2) y la inversión total que se ha realizado.

Tabla 4.1 Productos adquiridos, Inversión total realizada

Item	Descripcion	Qty	Precio Unitario	Precio Total
1	Solución de autenticación Vasco		$68.88	$6,888.00
1.1	Vacman Radius Middleware (licencia por usuario)	100	$37.95	$3,795.00
1.2	Vacman Radius Mantenimiento y Soporte (por año, licencia por usuario)	100	$9.49	$949.00
1.3	Digipass G03	100	$21.44	$2,144.00
2	Suplicante Cisco Secure Services Client (SSC)		$44.00	$44.00
2.1	SW Client 5.x wired and wireless devices	1	$0.00	$0.00
2.2	Specified seat count up to 250	1	$44.00	$44.00
			Total de Inversión:	$6,932.00

4.2 Desarrollo del cronograma

En esta sección se explica:

1. La definición de las actividades y
2. El establecimiento de la Secuencia y Duración de las actividades.

4.2.1 Definición de las actividades

La definición de las actividades se efectúan utilizando la técnica de Descomposición, se utilizarán plantillas proporcionadas por la Oficina de Gerencia de Proyectos (PMO), se utilizará el juicio de expertos y la planificación gradual.

4.2.2 Establecimiento de la secuencia y duración de las actividades

La secuencia de las actividades se efectúa utilizando la técnica del Método de Diagramación por Precedencia (PDM), Las dependencia se determina en base al análisis de los especialistas.

La duración de las actividades se efectúa utilizando el conocimiento de personal experimentado en proyectos similares es decir a través de la técnica del Juicio de Expertos y Estimación por Analogía donde se toma en cuenta la experiencia en proyectos similares.

De ambos procesos se obtiene los siguientes entregables.

a. Diagramas de red del cronograma del proyecto (Figura 4.1).
b. Lista de actividades y atributos (Tabla 4.2).
c. Estimación de la duración de la actividad (También incluida en la Tabla 4.1).

El diagrama de Gantt correspondiente se muestra en el Anexo D.

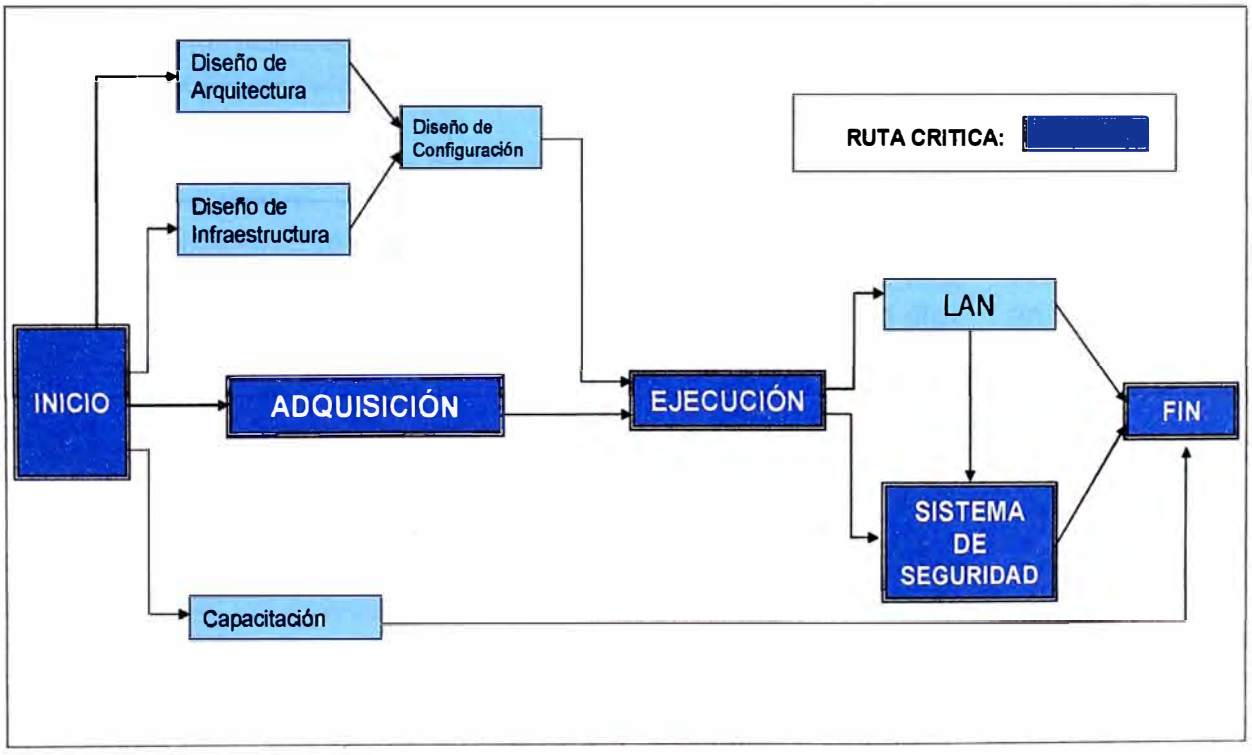

Figura 4.1 Diagrama de red del cronograma del proyecto

Tabla 4.2 Lista de actividades y atributos

EDT	Nombre de tarea	Tiempo	Inicio	Fin
1	Sistema de Control de Acceso	82 días	02/02/09	25/04/09
1.1	Diseño del Sistema	15 días	02/02/09	17/02/09
1.1.1	Diseño de arquitectura	10 días	02/02/09	12/02/09
1.1.2	Diseño de infraestructura	5 días	02/02/09	07/02/09
1.1.3	Diseño de configuración	5 días	12/02/09	17/02/09
1.2	Adquisición de software	31 días	12/02/09	15/03/09
1.2.1	Solicitud de compra de sofwares y DigiPass GO3	30 días	12/02/09	14/03/09
1.2.2	Entrega de Softwares y Digipass GO3	1 día	14/03/09	15/03/09
1.3	Instalación del Servidor Vacman Middleware	10 días	15/03/09	25/03/09
1.3.1	Provisión del servidor	3 días	15/03/09	18/03/09
1.3.1.1	Instalación del sistema operativo W2003	1 día	15/03/09	16/03/09
1.3.1.2	Actualización y Hardening	2 días	16/03/09	18/03/09
1.3.2	Configuración del Servidor	7 días	18/03/09	25/03/09
1.3.2.1	Instalación del software Vacman Middleware	1 día	18/03/09	19/03/09
1.3.2.2	Configuración de los Digipass	1 día	19/03/09	20/03/09
1.3.2.3	Configuración de los usuarios	5 días	20/03/09	25/03/09
1.4	Segmentación de la Red	19 días	17/02/09	08/03/09
1.4.1	Configuración de los switches	1 día	17/02/09	18/02/09
1.4.2	Configuración de las zonas en el firewall	3 días	18/02/09	21/02/09
1.4.3	Migración a los usuarios de la red plana a la red segmentada fija	10 días	21/02/09	03/03/09
1.4.4	Configuración de políticas fijas en el firewall	5 días	03/03/09	08/03/09
1.5	Configuración del Servidor Cisco ACS	3 días	25/03/09	28/03/09
1.5.1	Integración con el servidor Vacman Middleware	1 día	25/03/09	26/03/09
1.5.2	Configuración de los switches como Cliente Radius	1 día	26/03/09	27/03/09
1.5.3	Creación de usuarios con sus respectivos perfiles	1 día	27/03/09	28/03/09
1.6	Pruebas	27 días	08/03/09	04/04/09
1.6.1	Prueba de los acceso de los usuarios en la red sin autenticación	5 días	08/03/09	13/03/09
1.6.2	Pruebas de Comunicación entre el servidor ACS y Vacman Middleware	2 días	28/03/09	30/03/09
1.6.3	Pruebas Funcionamiento de la solución planteada	5 días	30/03/09	04/04/09
1.7	Despliegue	21 días	04/04/09	25/04/09
1.7.1	Distribución de los Digipass a los usuarios	5 días	04/04/09	09/04/09
1.7.2	Instalación de software Suplicante Cisco SSC	5 días	04/04/09	09/04/09
1.7.3	Capacitación sobre la plataforma	1 día	09/04/09	10/04/09
1.7.4	configuración de los puertos de los switches con 802.1X	15 días	10/04/09	25/04/09
1.8	Gestión del Proyecto	82 días	02/02/09	25/04/09
1.8.1	Iniciación	0 días	02/02/09	02/02/09
1.8.2	Planificación	30 días	02/02/09	04/03/09
1.8.3	Ejecución y Control	67 días	17/02/09	25/04/09
1.8.4	Cierre	0 días	25/04/09	25/04/09

CONCLUSIONES Y RECOMENDACIONES

1. Con la realización de este informe de suficiencia se pudieron identificar los conceptos de redes cableadas, seguridad para este tipo de redes y conceptos relacionados con los protocolos RADIUS, EAP, y el estándar 802.1X, además de la implementación de un sistema de seguridad a través de la autenticación de los usuarios para el acceso a una red cableada.

2. La implementación del control de acceso en la red cableada de la organización permitió contar con un sistema de seguridad, en el que sólo los usuarios que se autentiquen podrán accesar a la red; con lo anterior se aprecia que el sistema de seguridad implementado cubre la necesidad de la organización y dio solución a su problemática de restringir el acceso a personas no autorizadas, llevando consigo estadísticas sobre el número de dispositivos autenticados, las autenticaciones exitosos y lo fallidos.

3. Además de simplificar lo traslados dentro de las oficinas, eliminando la necesidad de reasignar manualmente los puertos o realizar cambios en el cableado cuando los empleados cambian de ubicación; se ha añadido un valor agregado que es la movilidad a los usuarios, que ahora pueden desplazarse con sus laptops y conectarse a cualquier punto de red y estar tranquilos que podrán acceder a sus recursos de siempre.

4. Finalmente con la implementación del Servidor Vacman Middleware se ha logrado reducir los riesgos de seguridad asociados con las contraseñas de un solo factor.

5. La implementación realizada no contempla altos mecanismos de seguridad que asegura que sólo hosts en buen estado pueden ingresar a la red, lo que se plantea aquí es garantizar el acceso sólo al personal autorizado, más no impedir que una PC correctamente autorizada puedan contaminar a la red con malwares; Por lo tanto como recomendación se ha planteado incrementar el nivel se seguridad del control de acceso a la red asegurando que los hosts autorizados tiene el antivirus y sistema operativo actualizado; y que sólo aplicaciones reconocidas por la empresa puedan ser usadas por el usuario; de no cumplir con dicha política deberá ser restringido, y ser derivado a una zona de cuarentena para una remediación.

6. Un punto importante sobre la realización de esta investigación es que sirve

como base para la implementación de un control de acceso para la red cableada o inalámbrica de cualquier organización cuando se desee tener un control sobre los usuarios que pueden accesar a la red, y brinda los conceptos importantes para ser implementado utilizando la parte de autenticación del estándar 802.1X.

ANEXO A
DIAGRAMAS FÍSICO Y LÓGICO

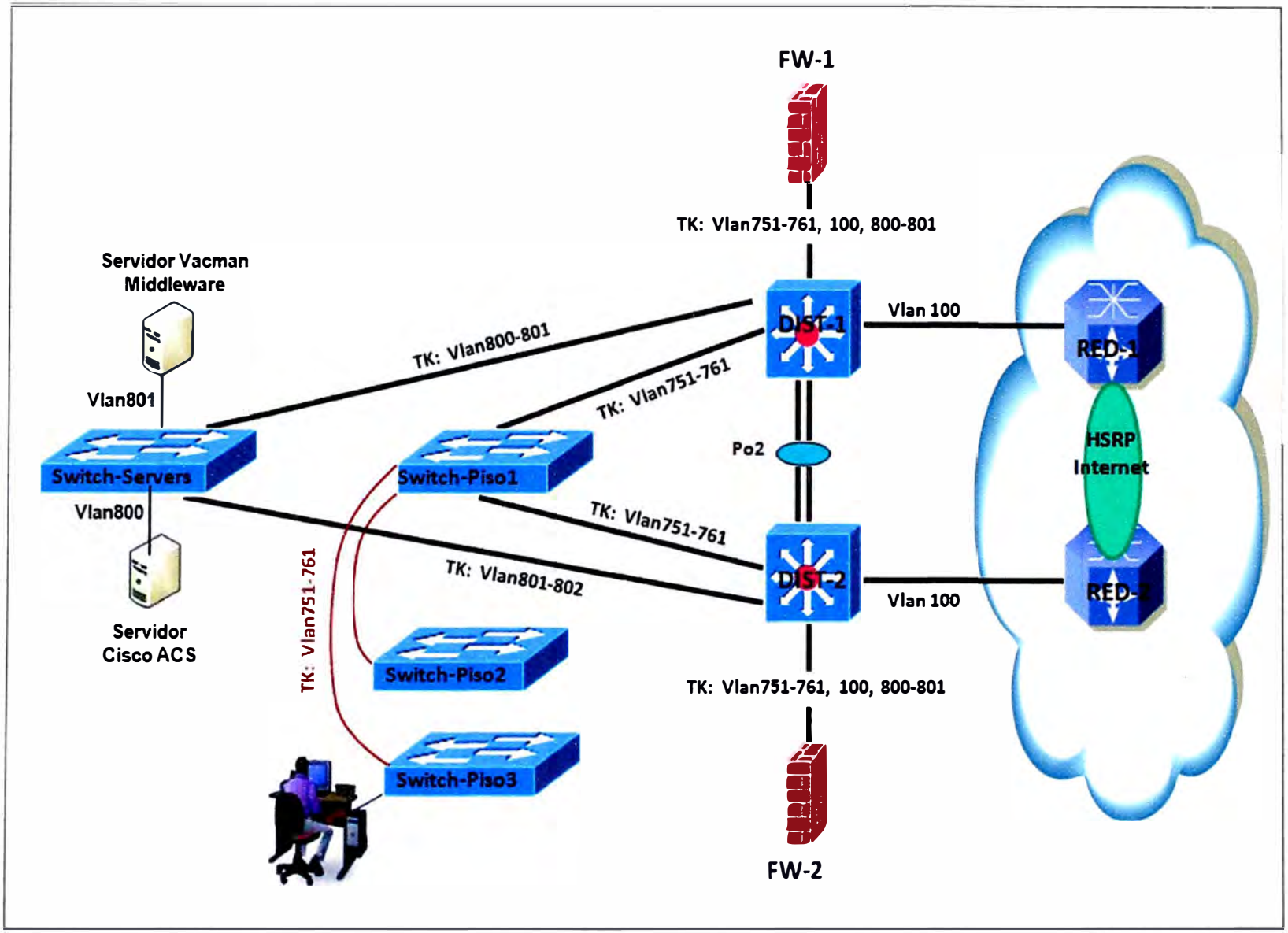

Figura A.1 Topología física

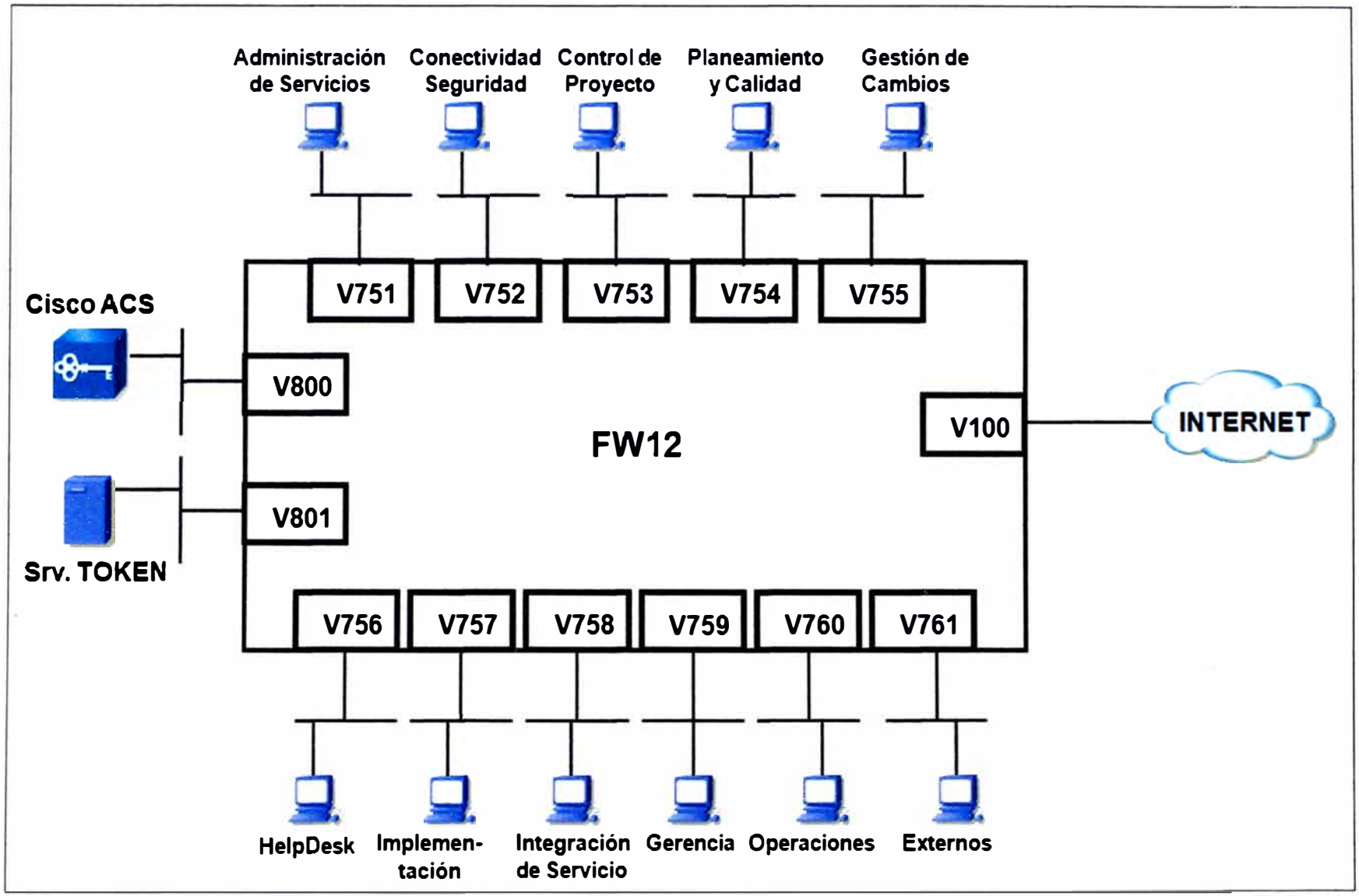

Figura A.2 Topología lógica

ANEXO B
PROCESO DE AUTENTICACIÓN Y CAPTURA DE TRAMAS

Figura B.1

Muestra el proceso de autenticación entre todos los elementos de la solución planteada en este trabajo de sustentación.

Figura B.2

Muestra el proceso de comunicación entre el suplicante y el autenticador.

Figura B.3

Se aprecia claramente el inicio de la comunicación con la trama numéro 1 EAPOL-START, y el éxito de la autenticación con la trama número 23 EAPOI-Success. Así mismo podemos ver el encapsulamiento del protocolo EAP sobre 802.1X.

Del mismo modo se ha capturado los paquetes que intercambiaron el autenticador, el servidor de autenticación y el servidor de token, en esas capturas se aprecia que los paquetes 99 y 100 son cuando el servidor de autenticación con IP 192.168.176.5 envía un paquete RADIUS Access-Request al Servidor de Token con IP 192.168.177.111, este le responde con un Access-Accept, con el que confirma que el OTP que ingresó el usuario es correcto.

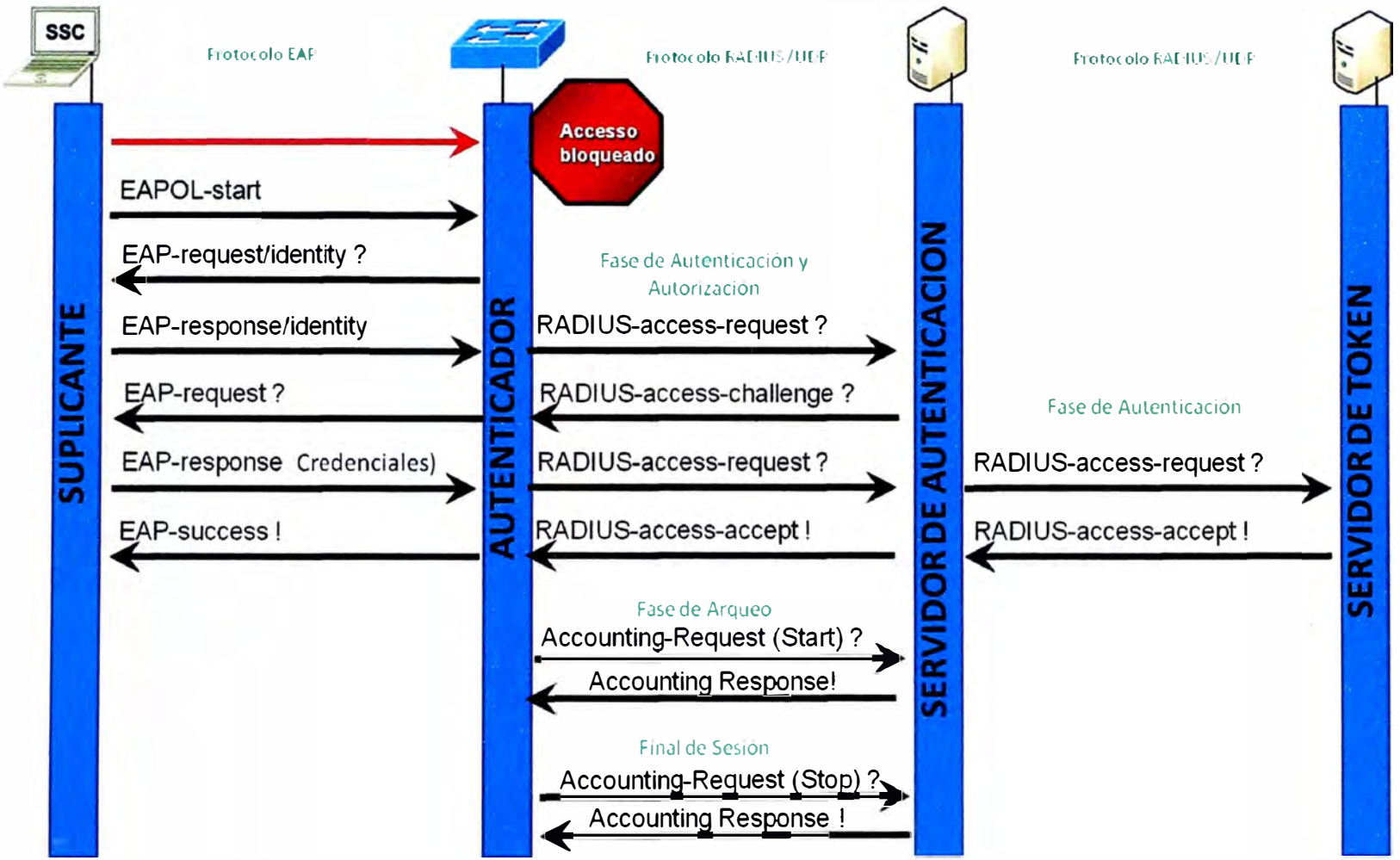

Figura B.1 Proceso de autenticación

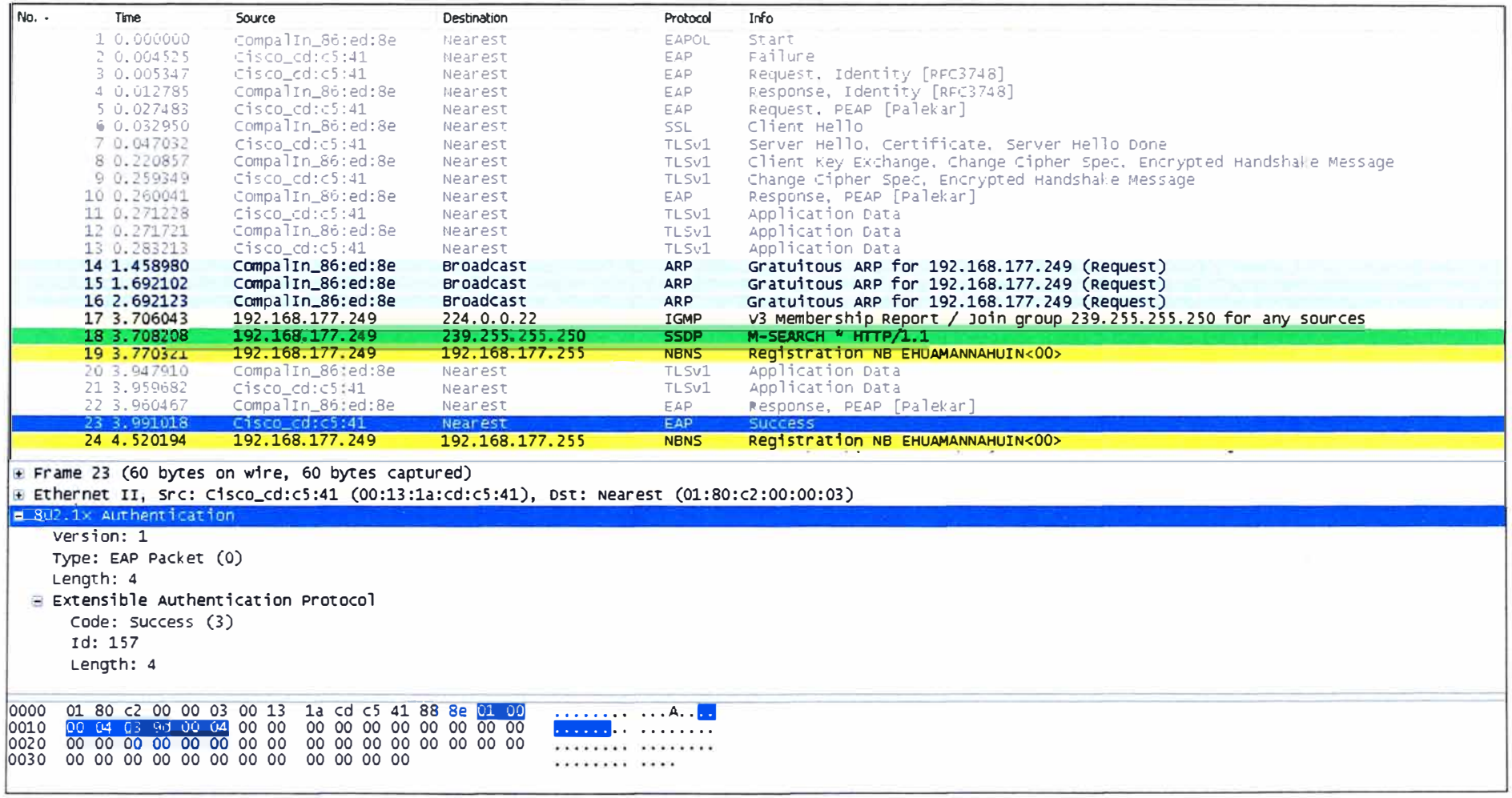

Figura B.2 Capturas de tramas de una autenticación exitosa

No.	Time	Source	Destination	Protocol	Info
84	145.096864	192.168.176.106	192.168.176.5	RADIUS	Access-Request(1) (id=118, l=133)
87	145.100288	192.168.176.5	192.168.176.106	RADIUS	Access-Challenge(11) (id=118, l=75)
88	145.116039	192.168.176.106	192.168.176.5	RADIUS	Access-Request(1) (id=119, l=204)
89	145.117081	192.168.176.5	192.168.176.106	RADIUS	Access-Challenge(11) (id=119, l=963)
90	145.450205	192.168.176.106	192.168.176.5	RADIUS	Access-Request(1) (id=120, l=474)
91	145.483877	192.168.176.5	192.168.176.106	RADIUS	Access-Challenge(11) (id=120, l=130)
92	145.495858	192.168.176.106	192.168.176.5	RADIUS	Access-Request(1) (id=121, l=154)
93	145.496473	192.168.176.5	192.168.176.106	RADIUS	Access-Challenge(11) (id=121, l=128)
94	145.509127	192.168.176.106	192.168.176.5	RADIUS	Access-Request(1) (id=122, l=199)
95	145.509708	192.168.176.5	192.168.176.106	RADIUS	Access-Challenge(11) (id=122, l=128)
98	167.283022	192.168.176.106	192.168.176.5	RADIUS	Access-Request(1) (id=123, l=199)
99	167.285035	192.168.176.5	192.168.177.111	RADIUS	Access-Request(1) (id=19, l=93)
100	167.421151	192.168.177.111	192.168.176.5	RADIUS	Access-Accept(2) (id=19, l=20)
101	167.421824	192.168.176.5	192.168.176.106	RADIUS	Access-Challenge(11) (id=123, l=112)
102	167.433640	192.168.176.106	192.168.176.5	RADIUS	Access-Request(1) (id=124, l=154)
103	167.442434	192.168.176.5	192.168.176.106	RADIUS	Access-Accept(2) (id=124, l=233)
104	167.465430	192.168.176.106	192.168.176.5	RADIUS	Accounting-Request(4) (id=124, l=193)
105	167.701610	192.168.176.5	192.168.176.106	RADIUS	Accounting-Response(5) (id=124, l=20)

Figura B.3 Conversación Autenticador, Srv.Autenticación y Srv. De Token

ANEXO C
CÁLCULO DE LA SEGMENTACIÓN DE LA RED

Para hacer un cálculo de Subneting se debe saber el número de redes que se quieren conseguir y el numero de host necesarios por red. Siempre se debe tener en cuenta el número máximo de host que tendrá que haber en una subred, ya que todas las subredes dispondrán de la misma capacidad de Host.

Los datos que se conoce es el ID y la máscara de la red.

ID de la red: 192.168.173.0

Máscara: 255.255.255.0

O utilizando el método llamado CIDR o classless:

ID de red + Máscara: 192.168.173./24

Donde el 24 es el número de unos desde la izquierda que tendrá la máscara de subred.

a. Cálculo de la máscara de subred

Para calcular la máscara se debe utilizar la siguiente formula:

$$\#Subred \leq 2^n - 2 \qquad \text{(C.1)}$$

Donde "n" es el número de unos que se deben agregar a la máscara y además el resultado debe ser mayor o igual a 10 (número de redes).

$2^2 - 2 = 2 >= 10$ (Falso)

$2^3 - 2 = 6 >= 10$ (Falso)

$2^4 - 2 = 14 >= 10$ (Verdadero)

Por tanto si se eleva a 4, la condición si cumple, así que se deben añadir 4 unos a la mascara.

Mascara Original: 255.255.255.0

Mascara Original en Binario: 11111111.11111111.11111111.00000000

Mascara Modificada en Binario: 11111111.11111111.11111111. **1111**0000

Mascara Modificada en Decimal: 255.255.255.240

b. Cálculo del número de Hosts

Para calcular el número de Hosts se debe utilizar la siguiente formula:

$$\#Host \leq 2^m - 2 \qquad \text{(C.2)}$$

Donde "m" es el número de ceros de la mascara, además el resultado deber ser mayor o igual a 10 (número de hosts por cada área de trabajo). En este caso el número de ceros en binario después de modificarla son 4. Por lo tanto:

$2^4 - 2 = 14 >= 10$

"14" es el número de host que se podrían tener por cada subred. Como en el diseño se piden que el número de hosts sean 10, estaría resuelto el problema.

c. Tabla de asignación

Se tiene la máscara modificada en decimal 255.255.255.240 y la ID de Red

192.168.173.0.

Son 4 bits los que han añadido a la mascara, por tanto la ID de Red queda en binario de la siguiente forma:

192.168.173.0/28 <> 11000000.10101000.10101101.**XXXX**0000

Donde XXXX = posibles combinaciones de los 4 bits que se han obtenido al hallar el valor de la máscara después de hacer el Subnettig. Estas dan un total de 16 posibilidades las cuales se muestran en la Tabla C.1.

Tabla C.1 Lista de Subredes disponibles

Subnet	En Binario	En Decimal
1	11000000.10101000.10101101.**0000**0000	192.168.173.0
2	11000000.10101000.10101101.**0001**0000	192.168.173.16
3	11000000.10101000.10101101.**0010**0000	192.168.173.32
4	11000000.10101000.10101101.**0011**0000	192.168.173.48
5	11000000.10101000.10101101.**0100**0000	192.168.173.64
6	11000000.10101000.10101101.**0101**0000	192.168.173.80
7	11000000.10101000.10101101.**0110**0000	192.168.173.96
8	11000000.10101000.10101101.**0111**0000	192.168.173.112
9	11000000.10101000.10101101.**1000**0000	192.168.173.128
10	11000000.10101000.10101101.**1001**0000	192.168.173.144
11	11000000.10101000.10101101.**1010**0000	192.168.173.160
12	11000000.10101000.10101101.**1011**0000	192.168.173.176
13	11000000.10101000.10101101.**1100**0000	192.168.173.192
14	11000000.10101000.10101101.**1101**0000	192.168.173.208
15	11000000.10101000.10101101.**1110**0000	192.168.173.224
16	11000000.10101000.10101101.**1111**0000	192.168.173.240

ANEXO D
DIAGRAMA DE GANTT

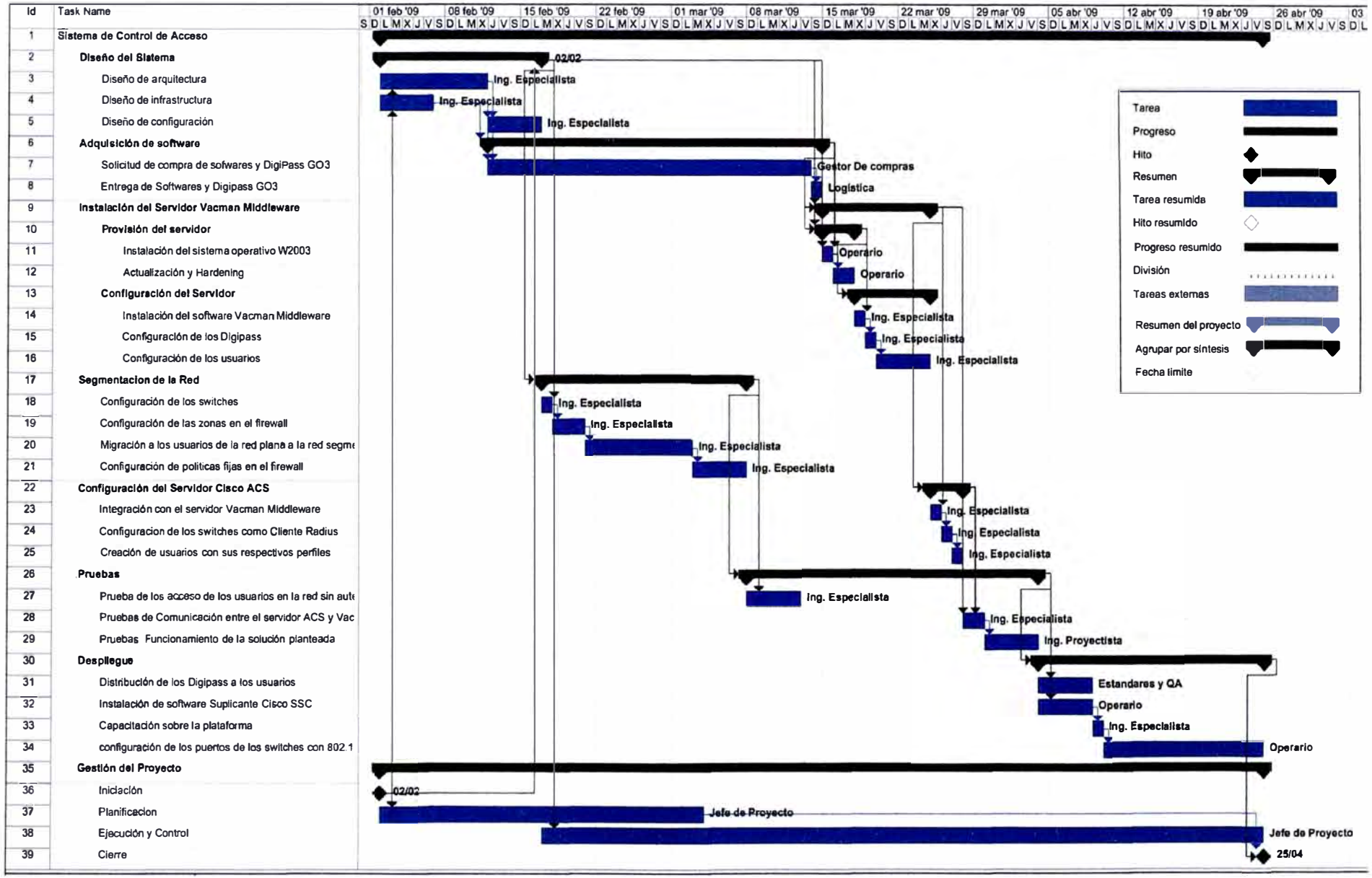

Figura C.1 Diagrama de Gantt del sistema de control de acceso

ANEXO E
GLOSARIO DE TÉRMINOS

AAA: Autenticación, Autorización y Arqueo, sistema en redes. Pronunciado "Triple A".

Ataque: Intento organizado y deliberado de una o más personas para causar daño o problemas a un sistema informático o red.

Confidencialidad: Consiste en asegurar que a la información sólo accede quien está autorizado para ello.

DHCP: Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de hosts). Proporciona un mecanismo para asignar dinámicamente direcciones IP a hosts, a fin de que las direcciones se puedan volver a utilizar cuando los hosts ya no las necesiten.

Encapsulamiento: Es el proceso por el cual los datos que se deben enviar a través de una red se deben colocar en paquetes que se puedan administrar y rastrear.

Hardware: Equipo informático. Todo aquello de un sistema informático que es tangible

Host: Máquina conectada a una red. Tiene un nombre que la identifica, el Hostname. La máquina puede ser una computadora, un dispositivo de almacenamiento por red, una impresora, etc.

NAC: Network Admission Control (Control de admisión a la red). Método para controlar el acceso a una red y evitar la entrada de virus informáticos. Mediante diferentes protocolos y productos de software, NAC verifica el estado de los hosts cuando intentan acceder a la red y gestiona la petición según el estado del host, denominado gestión de estado. Los hosts infectados se pueden colocar en cuarentena; a los hosts sin software de protección contra virus actualizado se les puede pedir que obtengan actualizaciones, y a los hosts no infectados con protección contra virus actualizada se les puede permitir el acceso a la red.

NAD: Network Access Device (Dispositivo de acceso a la red). En una implementación de NAC, el dispositivo que recibe una petición del host para iniciar sesión en la red. Un NAD, por lo general un router, colabora con el software del agente de gestión de estado que se ejecuta en el host, con el software de protección contra virus, así como con ACS y servidores de gestión y corrección de estado de la red para controlar el acceso a la misma y evitar las infecciones por virus informáticos

NAS: Servidor de acceso a la red. Plataforma que actúa de interfaz entre Internet y la red telefónica pública conmutada (PSTN). Gateway que conecta dispositivos asíncronos a una LAN o WAN mediante software de emulación de terminales y redes. Ejecuta el enrutado síncrono y asíncrono de los protocolos admitidos

PIN: Personal Identification Key. Número de Identificación Personal, es una contraseña o clave numérica que se utiliza para acceder a móviles, cajeros automáticos, servicios de telefonía, etc.

Protocolo: Estándar establecido. En lo referente a conectividad de redes, el empleo de un protocolo se realiza para direccionar y asegurar la entrega de paquetes a través de la red.

Proxy: Programa o dispositivo que realiza una acción en representación de otro, que sirve para permitir el acceso a Internet a todos los equipos de una organización.

Red: Una red de computadoras es una interconexión de computadoras para compartir información, recursos y servicios. Esta interconexión puede ser a través de un enlace físico (alambrado) o inalámbrico.

RADIUS: Remote Authentication Dial-In User Service. Protocolo de cuentas y autenticación para servidor de acceso que utiliza UDP como protocolo de transporte.

Router: Enrutador, encaminador. Dispositivo hardware o software para interconexión de redes de computadoras.

Seguridad: Característica de cualquier sistema (informático o no) el cual indique que esté libre de peligro, daño o riesgo

Software: Equipamiento lógico o soporte lógico de una computadora digital, comprende el conjunto de los componentes lógicos necesarios para hacer posible la realización de una tarea específica, en contraposición a los componentes físicos del sistema (hardware).

Switch: O Conmutados, es un dispositivo que permite la interconexión de redes sólo cuando esta conexión es necesaria.

TACACS+: Terminal Access Controller Access Control System Plus. Protocolo de cuentas y autenticación para servidor de acceso que utiliza TCP como protocolo de transporte.

TCP: TCP (Transmission Control Protocol). Protocolo de nivel de transporte orientado hacia la conexión que proporciona una transmisión dúplex de datos fiable.

Token: Es un bloque de texto categorizado por un operador, un identificador, un número, etc.

UDP: User Datagram Protocol (Protocolo de datagrama de usuario). Protocolo de nivel de transporte sin conexiones en el protocolo TCP/IP que pertenece a la familia de protocolos de Internet.

Virus: Programa que está diseñado para copiarse a sí mismo sin conocimiento del usuario y con la intención de infectar el sistema operativo y/o aplicaciones, cuyos efectos pueden variar dependiendo de cada virus: mostrar un mensaje, sobrescribir archivos, borrar archivos, enviar información confidencial mediante emails a terceros, etc.

BIBLIOGRAFÍA

[1] Cisco, "Material de estudio Academy de Networking de Cisco System (CCNA)" Exploration 4, 2008.

[2] Cisco, "Material de estudio Implementing Network Security (CCNA-Security)" 1ra Versión 1, 2009.

[3] Fern Hansen Yago, et al, "AAA/RADIUS/802.1x. Sistemas basados en la autenticación en Windows y Linux/GNU", Editorial Alfaomega Ra-Ma, 1a Edición Año 2009, Págs. 108-110.

[4] IEEE Standard 802.1X-2004 - Port Based Network Access Control.

[5] Jim Geir, "Implementing 802.1X Security Solutions For Wired and Wireless Networks", Wiley Publishing Inc., Indianapolis, 2008.

[6] Susan Hansche, et al, "Official ISC2 guide to the CISSP exam", Auerbach Publications, 2003.

[7] Cisco Systems : http://www.cisco.com

[8] VASCO: http://www.vasco.com/